URLAN SALGADO DE BARROS

UM SISTEMA BASEADO NA TEORIA DO PERIGO PARA DETECTAR ATAQUES JAMMING EM MANETS

CURITIBA

2011

URLAN SALGADO DE BARROS

UM SISTEMA BASEADO NA TEORIA DO PERIGO PARA DETECTAR ATAQUES JAMMING EM MANETS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.
Orientador: Prof. Aldri Luiz dos Santos
Coorientador: Profa. Michele Nogueira Lima

CURITIBA

2011

Barros, Urlan Salgado de
Um sistema baseado na teoria do perigo para detectar ataques jamming em manets / Urlan Salgado de Barros. – Curitiba, 2011.
108 f.: il., tabls.

Impresso.
Dissertação (mestrado) - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Aldri Luiz dos Santos
Coorientadora: Michele Nogueira Lima

1. Sistemas de comunicação móvel. 2. Redes de computadores – Medidas de segurança. I. Santos, Aldri Luiz dos. II. Lima, Michele Nogueira. III. Universidade Federal do Paraná. IV. Título.

CDD: 005.8

DEDICATÓRIA

Dedico este trabalho a todos aqueles que me apoiaram, em especial aos meus pais, Urias e Lenir, ao meu irmão Frederico, e à Karla.

AGRADECIMENTOS

A escrita deste trabalho não seria impossível sem a ajuda de inúmeras pessoas. Para não me esquecer de ninguém, eu preferi citar somente o nome de algumas pessoas e indicar os locais onde eu sempre frequentei.

Agradeço em primeiro lugar aos meus pais, Urias e Lenir, por todo carinho, apoio e cuidado em todos os momentos, tanto de felicidade e de amor, quanto de tristeza e de discussões. Ao meu irmão Frederico, pela amizade e companheirismo que eu tenho certeza que poucos irmãos possuem. À minha querida Karla, pelo carinho e amor que tem por mim, e também pelas palavras de incentivo e apoio nos momentos os quais eu pensava que não conseguiria terminar. E a todos os meus familiares que sempre torceram por mim e me incentivaram nos momentos mais complicados.

Agradeço aos meus orientadores, professores Aldri e Michele, pelas orientações dadas e pelas oportunidades que me deram para concluir o mestrado. Ao professor Luiz Henrique, o qual eu considero um amigo, pelas dicas, conselhos e orientações oferecidas para que eu conseguisse finalizar o mestrado. Aos demais professores e funcionários do DINF-UFPR, pelo ensinamento e auxílio durante esses anos. Também não posso deixar de citar os professores e amigos do DCC-UFLA, os quais tiveram grande influência na minha formação pessoal e profissional. Além disso, agradeço ao órgão CNPq por ter financiado toda a minha pesquisa acadêmica no mestrado. Espero que o governo continue incentivando a pesquisa científica no Brasil.

Agradeço a todos os amigos do laboratório de pesquisa NR2, pelos momentos de café (podem ter certeza que foi muito café!), brincadeiras, risadas e de discussão acerca dos mais diversos temas nerds, como redes de computadores, segurança de redes, filmes, séries, animes, artigos, entre inúmeros outros, e também agradeço à Celite, pelo *brainstorming* nas horas de aperto. Agradeço a todos os amigos da casa Mamadi Família, local onde eu me sentia como se estivesse morando na minha própria casa em Minas Gerais.

Agradeço aos meus amigos que moraram comigo na república, aos amigos da república

Jardins, aos amigos da academia e da aula de dança no CED-UFPR, aos colegas de mestrado, aos amigos do time de rugby Urutau e aos amigos da turma Cocobongo, pela amizade, compreensão e companheirismo. Agradeço também aos demais amigos que, até mesmo indiretamente, ajudaram em toda a minha vida até aqui. São tantos os amigos que eu gostaria de agradecer, mas que infelizmente a minha memória não permite que eu lembre de todos. Eu até posso esquecer o nome de alguém, porém tenham certeza que o rosto eu jamais esquecerei. Muito obrigado a todos por tudo!

Os três grandes fundamentos para se conseguir qualquer coisa são, primeiro, trabalho árduo; segundo, perseverança; terceiro, senso comum.

Thomas Edison

RESUMO

As redes sem fio possibilitam a comunicação de dispositivos computacionais portáteis, como celulares, *notebooks*, *palmtops*, entre outros. Um principal desafio à segurança das aplicações e serviços dependentes das redes sem fio é a vulnerabilidade das comunicações aos ataques *jamming*. No escopo das redes sem fio, as redes móveis ad hoc (MANETs - *Mobile Ad hoc Networks*) permitem que os usuários tenham mobilidade e acessem as informações de forma descentralizada empregando ondas eletromagnéticas através do meio de transmissão sem fio. Para tentar garantir a existência de uma MANET segura, robusta e confiável, é necessário desenvolver um sistema de detecção como contramedida inicial aos ataques *jamming*.

Em face às limitações dos sistemas de detecção de ataques *jamming* existentes, este trabalho propõe um sistema de detecção distribuído e flexível contra ataques *jamming* em MANETs. O sistema de detecção proposto, denominado DANTE (do inglês, ***D****etecting j****A****mming attacks by the da****N****ger* ***T****h****E****ory*), tem como inspiração a teoria do perigo, a qual possui características que inspiram o desenvolvimento de um sistema de detecção de ataques *jamming* nas MANETs, como a descentralização, a dinamicidade e a quantificação. O sistema DANTE é composto por uma arquitetura com três módulos, denominados medições e informações, detecção bio-inspirada e resposta ao ataque *jamming*. O módulo de medições e informações calcula os valores das medições estatísticas e coleta os dados provenientes da camada de enlace que sofreram interferência. O módulo de detecção bio-inspirada determina e quantifica os ataques na rede. O módulo de resposta ao ataque *jamming* toma uma ação apropriada de acordo com a quantificação do ataque.

Para avaliar o desempenho do sistema DANTE são empregados dois tipos diferentes de cenários. Os cenários são compostos por três dispositivos, os quais dois deles são legítimos e um atua como o atacante. No primeiro cenário, os dispositivos são vizinhos entre si, já no segundo cenário, o dispositivo atacante é vizinho somente de um dispositivo legítimo. A fim de avaliar o sistema DANTE são empregadas as métricas de desempenho denominadas

acurácia e precisão. Além disso, o sistema DANTE é comparado a um outro sistema de detecção de ataques *jamming* encontrado na literatura, denominado neste trabalho como CLADE. Os resultados de simulação mostram que o sistema DANTE possui um desempenho superior ao sistema CLADE. Além de obter a precisão de 100% nos ataques *jamming* deceptivo e reativo, o sistema DANTE alcançou os maiores resultados para a acurácia nos ataques *jamming* deceptivo, aleatório e reativo.

Palavras-chave: MANETs, ataques *jamming*, sistema de detecção, teoria do perigo.

ABSTRACT

Wireless networks make possible the communication between portable devices, such as cell phones, laptops, palmtops, among others. A main challenge to security of applications and services dependent of wireless networks is the communications vulnerability to jamming attacks. In wireless networks context, mobile ad hoc networks (MANETs) allow users to have mobility and access information in a decentralized way using electromagnetic waves to communicate by wireless medium. In order to assure the existence of a secure, robust and trustworthy MANET, it is necessary to develop a detection system against jamming attacks as initial countermeasure.

In face of existing detection systems limitations, this work proposes a detection system against jamming attacks to MANETs. The detection system proposed, called DANTE (***D****etecting j****A****mming attacks by the da****N****ger* ***T****h****E****ory*), has as inspiration danger theory, that is supported by the argumentation that immune system discerns between danger and absence of danger. DANTE system comprises an architecture with three modules, called informations and measures, bio-inspired detection and jamming response. Information and measurements module captures data from the link layer that suffered interference and calculates the values of statistical measures. Bio-inspired detection module identifies and quantifies the presence of jammers in a bio-inspired manner. The jamming response module takes an action, based on quantification, to mitigate the impact of jamming attack.

The performance of DANTE system is evaluated using two different scenarios. They comprise three devices, in which two serve as sender and receiver, and one acts as the attacker. In the first scenario all devices are neighbors, and in the second one, the attacker is neighbor only of sender. Two performance metrics, called accuracy and precision, are used in order to evaluate DANTE system. Further, DANTE system is compared with another jamming detection system, called in this work as CLADE. Simulation results show that DANTE system reaches a superior performance than CLADE system. Besides DANTE system obtains a precision rate of 100% in deceptive and reactive jamming at-

tacks, it reaches higher values than CLADE system to accuracy rate in deceptive, random and reactive jamming attacks.

Keywords: MANETs, jamming attacks, detection system, danger theory.

CONTEÚDO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BEB	***B**inary **E**xponential **B**ackoff* - Atraso Binário Exponencial
CD	**C**élulas **D**endríticas
CW	***C**ontention **W**indow* - Janela de Conteção
CBR	***C**onstant **B**it **R**ate* - Taxa de Bits Constante
CPT	**C**ontrole de **P**otência de **T**ransmissão
CRC	***C**yclic **R**edundancy **C**heck* - Verificação de Redundância Cíclica
CTS	***C**lear-**t**o-**S**end* - Livre-Para-Enviar
CERT	**C**entro de **E**studos, **R**esposta e **T**ratamento de Incidentes de Segurança
CLADE	*A **C**ross-**L**ayer **A**pproach to **DE**tect Jamming Attacks in Wireless Ad Hoc Networks* - Uma Abordagem Inter-Camada para Detectar Ataques *Jaming* em Redes Ad Hoc Sem Fio
CSMA/CA	***C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance* - Acesso Múltiplo com Verificação de Portadora com Anulação/Prevenção de Colisão
DCA	***D**endritic **C**ell **A**lgorithm* - Algoritmo de Células Dendríticas
DCF	***D**istributed **C**oordination **F**unction* - Função de Coordenação Distribuída
DoS	***D**enial **of** **S**ervice attack* - Ataque de Negação de Serviço
dDCA	***d**eterministic **D**endritic **C**ell **A**lgorithm* - Algoritmo Determinístico de Células Dendríticas
DIFS	***D**istributed **I**nter-**F**rame **S**pace* - Espaço Inter-Quadro Distribuído
DANTE	***D**etecting j**A**mming attacks by the da**N**ger **Th**e**O**ry* - Detectando Ataques *Jamming* através da Teoria do Perigo
MAC	***M**edia **A**ccess **C**ontrol* - Controle de Acesso ao Meio
MCAV	***M**ature **C**ontext **A**ntigen **V**alue* - Valor do Contexto de Maturidade

	do Antígeno
MANET	***M**obile **A**d Hoc **Net**work* - Rede Ad Hoc Móvel
NS	***N**etwork **S**imulator* - Simulador de Rede
NAV	***N**etwork **A**llocation **V**ector* - Vetor de Alocação de Rede
PCF	***P**oint **C**oordination **F**unction* - Função de Coordenação de Ponto
PAMPS	***P**athogen **A**ssociated **M**olecular **P**attern**s*** - Padrão Molecular Associado à Patogênia
RTS	***R**equest-**t**o-**S**end* - Requisição-Para-Enviar
SD	**S**istema de **D**etecção
SII	**S**istema **I**munológico **I**nato
SIH	**S**istema **I**munológico **H**umano
SIFS	***S**hortest **I**nter-**F**rame **S**pace* - Espaço Inter-Quadro Menor
TCP	***T**ransmission **C**ontrol **P**rotocol* - Protocolo de controle de transmissão

NOTAÇÃO

m	número de agentes artificiais
$I_1, ..., I_k$	informações provenientes da camada de enlace que sofreram colisão
$M_1, ..., M_n$	medições de avaliação
S_1 *e* S_2	saídas dos agentes artificiais
ag	agente artificial
I_α	número de informações examinadas pelo agente artificial ag
$\bar{i}$	número de iterações realizadas pelo agente artificial ag
T_v	número de iterações que o agente fará no algoritmo dDCA
$\bar{k}$	acumulação do nível de anomalia
N	somatório das medições de normalidade
A	somatório das medições de anormalidade
α	peso de anormalidade
β	peso de normalidade
Tem_{Det}	período de coleta de informações
T_{Med}	período de cálculo dos novos valores das medições
$MCAV$	proporção de informações examinadas sob um ambiente anômalo
Inf	número total de informações examinadas pelos agentes artificiais
M	somatório do número de informações processadas pelos agentes artificiais
K	valores de anomalia reais usando a magnitude do parâmetro $\bar{k}$
$\bar{k}_{ag}$	valor de $\bar{k}$ observado pelo agente artificial ag
vp	número de verdadeiros-positivos
fp	número de falsos-positivos
vn	número de verdadeiros-negativos
fn	número de falsos-negativos

CAPÍTULO 1

INTRODUÇÃO

As redes sem fio possibilitam a comunicação de dispositivos computacionais portáteis (nós) sem a necessidade do uso de cabos, como celulares, *notebooks*, *palmtops*, entre outros [1]. Enquanto o acesso predominante à Internet é feito por cabos ou por fibra óptica, com a popularização dos nós portáteis e das redes sem fio um número crescente de usuários passou a demandar o acesso às informações no trabalho, em casa ou mesmo quando estão em movimento. Por instância, tais usuários podem querer ler emails enquanto estão dentro de um ônibus ou mesmo revisar um projeto enquanto esperam pelo avião no aeroporto.

No contexto das redes sem fio, as redes ad hoc permitem que os usuários acessem as informações sem a necessidade de uma infraestrutura física. Essas redes normalmente são empregadas em ambientes onde não existe infraestrutura cabeada ou para celulares, ou se existe tal infraestrutura, ela não é adequada ou o custo de utilização é muito alto [2]. Nas redes ad hoc, os nós precisam trabalhar de uma forma que possibilite a descentralização dessas redes.

Para se comunicarem, os nós empregam rádios de comunicação que propagam dados para o meio de transmissão sem fio. Os rádios possuem programas responsáveis por padronizar a forma como é realizada a comunicação no meio. Tais programas necessitam prover suporte à comunicação ad hoc com o intuito de constituir uma rede descentralizada, isto é, uma rede ad hoc. Uma vez que o programa estabeleça que o rádio de comunicação entre no modo ad hoc, o suporte à comunicação ad hoc é realizado. Com isso, é possível constituir vários tipos de redes ad hoc, dentre elas, as redes ad hoc móveis.

As redes ad hoc móveis (MANETs - *Mobile Ad hoc Networks*) não apresentam qualquer infraestrutura fixa, além de possuírem topologia dinâmica [3]. Essa topologia dinâmica ocorre devido às mudanças do ambiente, onde nós móveis podem entrar e sair da rede a qualquer momento. Consequentemente, a rede precisa se autoconfigurar a fim de se

ajustar ao ambiente, à mobilidade dos nós e às necessidades dos usuários relacionadas aos tráfegos de dados. As MANETs possuem diferentes instâncias, tais como as redes de sensores sem fios, as redes veiculares e as redes corporais.

As redes de sensores sem fio consistem de um número de nós sensores (da ordem de dezenas a milhares) trabalhando de forma mútua para monitorar uma região e obter dados sobre o ambiente [4]. Os nós sensores geralmente são pequenos e possuem processamento e recursos computacionais limitados. Esses sensores podem medir e obter informações do ambiente e, baseado em um processo de decisão local, eles podem transmitir os dados para o usuário.

Uma rede veicular ad hoc é uma MANET desenvolvida para prover comunicação entre veículos próximos [3]. O principal objeito de uma rede veicular ad hoc é prover segurança e conforto para os passageiros. Para esse propósito, um dispositivo eletrônico especial é inserido dentro de cada veículo a fim de prover conectividade ad hoc para os passageiros e para o veículo.

Uma rede corporal consiste de múltiplos nós sensores capazes de amostrar e processar um ou mais sinais vitais do corpo humano, como a pressão sanguínea e a saturação do oxigênio, ou parâmetros de ambiente, como a temperatura, a umidade e a luz [5]. Tipicamente, esses sensores estão localizados de forma estratégica no corpo humano ou escondidos nas roupas, o que permite o monitoramento por prolongados períodos de tempo. Uma vez que os sensores são empregados, é criada uma rede ad hoc capaz de transmitir os sinais vitais dos usuários, facilitando a captura automática dos sinais e a triagem dos usuários em tempo real.

Dentre os grandes desafios existentes nas MANETs, como por exemplo aqueles relacionados tanto à mobilidade quanto a sua natureza não infraestruturada, existe o desafio relativo à segurança dessas redes [1]. As MANETs estão expostas a diversas vulnerabilidades de segurança, as quais podem ser exploradas por entidades maliciosas (atacantes). Os atacantes podem interromper o funcionamento da rede, causando um impacto considerável na disponibilidade dos recursos e das informações, ou violar a privacidade dos nós e dos dados, comprometendo a confidencialidade e a integridade das informações [6].

Além disso, as MANETS herdam os problemas de segurança das redes sem fio convencionais, tais como a escuta não autorizada e a interferência criada no meio de transmissão sem fio [1]. Essa interferência criada de forma maliciosa por um atacante recebe o nome na literatura de **ataque *jamming*** [7].

1.1 Problema

No ataque *jamming*, um atacante, chamado de *jammer*, emite ondas eletromagnéticas através do meio de transmissão sem fio. Isso é realizado para consumir os recursos da rede e causar prolongadas colisões de dados nos nós receptores [8]. Um ataque *jamming* é fácil de se efetuar pois (i) não necessita de *hardware* especial, (ii) pode ser implementado monitorando o meio de transmissão sem fio e transmitindo sinais na mesma frequência, e (iii) dependendo da forma como é executado, pode consumir poucos recursos do *jammer*, como a energia. Portanto, um ataque *jamming* pode degradar de forma significante o comportamento padrão da rede e ao mesmo tempo reduzir a quantidade de dados transferidos e recebidos pelos nós (vazão) [7, 9, 10].

De acordo com a taxonomia proposta em [7], os ataques *jamming* podem ser divididos em ativos e intermitentes. Nos ataques *jamming* ativos, os *jammers* comprometem uma região da rede transmitindo ondas eletromagnéticas de forma contínua para o meio sem fio. Embora esse ataque impeça qualquer comunicação dos nós que estão dentro do raio de atuação do *jammer*, o consumo de energia para a execução do ataque é alto. Por outro lado, nos ataques *jamming* intermitentes, os *jammers* reduzem o consumo de energia ao causarem colisões periódicas nos nós receptores.

Na literatura existem vários trabalhos que quantificam o impacto dos ataques *jamming* nas redes sem fio, tais como [11, 12, 13, 14]. Uma vez que as MANETs herdam os problemas de segurança das redes sem fio, os ataques *jamming* podem afetar várias instâncias das MANETs. Nas redes de sensores sem fio, [15, 16, 17] demonstram que os ataques *jamming* podem interromper o funcionamento normal da rede e degradar a vazão alcançada pelos nós. Relativamente às redes corporais, em [18] os autores mostram que os *jammers* podem deturpar de forma considerável as aplicações dependentes das redes

corporais, tais como aquelas que empregam tráfegos com tempo crítico cujas mensagens com grande atraso se tornam inválidas. Em relação às redes veiculares, [19] verificam que a força de sinal agregada do *jammer* e dos nós amplifica o efeito do ataque.

Uma contramedida para tentar garantir a sobrevivência e a existência de uma rede segura, robusta e confiável é o desenvolvimento de sistemas de detecção contra os ataques *jamming* [20]. A detecção de ataques *jamming* em redes sem fio é um problema desafiador, difícil e muitas vezes dispendioso. Apesar de existirem na literatura vários trabalhos que quantificam o impacto desses ataques nas redes sem fio, a pesquisa sobre a detecção dos ataques *jamming* é incipiente, sobretudo no escopo das MANETs. No que diz respeito às instâncias das MANETs, [7, 18, 21, 22] propõem abordagens de detecção dos ataques *jamming* no meio de transmissão sem fio. Contudo, essas tentativas de detecção possuem rígidas limitações impostas pela capacidade de adaptação dos *jammers* e pelas características das MANETs.

Os *jammers* podem se adaptar à rede ou empregar diferentes tipos de ataques *jamming*, evitando sua detecção e prejudicando o desempenho dos nós. Os sistemas que realizam a detecção devem também diferenciar as colisões criadas pelos *jammers* daquelas geradas pelas condições de operação da rede. Exemplos dessas condições são o congestionamento que ocorre quando os tráfegos de dados excedem a capacidade da rede e do canal, a interrupção da comunicação devido a falhas no transmissor e outros. Além disso, a detecção torna-se mais complexa e desafiante nas MANETs, devido as suas características intrínsecas como a adaptabilidade e a dinamicidade. Nas MANETs, as abordagens encontradas na literatura propõem soluções para detectar a ocorrência de ataques *jamming* [22, 23, 24, 25]. Essas abordagens de detecção possuem como desvantagem o uso de patamares de detecção **estáticos**, o emprego de **métricas simples**, a utilização de **comunicação local** e a **não quantificação** do ataque.

O emprego de patamares de detecção estáticos e estocásticos nas MANETs tem como desvantagem o aumento de falsos positivos. Isso ocorre devido à dinamicidade dessas redes. Além disso, tais patamares de detecção são ineficientes contra *jammers* intermitentes, pois eles se adaptam à rede e evitam a detecção.

O uso de métricas simples pode acarretar no aumento do número de falsos negativos da abordagem de detecção. Tal fato acontece em decorrência da baixa sensibilidade da métricas aos ataques. As métricas que auxiliam as abordagens a determinar a ocorrência de um ataque *jamming* devem sofrer variação conforme o *jammer* age na rede.

Os sistemas de detecção necessitam evitar a comunicação local na rede. Essa prática impede que o *jammer* conclua que o ataque ocasionou danos às comunicações da rede. O sistema também reduz o consumo de energia dos nós, o que aumenta o tempo de vida da rede, e restringe a sobrecarga gerada no meio de transmissão sem fio, o qual eleva a vazão alcançada pelos nós.

Por fim, as abordagens existentes não quantificam a importância do ataque *jamming* na rede. A quantificação tem como objetivo principal auxiliar as contramedidas no processo de reação contra os ataques [26]. Assim, uma vez que não ocorra a quantificação, as contramedidas muitas vezes tornam-se incapazes de reagir de forma eficaz contra os ataques *jamming*.

1.2 Objetivos e Contribuições

Diante dos problemas relacionados às desvantagens dos sistemas de detecção encontrados na literatura, à adaptabilidade dos *jammers* e aos desafios de segurança das MANETs, convém aos sistemas de detecção implementar seis requisitos para detectar os ataques *jamming* e prover auxílio às contramedidas reativas: (i) evoluir considerando as mudanças da rede e a adaptabilidade dos *jammers*, evitando tornar-se genérico ou específico; (ii) diferenciar as colisões geradas pelos *jammers* daquelas criadas pelo baixo desempenho do enlace ou pelo congestionamento da rede; (iii) empregar métricas mais dinâmicas e abrangentes que sejam sensíveis aos ataques; (iv) considerar o menor número possível de patamares, sendo tais patamares dinâmicos; (v) evitar a transmissão de informações para a rede as quais mencionem que o ataque obteve êxito ao interromper a comunicação dos nós; e (vi) quantificar a importância do ataque para auxiliar os mecanismos de reação.

Com base nos seis requisitos citados anteriormente, este trabalho tem como objetivo propor um sistema de detecção distribuído e flexível para tentar garantir a existência e a

sobrevivência das MANETs contra os ataques *jamming*. Para isso, o sistema de detecção tem como inspiração a **teoria do perigo** [27]. Essa teoria propõe uma abordagem efetiva de classificação e detecção de microorganismos vivos no sistema imunológico humano, sendo suportada pela argumentação de que o sistema discerne entre o perigo e a ausência de perigo. A teoria do perigo possui características, como a descentralização, a dinamicidade e a quantificação, que inspiram o desenvolvimento de um sistema de detecção de ataques *jamming* e que vão de encontro às características encontradas nas MANETs. Além disso, a adição da teoria do perigo torna-se atrativa no ambiente das MANETs, devido à aplicação do perigo como um fator determinante para detectar a anomalia presenciada no meio de transmissão sem fio.

Este trabalho apresenta as seguintes contribuições. O sistema DANTE (do inglês, ***D****etecting j****A****mming attacks by the da****N****ger* ***Th********E****ory*) o qual se inspira na teoria do perigo e possui o objetivo de detectar e quantificar os ataques *jamming* no meio de transmissão sem fio. O desenvolvimento de uma arquitetura com três módulos, denominados coleta e medições, detecção bio-inspirada e resposta ao ataque *jamming*. O módulo de medições e informações calcula os valores das medições estatísticas e coleta os dados provenientes da camada de enlace. O módulo de detecção bio-inspirada determina e quantifica os ataques na rede. O módulo de resposta ao ataque *jamming* toma uma ação apropriada de acordo com a quantificação do ataque. Cada nó da rede possui todos os módulos do sistema, sendo que os nós agem como monitores, coletando todos os pacotes que alcançam a camada de enlace.

A implementação dos ataques *jamming*, ativos e intermitentes, do sistema DANTE e de um outro sistema encontrado na literatura, denominado neste trabalho como CLADE [24], no simulador de redes NS *(Network Simulator)* versão 2.31. A implementação dos ataques *jamming* foi realizada na camada de enlace do simulador, devido aos ataques criarem colisões no meio de transmissão sem fio a um salto de distância. Os sistemas DANTE e CLADE também foram inseridos na camada de enlace, em decorrência dessa camada ter maior sensibilidade às colisões criadas pelos *jammers*.

A avaliação e a comparação do desempenho dos sistemas DANTE e CLADE diante dos

ataques *jamming* ativos e intermitentes. Para isso, são considerados dois cenários com três nós: um no qual o *jammer* é vizinho dos outros dois nós, e um no qual o *jammer* é vizinho de somente um nó. O desempenho dos sistemas foi mensurado a partir de duas métricas: a acurácia, a qual indica a proximidade dos resultados das medições com os valores reais, e a precisão, que denota a proporção dos acertos do sistema. Além disso, a quantificação do sistema DANTE é medida em duas métricas específicas do sistema, denominadas K e *MCAV (Mature Context Antigen Value)*. Os resultados de simulação, com um intervalo de confiança de 95%, mostram que o sistema DANTE possui um desempenho superior ao sistema CLADE. Além de obter a precisão de 100% nos ataques *jamming* deceptivo e reativo, o sistema DANTE alcançou os maiores resultados para a acurácia nos ataques *jamming* deceptivo, aleatório e reativo.

1.3 Estrutura da dissertação

Este trabalho está organizado em cinco capítulos. O Capítulo 2 fundamenta os principais conceitos empregados neste trabalho, contextualizando as MANETs, descrevendo o funcionamento do padrão IEEE 802.11 e definindo os ataques que exploram as vulnerabilidades das MANETs, sobretudo os ataques *jamming*. Além disso, esse capítulo explica os conceitos relacionados ao sistema imunológico humano, contextualizando a teoria do perigo e descrevendo o funcionamento dos algoritmos que se inspiram nessa teoria.

O Capítulo 3 descreve o sistema DANTE, o qual se inspira no funcionamento da teoria do perigo e detecta os ataques *jamming* nas MANETs. Esse capítulo apresenta uma visão geral do funcionamento do sistema de detecção, considerando as informações que serão classificadas e as métricas de aferição do enlace e do meio de transmissão sem fio. O capítulo também descreve como o sistema de detecção agrega todas as métricas obtidas; classifica as informações coletadas do meio sem fio; calcula valores que quantificam o nível de anomalia do meio sem fio; e determina a ocorrência de ataques *jamming* na rede através de patamares de detecção dinâmicos.

O Capítulo 4 avalia o desempenho do sistema DANTE diante dos ataques *jamming*. Para isso, são considerados cenários estáticos empregados por autores que avaliaram

os ataques *jamming* e um outro sistema de detecção denominado CLADE. Por fim, o Capítulo 5 apresenta as conclusões, as considerações finais e os trabalhos futuros.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo apresenta os fundamentos relacionados às redes ad hoc móveis, às formas de ataques nessas redes e aos sistemas de detecção de ataques. A Seção 2.1 contextualiza as redes ad hoc móveis e as suas principais características e aplicações. A Seção 2.2 apresenta o funcionamento do padrão IEEE 802.11. A Seção 2.3 expõe os principais tipos de ataques contra as MANETs. A Seção 2.4 contextualiza os ataques *jamming* e as medidas de defesa existentes. A Seção 2.5 define os conceitos acerca dos sistemas de detecção e as metodologias encontradas na literatura. A Seção 2.6 destaca os sistemas de detecção de ataques *jamming* em MANETs. A Seção 2.7 descreve o sistema imunológico humano, enfatizando suas características, e apresenta o algoritmo empregado por este trabalho.

2.1 Redes ad hoc móveis

As redes ad hoc móveis *(MANETs - Mobile Ad hoc Networks)* são redes compostas por dispositivos computacionais portáteis (nós), descentralizados e auto-organizáveis [3]. Os nós operam com energia limitada e são equipados com um ou mais rádios de comunicação sem fio. Os nós estabelecem a comunicação entre si empregando os rádios de comunicação que transmitem as ondas para o meio de comunicação sem fio.

Os nós transmissores empregam uma determinada potência de transmissão para enviar os dados ao meio de transmissão sem fio. Os nós receptores que estiverem dentro do raio de alcance da transmissão são considerados nós vizinhos e conseguem decodificar as ondas transmitidas. Esse tipo de comunicação é chamado de comunicação direta ou comunicação a um salto, a qual mantém a conectividade da rede em nível de enlace. Para padronizar o acesso ao meio de transmissão sem fio, garantindo a igualdade de acesso ao meio para todos os nós, as MANETs consideram padrões de transmissão, como o IEEE 802.11 [28],

o IEEE 802.15.4 [29], o IEEE 802.16 [30] e o IEEE 802.22 [31].

2.2 Padrão IEEE 802.11

O padrão IEEE 802.11 especifica os componentes da camada física e da camada de enlace do rádio. A camada física define o tipo de modulação e codificação empregados para o espalhamento do espectro. Já a camada de enlace, sobretudo a sub-camada MAC *(Media Access Control)*, estabelece o conjunto de regras que determinam como os nós realizam o acesso ao meio sem fio [28]. O padrão IEEE 802.11 usa adendos referentes à transmissão, como o *802.11a*, o *802.11b*, o *802.11g* e o *802.11n*, que consideram frequências não licenciadas, como as de 2.4 e 5.8 GHz.

Os bits recebidos pela camada física são repassados para a camada de enlace. Nessa camada, os bits são agrupados, recebendo a denominação de quadro, e passam pela verificação de redundância cíclica *(CRC - Cyclic Redundancy Check)* que detecta erros típicos causados por ruídos e interferências no meio de transmissão sem fio. Caso a verificação não encontre qualquer erro, o quadro é decodificado corretamente e então é processado pela camada de enlace. Uma vez que a verificação do código CRC detecte alguma inconsistência no quadro, como um erro ocorrido no momento da transmissão, esse quadro não é decodificado corretamente. Nesse caso, a camada de enlace pode tomar uma atitude corretiva, como refazer a verificação do quadro ou simplesmente o descartar e aguardar que o nó transmissor envie o quadro novamente.

Para controlar o acesso ao meio de transmissão sem fio, a sub-camada MAC do padrão IEEE 802.11 emprega duas funções distintas, denominadas PCF *(Point Coordination Function)* e DCF *(Distributed Coordination Function)*. Na função PCF, os nós realizam o acesso ao meio sem fio de maneira centralizada com o uso de pontos coordenadores. Tais pontos permitem que cada nó acesse o meio por um pequeno intervalo de tempo e não encontre o meio ocupado, tornando o acesso livre de contenção. Em contrapartida, na função DCF os nós acessam o meio sem fio de forma descentralizada.

A função DCF emprega o mecanismo CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)* para transferir os dados. O mecanismo CSMA/CA permite o acesso

múltiplo ao meio de transmissão sem fio e tenta prevenir colisões através da reserva virtual do canal, realizada pelo nó transmissor. A Figura 2.1 ilustra o funcionamento da função DCF, mostrando a interação entre um nó transmissor, um nó receptor e os nós vizinhos [32].

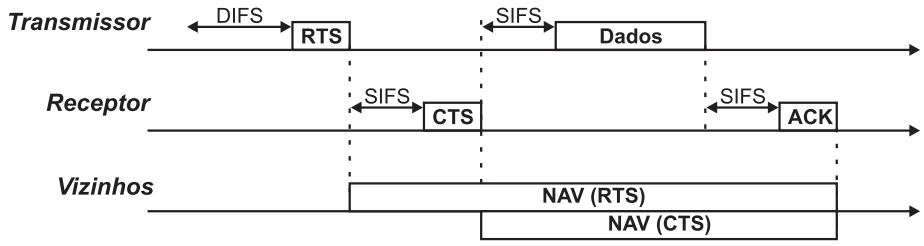

Figura 2.1: Funcionamento da função DCF - [28]

O nó transmissor monitora a atividade do meio de transmissão por um período de tempo DIFS *(Distributed Inter-Frame Space)*. Ao final desse período, o nó pode realizar a transmissão após determinar a inatividade do canal. Caso contrário, a função DCF emprega o algoritmo exponencial de *backoff* binário *(BEB - Binary Exponential Backoff)* para atrasar a transmissão do nó. Após o tempo DIFS, se o meio de transmissão estiver inativo, o nó transmissor inicia a transmissão usando o quadro de controle RTS *(Request-to-Send)*, para realizar a reserva virtual do meio para que não ocorram colisões no nó receptor. Além disso, o RTS contém o identificador do nó destino e o tempo que durará toda a transmissão. Qualquer nó vizinho que esteja monitorando o meio receberá o RTS. Ao decodificar o quadro RTS, os nós atualizarão o seu vetor de alocação da rede *(NAV - Network Allocation Vector)* com o tempo contido no quadro e atrasarão qualquer transmissão até o final desse tempo. O NAV consiste em um contador de tempo que decresce até zero e indica se o meio sem fio está ocupado.

Ao receber o quadro RTS, o nó destino monitora o meio sem fio por um período de tempo SIFS *(Shortest Inter-Frame Space)*. Estando o meio ocupado ao final desse período, o nó atrasa sua transmissão para não gerar colisões no nó receptor. Por outro lado, com a inatividade do meio sem fio, o nó receptor responde ao RTS do nó transmissor com um quadro de controle CTS *(Clear-to-Send)*. Esse quadro notifica o transmissor que o meio está livre para a transmissão dos dados. Além disso, o quadro CTS contém o tempo

de duração da transmissão, logo, todos os nós vizinhos que consigam decodificar o CTS devem atualizar o NAV com o tempo contido no quadro.

Ao receber o quadro CTS, o nó origem monitora o meio sem fio durante o período de tempo SIFS. Ao final desse período de espera, se o meio sem fio estiver inativo, o nó origem transmite o quadro de dados para o destino. Caso contrário, o nó transmissor atrasa a transmissão desse quadro. Por fim, após receber o quadro de dados, o nó receptor monitora o meio de transmissão por um período de tempo SIFS. Se o meio estiver inativo ao final desse período, o nó destino enviará um quadro ACK para o nó origem. Caso contrário, o nó destino atrasa a transmissão do quadro ACK.

2.3 Ataques em MANETs

Nas MANETs cada nó deve agir como um roteador, cooperando e repassando as informações para os outros nós da rede. A necessidade de cooperação entre os nós resulta em um problema de segurança, pois os protocolos assumem que os nós operam em um padrão pré-estabelecido. Além disso, o meio de comunicação sem fio favorece a atuação de usuários mal intencionados (atacantes), devido a esse meio ser compartilhado e aberto [1].

Os ataques contra as MANETs podem ser classificados em **passivos** e **ativos** [1]. Os ataques passivos são definidos como um conjunto de ataques que **não modificam** o funcionamento normal da rede. Ao mesmo tempo que um atacante continua participando da rede, repassando os pacotes, ele também pode auditar os pacotes em busca de informações sigilosas. Por exemplo, um atacante pode monitorar o meio de transmissão em busca de senhas e números de cartão de crédito que são enviados em texto claro, sem criptografia. No ataque ativo, o atacante **interage** e **deturpa** o funcionamento padrão da rede, degradando ou mesmo negando seus serviços. Os ataques ativos podem ser agrupados em quatro conjuntos: os ataques físicos, os ataques de mascaramento, os ataques de mau comportamento e os ataques de negação de serviço [6]. A Figura 2.2 ilustra os conjuntos de ataques ativos enfatizando os ataques *jamming*, estudados neste trabalho.

No ataque físico, o nó atacante causa dano ao *hardware* dos nós vizinhos, sendo o pulso eletromagnético um exemplo desse ataque. Tal pulso produz altas tensões que danificam

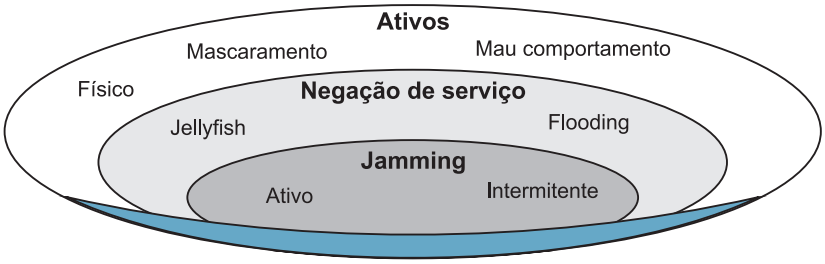

Figura 2.2: Conjuntos de ataques ativos - referência própria

os dispositivos eletrônicos que estejam dentro do seu raio de alcance. Já no ataque de mascaramento, o atacante age como outro nó para preservar sua anonimidade na rede e tornar a sua detecção mais complexa [33, 34]. No ataque de mau comportamento, o nó atacante obtém maior acesso aos recursos limitados da rede através da modificação dos parâmetros do rádio. Por instância, o atacante pode acessar o meio de transmissão com maior frequência, aumentar sua vazão e reduzir a igualdade de acesso ao meio de transmissão.

No ataque de negação de serviço *(DoS - Denial of Service)*, o nó atacante interrompe a disponibilidade dos serviços da rede. O CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) caracteriza um ataque DoS como uma tentativa explícita de impedir o uso legítimo de um determinado serviço [35]. Um atacante, ou até mesmo um grupo de atacantes, pode tornar um serviço indisponível para os nós legítimos por longos períodos de tempo. Como ilustrado na Figura 2.2, o ataque de negação de serviço possui algumas instâncias, tais como o *jellyfish*, o *flooding* e o *jamming*.

O ataque *jellyfish* tem como objetivo principal causar impacto no controle de congestionamento fim-a-fim dos nós. Em particular, várias aplicações, como transferência de arquivos e *web*, confiam no controle de congestionamento provido pelo protocolo TCP *(Transmission Control Protocol)*. Assim, o ataque *jellyfish* pode descartar pacotes de forma maliciosa por um curto período de tempo e causar um grande impacto na operação do protocolo TCP [36].

O ataque *flooding* visa paralizar o alvo (um computador ou uma rede) através da transmissão de um volume excessivo de tráfego. Por instância, para realizar esse ataque

um atacante transmite uma quantidade excessiva de tarefas a fim de paralizar os alvos. Uma vez que os alvos processem as tarefas, elas consomem facilmente os principais seus recursos, tais como capacidade de CPU, memória, bateria e vazão [37].

No escopo das redes sem fio, um atacante DoS pode transmitir ondas eletromagnéticas de forma maliciosa para o meio sem fio com o intuito de criar interferência nos nós receptores. Essa instância de ataque DoS é denominada de ataque *jamming*.

2.4 Ataques *jamming*

O **ataque *jamming*** impede que os nós troquem informações entre si utilizando o meio de transmissão sem fio [38]. Um atacante *jamming (jammer)* é uma entidade que interfere na transmissão e recepção física das comunicações sem fio. Em particular, quando um ataque *jamming* é executado, o *jammer* consome parte ou a completa capacidade do canal, além de causar falhas intermitentes ou permanentes na rede.

Por instância, a Figura 2.3 elucida o impacto de um ataque *jamming* na rede. Nessa rede existem vários nós distribuídos aleatoriamente. Num primeiro momento, a rede se encontra sob um comportamento normal onde os nós se comunicam empregando enlaces sem fio. Uma vez que o *jammer* inicia o ataque na rede, vários enlaces sem fio que estão dentro do raio de atuação do *jammer* são interrompidos, causando um impacto considerável em toda a rede.

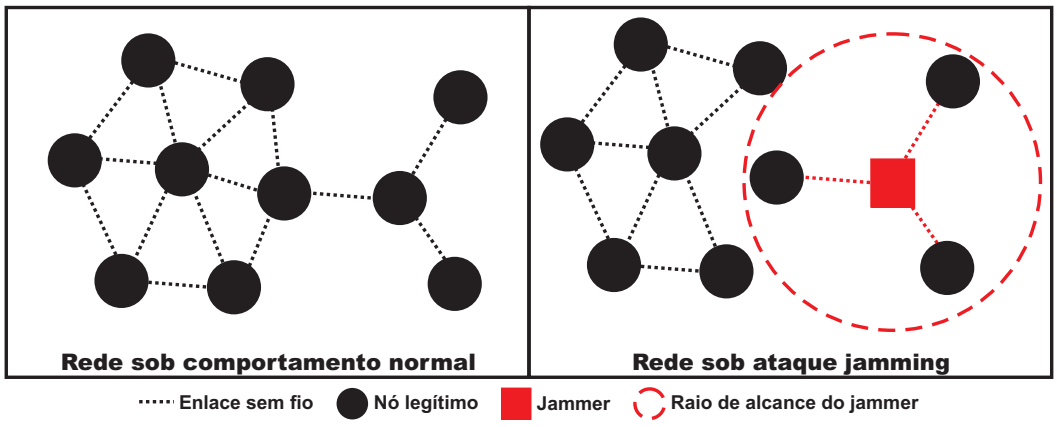

Figura 2.3: Interrupção do tráfego fim-a-fim pelo *jammer* - referência própria

Vários trabalhos têm quantificado o impacto dos ataques *jamming* nas redes sem

fio [11, 12, 13, 14, 16, 17, 39]. Esses ataques são simples e fáceis de serem realizados e, sobretudo, causam um grande impacto na rede com um baixo consumo de recursos do *jammer*. Os ataques *jamming* podem operar na camada física empregando ondas eletromagnéticas para corromper os enlaces de comunicação sem fio em uma área. Além disso, esses ataques também podem ocorrer na camada de enlace na qual um *jammer* causa interferências na rede monitorando o meio de transmissão sem fio e reagindo de acordo com os quadros recebidos do meio. A próxima subseção explica as instâncias de ataques *jamming* estudadas na literatura.

2.4.1 Tipos de ataques *jamming*

Os ataques *jamming* podem ser divididos em ativos e intermitentes [38]. A Figura 2.4 ilustra a classificação dos ataques *jamming*. No ataque *jamming* ativo, o *jammer* emite ondas eletromagnéticas constantemente em uma faixa de frequência, fazendo com que os nós encontrem o meio de transmissão sempre ocupado. Uma outra instância do ataque de *jamming* ativo é o ataque *jamming* deceptivo, na qual o atacante transmite quadros decifráveis para o meio sem fio. Com isso, os nós que estão dentro do raio de alcance do ataque supõem a existência de um tráfego legítimo na rede, mantendo o rádio no modo de recepção enquanto ocorre o ataque.

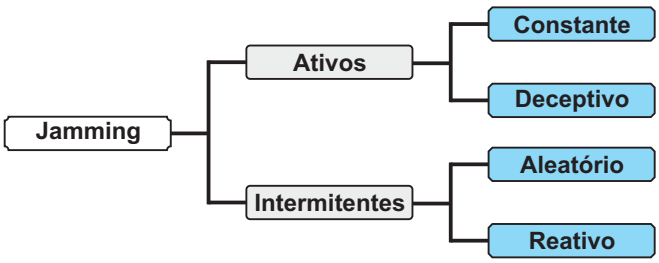

Figura 2.4: Classificação dos ataques *jamming* - referência própria

Nos ataques *jamming* intermitentes, os nós atacantes transmitem sinais eletromagnéticos para o meio sem fio de forma alternada a fim de consumir uma menor quantidade de energia [7]. Existem duas instâncias de ataques *jamming* intermitentes, o ataque *jamming* aleatório e o ataque *jamming* reativo. No ataque *jamming* aleatório, o atacante alterna entre períodos de transmissão do sinal e de ausência de transmissão. No ataque *jamming*

reativo, o *jammer* envia ondas eletromagnéticas de forma maliciosa para o meio de transmissão após detectar algum quadro no meio sem fio, podendo ser quadros de controle (RTS/CTS), de dados ou ACK.

Dentre as instâncias de ataques *jamming* intermitentes, o ataque *jamming* reativo é a instância mais complexa de ser detectada [40, 41]. Isso ocorre devido ao *jammer* criar interferência no meio sem fio em pequenos intervalos de tempo. Assim, os *jammers* reativos conseguem reduzir a vazão e a taxa de entrega dos nós, e ao mesmo tempo consumir menos energia, aumentando o seu tempo de vida na rede.

Entretanto, devido ao meio sem fio ser aberto, um *jammer* que seja vizinho à transmissão pode receber os quadros e utilizar um conhecimento prévio sobre o procedimento de comunicação para executar o ataque *jamming* na rede. Diante disso, Xu et al. apresentam três instâncias para o ataque *jamming* reativo, aquela contra o quadro CTS, a instância contra o quadro de dados e aquela contra o quadro ACK [7]. A fim de exemplificar essas três instâncias, são empregadas as Figuras 2.5, 2.6 e 2.7. Tais figuras são compostas por três nós vizinhos entre si, o transmissor, o receptor e o *jammer*, e um enlace sem fio entre o transmissor e receptor os quais consideram o protocolo de estabelecimento de quatro vias do padrão IEEE 802.11 para realizar a comunicação.

A Figura 2.5 ilustra o ataque *jamming* reativo contra o quadro CTS. A fim de realizar o ataque, o *jammer* aguarda pelo período de tempo SIFS e transmite a interferência para o meio sem fio após receber e decodificar o quadro RTS, de forma análoga ao nó receptor. Assim, o *jammer* causa colisão na recepção do quadro CTS pelo nó transmissor.

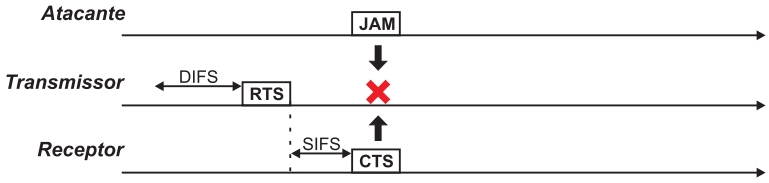

Figura 2.5: Ataque *jamming* reativo contra o quadro CTS - estendida de [7]

A Figura 2.6 ilustra o ataque *jamming* reativo contra o quadro de dados. Nesse ataque, o *jammer* espera pelo período de tempo SIFS e transmite a interferência para o meio sem fio após receber e decodificar o quadro CTS. Como consequência, o nó transmissor deverá

reiniciar a comunicação enviando o quadro RTS, devido à colisão que o *jammer* causa na recepção do quadro de dados pelo nó receptor..

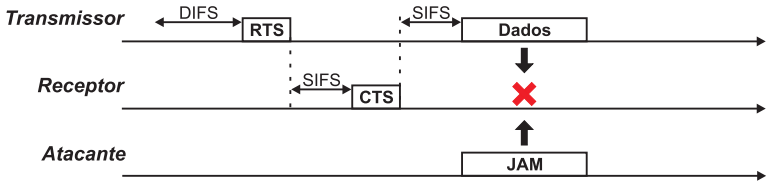

Figura 2.6: Ataque *jamming* reativo contra o quadro de dados - estendida de [7]

A Figura 2.7 ilustra o ataque *jamming* reativo contra o quadro ACK. O *jammer* atua criando interferência no quadro ACK, após detectar a transmissão do quadro de dados no meio sem fio e aguardar pelo período de tempo SIFS. Dentre as instâncias de ataques *jamming* reativos, aquela que cria interferências no quadro ACK é a mais complexa de ser detectada. Isso ocorre em consequência do número reduzido de colisões criadas pelo *jammer*. Enquanto o *jammer* reduz o consumo de energia por criar interferência somente nos quadros ACK, os nós legítimos consomem energia extra para refazer toda a comunicação, além de terem a taxa de entrega dos quadros reduzida [41].

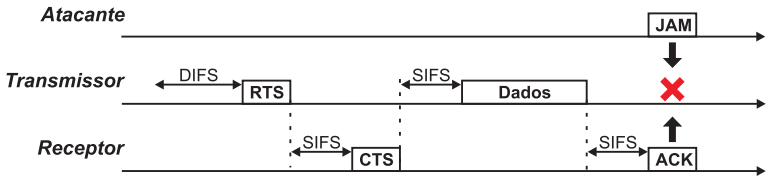

Figura 2.7: Ataque *jamming* reativo contra o quadro ACK - [7]

2.4.2 Estratégias de contramedidas

As abordagens de contramedidas a ataques *jamming* encontradas na literatura podem ser classificadas de três formas: a prevenção, a detecção e a resistência [42]. As medidas de prevenção evitam o raio de atuação do sinal do atacante. As medidas de detecção possibilitam aos nós determinarem a atuação de *jammers* no meio de transmissão sem fio. As medidas de resistência possibilitam que a rede continue funcionando mesmo sob a influência do *jammer*.

As estratégias para prevenir ataques *jamming* consistem na mobilidade dos nós [42,

43, 44, 45, 46], na modificação [41, 47] e na criação de novos protocolos para a camada MAC [48]. A estratégia comumente empregada para evitar o sinal do atacante é a mobilidade. Nela, os nós restabelecem a conectividade da rede através da movimentação para fora do raio de alcance do ataque. Enquanto os nós se movimentam, eles averiguam a ocorrência dos ataques *jamming*. A movimentação cessa após os nós saírem do raio de alcance do *jammer*. Contudo, os nós consomem muita energia para sair do raio de atuação dos atacantes e restabelecer a comunicação dos enlaces [42].

Em [41, 47], os autores previnem a rede contra os ataques *jamming* modificando o protocolo MAC. Entretanto, esse esquema pró-ativo reduz drasticamente a vazão da rede mesmo sem a influência de atacantes. Em [48], os autores definem um novo protocolo MAC que emprega comunicação em um único salto. Todavia, essa abordagem tem como desvantagens a necessidade e o custo para atualizar esse protocolo nos dispositivos sem fio.

Os sistemas de **detecção** são a primeira linha de defesa contra os ataques *jamming* [7]. Tais sistemas tentam diferenciar as colisões criadas por esses ataques no meio de transmissão sem fio daquelas que ocorrem devido à baixa qualidade do enlace. Além de detectar os ataques, esses sistemas devem quantificar o ataque para que alguma contramedida seja tomada. Os conceitos de sistemas de detecção são apresentados na Seção 2.5.

Várias estratégias têm buscado garantir a **resistência** da rede contra ataques *jamming*. As estratégias de resistência possuem como objetivo principal a redução do impacto do ataque *jamming* para que a rede continue sobrevivendo. As principais estratégias de resistência encontradas na literatura são: o uso de antenas direcionais [49], a correção adiantada de erros [50], o controle de potência de transmissão [51, 52], o roteamento empregando múltiplos caminhos [53, 54, 55] e a comunicação usando espalhamento de espectro [56, 57].

As antenas direcionais permitem que o nó transmissor irradie o sinal para o setor onde o nó destino se encontra [49]. Em geral, as antenas direcionais proveem melhor proteção aos ataques *jamming* do que as antenas omni-direcionais, as quais irradiam o sinal em toda uma área. Isso ocorre devido à forma de irradiação do sinal das antenas direcionais

tornar a recepção do sinal para o *jammer* mais complexa. Apesar do uso de antenas direcionais poder melhorar potencialmente a confidencialidade dos dados no ambiente hostil das MANETs e reduzir a probabilidade de um *jammer* ser capaz de coletar todas as mensagens dos nós origem e destino, as antenas direcionais requerem protocolos MAC mais sofisticados que aqueles que empregam antenas omni-direcionais.

A correção adiantada de erros é um tipo de processamento de sinal digital o qual melhora a confiança dos dados através da introdução de dados redundantes ao quadro. Esse dados redundantes permitem ao nó receptor detectar e possivelmente corrigir erros causados por alguma interferência no canal. Como o nome sugere, essa estratégia possibilita que o nó receptor corrija os dados sem a necessidade de requisitar a retransmissão do quadro original [50]. A correção adiantada de erros é sobretudo aplicada em situações nas quais as retransmissões possuem um custo relativamente alto. Contudo, essa estratégia reduz a vazão da rede devido aos quadros serem enviados empregando técnicas de modulação e codificação do sinal as quais são menos suceptíveis aos ruídos do meio.

O controle de potência de transmissão (CPT) permite que o nó modifique a quantidade de energia empregada no envio dos quadros. Em geral, o CPT é utilizado para prolongar o tempo de vida da rede e aumentar tanto o reuso espacial do meio de transmissão sem fio quanto a vazão da rede. Contudo, quando existe um *jammer* na rede, os nós legítimos podem aumentar a potência de transmissão como uma tentativa para competir contra o sinal irradiado pelo *jammer* ou reduzir a potência para o que *jammer* não conclua que ocorre algum tráfego no meio sem fio. De acordo com [51, 52], o CPT pode possibilitar que o nó receptor decodifique o quadro mesmo sob a influência do *jammer* na rede. No entanto, o CPT torna-se ineficaz uma vez que o *jammer* esteja próximo ao receptor.

Alguns protocolos de roteamento suportam múltiplos caminhos para o mesmo destino. Esses protocolos permitem a multiplexação de tráfego sobre múltiplas linhas, provendo melhor fluxo e confiança na transferência de dados. No contexto dos ataques *jamming*, o roteamento por múltiplos caminhos possibilita que os tráfegos de pacotes contornem a região de atuação de um ataque *jamming* [53, 54, 55].

A comunicação usando espalhamento de espectro permite que o nó irradie o sinal

de forma direta ou através do salto de canais para evitar a frequência interferida por um *jammer*. As técnicas de espalhamento de espectro geralmente confiam em códigos secretos os quais são compartilhados entre os pares de nós, transmissor e receptor, da comunicação. Esses códigos secretos permitem ao transmissor espalhar o sinal, em tempo e/ou em frequência, tal que um terceiro nó não consiga identificar a comunicação entre os dois nós [56, 57, 58]. Apesar dessas duas técnicas garantirem certa resistência contra alguns tipos de ataques *jamming*, elas necessitam que os pares de nós transmissor e receptor estabeleçam os códigos secretos antes de se comunicarem. Como o meio de transmissão sem fio possui natureza aberta, qualquer atacante que monitore o meio também saberá o código secreto compartilhado [59].

Para que as técnicas de resistência sejam utilizadas de uma forma eficaz, elas podem ser empregadas de forma reativa contra os ataques *jamming* [7]. Isso significa que em primeiro lugar o ataque deve ser detectado e quantificado, para que depois ocorra a reação ao ataque com base na quantificação.

2.5 Conceitos de sistemas de detecção

Um **sistema de detecção** (SD) é definido como um sistema que possui o objetivo de detectar atividades inapropriadas, incorretas ou anômalas na rede. Um SD examina as atividades específicas de uma máquina ou da rede e determina quando uma atividade é normal ou suspeita [60]. Um SD assume que tanto as atividades normais quanto as suspeitas são observáveis e possuem evidências distintas.

No núcleo de um SD está a capacidade de distinguir o comportamento normal e aceitável do sistema daquele que é anormal ou suspeito. Para isso, os SDs empregam metodologias capazes de detectar um atacante ou um comportamento anômalo na rede. Na literatura são encontradas duas classes principais de metodologia de detecção, as baseadas em assinaturas e as baseadas em anomalias.

Na metodologia de detecção baseada em assinaturas, o processo de detecção segue um conjunto de regras previamente definidas, comparando os eventos monitorados com padrões de atividades hostis previamente conhecidos. Qualquer evento que seja con-

dizente com alguma atividade hostil conhecida é tratado como um ataque. Contudo, essa metodologia não detecta novos tipos de ataques ou até mesmo antigos ataques modificados [61].

Na metodologia baseada em anomalias, o processo de detecção classifica uma atividade da rede ou do sistema como normal ou anômala. O principal benefício das abordagens de detecção baseadas em anomalias é o seu potencial para detectar eventos de ataques que não foram percebidos anteriormente. A classificação da atividade é fundamentada em heurísticas ou padrões que detectam qualquer atividade que esteja fora do comportamento normal da rede [62]. Os SDs classificam uma atividade como normal ou anômala, empregando um único classificador ou diversos classificadores combinados para aumentar a precisão da detecção [63].

Em geral, os SDs baseados em anomalias consistem dos seguintes módulos básicos [64]:

- **Parametrização**: nesse módulo as atividades observadas pelo sistema são representadas em uma forma pré-estabelecida.
- **Treinamento**: o comportamento normal ou anormal do sistema é caracterizado e um modelo correspondente é criado, sendo feito de forma automática ou manual.
- **Detecção**: uma vez que o modelo do sistema esteja disponível, ele é comparado com as próximas atividades. Caso uma atividade exceda um determinado patamar, ela é classificada como anômala e o sistema reage contra essa anomalia de forma autônoma ou através de uma notificação para o usuário.

As abordagens de detecção de anomalia podem ser classificadas em três principais categorias [65], aquelas baseadas em *estatística*, as baseadas em *conhecimento* e aquelas baseadas em *aprendizado de máquina*. A Figura 2.8 apresenta as três principais categorias e suas respectivas sub-classes, estendendo a classificação proposta em [64]. A figura adiciona as abordagens que empregam o sistema imunológico e destaca as técnicas bio-inspiradas.

Nas abordagens baseadas em estatística, um SD coleta dados referentes aos tráfegos da rede e gera um perfil que representa o comportamento estocástico da rede. Esse perfil

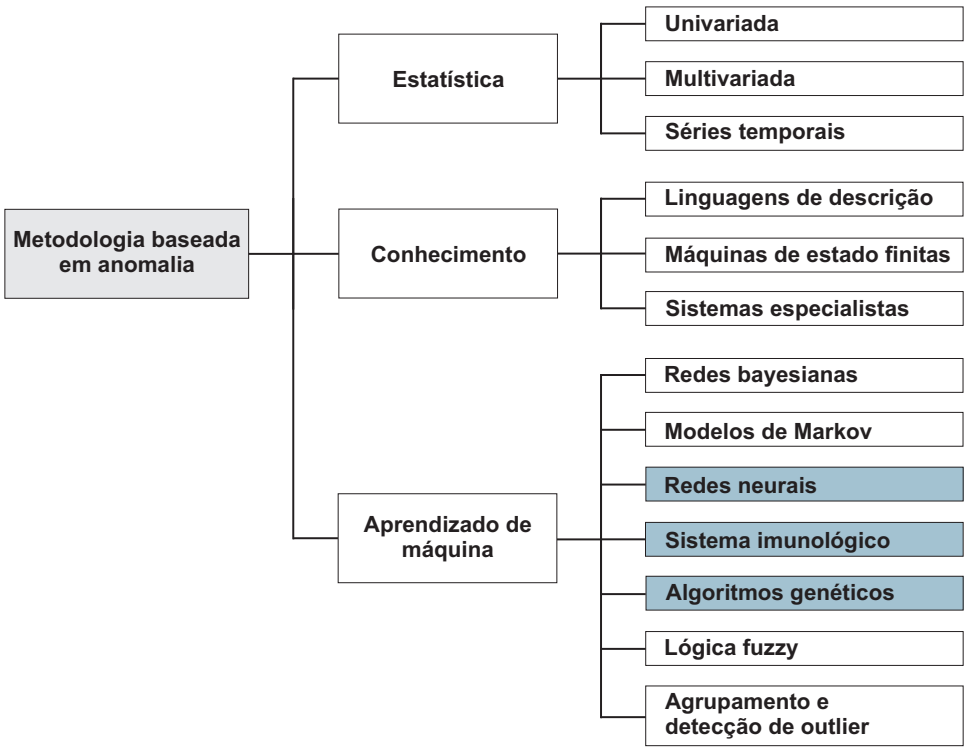

Figura 2.8: Principais categorias das abordagens de detecção de anomalia - estendida de [64]

é baseado em métricas, como taxa de entrega, taxa de conexões, qualidade do enlace, entre outras. O processo de detecção de anomalia considera dois conjuntos de dados, um que corresponde ao perfil atual, observado durante uma determinada janela de tempo, e um outro referente ao perfil estatístico do treinamento anteriormente utilizado. Ao final da coleta de dados, o perfil atual da rede é determinado e então é quantificado o valor de anomalia pela comparação dos dois perfis. O valor de anomalia indica a irregularidade de um evento específico, sendo que um SD determina a ocorrência da anomalia quando a quantificação excede o valor de um certo patamar.

Nas abordagens baseadas em conhecimento, um SD classifica os dados coletados de acordo com um conjunto de padrões que envolvem três etapas. Na primeira etapa, diferentes atributos e classes são identificados dos dados de treinamento. Na segunda etapa, o SD deduz um conjunto de padrões de classificação, parâmetros ou procedimentos. Na terceira etapa, os dados coletados são classificados de acordo com o conjunto de padrões deduzidos pelo SD. Um método mais restritivo é o baseado em especificação, no qual o modelo desejado é construído por um humano através de um conjunto de padrões que

procura determinar o comportamento normal do sistema.

Nas abordagens baseadas em aprendizado de máquina, um SD estabelece um modelo explícito ou implícito permitindo que os padrões analisados sejam categorizados. Em vários casos a aplicabilidade dos conceitos de aprendizado de máquina coincide com as técnicas estatísticas, apesar da aprendizagem de máquina ser focada na criação de modelos que melhorem o seu desempenho a partir de resultados anteriores. Logo, um SD baseado em aprendizado de máquina possui a habilidade de mudar sua estratégia de execução conforme ele adquire novas informações. Dentre as técnicas de aprendizado de máquina encontradas na literatura, aquelas que se inspiram em sistemas biológicos possibilitam que um SD detecte novos tipos de ataques e se adapte às mudanças da rede [65]. Os sistemas e algoritmos bio-inspirados mais empregados na literatura para a detecção de ataques são os algoritmos genéticos [66], as redes neurais artificiais [67] e o sistema imunológico artificial [68].

No entanto, as soluções tradicionais de SDs baseadas em anomalias não podem ser empregadas nas MANETs devido às características próprias dessas redes, como mobilidade, dinamicidade e flexibilidade. Visando a criação de sistemas mais robustos, Mishra et al. [69] argumentam que um SD para MANETs deve: (i) executar a detecção de forma contínua e transparente à rede; (ii) não introduzir novas vulnerabilidades na rede e nem no nó que o estiver executando; (iii) usar a menor quantidade de recursos possíveis para detectar as intrusões; e (iv) ter alta exatidão, alcançar altas taxas de verdadeiros-positivos e baixas taxas de falsos-positivos. Além disso, também é necessário que o SD quantifique o ataque para que alguma medida reativa seja tomada.

Na literatura são encontradas diversas abordagens baseadas em anomalias que tentam detectar ataques nas MANETs [70, 71, 72]. Contudo, elas falham ao tentar detectar os ataques *jamming*, visto que essas abordagens possuem a asserção que o evento de ataque deve ser distinto do evento normal. O evento do ataque *jamming*, isto é, a colisão criada pelos *jammers*, não difere das colisões ocasionadas pelo congestionamento que pode existir no meio de transmissão sem fio, o que dificulta a detecção e reduz a precisão dos SDs.

2.6 Sistemas de detecção de ataques *jamming* em MANETs

Esta seção contextualiza os trabalhos existentes na literatura que propõem detectar ataques *jamming* nas MANETs. Como a pesquisa de detecção de ataques *jamming* nas MANETs é ainda incipiente, esta seção explica três abordagens: aquela que emprega o coeficiente de correlação estatística [22, 23]; a abordagem inter-camada [24]; e a abordagem que considera a explicabilidade da colisão [25].

2.6.1 Abordagem empregando o coeficiente de correlação estatística

Ali Hamieh et al. [22] e Ali Hamieh e Jalel Ben-Othman [23] apresentam uma abordagem de detecção de ataques *jamming* reativos em MANETs baseada no coeficiente de correlação estatística. A correlação é a medida da relação entre duas variáveis, sendo que o resultado da correlação encontra-se entre -1 e 1. A Equação 2.1 calcula o coeficiente de correlação CC, a qual X e Y são dois conjuntos de variáveis, $cov(X, Y)$ é a covariância dos conjuntos X e Y, σ_X o desvio padrão do conjunto X e σ_Y o desvio padrão do conjunto Y. Os valores do coeficiente de correlação no intervalo $[-1.0, -0.5]$ e $[0.5, 1.0]$, isto é, próximos de -1.0 e 1.0, apresentam uma correlação forte, enquanto os valores próximos de 0 denotam a falta de uma relação útil.

$$CC = \frac{cov(X, Y)}{\sigma_X \times \sigma_Y} \tag{2.1}$$

De fato, a abordagem proposta em [22, 23] é composta de duas fases: uma de inicialização e uma de detecção. A fase de inicialização consiste no cálculo de um patamar de detecção quando a rede não está sob a influência de um ataque *jamming*. Na fase de detecção, o nó transmissor calcula o coeficiente de correlação entre o tempo de recepção o qual os pacotes foram recebidos corretamente e o tempo de recepção que os pacotes foram recebidos incorretamente, devido à baixa qualidade do enlace ou em decorrência da atuação de um *jammer* no meio de transmissão sem fio. Após coletar um determinado número de pacotes, a abordagem verifica se existe um *jammer* na rede. Caso o valor do

coeficiente de correlação seja maior que o patamar de detecção, significa que a rede está sob um ataque *jamming*.

Apesar da abordagem empregando o coeficiente de correlação estatística como métrica para a detecção de ataques *jamming* ser promissora, os trabalhos [22, 23] apresentam limitações. A fase de inicialização, a qual calcula um valor para o patamar de detecção, é executada pelos nós somente quando a rede não está sob a influência de um *jammer*. Uma vez que não é possível assegurar que a rede não está sob a influência de ataques *jamming*, sobretudo nas MANETs onde os nós entram e saem da rede com grande frequência, o valor calculado para o patamar de detecção pode se tornar inconsistente. Como consequência, pode ocorrer a redução do desempenho da abordagem.

Uma outra limitação se refere à tarefa de detecção, executada somente pelo nó transmissor. Para calcular o coeficiente de correlação, o nó utiliza o tempo de recepção dos pacotes que foram recebidos corretamente e o tempo de recepção dos pacotes os quais foram recebidos incorretamente. Os valores da correlação tanto para a rede sob a influência do ataque *jamming* quanto para a rede sem ataque, além de mostrarem uma forte correlação, isto é, acima de 0.5, os valores apresentaram magnitudes próximas. Por apresentarem valores próximos, o processo de detecção pode não distinguir o valor da correlação referente ao ataque do valor que se refere à rede sem ataque.

Por fim, os dois trabalhos não consideram outras instâncias de ataques *jamming* na avaliação, como os ataques *jamming* deceptivo e aleatório. Além disso, esses trabalhos não citam o tipo de ataque *jamming* reativo considerado na avaliação.

2.6.2 Abordagem inter-camada

Thamilarasu et al. [24] apresentam uma abordagem inter-camada para estimar o congestionamento da rede e detectar a presença do ataque *jamming* constante. Nesta dissertação, a abordagem inter-camada é nomeada CLADE, do inglês *(A **C**ross-**L**ayer **A**pproach to **DE**tect Jamming Attacks in Wireless Ad hoc Networks)*. A Figura 2.9 ilustra o fluxograma do sistema CLADE, o qual é composto por duas fases. A *fase 1* consiste de quatro testes que servem como indícios para verificar se a rede está sob um ataque *jamming* e a

fase 2 determina a existência de um *jammer* no meio sem fio.

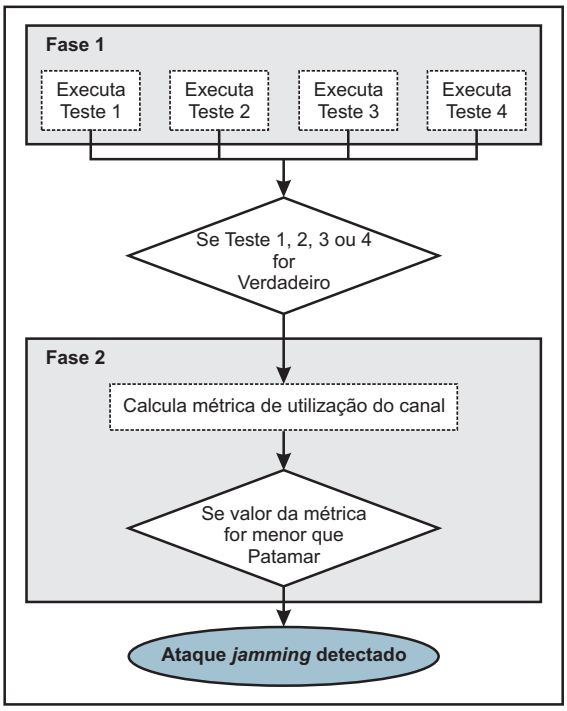

Figura 2.9: Algoritmo da abordagem inter-camada para detectar os ataques *jamming* - [24]

O primeiro teste da *fase 1* verifica um possível *jammer* na rede com base no cálculo do período de tempo que o meio de transmissão está ocupado. Quando um *jammer* interfere no meio de transmissão sem fio de forma contínua, o meio é sempre indicado pelos nós como ocupado. Para averiguar um possível *jammer* na rede, o nó compara o valor do período calculado com o valor do patamar de detecção estático. Caso o valor do período seja maior que o valor do patamar, existe a suspeita de um *jammer* na rede. No entanto, é difícil detectar o ataque baseado somente neste teste.

O segundo teste averigua a transmissão de inúmeros quadros RTS/CTS na rede. Através da análise dos endereços de origem e destino, é possível determinar a frequência que um nó transmite esses quadros. Uma vez que o número médio de transmissões de quadros RTS/CTS de um nó ultrapasse o número médio de transmissões dos outros nós no meio, existe o indício de um *jammer* na rede.

O terceiro teste indica um *jammer* na rede com base no cálculo do tempo que a reserva virtual do meio é feita. Quando os nós não recebem uma transmissão de dados durante

um grande período de tempo, a rede pode estar sob a influência de um ataque. Caso o meio de transmissão sem fio permaneça não ocupado por um período de tempo acima do valor de um patamar de detecção estático, significa que a rede pode estar sob ataque.

O quarto teste checa a existência de um ataque *jamming* através do número de retransmissões na rede. As colisões criadas pelo *jammer* resultam no aumento do número de retransmissões pelos nós afetados. A fim de verificar a ocorrência do ataque, os nós calculam o número médio de retransmissões dos seus respectivos nós vizinhos. Se o número médio de retransmissões de um nó vizinho for maior que a soma da média do número de retransmissões de todos os vizinhos, então existe a suspeita de um *jammer* na rede.

A partir do momento que um dos quatro testes da primeira fase indique a presença do ataque, a abordagem emprega a *fase 2*. Isso é feito devido aos testes não estarem sempre corretos em consequência das variações do meio de transmissão sem fio e do dinamismo das MANETs. Na *fase 2*, a abordagem calcula o valor da métrica que afere o tempo de utilização do canal e compara o valor dessa métrica com o valor do patamar de detecção. A Equação 2.2 calcula o tempo de utilização do canal U_{Ca}, o qual $T(Ca_{ocup})$ é o tempo que o canal esteve ocupado e $T(Ca_{inat})$ é o tempo o qual o canal esteve inativo. Para detectar os ataques *jamming*, a abordagem emprega um patamar de detecção estático. A abordagem determina que a rede sofre de um ataque *jamming* caso o tempo de utilização do canal seja maior que o valor desse patamar de detecção.

$$U_{Ca} = \frac{T(Ca_{ocup})}{T(Ca_{ocup}) + T(Ca_{inat})} \tag{2.2}$$

A abordagem inter-camada é ineficaz contra ataques *jamming* reativos. Isso ocorre devido a esses ataques não utilizarem o meio de transmissão constantemente. Além disso, os patamares de detecção empregados, tanto na primeira quanto na segunda fase, são estáticos e estocásticos, sendo não desejados nas MANETs e contra *jammers* que tentam se adaptar para evitar os sistemas e abordagens de detecção. Essa abordagem é comparada no Capítulo 4 ao sistema proposto neste trabalho.

2.6.3 Abordagem considerando a explicabilidade da colisão

Toledo e Wang [25] apresentam o conceito de explicabilidade da colisão para detectar os ataques *jamming* reativos. Esse trabalho tenta explicar as colisões que ocorrem nos nós receptores a partir de eventos observados em redes que empreguem o mecanismo CSMA/CA, como a função DCF do padrão IEEE 802.11. Como os *jammers* criam colisões na rede, essa abordagem observa a variabilidade na distribuição das colisões, diferenciando a operação normal da rede da anormal. A fim de determinar a ocorrência do ataque na rede, a abordagem calcula inicialmente a probabilidade que um nó contribui em uma determinada colisão. Posteriormente, a explicabilidade das colisões é calculada considerando os eventos da rede, sendo a explicabilidade sensível aos ataques *jamming* reativos.

Por fim, é proposto um detector *Kolmogorov-Smirnov* não paramétrico, no qual a distribuição de explicabilidade das colisões desvia de forma significante daquela sob a operação normal da rede. Ainda que este conceito seja um excelente indicador de anormalidade na rede, o detector empregado no trabalho considera patamares apenas estáticos para determinar a presença de um atacante, além de tornar complexa a detecção do ataque.

2.6.4 Discussão sobre os sistemas de detecção de ataques *jamming* para MANETs

A Tabela 2.1 resume as vantagens e desvantagens das abordagens de detecção de ataques *jamming* em MANETs. Em Ali Hamieh e Jalel Ben-Othman [23] e Ali Hamieh et al. [22], a abordagem correlaciona os tempos de recepção dos quadros válidos e inválidos para detectar a presença dos *jammers* reativos. Entretanto, o escopo da abordagem não considera outros tipos de ataques *jamming*. Thamilarasu et al. [24] consideram várias métricas de forma isolada para detectar o ataque *jamming* constante. Contudo, o uso dessas métricas separadamente e ao mesmo tempo empregando patamares estáticos torna-se uma abordagem ineficaz para o escopo das MANETs, devido às características de mobilidade da rede. Toledo e Wang [25] propõem a métrica de explicabilidade das colisões, que as de-

screve conforme os eventos na rede. Essa abordagem tem como desvantagem o uso de patamares estáticos para determinar a presença de um *jammer* e a complexidade da detecção do ataque. Além das abordagens de detecção de ataques *jamming* apresentadas, outras existem [7, 21]. No entanto, tais abordagens não têm como foco as MANETs.

Trabalhos	**Métricas de detecção**	**Ataque *Jamming***	**Vantagem**	**Desvantagem**
Ali Hamieh e Jalel Ben-Othman [23] e Ali Hamieh et al. [22]	• Tempo de recepção do pacote correto • Tempo de recepção do pacote incorreto	Reativo	• Facilidade de implementação • Forte correlação das métricas	• Não consideram outras instâncias de de ataques *jamming*
Thamilarasu et al. [24]	• Tempo de ocupação do meio • Número de quadros de controle transmitidos para o meio • Período de reserva do meio de transmissão • Número de retransmissões • Utilização do canal	Constante	• Alta taxa de detecção	• Ineficaz contra ataques *jamming* reativos • Uso de patamares estáticos
Toledo e Wang [25]	• Explicabilidade das colisões	Reativo	• Excelente indicador de anormalidade	• Emprego de patamares estáticos

Tabela 2.1: Sistemas de detecção de ataques *jamming* para MANETs.

2.7 Sistemas de detecção inspirados no sistema imunológico humano

O sistema imunológico humano (SIH) provê defesas contra diversos tipos de patogenias, como vírus, fungos, bactérias, parasitas e germes [73]. Ele atua de forma eficiente ao reconhecer padrões moleculares encontrados em microorganismos. O SIH também age de forma adaptativa ao extrair informações da patogenia analisada e as disponibiliza para futuros reconhecimentos de patogenias iguais ou semelhantes.

O SIH emprega três linhas de defesa para prover a proteção ao corpo. A Figura 2.10 apresenta as linhas de defesa. A primeira linha de defesa bloqueia a entrada de um grande número de patogenias no corpo. Ela consiste da pele e ocorre com secreções normais que matam as patogenias. A segunda linha de defesa (imunidade inata ou não específica) reconhece de maneira genérica as patogenias que conseguem invadir o corpo. Isso ocorre através da identificação do maior número possível de patogenias pela migração local de células, especialmente as fagocitárias, e também pela inflamação e febre. A terceira linha

de defesa (imunidade adaptativa ou adquirida) reconhece de maneira específica as patogenias através de células especiais que chegam ao local da infecção. Por não ser o foco deste trabalho, o sistema imunológico adaptativo não é descrito, porém uma descrição detalhada sobre esse sistema é encontrada em [73].

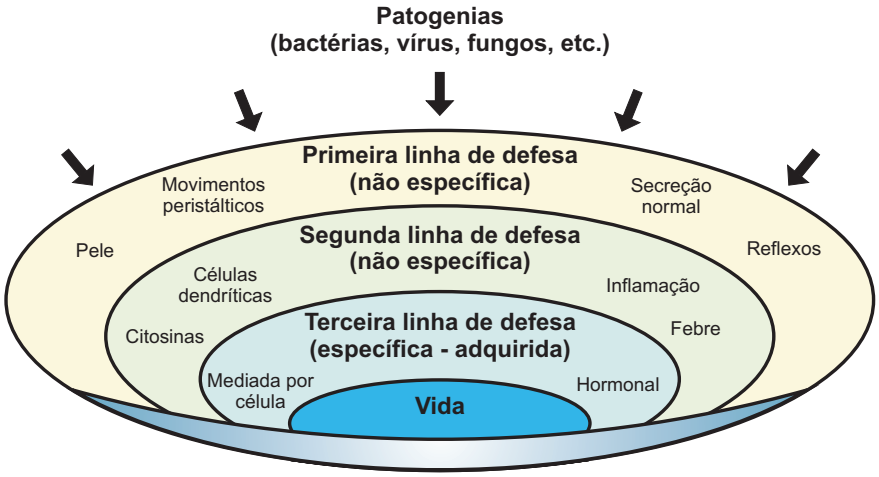

Figura 2.10: Linhas de defesa empregadas pelo sistema imunológico humano - modificado de [74]

O **sistema imunológico inato** (SII) pode ser encontrado em plantas, fungos, insetos e em organismos primitivos multi-celulares. Ele consiste de células e mecanismos que defendem o corpo de forma **genérica**, reagindo de maneira similar a uma grande variedade de microorganismos. As principais células que integram o SII são as **células dendríticas** (CD). Elas têm o propósito de coletar, processar e classificar os microorganismos invasores. Com isso, o sistema imunológico pode reagir de forma tolerante ou desencadear uma inflamação no local onde o microorganismo foi encontrado.

Matzinger propôs uma abordagem de funcionamento do SII denominada teoria do perigo [27]. Essa teoria se baseia na afirmação que o SII discerne entre o perigo e a ausência de perigo, sendo que as CDs ocupam um papel importante na defesa do organismo. Além de apresentarem os antígenos, as CDs são ativadas por **sinais** liberados na ocorrência tanto da morte natural das células *(apoptose)* quanto na morte prematura *(necrose)*. Caso a CD receba sinais seguros provenientes da apoptose das células, ela inibirá uma reação específica do sistema imunológico. Por outro lado, a CD que receber sinais de perigo resultantes da necrose das células, ativará a resposta imunológica do SIH. Esse

mecanismo regulatório diminui a geração de falsos positivos, além de aumentar a precisão de detecção das patogenias.

Os algoritmos que modelam o SIH reproduzem o comportamento e as propriedades de células imunológicas, como as células dendríticas [75]. Em geral, o desenvolvimento desses algoritmos é guiado pela discriminação entre as células do corpo (o próprio) e as patogenias (o não-próprio) [76]. As respostas imunológicas são ativadas quando o corpo encontra uma substância não-própria. Os algoritmos que se inspiram na teoria clássica necessitam de uma fase de treinamento, na qual o sistema é alimentado com dois conjuntos de dados, o próprio e o não-próprio.

Os SDs baseados em algoritmos que se inspiram na teoria clássica geram um grande número de falsos positivos e falsos negativos [76]. Os falsos positivos ocorrem porque os conjuntos de dados próprios para o treinamento do sistema nunca estão completos. Logo, os SDs falham em reconhecer dados próprios que ainda não foram vistos. Uma forma de contornar esse problema está no uso da generalização do conjunto próprio. Contudo, essa generalização ocasiona o aumento do número de falsos negativos. Já um conjunto de dados não-próprio incompleto é a principal causa dos SDs não conseguirem detectar eventos existentes não-próprios, podendo ser explorados por atacantes caso permaneçam não conhecidos por um longo período de tempo.

Além disso, a teoria clássica não consegue explicar alguns problemas do sistema imunológico, como a autoimunidade, onde vários elementos próprios são eliminados enquanto outros não-próprios podem não ser destruídos. Para resolver os problemas apresentados pela teoria clássica, Matzinger propôs a teoria do perigo [27]. Os seus princípios têm direcionado o desenvolvimento de algoritmos bio-inspirados. A partir da teoria do perigo foram criados dois algoritmos: o clássico de células dendríticas *(DCA - Dendritic Cell Algorithm)* [77] e o determinístico de células dendríticas *(dDCA - deterministic Dendritic Cell Algorithm)* [78].

O DCA correlaciona os fluxos de dados e classifica os dados idênticos como sendo normais ou anômalos [77]. Para isso, o DCA emprega os seguintes componentes: as medidas de avaliação, os conjuntos de informações, uma população de agentes artificiais

e os patamares dinâmicos. As medidas de avaliação são métricas estatísticas que aferem o desempenho da rede. O DCA divide tais medidas em três conjuntos: de normalidade, PAMPS *(Pathogen Associated Molecular Patterns)* e de anormalidade. As medidas de avaliação que sofrem crescimento quando a rede possui um comportamento normal são denominadas de medidas de normalidade. Elas representam o comportamento normal da rede. As medidas PAMPS indicam com maior exatidão que a rede se encontra sob um ataque. Já as medidas de anormalidade podem ou não indicar a presença de algum ataque na rede, entretanto, a probabilidade de existir um ataque aumenta conforme as medidas de anormalidade também aumentam. As informações compreendem os dados coletados que trafegam pela rede, representando os *antígenos* no contexto biológico. Tais informações são analisadas em conjunto com as medidas de avaliação pelos agentes artificiais.

O algoritmo possui uma população de agentes artificiais que reproduzem o comportamento das *células dendríticas* no contexto biológico. Cada agente que constitui a população possui um patamar de migração aleatório que limita o seu tempo de atuação *(tempo de vida)* no algoritmo. Para relacionar as informações coletadas, um sub-conjunto da população de agentes é selecionado de forma aleatória considerando os três conjuntos de medidas de avaliação. O algoritmo calcula três valores de saída para cada agente. Tais valores representam a quantificação do nível de anomalia de um grupo de informações. O primeiro valor de saída denota a coestimulação do agente, sendo usado de forma direta no seu tempo de vida. Já os dois outros valores de saída do agente representam o contexto semi-maduro e o maduro presenciado pelo agente. O contexto semi-maduro representa a tolerância do algoritmo perante a anomalia observada na rede. Por outro lado, o contexto maduro indica a estimulação do agente perante o ataque. Uma vez que a coestimulação ultrapasse o tempo de vida do agente, as informações e o contexto presenciado pelo agente são salvos para posterior análise. Por fim, com base nos valores de saída dos agentes artificiais, o algoritmo calcula um novo valor para o patamar de detecção dinâmico denominado MCAV *(Mature Context Antigen Value)*. Esse valor é calculado através da divisão do somatório do número de informações presenciadas pelos agentes artificiais sob um contexto maduro dividido pelo número total de informações analisadas pelos agentes.

A maioria das pesquisas que empregam o algoritmo DCA estão dentro do escopo da segurança de redes [78]. O algoritmo é aplicado com sucesso na detecção de ataques que realizam o escaneamento de portas [75] e em ataques nos quais os nós que seguem o comportamento normal da rede [79]. Contudo, o DCA considera variáveis estocásticas que tornam complexa a sua análise sistemática. Além de serem estocásticas, as variáveis são estáticas, sendo não desejáveis nas MANETs devido à dinamicidade dessas redes.

Para evitar o uso de variáveis estocásticas, além de tornar mais simples a sua análise, Greensmith e Aickelin criaram o algoritmo dDCA [78]. Greensmith e Aickelin melhoraram o algoritmo DCA da seguinte forma: (i) os três conjuntos de medidas de avaliação (normalidade, PAMPS e anormalidade) foram reduzidos para somente dois conjuntos, o de normalidade e o de anormalidade, as medidas PAMPS foram removidas por possuírem o mesmo comportamento das medidas de anormalidade; (ii) o patamar de migração aleatório que limita o tempo de vida de um agente é substituído por um patamar que segue uma distribuição estatística uniforme; (iii) o armazenamento dedicado e a amostragem das informações foram substituídas pela amostragem de todas as informações pelos agentes; (iv) os valores de saída dos agentes artificiais são calculados uma vez para toda a população e; (v) somente um fator ($\bar{k}$) que demonstra o contexto presenciado é calculado para cada agente, sendo que os valores negativos de ($\bar{k}$) representam um contexto benigno e os valores positivos um contexto malicioso.

Ao final do processo de detecção, o dDCA verifica a existência da anomalia através da correlação das informações com o agrupamento das medidas. Além de calcular o valor para o patamar de detecção $MCAV$, o algoritmo também calcula o valor para um novo patamar de detecção, denominado K. Esse patamar leva em consideração os valores de contexto $\bar{k}$ e provê valores reais para a detecção. Ao final da fase de detecção, o algoritmo calcula o valor de um patamar de detecção dinâmico T_K. Uma vez que o patamar T_K é aplicado aos valores K_i, o sistema classifica qualquer valor acima desse patamar como anômalo e valores abaixo como normais.

O algoritmo dDCA possui características que o tornam interessante para este trabalho. Além de obter resultados significantes ao ser comparado com outras abordagens de de-

tecção [78], o algoritmo dDCA é adaptativo. Isso ocorre devido ao algoritmo se inspirar na teoria do perigo, sendo desejável no contexto das MANETs. Além disso, o algoritmo emprega agentes artificiais que agrupam as medidas de avaliação, relacionam as informações coletadas do meio de transmissão e combinam os valores de contexto dos classificadores para calcular os valores do patamares dinâmicos a fim de detectar a anomalia.

2.8 Resumo

Este capítulo apresentou os conceitos relacionados às MANETs, aos ataques *jamming* e aos sistemas de detecção de ataques *jamming*. Esses ataques são realizados no meio de transmissão sem fio, reduzindo a vazão dos tráfegos e aumentando o consumo de energia dos nós vítimas do ataque. Contudo, as abordagens existentes que tentam detectar os ataques *jamming* nas MANETs são ineficazes pois apenas empregam métricas isoladas de avaliação e patamares estáticos e estocásticos.

Uma forma de corrigir e melhorar as fragilidades observadas pelos sistemas de detecção de ataques *jamming* atuais é o uso de algoritmos bio-inspirados. Tais algoritmos modelam o comportamento da natureza a fim de melhorar as técnicas computacionais. Dentre as teorias que descrevem o funcionamento do sistema imunológico humano, a teoria do perigo tem inspirado o desenvolvimento de algoritmos, que empregam o perigo para determinar anomalias. Na literatura são encontrados dois principais algoritmos inspirados no funcionamento da teoria do perigo, o algoritmo DCA e o algoritmo dDCA. Tais algoritmos possuem características como a descentralização, a tolerância a erros, a dinamicidade, a adaptabilidade, a identificação do perigo, os critérios de avaliação, os classificadores e o uso de patamares dinâmicos. Com base nessas características, o Capítulo 3 propõe um sistema de detecção de ataques jamming para MANETs que se inspira na teoria do perigo.

CAPÍTULO 3

O SISTEMA DANTE

Este capítulo descreve um sistema para detecção de ataques *jamming* em redes móveis ad hoc. Este sistema, inspirado no funcionamento do sistema imunológico humano, tem como objetivo detectar os ataques no meio de transmissão sem fio, diferenciando as colisões geradas pelos atacantes daquelas criadas pela baixa qualidade do enlace. O sistema também quantifica o impacto dos ataques a fim de auxiliar medidas reativas. A Seção 3.1 apresenta a visão geral do funcionamento do sistema proposto, a qual descreve as suas características e os seus principais elementos. A Seção 3.2 apresenta a arquitetura do sistema e define cada um dos seus módulos e componentes.

3.1 Visão geral

O sistema proposto, denominado **DANTE** (do inglês, ***D****etecting j****A****mming attacks by the da****N****ger* ***Th****E****o****ry*), tem como objetivo detectar e quantificar os ataques *jamming* nas redes móveis ad hoc *(MANETs - Mobile Ad Hoc Networks)*. O sistema considera a dinamicidade das MANETs e a adaptabilidade dos atacantes, sendo totalmente distribuído e auto-organizável. O sistema DANTE assume que cada nó pertencente à MANET atua como um monitor, observando as transmissões locais e coletando as informações transmitidas no meio de comunicação sem fio pelos nós vizinhos. Essa asserção é plausível utilizando qualquer rádio que atue em modo promíscuo, isto é, em modo ad hoc, como aqueles que empregam a função DCF *(Distributed Coordination Function)* do padrão IEEE 802.11 [28]. Além disso, cada nó da rede realiza a detecção de forma separada, o que garante a não existência de um ponto único de falha na rede.

Em relação à abordagem de detecção foi escolhida aquela baseada em anomalias. Essa escolha se baseia nas características dos *jammers* os quais podem modificar a forma como realizam o ataque na rede, a fim de tornar a detecção mais difícil e complexa.

Relativamente à categoria da abordagem de detecção baseada em anomalias, o sistema DANTE considera uma técnica bio-inspirada de aprendizado de máquina. A técnica é inspirada no funcionamento da teoria do perigo na qual o sistema imunológico humano discerne entre o perigo e a ausência de perigo [27]. Essa técnica permite que o sistema DANTE modifique de forma dinâmica os valores dos patamares usados para a detecção e quantifique o impacto dos ataques para que medidas reativas sejam tomadas [75, 80].

O sistema DANTE é composto dos seguintes elementos: as **informações** coletadas da camada de enlace, as **medições de avaliação**, os **agentes artificiais**, as **saídas** dos agentes e o **componente de combinação e decisão**. As informações são definidas como os cabeçalhos dos quadros provenientes da camada de enlace, tanto os que foram decodificados corretamente quanto aqueles que sofreram algum tipo de interferência. Para garantir o aproveitamento de recursos do dispositivo, o sistema considera somente o cabeçalho do quadro por conter os dados úteis para a detecção da anomalia. As informações correspondem aos *antígenos* no contexto biológico.

As **medições de avaliação** são métricas estatísticas que aferem a qualidade do meio de transmissão e dos enlaces vizinhos. Essas medições correspondem na biologia aos *sinais* gerados pela morte das células de um indivíduo. Os **agentes artificiais** equivalem às *células dendríticas*, isto é, as células ativadoras do *sistema imunológico*. Uma vez que os nós da rede atuam como monitores, cada nó possui vários agentes artificiais os quais relacionam as informações do meio de sem fio com base nas medições de avaliação.

As **saídas** quantificam a anomalia presenciada no meio de transmissão sem fio com base nos agentes artificiais e no processamento das informações e das medições. Tais saídas equivalem às *moléculas co-estimulatórias* do *sistema imunológico*. Por fim, o sistema DANTE, o qual é empregado por cada nó, utiliza o **componente de combinação e decisão** parar agregar os valores de saída dos agentes artificiais, quantificar o ataque e determina a existência do *jammer*, além de diferenciar as colisões causadas pelos *jammers* daquelas geradas pela baixa qualidade de enlace.

A Figura 3.1 ilustra a visão geral do funcionamento do sistema DANTE em um nó da rede. Essa figura é composta por m agentes artificiais, k informações I, n medições

M, duas saídas S e um componente de combinação e decisão. O sistema emprega os m agentes artificiais para relacionar as informações provenientes da camada de enlace $I_1, I_2, I_3, ..., I_{k-2}, I_{k-1}, I_k$. Uma vez que existam informações as quais sofreram algum tipo de interferência, cada agente agrupa e aplica as medições de avaliação $M_1, M_2, M_3, ..., M_n$ a fim de verificar se a interferência é anômala. Em outras palavras, os agentes verificam se qualquer interferência nas informações ocorreu em decorrência da ação de um *jammer* na rede. Além disso, os agentes calculam os valores das saídas S_1 e S_2 referentes à anomalia observada no meio de transmissão. Ao final do processo, o sistema DANTE emprega o componente de combinação e decisão para combinar as saídas dos m agentes artificiais e detectar a atuação do *jammer* na rede.

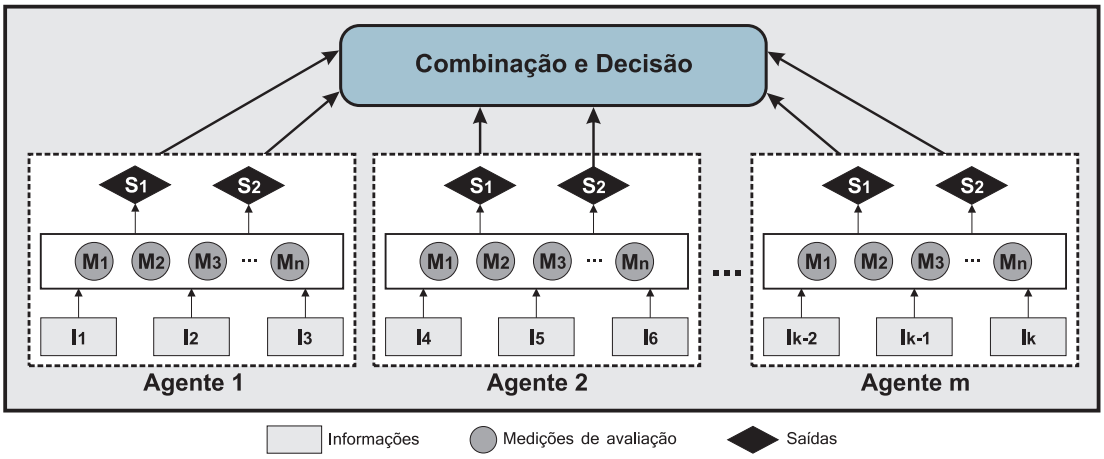

Figura 3.1: Visão geral do funcionamento do sistema - referência própria

3.2 Arquitetura do sistema DANTE

A arquitetura do sistema DANTE é composta por três módulos, denominados **coleta e medições**, **detecção bio-inspirada** e **resposta ao ataque *jamming***, como ilustrada na Figura 3.2. O módulo de coleta e medições captura os quadros provenientes da camada de enlace que sofreram colisão e calcula o desempenho do meio de transmissão sem fio e dos enlaces vizinhos. O módulo de detecção bio-inspirada determina e quantifica a ocorrência do ataque *jamming* no meio de transmissão. E o módulo de resposta ao ataque *jamming* reage conforme a detecção e quantificação do ataque.

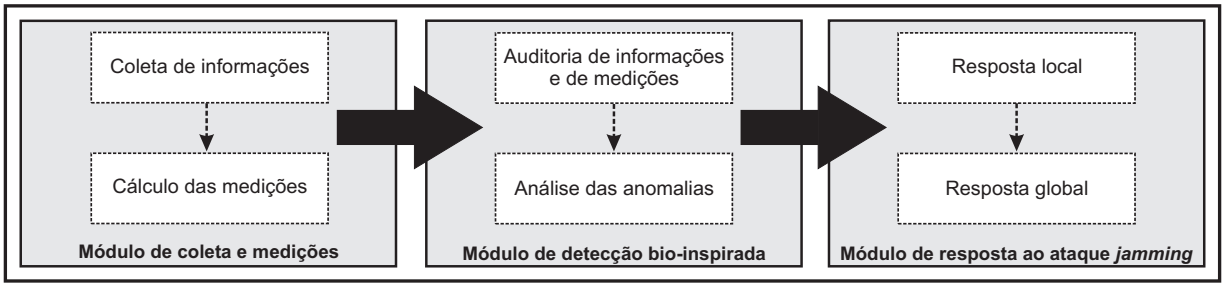

Figura 3.2: Arquitetura do sistema DANTE - referência própria

O principal módulo da arquitetura é o de detecção bio-inspirada. Ele possui os procedimentos que determinam se a rede está sob o efeito de ataques *jamming*. Os módulos de medições e informações e de resposta ao ataque *jamming* proveem suporte ao módulo de detecção bio-inspirada. O sistema DANTE realiza a detecção ao final do período de tempo Tem_{Det}. Esse período é um valor constante que define o intervalo de tempo no qual o sistema coleta as informações e calcula novos valores para as medições. As próximas subseções detalham cada um dos módulos presentes na arquitetura.

3.2.1 Módulo de coleta e medições

O módulo de *coleta e medições* captura os quadros provenientes da camada de enlace que sofreram colisões e calcula novos valores para as medições estatísticas de avaliação do meio de transmissão sem fio e dos enlaces vizinhos. A Figura 3.3 ilustra o módulo de *medições e informações*. Esse módulo é composto por dois componentes, denominados **coleta de informações** e **cálculo das medições**.

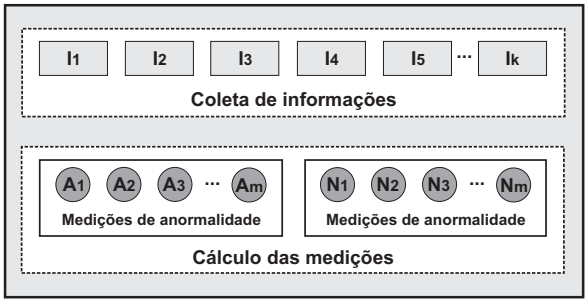

Figura 3.3: Módulo de coleta e medições - referência própria

O componente *coleta de informações* captura de maneira promíscua o cabeçalho dos quadros que sofreram colisão provenientes da camada de enlace durante o período de

tempo Tem_{Det}. No sistema, esses quadros são denominados de informações. A Figura 3.3 ilustra o componente coleta de informações, sendo composto por k informações I. Tais informações são empregadas como indícios da atuação dos *jammers* no meio de transmissão sem fio, os quais criam colisões e reduzem o desempenho dos nós. Elas também são necessárias para averiguar se as colisões foram realmente criadas por um *jammer* ou geradas pela baixa qualidade do enlace. Contudo, para que o sistema execute a detecção de forma adequada é necessário um número suficiente de informações.

O bom desempenho do sistema é diretamente proporcional ao número de informações capturadas. Nos ataques *jamming* ativos, o número de informações coletadas é alto, o que auxilia o processo de detecção. Porém, existe o problema da baixa quantidade de informações criadas pelos ataques *jamming* intermitentes, limitando a execução do sistema [7]. Para mitigar esse problema, o sistema DANTE emprega a técnica de multiplicador de informações [81] a qual cria múltiplas cópias de uma mesma informação após coletá-la da camada de enlace.

O componente de *cálculo das medições* quantifica o desempenho dos enlaces vizinhos empregando medições estatísticas. O componente calcula novos valores para as medições a cada período T_{Med}, sendo T_{Med} uma constante com o valor menor que Tem_{Det}. Isso é feito para assegurar que o sistema terá um número maior de medições com relação ao número de informações a serem processadas.

As medições devem auxiliar o sistema na detecção de um grande número de ataques e na diferenciação das colisões criadas pelos *jammers* em relação às colisões geradas pelos eventos de congestionamento da rede ou instabilidade dos enlaces. Além disso, as medições devem evitar o aumento do consumo de recursos no processo de detecção. Como explicado no Capítulo 2, a teoria do perigo é suportada pela argumentação de que o sistema discerne entre o perigo e a ausência de perigo. Com base nessa asserção, o componente *cálculo das medições* emprega dois conjuntos de medições para discernir o comportamento bom do comportamento ruim, as medições de anormalidade e normalidade, as quais representam o perigo e ausência de perigo, respectivamente. A Figura 3.3 ilustra os dois conjuntos de medições, sendo que cada conjunto emprega m medições estatísticas para estabelecer o

desempenho dos enlaces vizinhos.

As medições de normalidade denotam que o meio de transmissão sem fio e a rede estão em um comportamento normal e aceitável pelo sistema DANTE. Quanto mais próximo de 1 for o valor das medições de normalidade, maior é o **equilíbrio** encontrado na rede. O componente de cálculo das medições emprega duas medições para avaliar a normalidade da rede. Tais medições são consideradas por sofrerem atenuação quando um *jammer* executa o ataque na rede, como demonstrado em [40]:

Taxa de transmissão de dados úteis ($TaxDadUte_{Tx}$): esta medição calcula a taxa de dados úteis transmitidos pelo nó referente à carga útil do quadro de dados. Esta taxa é calculada com base na quantidade de *bytes* úteis transmitidos ($BytUte_{Tx}$), isto é, a carga útil transmitida, dividido pela quantidade total de *bytes* transmitidos ($TotByt_{Tx}$):

$$TaxDadUte_{Tx} = \frac{BytUte_{Tx}}{TotByt_{Tx}} \tag{3.1}$$

Taxa de recebimento de dados úteis ($TaxDadUte_{Rx}$): esta medição calcula a taxa de dados úteis recebidos pelo nó referente à carga útil do quadro de dados. Esta taxa é calculada com base na quantidade de *bytes* úteis recebidos ($BytUte_{Rx}$), isto é, a carga útil recebida, dividido pela quantidade total de *bytes* recebidos ($TotByt_{Rx}$):

$$TaxDadUte_{Rx} = \frac{BytUte_{Rx}}{TotByt_{Rx}} \tag{3.2}$$

Contudo, somente as medições de normalidade não são capazes de determinar a ocorrência de ataques *jamming* no meio de transmissão sem fio. A definição de medições sensíveis ao desequilíbrio da rede também é necessária, pois elas enfatizam que os nós se encontram em um ambiente perigoso. Enquanto as medições de normalidade determinam o nível de equilíbrio da rede, as medições de anormalidade revelam a possível presença de um ataque no meio.

As medições de anormalidade representam uma quantificação que é diretamente proporcional ao desequilíbrio dos enlaces e do meio de transmissão sem fio. Quanto mais próximo de 1 for o valor dessas medições, maior será o **desequilíbrio** encontrado na rede. O componente de cálculo das medições considera duas medições para verificar a anormalidade na rede. Essas medições são consideradas por variarem fortemente quando um *jammer* atua na rede [7, 15, 82, 83]:

Taxa de colisão de quadros ($TaxCol$): indica a taxa de quadros provenientes da camada de enlace que sofreram colisões. Esta taxa é calculada pelo número de quadros que sofreram colisão ($QuaCol$) dividido pelo número total de quadros coletados da camada de enlace ($TotQua_{Rx}$):

$$TaxCol = \frac{QuaCol}{TotQua_{Rx}} \tag{3.3}$$

Taxa de bloqueio do rádio ($TaxBloqRad$): os nós que se encontram no raio de alcance de qualquer transmissão devem bloquear seus rádios para não causar colisões nos nós receptores [28], como explicado no Capítulo 2. Esta taxa é calculada pelo período que o nó permaneceu com o rádio bloqueado ($TemBloqRad$) com relação ao período que o sistema DANTE realiza a detecção Tem_{Det}:

$$TaxBloqRad = \frac{TemBloqRad}{Tem_{Det}} \tag{3.4}$$

A Tabela 3.1 sintetiza as medições de avaliação, tanto de normalidade quanto de anormalidade, empregadas pelo componente *cálculo das medições*. Essa tabela apresenta o nome, a medição, o tipo e a descrição de cada medição de avaliação pertencente ao componente. O componente utiliza as medições por expressarem a variação que ocorre na rede. A variação auxilia na detecção dos ataques *jamming* por ocorrer devido a atuação dos *jammers*.

Nome	Medição	Tipo	Descrição
Taxa de dados úteis transmitidos	$TaxDadUte_{Tx}$	Normalidade	Quantidade de *bytes* úteis transmitidos dividido pela quantidade total de *bytes* transmitidos ao meio sem fio
Taxa de dados úteis recebidos	$TaxDadUte_{Rx}$	Normalidade	Quantidade de *bytes* úteis recebidos dividido pela quantidade total de *bytes* coletados da camada de enlace
Taxa de colisão de quadros	$TaxCol$	Anormalidade	Número de quadros que sofreram colisão dividido pelo número total de quadros provenientes da camada de enlace
Taxa de bloqueio do rádio	$TaxBloqRad$	Anormalidade	Período de tempo que o nó permaneceu com o rádio bloqueado dividido pelo tempo Tem_{Det} que o sistema DANTE realiza a detecção

Tabela 3.1: Síntese das medições de avaliação

3.2.2 Módulo de detecção bio-inspirada

O módulo de detecção bio-inspirada determina e quantifica a ocorrência de ataques *jamming* na rede. Ele é acionado pelo sistema ao final do período de tempo Tem_{Det}. Esse módulo possui dois componentes denominados **auditoria das informações e medições** e **análise das anomalias**. A Figura 3.4 ilustra os componentes e os seus principais elementos, além das iterações existentes.

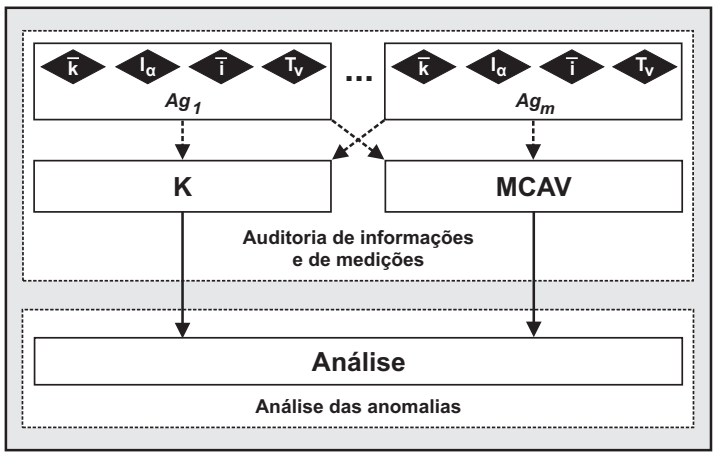

Figura 3.4: Módulo de detecção bio-inspirada - referência própria

O componente *auditoria das informações e das medições* determina e quantifica a ocorrência de ataques *jamming* na rede. Para isso, o componente considera o algoritmo dDCA *(deterministic Dendritic Cell Algorithm)*. O dDCA se inspira na teoria do perigo [78], na qual agentes artificiais reproduzem o comportamento das *células dendríticas*. Como ilustrado na Figura 3.4, o algoritmo emprega m agentes artificiais para processar as informações, agregar os valores das medições e quantificar a anomalia. De

forma resumida, os agentes artificiais recebem dois conjuntos de entradas, realizam uma sequência de procedimentos e calculam duas saídas. Como entrada, os agentes recebem as informações coletadas pelo componente coleta de informações e as medições calculadas pelo componente cálculo das medições. E como saídas, os agentes quantificam a anomalia.

O algoritmo dDCA emprega os agentes artificiais para examinar as informações, processar as medições e verificar o evento de anomalia no meio de transmissão sem fio. Isso é feito da mesma forma como realizado no SIH, onde as células dendríticas examinam os microorganismos e processam os sinais de morte das células no tecido humano. Os agentes artificiais possuem quatro parâmetros principais: o T_v, o I_α, o $\bar{i}$ e o $\bar{k}$.

O parâmetro T_v indica o tempo de vida do agente, isto é, o número máximo de iterações que o agente fará no algoritmo. Como o algoritmo dDCA reproduz o funcionamento do SIH, os agentes artificiais possuem um tempo de vida limitado, assim como as *células dendríticas* no *contexto biológico*. Além disso, cada agente artificial possui um tempo de vida diferente. Isso é feito para gerar uma diversidade na população de agentes artificiais e criar um efeito de janela de tempo variável com diferentes agentes processando as informações e as medições. No algoritmo, esse tempo é escolhido segundo uma distribuição uniforme [78].

Durante o seu tempo de vida, o agente artificial analisa um pequeno sub-conjunto das informações e processa as medições. O parâmetro I_α representa o número de informações examinadas pelo agente artificial, sendo que cada informação é examinada uma única vez por um agente. Já o parâmetro $\bar{i}$ informa o número de iterações realizadas pelo agente antes do parâmetro T_v terminar. Por fim, o parâmetro $\bar{k}$ representa a anomalia presenciada por um agente artificial durante o seu tempo de vida T_v.

Para auxiliar os agentes a determinar se as informações são anômalas ou não, o dDCA calcula o valor do parâmetro k. Esse parâmetro representa a acumulação do nível de anomalia presenciado pelo agente durante o processo de detecção e denota as circunstâncias que um evento ocorreu. O parâmetro k é calculado pela Equação 3.5, na qual A e N representam o somatório das medições de anormalidade e normalidade, respectivamente; e os pesos α e β são valores constantes que controlam qual o conjunto de

medições será enfatizado pelo sistema. Cada agente é exposto às mesmas medições e as processa da mesma forma. Isso é feito para otimizar o processamento dessas medições, pois elas são calculadas somente uma vez para todos os agentes.

$$k = \alpha \times A - \beta \times N \tag{3.5}$$

A fim de limitar o tempo de vida do agente artificial, o algoritmo dDCA emprega o parâmetro *csm*. Ele reproduz a acumulação dos valores das medições de normalidade e anormalidade, de maneira similar ao SIH, onde as moléculas coestimulatórias representam a acumulação dos sinais de morte das células. Esse parâmetro é calculado pela Equação 3.6. Assim que o parâmetro T_v do agente expira, isto é, alcança um valor menor ou igual a zero, o algoritmo verifica o parâmetro $\bar{k}$. Uma vez que o valor desse parâmetro seja maior que zero, o algoritmo considera o número I_α de informações desse agente como anômalas, caso contrário, as informações são consideradas como normais. Por fim, o algoritmo armazena na memória os parâmetros $\bar{k}$, I_α e $\bar{i}$ do agente e o reinicializa para passar novamente por todo o processo de auditoria.

$$csm = \alpha \times A + \beta \times N \tag{3.6}$$

Ao final do processo de auditoria das informações e medições, o algoritmo dDCA calcula valores para duas saídas denominadas K e $MCAV$ *(Mature Context Antigen Value)*. Para calcular os novos valores, o algoritmo combina os valores dos parâmetros dos agentes artificiais. A saída $MCAV$ representa a proporção de informações dos agentes que foram consideradas como anômalas. A Equação 3.7 calcula o valor da saída $MCAV$, representada pela taxa do somatório M do número de informações dos agentes classificadas como anômalas dividido pelo número total de informações (Inf) examinadas pelos agentes. Essa saída retorna um valor entre 0 e 1, na qual a probabilidade das informações serem anômalas aumenta conforme esse valor tende a 1. Contudo, a saída $MCAV$ não demonstra a grandeza da diferença entre os valores positivos e negativos da anomalia $\bar{k}$ observado por um agente ag.

$$MCAV = \frac{M}{Inf} \tag{3.7}$$

A saída K deriva do parâmetro $\bar{k}$ dos agentes artificiais. Essa saída representa os valores de anomalia reais e auxilia na medição da variação dos processos normais e anômalos [78], como o congestionamento na rede ou as colisões criadas pelos *jammers*, respectivamente. A Equação 3.8 calcula o nível de anomalia presenciado no meio de transmissão sem fio usando a magnitude do parâmetro $\bar{k}$. A equação calcula a saída K a partir do somatório de $\bar{k}$ dividido pelo somatório de I_α, na qual $\bar{k}$ é o valor de anomalia observado por um agente ag e I_α é o número de informações examinadas por esse mesmo agente. Essa equação retorna valores reais dependentes do conjunto de métricas de entrada. A saída K pode ser empregada a fim de calcular a grandeza da anomalia presenciada no meio de transmissão sem fio. Por instância, o sistema DANTE poderia considerar essa saída para verificar o impacto que os *jammers* ocasionam na rede.

$$K = \frac{\sum_m \bar{k}}{\sum_m I_\alpha} \tag{3.8}$$

O componente *análise das anomalias* determina a ocorrência de ataques *jamming* no meio de transmissão sem fio. Para este propósito, o sistema DANTE emprega a saída $MCAV$ do algoritmo dDCA. A fim de identificar o *jammer* na rede, o componente *análise das anomalias* emprega um patamar de detecção. Uma vez que os valores da saída MCAV variam entre 0 e 1, o valor do patamar de detecção próximo de 1 denota que o sistema DANTE é tolerante às colisões criadas na rede. Em contrapartida, o valor do patamar próximo de 0 representa que o sistema não possui qualquer tolerância às colisões.

Em decorrência da saída MCAV quantificar a anomalia presenciada pelos agentes artificiais, qualquer valor acima do patamar de detecção indica que as informações capturadas pelo módulo *coleta e medições* são anômalas. Tal fato denota que a rede se encontra sob a influência de um ataque *jamming*. Por outro lado, os valores da saída MCAV iguais a zero indicam que as colisões capturadas pelo sistema ocorreram devido à baixa qualidade do enlace ou ao congestionamento na rede.

3.2.3 Módulo de resposta ao ataque *jamming*

O módulo de resposta ao ataque *jamming* tem a finalidade de reagir contra os ataques *jamming* após a detecção realizada pelo módulo de detecção bio-inspirada. O módulo de resposta ao ataque *jamming* consiste em dois componentes, um referente à resposta local e o outro referente à resposta global. Na resposta local, o sistema pode modificar parâmetros locais para reduzir a ação dos eventuais *jammers*. Na resposta global, o sistema pode desencadear a reação em nível de rede. Apesar desse módulo não ser o foco principal do presente trabalho, são exemplificadas algumas possíveis reações contra os ataques *jamming*.

Como reações locais, um nó transmissor pode empregar técnicas de controle de potência de transmissão (CPT) [51, 52] ou considerar o salto de frequência para evitar a frequência utilizada pelo *jammer* [7, 9]. O CPT tem como objetivo aumentar o tempo de vida dos nós na rede, ao reduzirem a potência de transmissão empregada no envio dos quadros [84]. Contudo, a partir do momento que é detectada a presença de um *jammer* no meio de transmissão sem fio, a técnica de CPT necessita aumentar a potência de transmissão do quadro.

A Figura 3.5 ilustra uma rede composta por três nós, os quais dois nós são legítimos e um nó atua como *jammer*. Na rede com CPT sob ataque *jamming*, os nós possuem um enlace sem fio estabelecido empregando uma potência de transmissão com o raio de alcance R_{No}. O *jammer*, por sua vez, tenta deturpar esse enlace sem fio utilizando uma potência de transmissão com o raio de alcance R_{Jammer}. Como a potência de transmissão empregada pelo *jammer* é maior que a potência de transmissão usada pelos nós, eles não conseguiram se comunicar. Uma forma de tentar reagir contra o ataque estaria em aumentar a potência de transmissão. O aumento da potência é realizado para assegurar que o quadro seja decodificado de forma correta nos nós receptores. Portanto, é viável o estudo de técnicas de CPT que sejam conscientes ao ataques *jamming*.

No salto de frequência, os nós tentam mitigar os ataques *jamming* ao transmitirem os quadros empregando diferentes canais daqueles obstruídos pelo *jammer*. Na abordagem tradicional de salto de frequência, um par de nós transmissor/receptor necessita saber

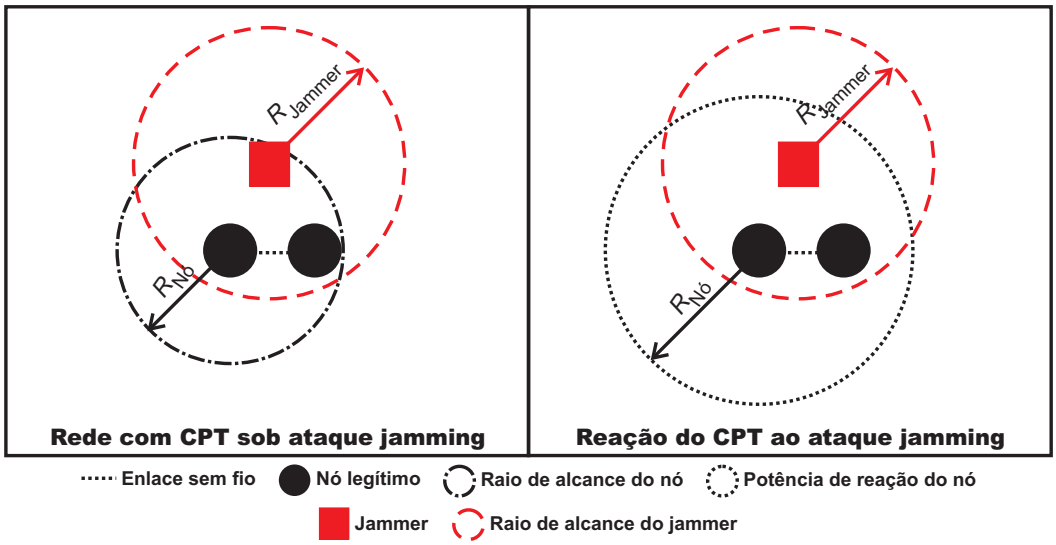

Figura 3.5: Reação do controle de potência de transmissão ao ataque *jamming* - referência própria

a semente do salto, a qual é negociada pelos nós no início da transmissão. A partir da semente, o par transmissor/receptor consegue saltar para um mesmo canal de operação do rádio e se comunicar. A Figura 3.6 ilustra a comunicação de um enlace sem fio que emprega um protocolo de estabelecimento de conexão de quatro vias, como executado pela função DCF do padrão IEEE 802.11. Na comunicação sem salto de frequência, como o *jammer* cria interferências no canal, existe uma grande probabilidade do atacante causar colisão no quadro durante a recepção, fazendo com que o quadro seja descartado e necessite ser retransmitido. Uma vez que os nós legítimos, os quais estão dentro do raio de alcance do *jammer*, detectem a ocorrência do ataque *jamming*, eles empregam a comunicação com salto de frequência reativo.

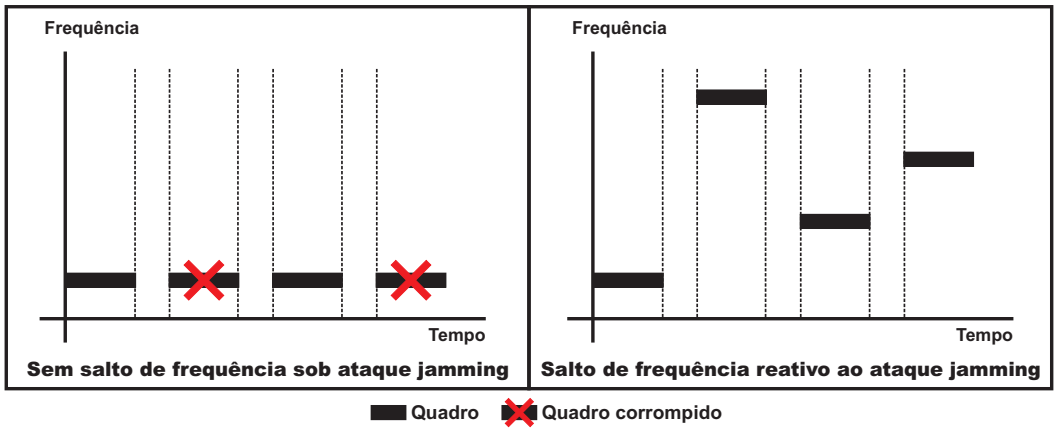

Figura 3.6: Reação com salto de frequência reativo ao ataque *jamming* - referência própria

Contudo, a abordagem tradicional possui o problema relacionado à necessidade da troca da semente de salto [56]. Como a semente é transmitida de forma aberta pelo par transmissor/receptor através do meio de transmissão sem fio, o *jammer* também saberá a semente e continuará causando impacto na rede. Para mitigar esse problema, os nós podem empregar as saídas do algoritmo dDCA como sementes para realizar a comunicação com salto de frequência reativo.

Com o intuito de realizar o salto para um mesmo canal sem uma troca pré-estabelecida da semente, os nós legítimos podem considerar como semente uma ou as duas saídas do algoritmo dDCA. A partir da reciprocidade na quantificação das saídas calculadas pelos nós, isto é, os valores das saídas $MCAV$ e K convirjam para os mesmos valores, cada nó modificará da mesma maneira o canal de operação do seu rádio. Dessa forma, os nós continuarão se comunicando mesmo sob a influência do ataque *jamming* no meio de transmissão sem fio, tolerando o ataque e garantindo a sobrevivência da rede.

A fim de realizar a reação global, é possível citar como exemplos para contornar a área de atuação do *jammer* a modificação da rota de um tráfego e o emprego do roteamento em múltiplos caminhos [54, 55]. A modificação da rota é possível caso o protocolo de roteamento seja consciente sobre o ataque na rede. Para isso, o protocolo de roteamento pode considerar como métricas de roteamento a quantificação do sistema DANTE, realizada pelas saídas $MCAV$ e K do módulo de detecção bio-inspirada.

3.3 Resumo

Este capítulo apresentou **DANTE**, um sistema de detecção de ataques *jamming* para MANETs. O sistema é inspirado no funcionamento do sistema imunológico humano, sendo totalmente distribuído e auto-organizável. Ele é composto por três módulos: coleta e medições, detecção bio-inspirada e resposta ao ataque *jamming*.

Os nós que compõem a rede possuem os módulos da arquitetura do sistema DANTE. O módulo de coleta e medições captura os quadros que sofreram colisão da camada de enlace e calcula valores para as medições estatísticas empregadas pelo sistema. O módulo de detecção bio-inspirada emprega o algoritmo dDCA para quantificar e determinar a

ocorrência dos ataques *jamming* na rede. Por fim, o módulo de resposta ao ataque *jamming* implementa mecanismos de reação que são ativados de acordo com os resultados da detecção e da quantificação.

CAPÍTULO 4

AVALIAÇÃO E DISCUSSÕES

Este capítulo apresenta as avaliações de desempenho para detecção de ataques *jamming* do sistema DANTE. A Seção 4.1 apresenta o ambiente de desenvolvimento empregado na avaliação do sistema diante dos ataques *jamming*. A Seção 4.2 exibe os modelos de ataques *jamming* usados na avaliação. A Seção 4.3 expõe os cenários e os parâmetros usados nas simulações. A Seção 4.4 especifica as métricas consideradas para avaliar o desempenho do sistema. A Seção 4.5 apresenta a análise do sistema DANTE considerando um cenário onde o *jammer* é vizinho dos nós origem e destino e a comparação dos sistemas de detecção de ataques *jamming* DANTE e CLADE nesse cenário.

4.1 Ambiente de desenvolvimento

O simulador de redes *Network Simulator* (NS) versão 2.31 foi utilizado para avaliar o desempenho do sistema DANTE. O NS2 é um simulador de redes sequencial de eventos discretos, controlado por um escalonador de eventos. O escalonador mantém uma lista de eventos ordenada pelo *timestamp* dos eventos, verifica o evento com o menor *timestamp* da lista e o executa. O evento realiza uma atividade e possivelmente adiciona outros eventos na lista de eventos. Depois da execução da atividade pelo evento, o escalonador retorna o controle do simulador e executa o próximo evento.

O simulador NS2 é escrito na linguagem C++ e emprega um interpretador OTcl. O simulador considera duas linguagens devido a duas necessidades. A primeira requer a implementação de protocolos e algoritmos que possam manipular de forma eficiente *bytes* e pacotes. Já a segunda requer a variação de parâmetros de configuração, como modificação da topologia, padrões de tráfego, etc.

O simulador NS2 implementa as partes básicas do padrão IEEE 802.11 através da linguagem C++. Tais partes básicas são compostas pelas camadas MAC, a qual emprega a

função DCF através do mecanismo CSMA/CA, e física, que provê uma abstração do meio de transmissão sem fio. A implementação dessas duas camadas considera funções básicas tais como, sensibilidade de ocupação do meio, transmissão e recebimento de pacotes, e um modelo básico de sinalização de rádio.

A sinalização de rádio é representada através da potência de transmissão usada pelos nós na transferência de pacotes. A força de sinal no nó receptor determina se um pacote foi recebido corretamente ou não. Para isso, são consideradas constantes pré-definidas para comparar a potência de recepção de um pacote. No entanto, essa forma de verificação de recebimento não condiz ao observado no mundo real. A fim de resolver esse problema, considerou-se o módulo dei80211mr [85].

O módulo denominado dei80211mr foi aplicado para prover um modelo mais realístico de recepção e transmissão de pacotes das camadas física e de enlace [85]. Esse módulo modela a taxa de erros de pacotes e verifica se um quadro foi recebido corretamente pela camada de enlace calculando a relação interferência sinal ruído, definida pela força de sinal recebido, o ruído térmico do meio e a interferência gerada pelos outros nós. A interferência é calculada de acordo com um modelo Gaussiano que checa por transmissões simultâneas nos nós receptores. O ruído térmico considerado pelo módulo é constante por padrão.

4.2 Ataques *jamming* considerados nas avaliações

Esta seção exibe os ataques *jamming* considerados nas avaliações. Como explicado no Capítulo 2, os ataques *jamming* podem ser divididos em ativos e intermitentes. Enquanto um ataque *jamming* ativo ocupa de maneira constante o meio de transmissão sem fio, os ataques *jamming* intermitentes ocupam o meio sem fio de forma alternada. Os modelos de ataques *jamming* empregados para avaliar o desempenho do sistema DANTE foram o deceptivo, o aleatório e o reativo.

O ataque *jamming* deceptivo foi considerado devido à forma como é implementada a camada física do módulo dei80211mr. O módulo implementa a transmissão de pacotes ao invés de empregar a transmissão bit a bit. Por não empregar a transmissão bit a bit,

torna-se impraticável a utilização de um outro modelo de ataque *jamming* ativo, o ataque *jamming* constante.

O ataque *jamming* aleatório considera dois períodos de tempo que seguem uma distribuição uniforme: um de inatividade e um de atividade. No período de inatividade, cujo *jammer* não realiza o ataque, o tempo varia entre 1 e 8 segundos. No período de atividade, cujo *jammer* ocupa o meio sem fio, o tempo varia entre 1 e 5 segundos. Os valores escolhidos para os períodos de atividade e inatividade, observados em [51], representam uma forma balanceada do ataque *jamming* aleatório.

Para avaliar o ataque *jamming* reativo, foi considerada a instância reativa ao quadros de dados. Nessa instância o *jammer* cria interferência na recepção dos quadros ACK. O ataque *jamming* reativo ao quadro de dados apresenta maior impacto na rede a um baixo consumo de energia do *jammer* [40, 41].

4.3 Cenários de avaliação

Para avaliar o desempenho do sistema DANTE são considerados dois tipos diferentes de cenários estáticos. A Figura 4.1 ilustra esses cenários compostos por três nós, os dois nós legítimos **A** e **B**, e o *jammer* **J**. A Figura 4.1(a) apresenta o **cenário 1** considerado por Xu et al. [38], no qual os nós são vizinhos entre si. A distância entre os nós é a mesma, isto é, a distância do nó **A** para o nó **B** ($d(A, B)$) é de dois metros, a distância $d(A, J)$ é de dois metros e a distância $d(B, J)$ é de dois metros. A Figura 4.1(b) ilustra o **cenário 2** empregado por Zhang et al. [41]. A distância do nó **J** para o nó **A** ($d(J, A)$) é de 95 metros e a distância $d(A, B)$ é de 105 metros. O *jammer* **J** está mais próximo do nó **A** que o nó **B** para assegurar que a potência de recepção do sinal do atacante seja maior que a potência de recepção de **B**. Por apresentar resultados semelhantes àqueles encontrados no cenário 1, as análises do cenário 2 encontram-se no Apêndice A.

A Tabela 4.1 sintetiza os parâmetros usados nas simulações. Cada simulação ocorre em um tempo de 300 segundos. Tanto os nós legítimos quanto o *jammer* possuem somente um rádio de comunicação sem fio. Tal rádio emprega o padrão IEEE 802.11b, juntamente com a função DCF *(Distributed Coordination Function)*, que possui os quadros de controle RTS

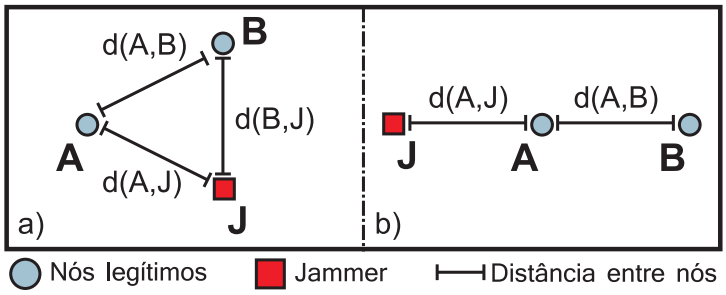

Figura 4.1: Cenários de simulação - referência própria

e CTS habilitados. O rádio opera na frequência de 2.4 GHz com potência de transmissão máxima de 200 mWatts, tendo um raio de alcance de decodificação de quadros menor que 200 metros, devido ao ruído térmico de -105 dBm. Além disso, o rádio utiliza uma taxa de transferência de dados nominal de 11 Mbps e uma taxa de transferência de quadros de controle nominal de 1 Mbps. Os nós legítimos se comunicam empregando um tráfego do tipo UDP com taxa de bits constante *(CBR - Constant Bit Rate)* de 1024 Kbps. Esse tráfego é iniciado com 2 segundos de simulação e finalizado com 250 segundos. Os *jammers* atuam sob a rede durante um período de tempo entre 5 e 100 segundos.

Parâmetro	**Valor**
Número de nós	3
Tempo de simulação	300 segundos
Área	500 metros x 500 metros
Fluxo de dados utilizado	1024 Kbps (CBR/Pacotes UDP)
Tamanho do pacote de dados	512 bytes
Início e fim da transmissão do fluxo de dados	2 e 250 segundos
Padrão MAC	IEEE 802.11b DCF
Transferência de dados na camada de enlace	11 Mbps
Transferência de quadros de controle	1 Mbps
Potência de transmissão máxima do rádio	200 mWatts
Ruído térmico	-105 dBm
Início e término dos ataques	5 e 100 segundos

Tabela 4.1: Parâmetros de simulação dos cenários

A Tabela 4.2 resume os parâmetros empregados no sistema DANTE. O sistema realiza a detecção a cada 1 segundo, sendo que a cada 0.01 segundo o sistema calcula novos valores para as medições. Esses valores empíricos são empregados para tentar assegurar a eficiência do sistema. Além disso, durante as simulações, foram variados o número de agentes artificiais e os multiplicadores de informações.

Parâmetro	Valor
Período de cálculo de medições	0.01 segundo
Número de agentes artificiais	1, 5, 10, 25, 50 e 100
Multiplicadores de informações	1, 5, 10, 25 e 50
Peso de normalidade	2
Peso de anormalidade	1

Tabela 4.2: Parâmetros de simulação do sistema DANTE

O número de agentes artificiais considerado na avaliação é 1, 5, 10, 25, 50 e 100, como empregado por Greensmith e Aicklein [78]. Os autores enfatizam que ocorre maior variação nos resultados quando a quantidade de agentes varia entre 1 e 100. O número de multiplicadores de informações empregado nas simulações é 1, 5, 10, 25 e 50, como utilizado por Manzoor et al. [80]. Apesar desses autores empregarem até 100 multiplicadores de informações, foi observado que a eficácia do algoritmo dDCA não sofre variação quando o número de multiplicadores varia entre 50 e 100. Os valores dos pesos de normalidade e anormalidade são 2 e 1, como considerado em [78]. Uma possível explicação para o peso de normalidade ser maior que o peso de anormalidade é para evitar que o sistema não detecte de forma equivocada o mau funcionamento da rede como sendo um ataque *jamming*, o que acarretaria no aumento do número de falsos-negativos. As variações dos parâmetros são consideradas para demonstrar a escalabilidade do sistema. Para cada variação foram realizadas 35 simulações, indicando um intervalo de confiança de 95%.

4.4 Métricas de desempenho

A fim de avaliar o sistema DANTE foram empregadas as métricas de desempenho denominadas acurácia e precisão [86], e também a quantificação do sistema diante dos ataques *jamming* através das saídas MCAV (*Mature Context Antigen Value*) e K [78], as quais são apresentadas no Capítulo 3.

- **Acurácia**: a medição de um sistema pode ser considerada válida se o sistema possui altos valores para a acurácia e precisão [86]. A acurácia indica a exatidão dos resultados das medições, representando a confiabilidade daquela estimativa ou valor. A Equação 4.1 calcula a acurácia do sistema DANTE empregado pelos nós legítimos,

na qual $\sum_i vp$ representa o somatório do número de verdadeiros-positivos, $\sum_i vn$ indica o somatório do número de verdadeiros-negativos, $\sum_i fp$ denota o somatório do número de falsos-positivos, $\sum_i fn$ representa o somatório do número de falsos-negativos e i o número de nós legítimos da rede. A acurácia está compreendida entre os valores 0% e 100%, sendo que os valores próximos de 100% denotam uma maior acurácia do sistema.

$$Acuracia = \frac{\sum_i vp + \sum_i vn}{\sum_i vp + \sum_i fp + \sum_i vn + \sum_i fn} \tag{4.1}$$

- **Precisão**: um sistema ao possuir alta exatidão não significa que ele também possua alta precisão e vice-versa. A precisão é definida como a proporção dos verdadeiros-positivos contra todos os resultados positivos, que incluem os verdadeiros-positivos e os falsos-positivos. A Equação 4.2 calcula a precisão do sistema DANTE empregado pelos nós legítimos. A precisão está contida entre os valores 0 e 100%, sendo que os valores próximos de 100% denotam uma maior precisão do sistema.

$$Precisao = \frac{\sum_i vp}{\sum_i vp + \sum_i fp} \tag{4.2}$$

- **MCAV**: representa a proporção de informações que foram examinadas pelos agentes sob um contexto anômalo. Essa saída consiste da taxa do somatório do número de informações pelos agentes artificiais que tiveram seu tempo de vida extinto dividido pelo número total de informações examinadas pelos agentes. A saída MCAV retorna valores entre 0 e 1. A probabilidade das informações serem anômalas aumenta conforme esse valor tende a 1.

- **K**: denota os valores de anomalia reais e auxilia na medição da variação dos processos normais, como o congestionamento na rede, e anômalos, como a interferência criada por *jammers*. Esta saída é empregada devido à saída MCAV não demonstrar a grandeza da diferença entre os valores positivos e negativos da anomalia observada por um agente artificial. A saída K consiste dos valores de anomalia dos agentes

dividido pelo somatório do número de informações examinadas pelo agente.

4.5 Cenário 1: *Jammer* vizinho dos nós origem e destino

Nesta seção são apresentadas as análises dos resultados das simulações considerando o cenário 1. Esse cenário representa aquele ilustrado na Figura 4.1(a). Esta seção é dividida em duas partes. A primeira parte tem como objetivo analisar o desempenho do sistema DANTE e a quantificação dos ataques através das métricas MCAV e K no cenário 1. Além disso, são avaliados os parâmetros do sistema DANTE a fim de escolher aqueles que possuem o melhor desempenho para serem comparados ao sistema CLADE. A segunda parte realiza uma análise comparativa do desempenho dos sistemas DANTE e CLADE diante dos ataques *jamming* no cenário 1.

4.5.1 Análise inicial do sistema DANTE

Ataque *jamming* deceptivo

A Figura 4.2 ilustra a acurácia do sistema DANTE. O sistema obteve acurácia constante de 100% ao empregar qualquer número de agentes artificiais e independente do número de multiplicadores de informações empregado. A Figura 4.3 ilustra a precisão do sistema DANTE, o qual obteve precisão constante de 100% ao considerar qualquer número de agentes artificiais e independente do número de multiplicadores de informações utilizado. Como os nós legítimos sempre encontraram o meio de transmissão sem fio ocupado, em decorrência do ataque realizado pelo *jammer*, a comunicação entre os nós **A** e **B** deixou de ocorrer. Logo, os valores das medidas de anormalidade aumentaram enquanto os valores das medidas de normalidade diminuíram, auxiliando o sistema na detecção do ataque. Além disso, a técnica de multiplicador de informações não apresentou influência na detecção do sistema.

Para apresentar os valores das saídas MCAV e K, foram fixados o número dos multiplicadores de informações e dos agentes artificiais. O número de multiplicadores de informações foi fixado em 1, por não apresentar alteração na acurácia e na precisão do

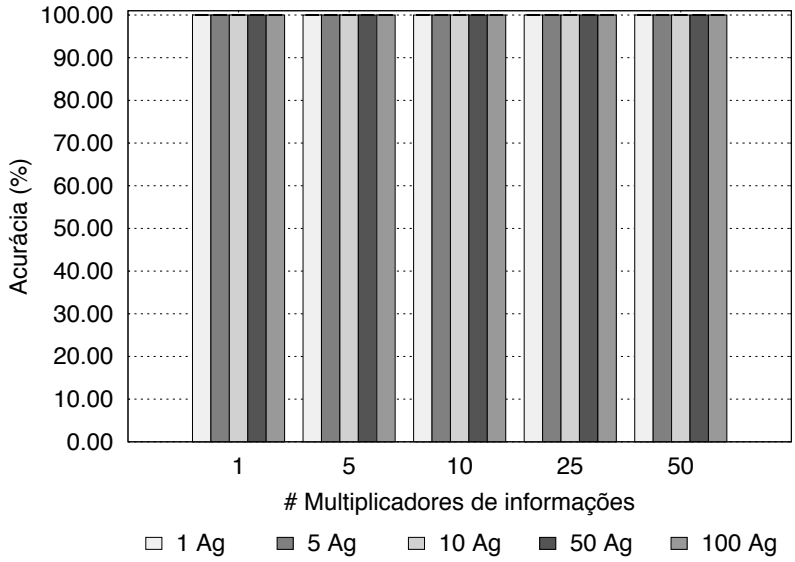

Figura 4.2: Acurácia do sistema diante do ataque *jamming* deceptivo no cenário 1

sistema. Embora a acurácia seja igual para qualquer número de agentes artificiais, os valores dos agentes foram fixados em 1 e 5 por representarem um menor custo ao sistema com relação ao número de iterações realizadas pelo algoritmo dDCA.

A Figura 4.4 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming* deceptivo. A Figura 4.4(a) mostra o resultado das saídas MCAV dos nós **A** e **B** utilizando o sistema DANTE, que emprega 1 agente artificial. Já a Figura 4.4(b) ilustra as saídas MCAV do sistema considerando 5 agentes artificiais.

Durante a execução do ataque *jamming* deceptivo, entre 5 e 100 segundos de simulação, os nós **A** e **B** empregando 1 e 5 agentes artificiais obtiveram valores para a saída MCAV que alcançam 1% em média. Isso ocorreu devido à ocupação do meio de transmissão sem fio pelo *jammer*. Logo, é possível concluir que todas as informações coletadas pelo sistema são anômalas.

A Figura 4.5 ilustra a saída K do sistema DANTE ao longo do tempo diante do ataque *jamming* deceptivo. A Figura 4.5(a) mostra o resultado das saídas K dos nós **A** e **B** utilizando o sistema DANTE, que emprega 1 agente artificial. A Figura 4.5(b) ilustra as saídas K do sistema, empregado pelos nós **A** e **B** que consideram 5 agentes artificiais.

Durante a execução do ataque *jamming* deceptivo, os nós **A** e **B** empregando 1 agente artificial obtiveram valores para o K que alcançam 0.30 em média. Quando o número

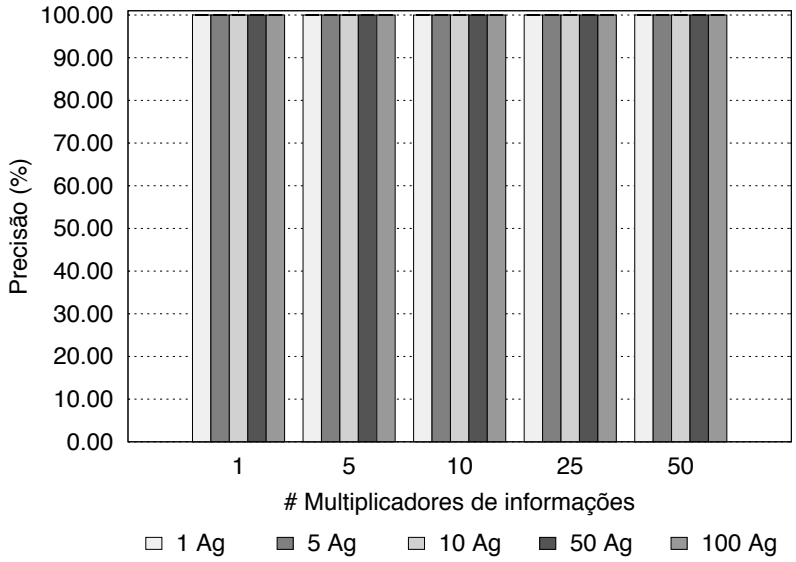

Figura 4.3: Precisão do sistema diante do ataque *jamming* deceptivo no cenário 1

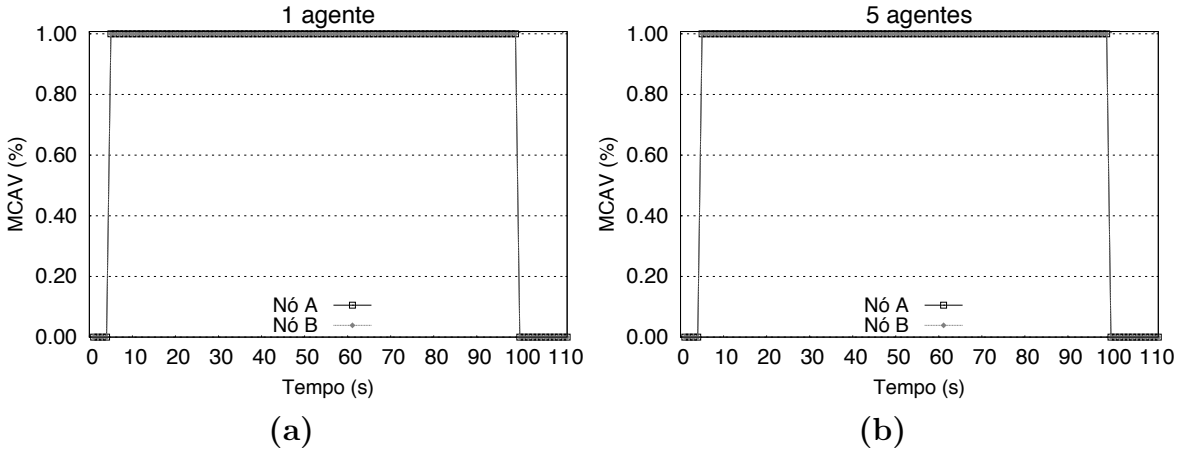

Figura 4.4: Saída MCAV do sistema diante do ataque *jamming* deceptivo no cenário 1

de agentes é aumentado para 5, os nós **A** e **B** alcançaram em média o valor 1.52. Essa saída apresentou valores que aumentam de forma proporcional à quantidade de agentes artificiais empregados pelo sistema. Isso ocorre em consequência da saída K ser calculada a partir do somatório dos valores de anomalia dos agentes artificiais.

Ataque *jamming* aleatório

A Figura 4.6 ilustra a acurácia do sistema DANTE, o qual é empregado pelos nós legítimos. O sistema obteve acurácia de 81% ao empregar 1 agente artificial e independente do número de multiplicadores de informações considerado. Quando o número de agentes variou em 5, 10, 50 ou 100, o sistema obteve valores para a acurácia que na média al-

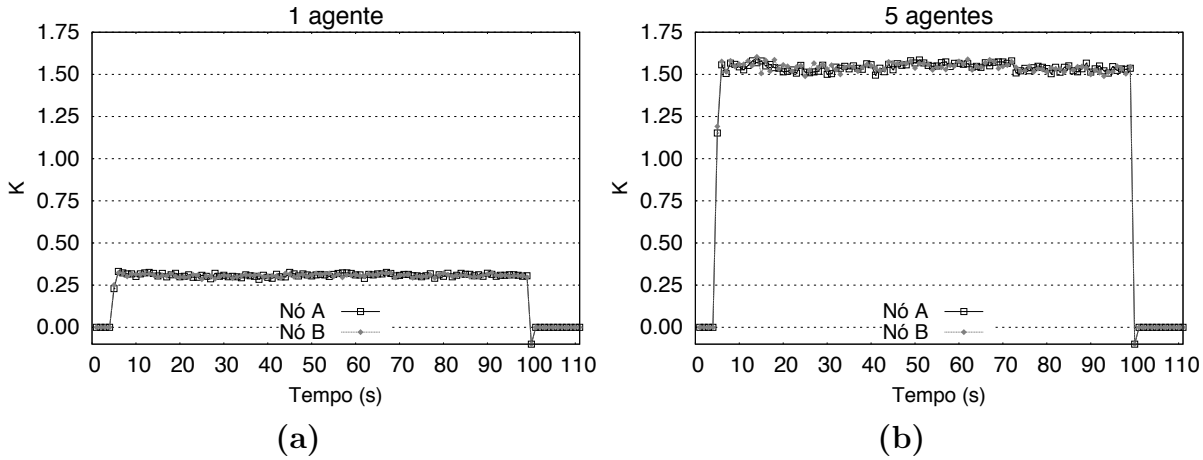

Figura 4.5: Saída K do sistema diante do ataque *jamming* deceptivo no cenário 1

cançaram 82%. A Figura 4.7 ilustra a precisão do sistema DANTE. O sistema obteve valores para a precisão que alcançaram na média 42%, considerando 1 agente artificial e independente do número de multiplicadores de informações utilizado. A partir do momento que o número de agentes variou em 5, 10, 50 ou 100, o sistema obteve valores para a precisão que na média alcançaram 44%. O sistema DANTE obteve baixos valores para a acurácia e para a precisão ao tentar detectar o ataque *jamming* aleatório. Isso ocorreu devido ao sistema tratar de forma inadequada as colisões criadas pela aleatoriedade do ataque. Uma explicação para esse fato está na sensibilidade da saída MCAV.

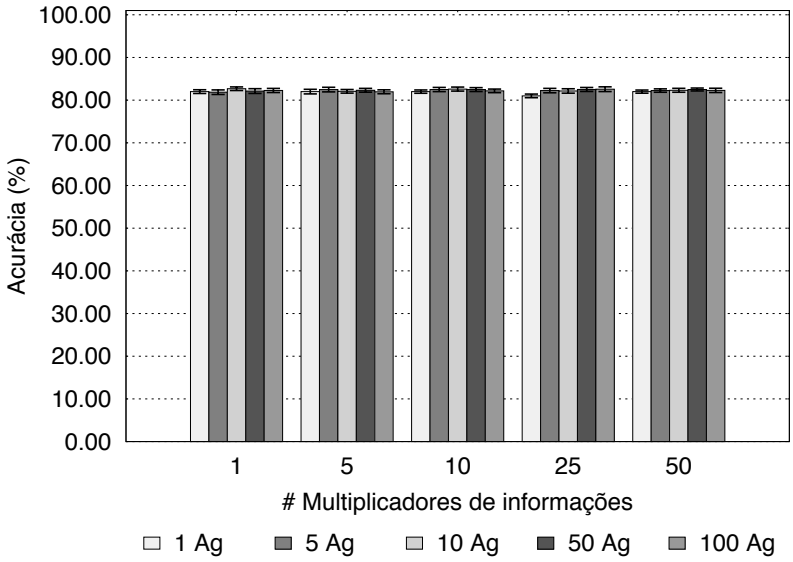

Figura 4.6: Acurácia do sistema diante do ataque *jamming* aleatório no cenário 1

Para apresentar os valores das saídas MCAV e K, foram fixados o número dos mul-

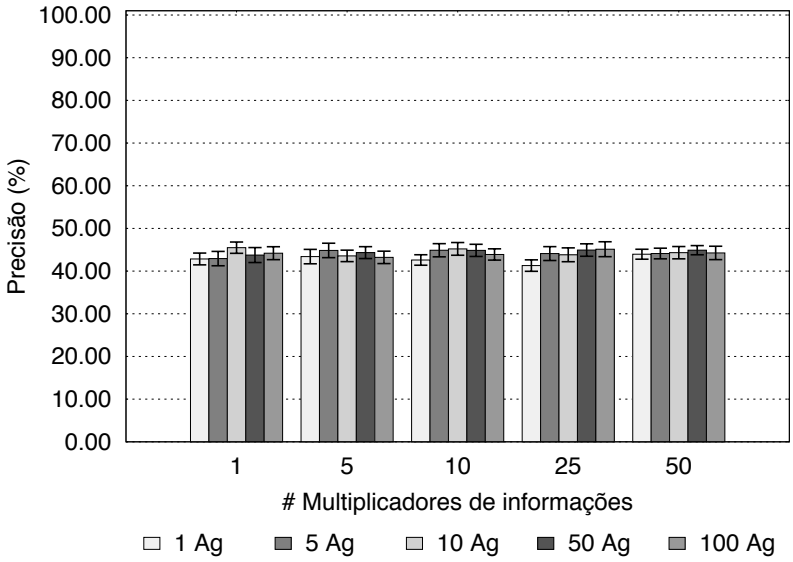

Figura 4.7: Precisão do sistema diante do ataque *jamming* aleatório no cenário 1

tiplicadores de informações e dos agentes artificiais. O número de multiplicadores de informações foi fixado em 1, por não apresentar alteração na acurácia e precisão do sistema. Os valores dos agentes artificiais foram fixados em 1 e 5, por apresentarem pouca alteração na acurácia do sistema.

A Figura 4.8 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming* aleatório. A Figura 4.8(a) mostra as saídas MCAV dos nós **A** e **B** utilizando o sistema DANTE, que emprega 1 agente artificial. Já a Figura 4.8(b) ilustra as saídas MCAV do sistema considerando 5 agentes artificiais.

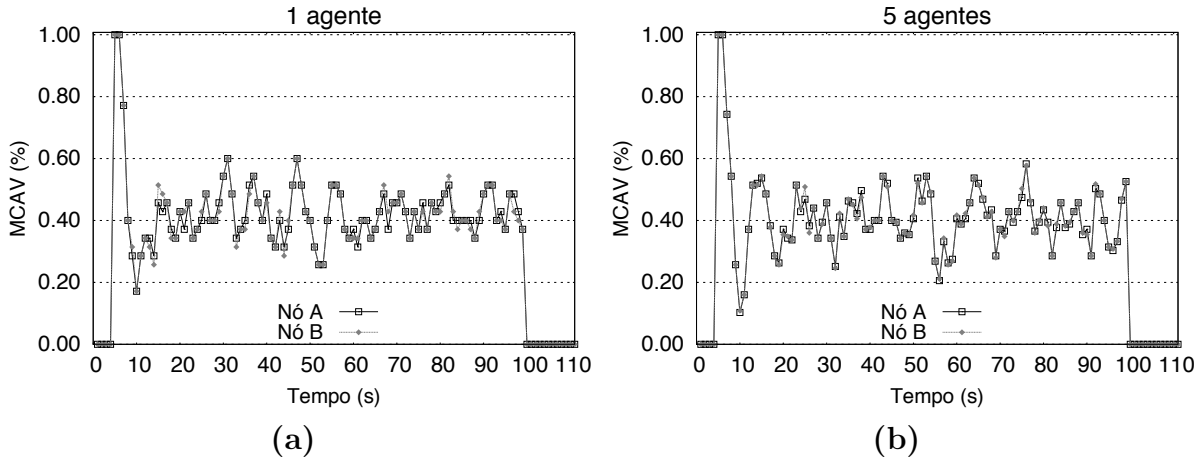

Figura 4.8: Saída MCAV do sistema diante do ataque *jamming* aleatório no cenário 1

Durante a execução do ataque *jamming*, entre 5 e 100 segundos de simulação, os nós

A e **B** empregando o sistema com 1 agente artificial obtiveram valores entre 0.18% e 0.60% em média, respectivamente. Ao considerar 5 agentes, o sistema utilizado pelos nós legítimos **A** e **B** obteve valores para o MCAV entre 0.14% e 0.59% em média, respectivamente. A redução tanto na acurácia quanto na precisão da detecção pode ser explicada pelo uso da saída MCAV para detectar o ataque *jamming* aleatório. Como nesse ataque o *jammer* alterna os períodos de atividade e inatividade, o comportamento esperado para a saída MCAV era que em alguns momentos essa saída apresentasse o valor 0%, demonstrando que não ocorria qualquer anomalia na rede. Contudo, é possível observar que nos momentos em que o *jammer* não estava atuando na rede a saída MCAV se manteve acima de 0%.

A Figura 4.9 ilustra a saída K do sistema DANTE ao longo do tempo diante do ataque *jamming* aleatório. A Figura 4.9(a) mostra as saídas K do sistema que considera 1 agente artificial e é empregado pelos nós **A** e **B**. Já a Figura 4.8(b) ilustra as saídas MCAV do sistema usando 5 agentes artificiais.

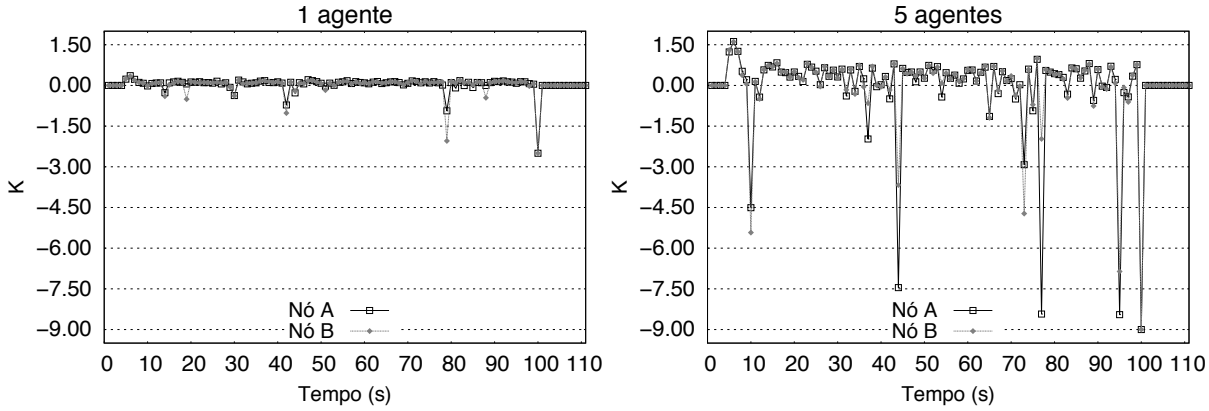

Figura 4.9: Saída K do sistema DANTE diante do ataque *jamming* aleatório no cenário 1

Durante a execução do ataque *jamming*, entre 5 e 100 segundos de simulação, o sistema utilizando 1 agente artificial obteve valores para a saída K que variam entre -2.8 e 0.2 em média, tanto para o nó **A** quanto para o nó **B**. Ao empregar 5 agentes, o sistema obteve valores entre -9 e 1.5 em média. A saída K mostrou maior sensibilidade ao ataque que a saída MCAV. Os valores da saída K apresentaram alternância entre positivo e negativo, indicando a anomalia presenciada no meio de transmissão sem fio pelos agentes artificiais.

Ataque *jamming* reativo

As Figuras 4.10 e 4.11 ilustram a acurácia e a precisão do sistema DANTE empregado pelos nós legítimos. O sistema ao empregar 1 e 5 agentes artificiais obteve valores médios para acurácia em torno de 89% e 99%, respectivamente, e para precisão, em torno de 68% e 99%, independente do número de multiplicadores de informações utilizado. Quando o número de agentes variou em 10, 50 ou 100, o sistema alcançou a acurácia e a precisão de 100%, independente do número de multiplicadores de informações considerado.

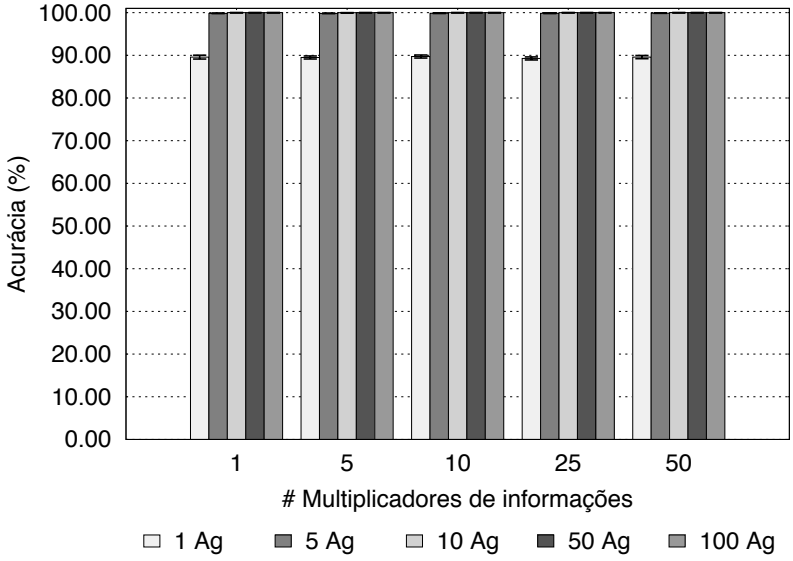

Figura 4.10: Acurácia do sistema diante do ataque *jamming* reativo no cenário 1

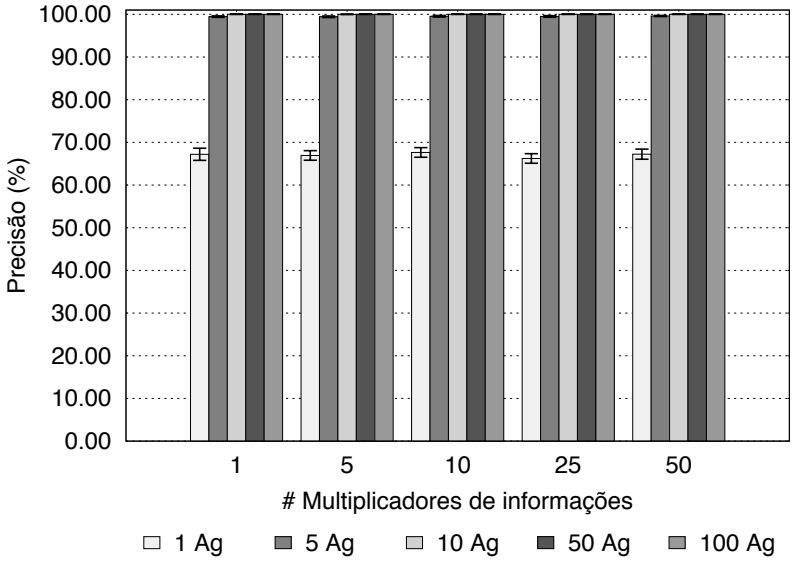

Figura 4.11: Precisão do sistema diante do ataque *jamming* reativo no cenário 1

A fim de apresentar os valores das saídas MCAV e K, foram fixados o número dos

multiplicadores de informações e dos agentes artificiais. O número de multiplicadores de informações foi fixado em 1, por não apresentar alteração na acurácia do sistema. Já o número de agentes artificiais foi fixado em 1 e 5.

A Figura 4.12 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming* reativo. A Figura 4.12(a) exibe as saídas MCAV dos nós **A** e **B** utilizando o sistema DANTE, que emprega 1 agente artificial. Já a Figura 4.12(b) ilustra as saídas MCAV do sistema considerando 5 agentes artificiais.

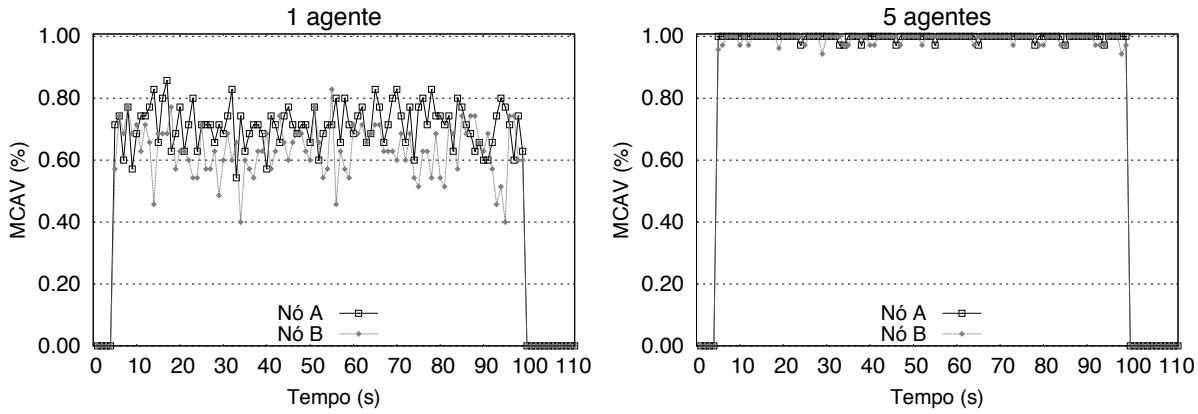

Figura 4.12: Saída MCAV do sistema diante do ataque *jamming* reativo no cenário 1

Durante a execução do ataque *jamming*, o sistema com 1 agente artificial obteve em média valores para a saída MCAV entre 0.55% e 0.85% quando empregado pelo nó **A**, e valores entre 0.40% e 0.81% quando utilizado pelo nó **B**. Ao aumentar o número de agentes para 5, os nós **A** e **B** obtiveram valores próximos de 1% em média. A estabilidade da saída MCAV é dependente do número de agentes. Enquanto a saída MCAV sofreu grande variação com 1 agente artificial, ela apresentou maior estabilidade quando o número de agentes foi alterado para 5.

A Figura 4.13 ilustra a saída K do sistema DANTE ao longo do tempo diante do ataque *jamming* reativo. A Figura 4.13(a) exibe as saídas K dos nós **A** e **B** considerando o sistema DANTE, que utiliza 1 agente artificial. Já a Figura 4.13(b) ilustra as saídas K do sistema considerando 5 agentes artificiais.

Durante o ataque *jamming*, entre 5 e 100 segundos de simulação, o sistema com 1 agente artificial obteve em média valores entre -0.20 e 0.12 quando empregado pelo nó **A**,

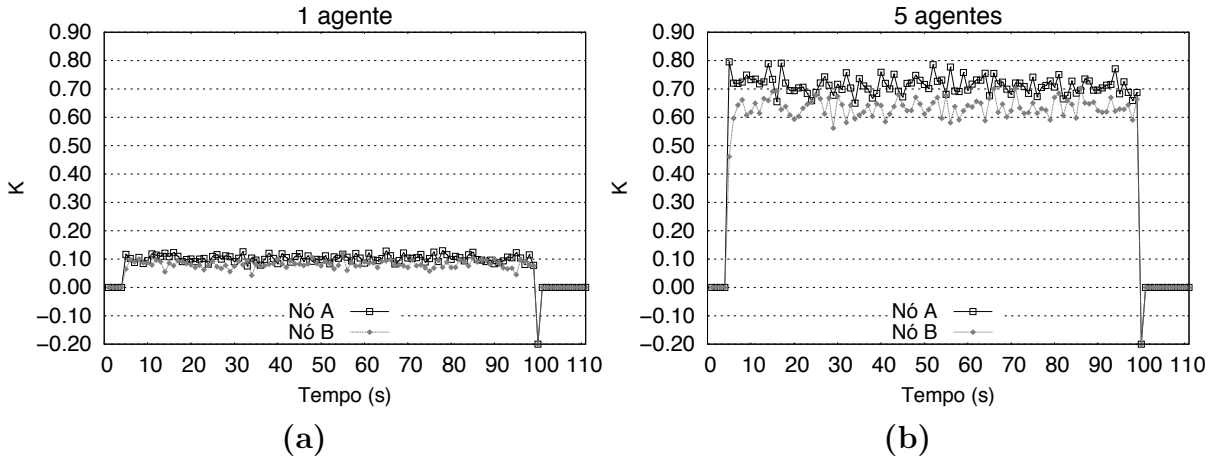

Figura 4.13: Saída K do sistema diante do ataque *jamming* reativo no cenário 1

e valores entre -0.20 e 0.10 quando utilizado pelo nó **B**. Ao aumentar o número de agentes para 5, o nó **A** obteve valores entre -0.20 e 0.80, e o nó **B**, valores entre -0.20 e 0.70. Como mencionado anteriormente, a saída K apresentou valores que aumentam de forma proporcional ao aumento do número de agentes, por ser calculada a partir do somatório da anomalia presenciada pelos agentes artificiais.

Síntese da análise inicial do sistema DANTE

A Tabela 4.3 sintetiza os melhores resultados para a acurácia e a precisão obtidos pelo sistema DANTE diante dos ataques *jamming* no cenário 1. O número de iterações do algoritmo dDCA, empregado pelo sistema DANTE, é diretamente proporcional ao número de agentes artificiais e multiplicadores informações. Portanto, é interessante escolher valores para esses dois parâmetros que reduzam o número de iterações e que, de forma simultânea, consigam um alto desempenho. A partir dos resultados demonstrados, conclui-se que o sistema DANTE consegue o melhor desempenho empregando um número de agentes artificiais e multiplicadores de informações igual a 10 e 1, respectivamente.

4.5.2 Comparação dos sistemas DANTE e CLADE

Nesta seção são apresentadas as análises da comparação dos sistemas DANTE e CLADE empregando o cenário 1. Esse cenário representa aquele ilustrado na Figura 4.1(a). Os parâmetros utilizados nas simulações são os mesmos exibidos na Tabela 4.1.

Ataque *jamming*	**Acurácia**	**Precisão**	**Número de agentes artificiais**	**Multiplicadores de informações**
Deceptivo	100%	100%	1, 5, 10, 50, 100	1, 5, 10, 25, 50
Aleatório	82%	44%	10	1, 10, 50
Reativo	100%	100%	10, 50, 100	1, 5, 10, 25, 50

Tabela 4.3: Síntese dos melhores resultados da acurácia e da precisão obtidos pelos sistemas DANTE diante dos ataques *jamming* no cenário 1

O sistema CLADE emprega três patamares de detecção estáticos e estocásticos, os quais necessitam ser escolhidos previamente. Os valores dos patamares de detecção avaliados são 0.0, 0.25, 0.50, 0.75 e aleatório. Enquanto o valor 0.25 permite que o sistema torne-se mais sensível aos ataques, o valor 0.75 torna o sistema menos sensível e propenso a erros. O valor aleatório segue uma distribuição uniforme e está compreendido entre os valores 0.0 e 0.75, a fim de garantir que os patamares não alcancem valores extremos.

A fim de comparar o sistema DANTE, foram fixados os seguintes parâmetros do sistema: número de agentes artificiais e multiplicadores de informações. A partir das análises realizadas anteriormente, concluiu-se que o sistema DANTE obtém os melhores resultados empregando um número de agentes artificiais e multiplicadores de informações igual a 10 e 1, respectivamente. Além disso, foram utilizados os mesmos valores para os pesos de normalidade e anormalidade, exibidos na Tabela 4.2.

Nesta seção também são avaliados outros valores para o patamar de detecção do sistema DANTE, o qual é comparado com o valor da saída MCAV do sistema. A avaliação de outros valores para o patamar é justificada devido ao sistema DANTE alcançado resultados relevantes considerando um valor igual a zero para o patamar de detecção. Tais valores para o patamar de detecção são os mesmos usados pelo sistema CLADE, isto é, 0.0, 0.25, 0.50, 0.75 e aleatório.

Além disso, também é avaliado o período necessário para os sistemas coletarem os pacotes do meio de transmissão sem fio. Isso é realizado com o intuito de averiguar a latência necessária para os sistemas detectarem os *jammers* no meio de transmissão sem fio. Os valores estocásticos dos períodos de coleta são 0.25, 0.50, 0.75 e 1 segundo. As métricas consideradas na comparação são a acurácia e a precisão, explicadas na Seção 4.4.

Ataque *jamming* deceptivo

As Figuras 4.14 e 4.15 ilustram a acurácia e precisão obtidas pelos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo. O sistema DANTE possui um desempenho superior ao sistema CLADE. Apesar da redução do período de captura dos quadros afetar o desempenho do sistema DANTE, em períodos de coleta maiores como de 0.75 e 1 segundo, esse sistema obtem a acurácia de 83% e 100%, respectivamente. A melhora de desempenho do sistema DANTE pode ser explicado através do funcionamento dos agentes artificiais. Quanto maior a quantidade de informações obtidas e verificadas pelos agentes, maior é a probabilidade de acerto da identificação da anomalia.

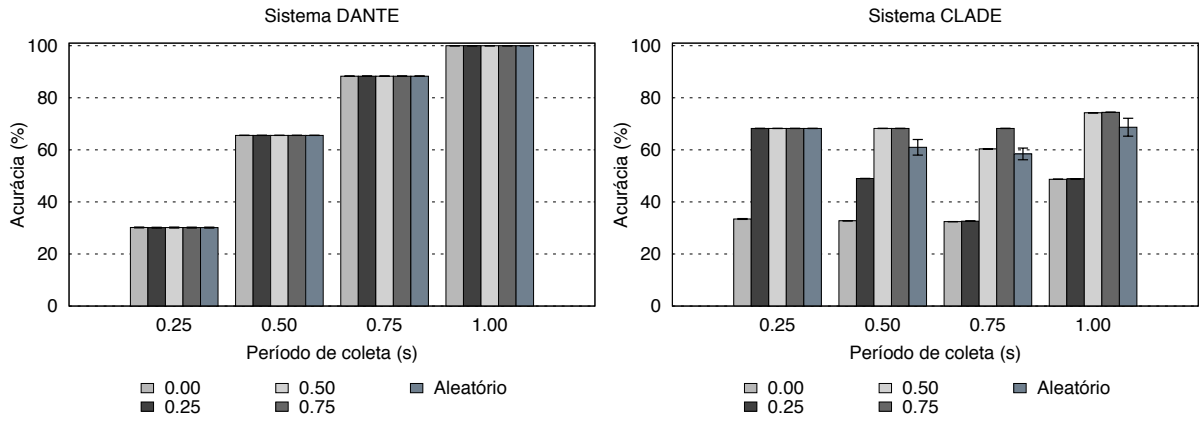

Figura 4.14: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo no cenário 1

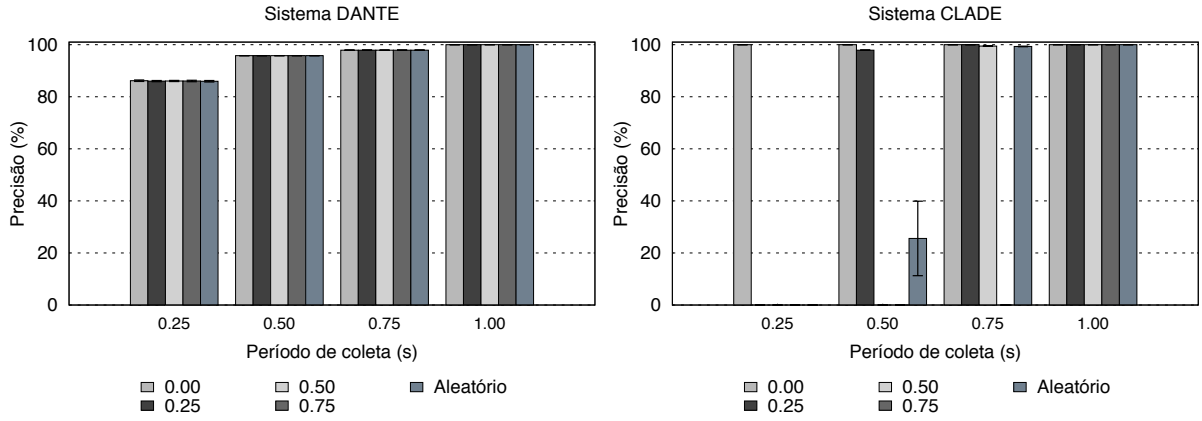

Figura 4.15: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo no cenário 1

Relativamente ao sistema CLADE, ele obteve um pior desempenho que o sistema DANTE diante do ataque *jamming* deceptivo. A explicação para esse fato pode ser

baseada nas medições empregadas pelo sistema. O seu desempenho é reduzido de maneira drástica uma vez que as medições indiquem de forma equivocada que ocorre no meio de transmissão sem fio um ataque ou um tráfego de dados. Tal fato acarretaria no aumento de falsos-positivos e falsos-negativos, o qual é refletido nas métricas acurácia e precisão. Além disso, no sistema CLADE existe a necessidade de encontrar um ponto de equilíbrio o qual permita que tanto a acurácia quanto a precisão alcancem resultados relevantes. Esse ponto de equilíbrio é encontrado quando o sistema CLADE emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50.

Ataque *jamming* aleatório

As Figuras 4.16 e 4.17 ilustram a acurácia e a precisão obtidas pelos sistemas DANTE e CLADE diante do ataque *jamming* aleatório. Da mesma forma como avaliado no ataque *jamming* deceptivo, o sistema DANTE tem o seu desempenho melhorado de acordo com o aumento do período de coleta. Isso ocorre devido à necessidade dos agentes artificiais coletarem uma certa quantidade de quadros que sofreram colisão. Quanto maior o número de colisões capturadas, maior é a probabilidade do sistema acertar a ocorrência de um ataque no meio de transmissão sem fio. Contudo, embora o sistema DANTE tenha obtido valores relevantes para acurácia, o mesmo não ocorre com a precisão. O sistema DANTE não soube lidar com a aleatoriedade do ataque, alcançando resultados pouco relevantes. A aleatoriedade do ataque teve como consequência o aumento do número de falsos-positivos produzidos pelo sistema, o que reduziu a precisão do sistema.

Como observado anteriormente, no sistema CLADE existe a necessidade de encontrar um ponto de equilíbrio o qual permita que tanto a acurácia quanto a precisão alcancem resultados relevantes. No ataque *jamming* aleatório, esse ponto de equilíbrio é encontrado quando o sistema CLADE emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50. Considerando esse ponto de equilíbrio, apesar do sistema CLADE obter um valor para a acurácia 13% menor que aquele alcançado pelo sistema DANTE, o sistema CLADE obteve um valor para a precisão 35% maior que o alcançado pelo sistema DANTE. Com base nesses resultados, é possível supor que o sistema CLADE obteve

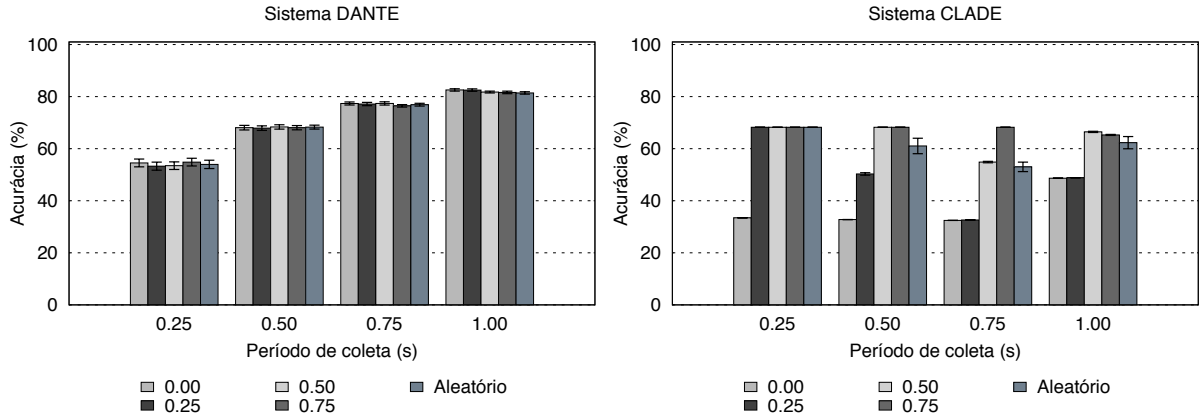

Figura 4.16: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* aleatório no cenário 1

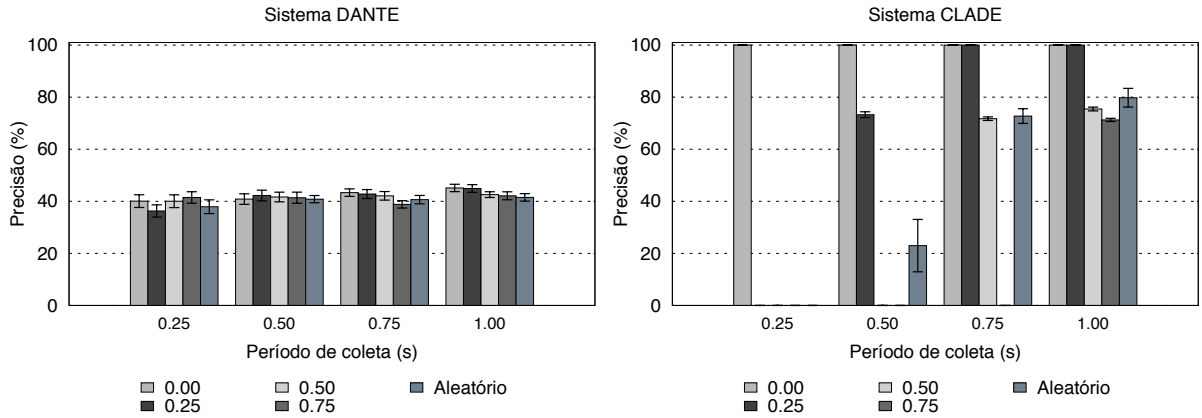

Figura 4.17: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* aleatório no cenário 1

resultados significantes tanto quanto aqueles alcançados pelos sistema DANTE.

Ataque *jamming* reativo

Como mencionado em artigos encontrados na literatura [7, 40, 41], o ataque *jamming* reativo é o mais complexo de ser detectado, sobretudo a instância que emprega colisões nos quadros ACK. Entretanto, pode-se perceber que o sistema DANTE obteve resultados relevantes na detecção do ataque *jamming* reativo. Isso é elucidado pelas Figuras 4.18 e 4.19, as quais ilustram a acurácia e a precisão alcançadas pelos sistemas DANTE e CLADE.

Da mesma forma como avaliado nos ataques *jamming* deceptivo e aleatório, o mesmo comportamento ocorre no ataque *jamming* reativo, no qual o desempenho do sistema

DANTE melhora conforme o período de coleta é aumentado. Como mencionado anteriormente, quanto maior o número de colisões capturadas, maior é a probabilidade do sistema acertar a ocorrência de um ataque na rede. O mesmo comportamento pode ser observado na métrica precisão, a qual é diretamente proporcional ao período de coleta. Ao se comparar os melhores valores da acurácia dos dois sistemas, é possível concluir que o sistema DANTE alcançou uma acurácia 28% maior que o sistema CLADE. Concomitantemente à precisão, ambos os sistemas alcançaram acurácia máxima de 100%. Além disso, a modificação do valor do patamar de detecção não alterou o desempenho do sistema DANTE.

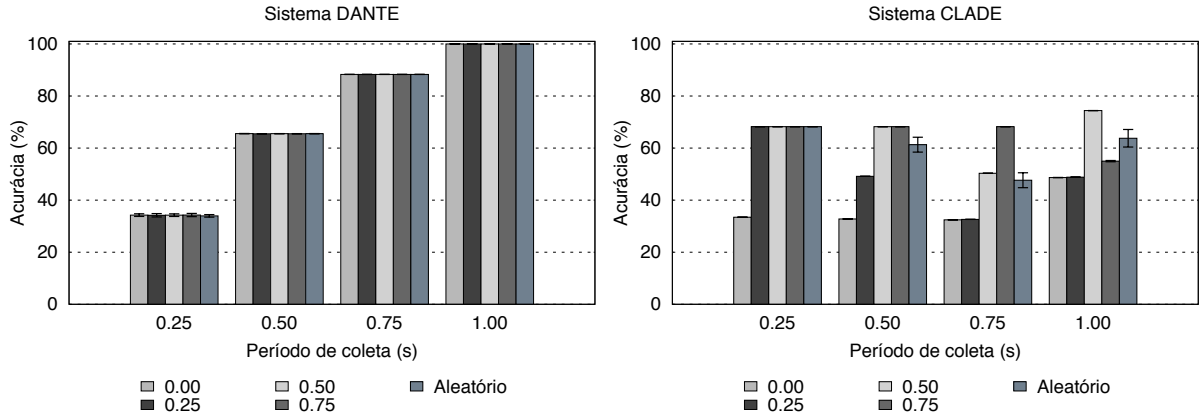

Figura 4.18: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* reativo no cenário 1

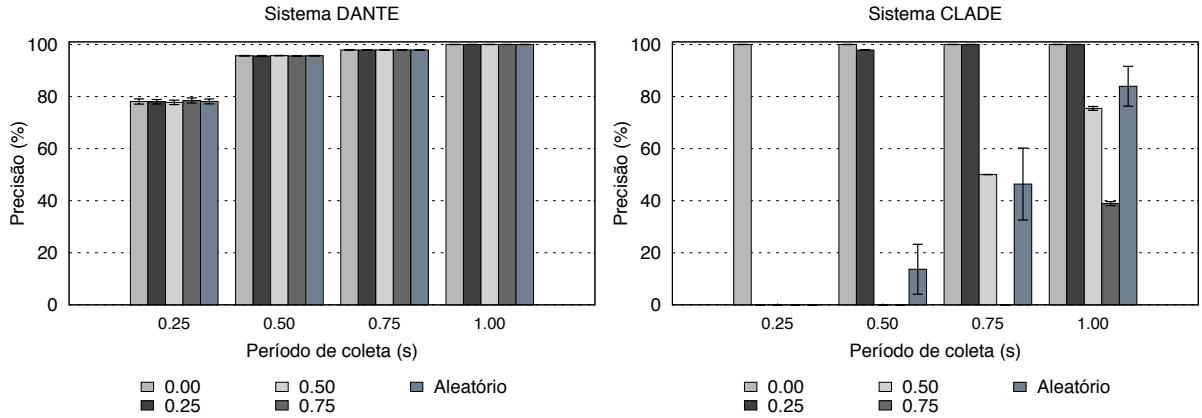

Figura 4.19: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* reativo no cenário 1

Como observado na análise dos ataques anteriores, o sistema CLADE necessita de um ponto de equilíbrio. Esse ponto permite que tanto a acurácia quanto a precisão alcancem

resultados relevantes. No ataque *jamming* reativo, esse ponto de equilíbrio é observado quando o sistema CLADE emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50. Considerando os gráficos da acurácia e da precisão nesse ponto de equilíbrio, é possível concluir que, apesar do sistema CLADE ter alcançado a precisão de 100%, o sistema não conseguiu lidar com o ataque *jamming* reativo. Isso ocorreu devido ao número de falsos-negativos obtidos pelo sistema, produzindo um impacto direto na métrica de acurácia.

Síntese da comparação dos sistemas DANTE e CLADE

A Tabela 4.4 resume os melhores resultados para a acurácia, obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming* deceptivo, aleatório e reativo. O sistema DANTE alcançou maiores resultados para a acurácia que o sistema CLADE. Enquanto no ataque *jamming* aleatório o sistema DANTE obteve a acurácia 13% maior que o sistema CLADE, nos ataques *jamming* deceptivo e reativo a diferença alcançou 28%.

Sistema	**Ataque *jamming***	**Acurácia**	**Período de coleta**	**Patamar de detecção**
DANTE	Deceptivo	100%	1 segundo	-
	Aleatório	82%	1 segundo	-
	Reativo	100%	1 segundo	-
CLADE	Deceptivo	72%	1 segundo	0.50
	Aleatório	69%	1 segundo	0.50
	Reativo	72%	1 segundo	0.50

Tabela 4.4: Síntese dos melhores resultados para a acurácia obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming*

A Tabela 4.5 sintetiza os melhores resultados para a precisão, alcançados pelos sistemas DANTE e CLADE sob os ataques *jamming* deceptivo, aleatório e reativo. Relativamente à precisão, o sistema CLADE obteve um rendimento superior aquele alcançado pelo sistema DANTE. Nos ataques *jamming* deceptivo e reativo, ambos os sistemas alcançaram 100% de precisão. Contudo, no ataque *jamming* aleatório, o sistema CLADE obteve a precisão 28% maior que o sistema DANTE.

A partir dos resultados demonstrados é possível realizar as seguintes afirmações referentes aos sistemas DANTE e CLADE. O sistema DANTE apresenta o melhor desempenho

Sistema	Ataque *jamming*	Precisão	Período de coleta	Patamar de detecção
DANTE	Deceptivo	100%	1 segundo	-
	Aleatório	44%	1 segundo	-
	Reativo	100%	1 segundo	-
CLADE	Deceptivo	100%	1 segundo	0.50
	Aleatório	72%	1 segundo	0.50
	Reativo	100%	1 segundo	0.50

Tabela 4.5: Síntese dos melhores resultados para a precisão obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming*

ao considerar o período de coleta igual a 1 segundo. A modificação do valor do patamar de detecção não altera o desempenho do sistema DANTE nos ataques *jamming* deceptivo e reativo e não existe alteração significante no desempenho desse sistema no ataque *jamming* aleatório. Em relação ao sistema CLADE, o ponto de equilíbrio é encontrado quando o sistema emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50.

Por fim, conclui-se que o sistema DANTE possui um desempenho superior ao sistema CLADE no cenário 1. O sistema DANTE obteve a precisão de 100% nos ataques *jamming* deceptivo e reativo. Além disso, o sistema DANTE alcançou os maiores resultados para a acurácia em todos os três ataques *jamming* analisados.

4.6 Resumo

Neste capítulo foi apresentada a avaliação do sistema DANTE diante dos ataques *jamming* deceptivo, aleatório e reativo. Para isso, foram considerados dois cenários. No primeiro cenário, todos os nós são vizinhos entre si, já no segundo, o *jammer* é vizinho do nó origem, que por sua vez é vizinho do nó destino. Os resultados de simulação mostraram que o sistema DANTE é eficaz ao detectar os ataques *jamming* deceptivo e reativo, através das métricas de desempenho denominadas acurácia e precisão. Para auxilar na detecção dos ataques, foi utilizada a técnica de multiplicação de informações. Entretanto, essa técnica não apresentou resultados significativos nos ataques analisados. Além disso, o sistema DANTE foi comparado a um outro sistema de detecção de ataques *jamming* encontrado na literatura, denominado CLADE.

O sistema DANTE apresentou um desempenho superior ao sistema CLADE nos dois cenários avaliados diante dos ataques *jamming*. O sistema DANTE obteve a precisão de 100% nos ataques *jamming* deceptivo e reativo. Além disso, o sistema DANTE alcançou os melhores resultados para a acurácia em todos os três ataques *jamming* analisados.

CAPÍTULO 5

CONCLUSÕES E TRABALHOS FUTUROS

A realização de uma rede móvel ad hoc robusta e segura depende da habilidade de entender os ataques e seus impactos no desempenho e segurança da rede. As restrições encontradas no ambiente ad hoc, tais como falta de infraestrutura física, recursos disponíveis limitados, e operação em um ambiente hostil, introduzem uma variedade de vulnerabilidades e criam desafios às seguranças das redes móveis ad hoc. Um grande desafio em alcançar uma rede segura é a vulnerabilidade intrínseca da comunicação das redes sem fio ao ataque *jamming*.

O atacante *jamming*, denominado *jammer*, emite ondas eletromagnéticas de forma maliciosa através do meio de transmissão sem fio. Isso é realizado para consumir os recursos da rede e causar prolongadas colisões de dados nos nós receptores. Um ataque *jamming* não necessita de *hardware* especial, pode consumir poucos recursos do *jammer*, como a energia, e pode ser implementado monitorando o meio de transmissão sem fio aberto e transmitindo ondas na mesma frequência.

Diante disso, este trabalho propôs um sistema de detecção de ataques *jamming* para redes móveis ad hoc denominado DANTE (***D****etecting j****A****mming attacks by the da****N****ger* ***T****h****E****ory*). Para detectar a atuação dos ataques *jamming* e se adaptar às mudanças na redes ad hoc, o sistema DANTE considera uma técnica bio-inspirada de aprendizado de máquina. A técnica é inspirada no funcionamento da teoria do perigo, na qual o sistema imunológico humano discerne entre o perigo e a ausência de perigo.

O sistema DANTE possui as seguintes características cujos outros sistemas de detecção de ataques jamming não possuem. O sistema evolui considerando as mudanças da rede e a adaptabilidade dos jammers. Ele emprega medições mais dinâmicas e abrangentes, as quais são sensíveis aos ataques *jamming*. O sistema considera somente um patamar de detecção e não emprega nenhuma forma de comunicação para indicar que detectou o ataque. Por fim, o sistema DANTE quantifica a importância do ataque a fim de auxiliar

os mecanismos de reação.

O sistema emprega uma arquitetura composta por três módulos, denominados coleta e medições, detecção bio-inspirada e resposta ao ataque *jamming*. O módulo de medições e informações captura as informações provenientes da camada de enlace que sofreram colisão e calcula o desempenho do meio de transmissão sem fio e dos enlaces vizinhos. O módulo de detecção bio-inspirada determina e quantifica a ocorrência do ataque *jamming* no meio de transmissão sem fio. E o módulo de resposta ao ataque *jamming* reage conforme a detecção e quantificação do ataque.

O sistema DANTE foi avaliado em dois cenários largamente empregados na literatura. Esse cenários são compostos por três nós, sendo dois nós legítimos e um nó atuando como o *jammer*. No primeiro cenário, os nós são vizinhos entre si, já no segundo, o *jammer* é vizinho de um nó legítimo que é vizinho de outro nó legítimo. Como métricas para avaliar o desempenho do sistema DANTE foram empregadas a acurácia e a precisão, e para quantificar o sistema foram utilizadas as saídas MCAV e K. As instâncias dos ataques *jamming* avaliadas foram deceptivo, aleatório e reativo. Para auxilar na detecção dos ataques, foi empregada a técnica de multiplicação de informações. Entretanto, essa técnica não apresentou resultados relevantes nos ataques analisados. Além disso, o sistema DANTE foi comparado a um outro sistema de detecção de ataques *jamming* encontrado na literatura, denominado neste trabalho como CLADE.

Os resultados de simulação mostraram que o sistema DANTE obteve acurácia e precisão máximas na detecção dos ataques *jamming* deceptivo e reativo. Como discutido, a probabilidade do sistema acertar a detecção do ataque aumenta conforme o número de agentes artificiais aumenta. No que diz respeito às saídas MCAV e K, elas apresentaram resultados condizentes com esses ataques, auxiliando o sistema na tarefa de detecção.

Em relação à análise comparativa dos sistemas, o sistema DANTE apresentou um desempenho superior ao sistema CLADE nos dois cenários avaliados diante dos ataques *jamming*. O sistema DANTE obteve a precisão de 100% nos ataques *jamming* deceptivo e reativo. Além disso, o sistema DANTE alcançou os melhores resultados para a acurácia em todos os três ataques *jamming* analisados. No entanto, o sistema DANTE não soube

lidar de forma satisfatória com o comportamento do ataque *jamming* aleatório. Isso ocorreu devido à saída MCAV ter apresentado menos sensibilidade ao ataque que a saída K. Uma forma de melhorar o desempenho do sistema DANTE diante do ataque *jamming* aleatório, seria considerar o meio de transmissão sem fio anômalo quando os valores da saída K estiverem acima de zero.

Como trabalhos futuros é possível mencionar o seguinte. A criação de uma métrica de quantificação que correlacione as saídas dos agentes artificiais com o número de colisões processadas por esses agentes. A melhoria da acurácia e da precisão do sistema DANTE diante do ataque *jamming* aleatório. O desenvolvimento de respostas aos ataques *jamming* que considerem a quantificação dos ataques. A realização de experimentos em ambientes reais.

O sistema DANTE emprega duas saídas a fim de quantificar os ataques *jamming*, a saída MCAV e a saída K. A saída MCAV indica a proporção das informações coletadas pelo sistema que são anômalas, já a saída K denota os valores de anomalia reais e auxilia na medição da variação dos processos normais. Todavia, faz-se necessário o emprego de uma métrica que permita que o sistema quantifique a anomalia em diferentes níveis. Para isso, é possível correlacionar os valores reais de anomalia observados pelos agentes artificiais com as informações capturadas pelo sistema classificadas como anômalas.

O sistema apresentou baixo desempenho sob a atuação do ataque *jamming* aleatório quando comparado aos outros ataques *jamming*. Além de empregar os valores acima de zero da saída MCAV como um indício da anomalia no meio de transmissão sem fio, deve-se também considerar a saída K. Dessa forma, as saídas seriam utilizadas de maneira híbrida como indícios de anomalia.

Este trabalho teve como foco a detecção dos ataques *jamming*. O desenvolvimento de um sistema de detecção contra os ataques *jamming* é uma contramedida inicial para tentar garantir a existência de uma rede móvel ad hoc segura, robusta e confiável. Entretanto, é necessário que a rede continue sobrevivendo mesmo sob a ameaça de ataques. Um outro trabalho futuro é o desenvolvimento de mecanismos e protocolos que reajam de forma adaptativa aos ataques *jamming* e garantam a sobrevivência da rede.

Em particular, as reações deveriam considerar a quantificação do ataque como um parâmetro de entrada para a adaptação do mecanismo de reação. Os capítulos 2 e 3 contextualizaram as principais estratégias que tentam garantir a resistência da rede contra os ataques *jamming*, como por exemplo o controle de potência de transmissão e o salto de frequência. Tais técnicas poderiam ser modificadas a fim de empregar as saídas MCAV e K do sistema DANTE como parâmetros de entrada.

Além dos trabalhos futuros citados anteriormente, os resultados apresentados neste trabalho poderiam ser validados em um ambiente real. Como sugestão, a integração da arquitetura do sistema DANTE poderia ser realizada na camada de enlace do núcleo do sistema operacional GNU/Linux ou de forma conjunta com outros sistemas de detecção presentes na literatura, como [87].

BIBLIOGRAFIA

[1] Prasant Mohapatra and Srikanth V. Krishnamurthy. *Ad Hoc Networks Technologies and Protocols*. Springer Science, 2005.

[2] Mohammad Ilyas and Richard C. Dorf. *The handbook of ad hoc wireless networks*. CRC Press, Inc., 2003.

[3] Azzedine Boukerche. *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks*. Wiley-IEEE Press, 2008.

[4] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52:2292–2330, Abril 2008.

[5] Chris Otto, Aleksandar Milenkovic, Corey Sanders, and Emil Jovanov. System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring. *Journal of Mobile Multimedia*, 1(4):307–326, Janeiro 2006.

[6] Erdal Cayirci. *Security in Wireless Ad Hoc and Sensor Networks*. John Wiley & Sons, 2009.

[7] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang. Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network*, 20(3):41–47, Junho 2006.

[8] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, second edition, 2008.

[9] Konstantinos Pelechrinis, Christos Koufogiannakis, and Srikanth V. Krishnamurthy. Gaming the jammer: is frequency hopping effective? In *Proceedings of the 7th international conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT'09)*, pages 187–196. IEEE Press, Junho 2009.

[10] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, 11(4):42–46, 2009.

[11] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the Performance of IEEE 802.11 under Jamming. In *Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM'08)*, pages 1265–1273. IEEE, Abril 2008.

[12] Eitan Altman, Konstantin Avrachenkov, and Andrey Gamaev. Jamming in wireless networks: The case of several jammers. In *Proceedings of the International Conference on Game Theory for Networks (GAMENETS'09)*, pages 59–65. IEEE, Maio 2009.

[13] Eitan Altman, Konstantin Avrachenkov, and Andrey Gamaev. Jamming in wireless networks under uncertainty. In *Proceedings of the 7th international conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT'09)*, pages 59–65. IEEE Press, Junho 2009.

[14] Seth Gilbert, Rachid Guerraoui, and Calvin Newport. Of malicious motes and suspicious sensors. *Theoretical Computer Science*, 410(6–7):546–569, Fevereiro 2009.

[15] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, 9(8):1119–1133, Agosto 2010.

[16] Lifeng Sang and Anish Arora. Capabilities of Low-Power Wireless Jammers. In *Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM'09)*, pages 2551–2555. IEEE, Abril 2009.

[17] Jahangir H. Sarker and Hussein T. Mouftah. Effect of Jamming Signals on Wireless Ad Hoc and Sensor Networks. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'09)*, pages 1–6. IEEE, Dezembro 2009.

[18] Zhuo Lu, Wenye Wang, and Cliff Wang. From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time-Critical Traffic. In *Proceedings of the 30th IEEE International Conference on Computer Communication (INFOCOM'11)*, pages 1871–1879. IEEE, Abril 2011.

[19] Jeremy J. Blum, Andrew Neiswender, and Azim Eskandarian. Denial of Service Attacks on Inter-Vehicle Communication Networks. In *Proceedings of the 11th IEEE International Conference on Computer Communication (ITSC'08)*, pages 797–802. IEEE, Outubro 2008.

[20] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications Magazine*, 1(1):38–47, Fevereiro 2004.

[21] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. Denial of Service Attacks in Wireless Networks: The case of Jammers. *IEEE Communications Surveys & Tutorials*, 12(4):1–13, Maio 2010.

[22] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. Detection of Radio Interference Attacks in VANET. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'09)*, pages 1–5. IEEE, Dezembro 2009.

[23] Ali Hamieh and Jalel Ben-Othman. Detection of Jamming Attack in Wireless Ad Hoc Networks Using Error Distribution. In *Proceedings of the IEEE International Conference on Communcations (ICC'09)*, pages 1–6. IEEE, Junho 2009.

[24] Geethapriya Thamilarasu, Sumita Mishra, and Ramalingam Sridhar. A Cross-layer approach to Detect Jamming Attacks in Wireless Ad Hoc Networks. In *Proceedings of IEEE Military Communications Conference (MILCOM'06)*, pages 1–7. IEEE, 2006.

[25] Alberto Lopez Toledo and Xiaodong Wang. Detecting MAC Layer Collision Abnormalities in CSMA/CA Wireless Networks. In *Proceedings of IEEE International Conference on Communications (ICC'08)*, pages 1598–1604. IEEE, Maio 2008.

[26] Parminder Chhabra, Clayton Scott, Eric D. Kolaczyk, and Mark Crovella. Distributed Spatial Anomaly Detection. In *Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM'08)*, pages 1705–1713. IEEE, Abril 2008.

[27] Polly Matzinger. Tolerance, Danger, and the Extended Family. *Annual Review of Immunology*, 12:991–1045, Abril 1994.

[28] Matthew Gast. *802.11 Wireless Networks: The Definitive Guide*. O'Reilly Media, Inc., second edition, 2005.

[29] Fred Eady. *Hands-On ZigBee: Implementing 802.15.4 with Microcontrollers (Embedded Technology)*. Newnes, 2007.

[30] Jeffrey G. Andrews, Arunabha Ghosh, and Rias Muhamed. *Fundamentals of WiMAX: Understanding Broadband Wireless Networking (Prentice Hall Communications Engineering and Emerging Technologies Series)*. Prentice Hall PTR, 2007.

[31] I.F. Akyildiz, L. Won-Yeol, M.C. Vuran, and S. Mohanty. A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40–48, Abril 2008.

[32] Eun-Sun Jung and Nitin H. Vaidya. A power control MAC protocol for ad hoc networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking (MOBICOM'02)*, pages 36–47. ACM, Setembro 2002.

[33] Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, and Luiz Carlos P. Albini. Identity-Based Key Management in Mobile Ad Hoc Neworks: Techniques and Applications. *IEEE Wireless Communications Magazine*, 15(5):46–52, Outubro 2008.

[34] J. Montenegro. RFC 4953: Defending TCP Against Spoofing Attacks, Julho 2007. http://tools.ietf.org/html/rfc4953.

[35] CERT CC. Denial of Service, Junho 2001. http://www.cert.org/tech_tips/denial_of_service.html.

[36] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly. Denial of Service Resilience in Ad Hoc Networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking (MOBICOM'04)*, pages 202–215. ACM, Setembro 2004.

[37] Yinghua Guo. *Defending MANETs Against Flooding Attacks by Detective Measures*. PhD thesis, University of South Australia, Australia, Abril 2008.

[38] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MOBIHOC'05)*, pages 46–57. ACM, Maio 2005.

[39] RaviTeja Chinta, Tan F. Wong, and John M. Shea. A Cross-layer approach to Detect Jamming Attacks in Wireless Ad Hoc Networks. In *Proceedings of IEEE Military Communications Conference (MILCOM'09)*, pages 1–7. IEEE, Outubro 2009.

[40] A. Proaando and L. Lazos. Selective Jamming Attacks in Wireless Networks. In *Proceedings of the IEEE International Conference on Communcations (ICC'10)*, pages 1–6. IEEE, Maio 2010.

[41] Zhiguo Zhang, Jingqi Wu, Jing Deng, and Meikang Qiu. Jamming ACK Attack to Wireless Networks and a Mitigation Approach. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'08)*, pages 1–5. IEEE, Novembro 2008.

[42] Mario Strasser. *Novel Techniques for Thwarting Communication Jamming in Wireless Networks*. PhD thesis, ETH, Zurich, Switzerland, 2009.

[43] Alexandra Czarlinska and Deepa Kundur. Towards characterizing the effectiveness of random mobility against actuation attacks. *Computer Communications*, 30(13):2546–2559, Setembro 2007.

[44] Ke Ma and Wade Trappe Yanyong Zhang. Mobile network management and robust spatial retreats via network dynamics. In *Proceedings of the International Conference on Mobile Adhoc and Sensor Systems (MAHSS'05)*, pages 242–249. IEEE, Novembro 2005.

[45] Korporn Panyim and Prashant Krishnamurthy. A hybrid key predistribution scheme for sensor networks employing spatial retreats to cope with jamming attacks. In *Proceeding of the 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing (COLLABORATECOM'08)*, pages 715–731. Springer Berlin Heidelberg, Junho 2008.

[46] Wenyuan Xu, Timothy Wood, Wade Trappe, and Yanyong Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proceedings of the 3rd ACM workshop on Wireless security (WISE'04)*, pages 80–89. ACM, Novembro 2004.

[47] Rohit Negi and Arjunan Rajeswaran. DoS analysis of reservation based MAC protocols. In *Proceedings of the IEEE International Conference on Communications (ICC'05)*, pages 3632–3636. IEEE, Maio 2005.

[48] Baruch Awerbuch, Andrea Richa, and Christian Scheideler. A jamming-resistant mac protocol for single-hop wireless networks. In *Proceedings of the 27th ACM symposium on Principles of distributed computing (PODC'08)*, pages 45–54. ACM, Agosto 2008.

[49] Guevara Noubir. On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility. In *Proceedings of the International Conference on Wired / Wireless Internet Communications, Lecture Notes in Computer Science (WWIC'04)*, pages 186–200. Springer, Fevereiro 2004.

[50] Chris Karlof, Naveen Sastry, Yaping Li, , and Doug Tygar. Distillation Codes and Applications to DoS Resistant Multicast Authentication. In *Proceedings of the 11th Network and Distributed Systems Security Symposium (NDSS'04)*, pages 37–56. Springer, Fevereiro 2004.

[51] Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V. Krishnamurthy, and Christos Gkantsidis. ARES: an anti-jamming reinforcement system for 802.11 networks. In *Proceedings of the 5th international conference on emerging networking experiments and technologies (CONEXT'09)*, pages 181–192. ACM, Dezembro 2009.

[52] Wenyuan Xu. On Adjusting Power to Defend Wireless Networks from Jamming. In *Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MOBIQUITOUS'07)*, pages 1–6. IEEE Computer Society, Agosto 2007.

[53] Vladimir Berman and Biswanath Mukherjee. Data Security in MANETs using Multipath Routing and Directional Transmission. In *Proceedings of the IEEE International Conference on Communications (ICC'06)*, pages 2322–2328. IEEE, Junho 2006.

[54] Mihui Kim and Kijoon Chae. DMP: Detouring Using Multiple Paths against Jamming Attack for Ubiquitous Networking System. *Sensors*, 10(4):3626–3640, Abril 2010.

[55] Patrick Tague, Sidharth Nabar, James A. Ritcey, David Slater, and Radha Poovendran. Throughput Optimization for Multipath Unicast Routing Under Probabilistic Jamming. In *Proceedings of the Personal, Indoor and Mobile Radio Communications (PIMRC'08)*, pages 1–5. IEEE, Setembro 2008.

[56] Leemon C. Baird, William L. Bahn, Michael D. Collins, Martin C. Carlisle, and Sean C. Butler. Keyless jam resistance. In *Proceedings of the IEEE Information Assurance and Security Workshop (IAW'07)*, pages 143–150. IEEE Computer Society, Junho 2007.

[57] Jerry T. Chiang and Yih-Chun Hu. Dynamic Jamming Mitigation for Wireless Broadcast Networks. In *Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM'08)*, pages 1211–1219. IEEE, Abril 2008.

[58] Leemon C. Baird III, William L. Bahn, and Michael D. Collins. Jam-Resistant Communication Without Shared Secrets Through the use of Concurrent Codes. Technical report, U.S. Air Force Academy, U.S.A., 2007.

[59] Mario Strasser, Christina Pöpper, and MarioC agalj. Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, pages 64–78. IEEE Computer Society, Maio 2008.

[60] Michael G. Solomon and Mike Chapple. *Information Security Illuminated*. Jones and Bartlett Publishers, Inc., 2005.

[61] Adetokunbo Makanju, Patrick LaRoche, and A. Nur Zincir-Heywood. A Comparison Between Signature and GP-Based IDSs for Link Layer Attacks on WiFi Networks. In *Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA'07)*, pages 213–219. IEEE, Abril 2007.

[62] Stefan Axelsson. Intrusion Detection Systems: A Survey and Taxonomy. Technical report, Chalmers University of Technology, Department of Computer Engineering, Göteborg, Sweden, 2000.

[63] Ayesha Binte Ashfaq, Mobin Javed, Syed Ali Khayam, and Hayder Radha. An Information-Theoretic Combining Method for Multi-Classifier Anomaly Detection Systems. In *Proceedings of IEEE International Conference on Communications (ICC'10)*, pages 1–5. IEEE, Maio 2010.

[64] Pedro Garcia-Teodoro, Jesús E. Díaz-Verdejo, Gabriel Maciá-Fernández, and E. Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2):18–28, Fevereiro 2009.

[65] Vipin Kumar, Jaideep Srivastava, and Aleksandar Lazarevic. *Managing cyber threats: issues, approaches, and challenges*. Springer-Verlag, first edition, 2005.

[66] David E. Goldberg. *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley Longman Publishing Co., Inc., 1989.

[67] Kevin Gurney. *An Introduction to Neural Networks*. Taylor & Francis, Inc., 1997.

[68] J. Doyne Farmer, Norman H. Packard, and Alan S. Perelson. The immune system, adaptation, and machine learning. *Physica D*, 2(1-3):187–204, Outubro 1986.

[69] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha. Intrusion detection in wireless ad hoc networks. *IEEE Wireless Communications Magazine*, 11(1):48–60, Fevereiro 2004.

[70] Tiranuch Anantvalee, , and Jie Wu. A Survey on Intrusion Detection in Mobile Ad Hoc Networks. In Yang Xiao, Xuemin Sherman Shen, and Ding-Zhu Du, editors, *Wireless Network Security*, Signals and Communication Technology, pages 159–180. Springer US, 2006.

[71] Miss Marianne Amir Azer, Sherif Mohammed El-Kassas, and Magdy Saeed El-Soudani. A Survey on Anomaly Detection Methods for Ad Hoc Networks. *Ubiquitous Computing and Communication Journal*, 2(3):67–76, 2005.

[72] Bo Sun, Lawrence Osborne, Yang Xiao, and Sghaier Guizani. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Wireless Communications Magazine*, 14(5):56–63, Outubro 2007.

[73] Bruce Alberts, Alexander Johnson, Julian Lewis, Martin Raff, Keith Roberts, and Peter Walter. *Molecular Biology of the Cell*. Garland Science, fourth edition, 2002.

[74] Linhas de defesa do corpo humano. http://www.softchalk.com/lessonchallenge/lesson/immunesystems/blood_009008.jpg. Acessado em setembro 2011.

[75] Julie Greensmith, Uwe Aickelin, and Gianni Tedesco. Information fusion for anomaly detection with the dendritic cell algorithm. *Information Fusion*, 11(1):21–34, Janeiro 2010.

[76] Shelly Xiaonan Wu and Wolfgang Banzhaf. The use of computational intelligence in intrusion detection systems: A review. *Applied Soft Computing*, 10(1):1–35, Janeiro 2010.

[77] Julie Greensmith. *The Dendritic Cell Algorithm*. PhD thesis, University of Nottingham, United Kingdom, Outubro 2007.

[78] Julie Greensmith and Uwe Aickelin. The Deterministic Dendritic Cell Algorithm. In *Proceedings of the 7th International Conference on Artificial Immune Systems (ICARIS'2008)*, pages 291–303. Springer Berlin / Heidelberg, Junho 2008.

[79] Jungwon Kim, Peter Bentley, Christian Wallenta, Mohamed Ahmed, and Stephen Hailes. Danger Is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm. In *Proceedings of the 5th International Conference on Artificial Immune Systems (ICARIS'2006)*, pages 390–403. Springer Berlin / Heidelberg, 2006.

[80] Salman Manzoor, M. Zubair Shafiq, S. Momina Tabish, and Muddassar Farooq. A Sense of 'Danger' for Windows Processes. In *Proceedings of the 8th International Conference on Artificial Immune Systems (ICARIS'09)*, pages 220–233. Springer-Verlag, Agosto 2009.

[81] Feng Gu, Julie Greensmith, and Uwe Aickelin. Further Exploration of the Dendritic Cell Algorithm: Antigen Multiplier and Time Windows. In *Proceedings of the 7th International Conference on Artificial Immune Systems (ICARIS'08)*, pages 142–153. Springer, Junho 2008.

[82] Murat Çakiroğlu and Ahmet Turan Özcerit. Jamming detection mechanisms for wireless sensor networks. In *Proceedings of the 3rd international conference on Scalable information systems (INFOSCALE'08)*, pages 1–8. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Junho 2008.

[83] Ying Lin and Mingyan Li. Distributed detection of jamming and defense in wireless sensor networks. In *Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS'09)*, pages 829–834. IEEE, Março 2009.

[84] Jeffrey Philip Monks, Vaduvur Bharghavan, and Wen mei W. Hwu. Transmission power control for multiple access wireless packet networks. In *Proceedings of the 25th Annual IEEE Conference on Local Computer Networks (LCN'00)*, pages 12–21. IEEE Computer Society, Novembro 2000.

[85] Nicola Baldo, Federico Maguolo, Marco Miozzo, Michele Rossi, and Michele Zorzi. ns2-MIRACLE: a modular framework for multi-technology and cross-layer support in network simulator 2. In *Proceedings of the 2nd international conference on Performance evaluation methodologies and tools (VALUETOOLS'07)*, pages 1–8. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Outubro 2007.

[86] David L. Olson and Dursun Delen. *Advanced Data Mining Techniques*. Springer-Verlag, 2008.

[87] Maxim Raya, Imad Aad, Jean-Pierre Hubaux, and Alaeddine El Fawal. DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots. *IEEE Transactions on Mobile Computing*, 5(12):1691–1705, Dezembro 2006.

APÊNDICE A

RESULTADOS DA AVALIAÇÃO DE DESEMPENHO DO SISTEMA DANTE NO CENÁRIO 2

Este apêndice apresenta os resultados da avaliação de desempenho do sistema DANTE no cenário 2. Este cenário, o qual é empregado por Zhang et al. [41], é ilustrado na Figura 4.1(b). Os resultados apresentados para esse cenário são similares aos resultados apresentados na Seção 4.5. Os parâmetros considerados nas simulações do cenário 2 são os mesmos apresentados na Seção 4.3.

A.1 Cenário 2: *Jammer* vizinho do nó origem

Esta seção é dividida em duas partes. A primeira parte tem como objetivo analisar o desempenho do sistema DANTE e a quantificação dos ataques através das métricas MCAV e K. Além disso, são avaliados os parâmetros do sistema DANTE a fim de escolher aqueles que possuem o melhor desempenho para serem comparados com o sistema CLADE. A segunda parte realiza uma análise comparativa do desempenho dos sistemas DANTE e CLADE diante dos ataques *jamming* no cenário 2.

A.1.1 Análise inicial do sistema DANTE

Ataque *jamming* deceptivo

As Figuras A.1 e A.2 ilustram a acurácia e a precisão do sistema DANTE empregado pelos nós legítimos. O sistema obteve acurácia e precisão constantes com um valor de 100% ao empregar qualquer número de agentes artificiais e independente do número de multiplicadores de informações utilizado. Assim como analisado no cenário 1, os nós legítimos sempre encontraram o meio de transmissão sem fio ocupado em decorrência do ataque *jamming* deceptivo. Apesar do *jammer* ser vizinho somente do nó **A**, o atacante

conseguiu criar interferência até mesmo no nó **B**, que estava a uma distância de 200 metros do *jammer*. Essa interferência foi tratada corretamente pelo nó **B** como anômala. Além disso, a técnica de multiplicador de informações não apresentou influência na detecção do sistema.

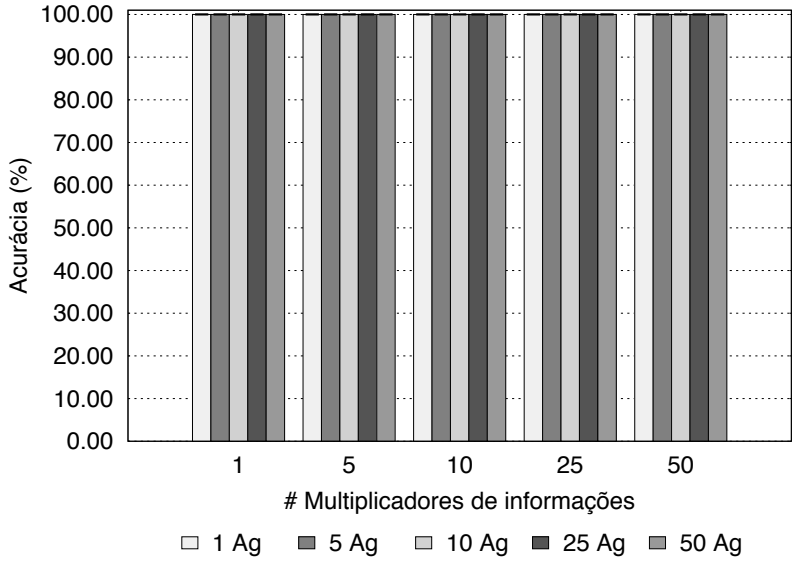

Figura A.1: Acurácia do sistema diante do ataque *jamming* deceptivo no cenário 2

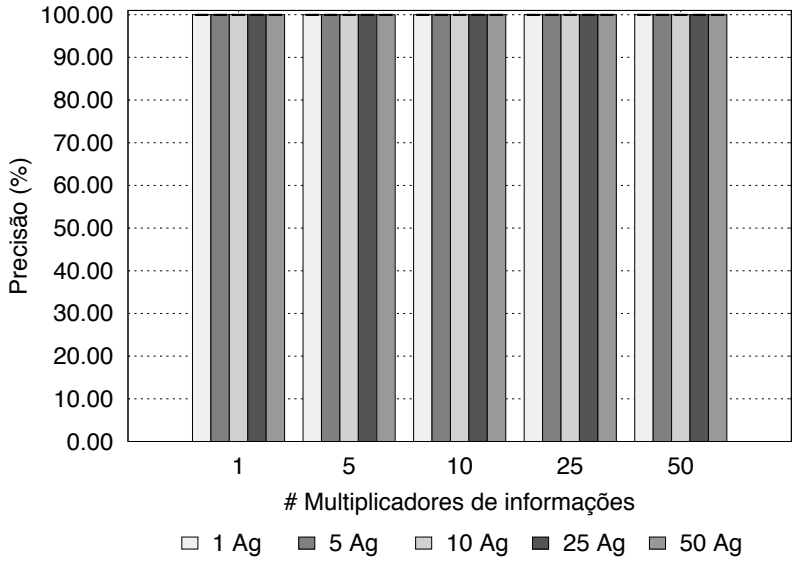

Figura A.2: Precisão do sistema diante do ataque *jamming* deceptivo no cenário 2

A fim de apresentar os valores das saídas MCAV e K, foram fixados o número dos multiplicadores de informações em 1 e dos agentes artificiais em 1 e 5. O número de multiplicadores de informações foi fixado em 1 por não apresentar qualquer alteração na acurácia do sistema. O número de agentes foi fixado em 1 e 5 pelas mesmas razões

apresentadas nas avaliações do ataque *jamming* deceptivo no cenário 1. As razões podem ser justificadas pela redução de iterações realizadas pelo algoritmo dDCA no processo de detecção dos ataques quando o número de agentes artificiais é reduzido.

A Figura A.3 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming*. A Figura A.3(a) mostra as saídas MCAV dos nós **A** e **B** utilizando o sistema DANTE, que emprega 1 agente artificial. A Figura A.3(b) ilustra as saídas MCAV do sistema considerando 5 agentes artificiais. Durante a atuação do ataque *jamming*, entre 5 e 100 segundos de simulação, os nós **A** e **B** empregando 1 e 5 agentes artificiais obtiveram valores para o MCAV que alcançam 1% em média. Isso ocorreu devido à ocupação do meio de transmissão sem fio pelo *jammer*.

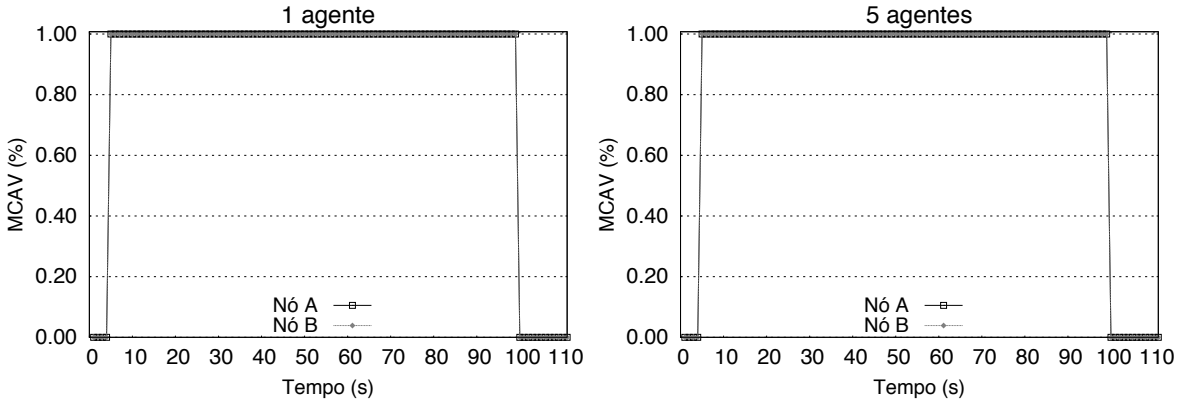

Figura A.3: Saída MCAV do sistema diante do ataque *jamming* deceptivo no cenário 2

A Figura A.4 ilustra a saída K do sistema DANTE ao longo do tempo diante do ataque *jamming* deceptivo. A Figura A.4(a) exibe as saídas K dos nós **A** e **B** utilizando o sistema DANTE, que considera 1 agente artificial. Já a Figura A.4(b) ilustra as saídas K do sistema, o qual é empregado pelos nós **A** e **B**, considerando 5 agentes artificiais.

Durante a execução do ataque *jamming*, os nós **A** e **B** usando 1 agente artificial obtiveram valores para o K que alcançam 0.30 em média. Ao variar o número de agentes para 5, o sistema empregado pelos nós **A** e **B** alcançou em média o valor 1.52. Como observado anteriormente, a saída K apresentou valores que aumentaram de forma proporcional à quantidade de agentes artificiais empregados pelo sistema, quantificando a anomalia que ocorria no meio de transmissão sem fio.

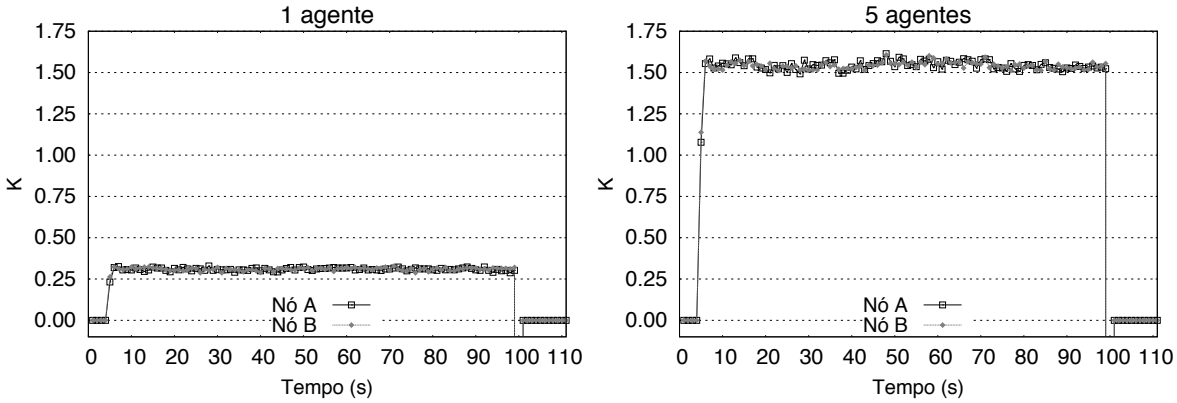

Figura A.4: Saída K do sistema diante do ataque *jamming* deceptivo no cenário 2

Ataque *jamming* aleatório

A Figura A.5 ilustra a acurácia do sistema DANTE diante do ataque *jamming* aleatório. O sistema obteve a acurácia de 81% ao utilizar 1 agente artificial e independente do número de multiplicadores de informações empregado. Quando o número de agentes variou em 5, 10, 50 ou 100, o sistema obteve valores para a acurácia que na média alcançaram 82%.

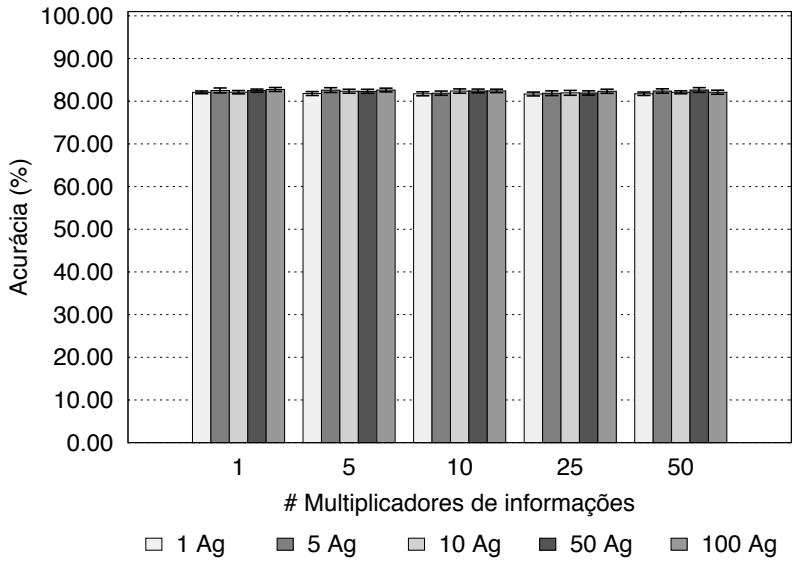

Figura A.5: Acurácia do sistema diante do ataque *jamming* aleatório no cenário 2

A Figura A.6 ilustra a precisão do sistema DANTE empregado pelos nós legítimos sob o ataque *jamming* aleatório. O sistema alcançou a precisão média de 42% ao usar 1 agente artificial e independente do número de multiplicadores de informações considerado. Quando o número de agentes foi alterado para 5, 10, 50 ou 100, o sistema obteve valores

para a precisão que na média alcançaram 44%. Da mesma forma como analisado no cenário 1, o sistema DANTE atingiu baixos valores para a precisão ao tentar detectar o ataque *jamming* aleatório em comparação aos outros ataques.

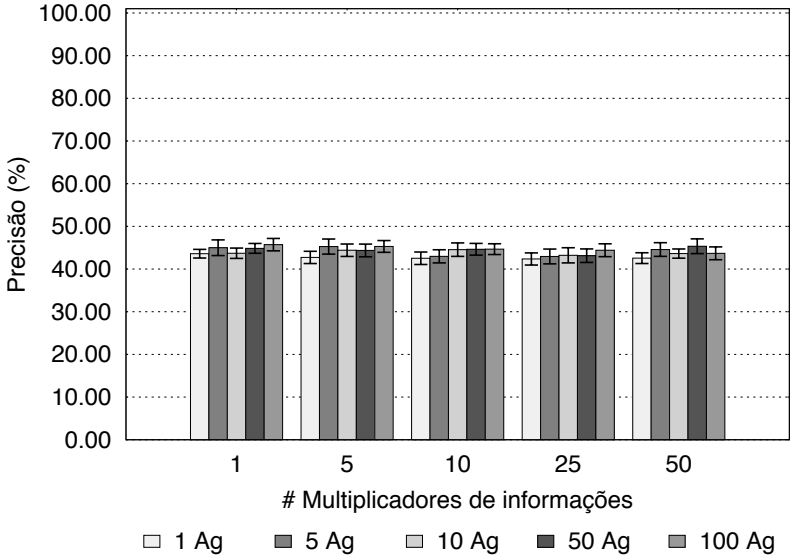

Figura A.6: Precisão do sistema diante do ataque *jamming* aleatório no cenário 2

A fim de apresentar os valores das saídas MCAV e K, foram fixados o número dos multiplicadores de informações e dos agentes artificiais. O número de multiplicadores de informações foi fixado em 1, e dos agentes artificiais, em 1 e 5. Isso foi feito por motivos análogos aos mencionados na avaliação do ataque *jamming* deceptivo cenário 2.

A Figura A.7 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming* aleatório. A Figura A.7(a) mostra as saídas MCAV do sistema DANTE empregado pelos nós legítimos **A** e **B**, o qual considera 1 agente artificial. Já a Figura A.7(b) ilustra as saídas MCAV do sistema utilizando 5 agentes artificiais.

Durante a execução do ataque *jamming*, entre 5 e 100 segundos de simulação, o sistema com 1 agente artificial, empregado pelos nós **A** e **B**, obteve valores para a saída MCAV entre 0.22% e 1% em média. Ao empregar 5 agentes, o sistema atingiu valores para o MCAV entre 0.15% e 1% em média, durante a execução do ataque. O ataque *jamming* aleatório possui períodos de atividade e inatividade. Contudo, nota-se que a saída MCAV na Figura A.7 não atingiu 0% em momento algum. Como o sistema DANTE emprega os valores da saída MCAV para detectar possíveis anomalias, a acurácia, e sobretudo

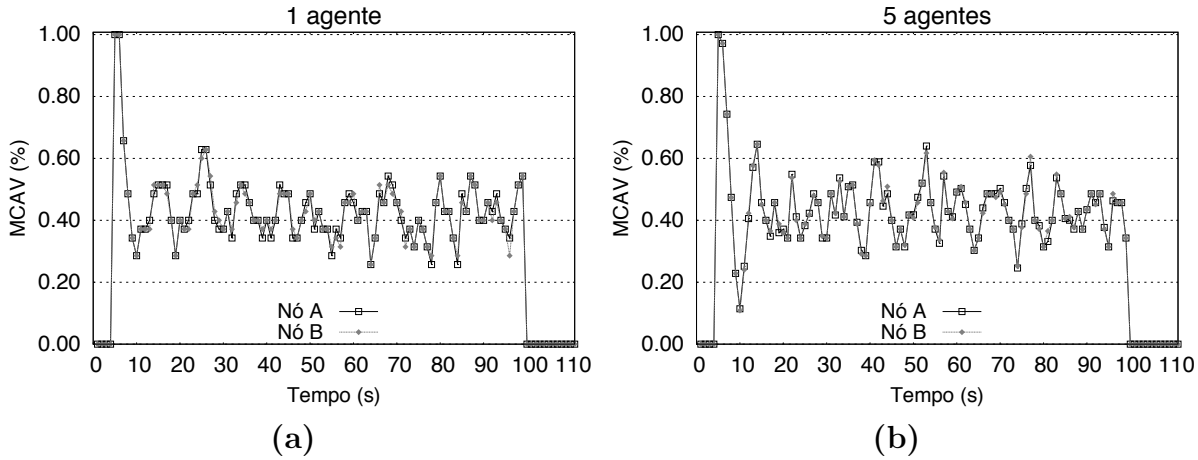

Figura A.7: Saída MCAV do sistema diante do ataque *jamming* aleatório no cenário 2

a precisão, sofreram drástica redução, quando comparado aos resultados analisados nos outros ataques *jamming*.

A Figura A.8 ilustra a saída K do sistema DANTE. A Figura A.8(a) exibe as saídas K do sistema, utilizado pelos nós **A** e **B**, que considera 1 agente artificial. Já a Figura A.8(b) ilustra as saídas K do sistema usando 5 agentes artificiais.

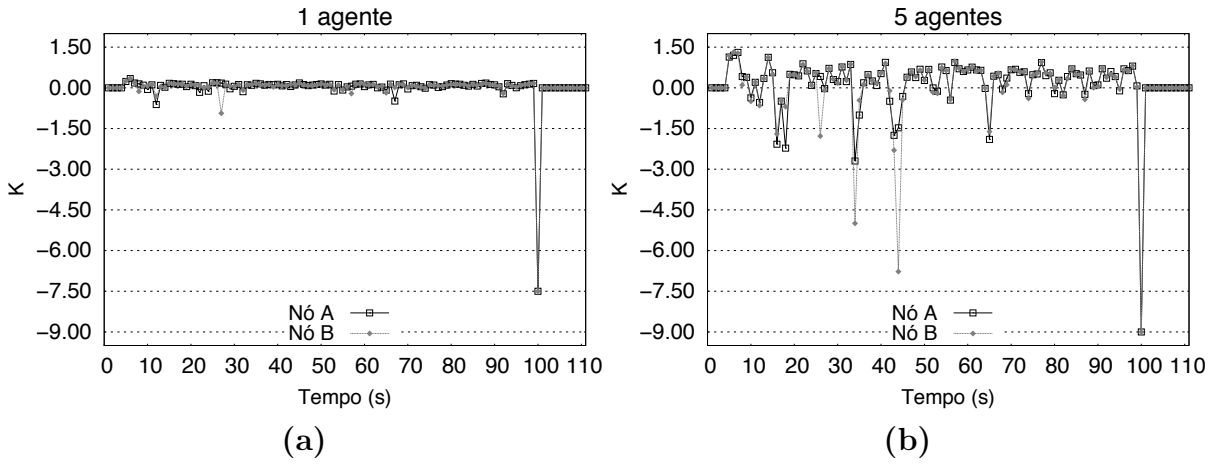

Figura A.8: Saída K do sistema diante do ataque *jamming* aleatório no cenário 2

Durante a atuação do ataque *jamming*, o sistema considerando 1 agente artificial obteve valores para a saída K que variam entre -7.5 e 0.2 em média, tanto para o nó **A** quanto para o nó **B**. Ao empregar 5 agentes, o sistema obteve valores entre -9 e 1.49 em média. A saída K obteve maior sensibilidade ao ataque *jamming* aleatório que a saída MCAV. Os valores da saída K apresentaram alternância entre positivo e negativo, indicando os períodos que o *jammer* atuou no meio de transmissão sem fio.

Ataque *jamming* reativo

As Figuras A.9 e A.10 exibem a acurácia e a precisão do nó legítimo **A** empregando o sistema DANTE diante do ataque *jamming* reativo. Somente a acurácia e a precisão do nó **A** foram consideradas, em consequência das colisões criadas pelo *jammer* serem recebidas somente por esse nó. O sistema obteve uma acurácia praticamente constante com um valor em torno de 100%, independente do número de agentes artificiais e multiplicadores de informações utilizado.

Apesar da distância entre o nó **A** e o *jammer* ser de 95 metros e o número de colisões criado pelo ataque *jamming* reativo ao quadro de dados ser menor que o número criado pelos outros ataques *jamming* [40], o nó **A** obteve a acurácia e a precisão de 100%. Uma possível explicação para esse resultado é que o número de colisões foi o suficiente para auxiliar o sistema na detecção. Como o número de colisões é suficiente para garantir que o sistema consiga detectar o ataque, a técnica de multiplicador de informações não apresentou influência na detecção do ataque.

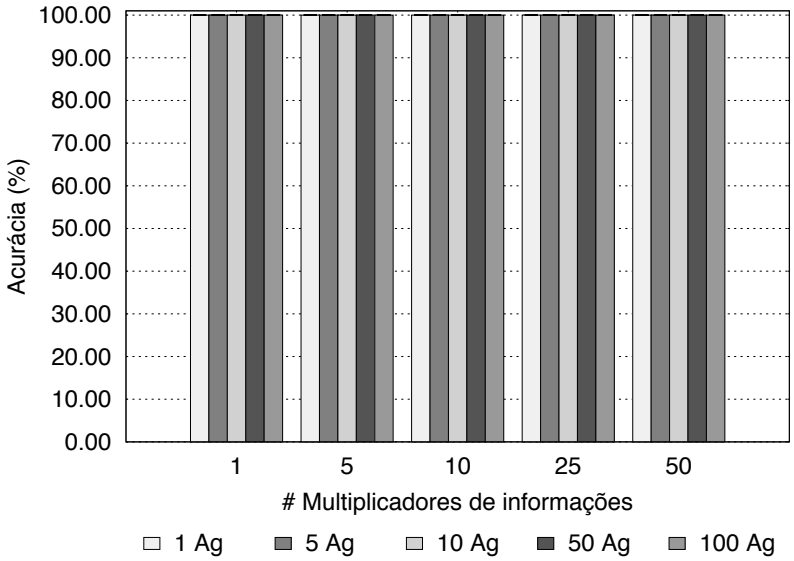

Figura A.9: Acurácia do sistema diante do ataque *jamming* reativo no cenário 2

Para apresentar os valores das saídas MCAV e K, foram fixados o número dos multiplicadores de informações e dos agentes artificiais. O número de multiplicadores de informações foi fixado em 1, por não apresentar alteração na acurácia e precisão do sistema. Embora a acurácia e a precisão sejam iguais para qualquer número de agentes

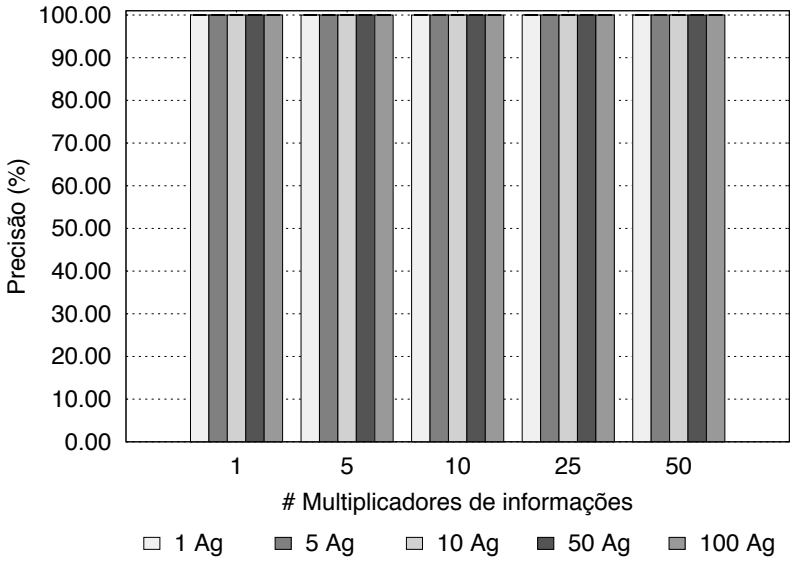

Figura A.10: Precisão do sistema diante do ataque *jamming* reativo no cenário 2

artificiais, os números dos agentes foram fixados em 1 e 5, por representarem os menores valores.

A Figura A.11 ilustra a saída MCAV do sistema DANTE ao longo do tempo diante do ataque *jamming* aleatório. A Figura A.11(a) exibe as saídas MCAV do sistema DANTE empregado pelos nós legítimos **A** e **B**, o qual considera 1 agente artificial. Já a Figura A.11(b) ilustra as saídas MCAV do sistema utilizando 5 agentes artificiais.

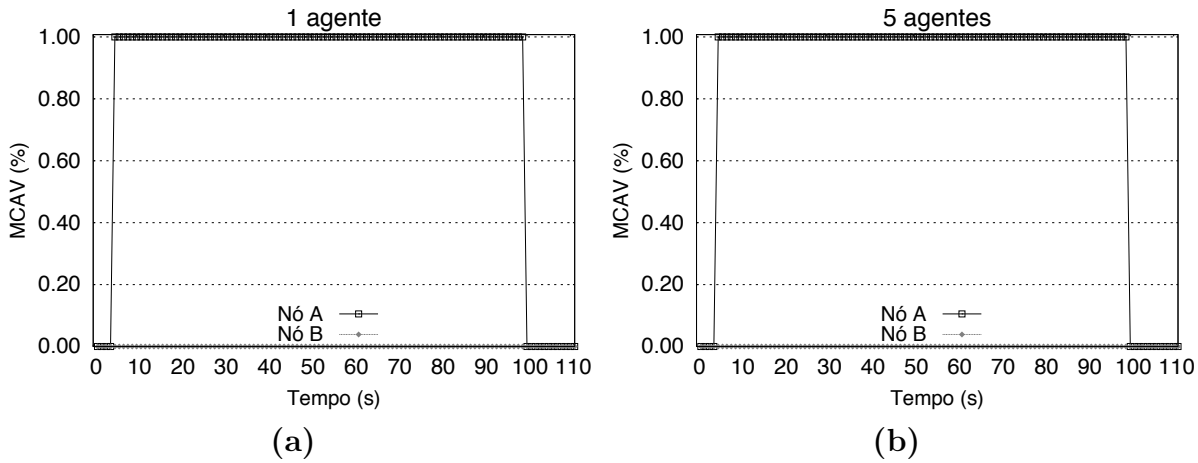

Figura A.11: Saída MCAV do sistema diante do ataque *jamming* reativo no cenário 2

Durante o ataque *jamming*, entre 5 e 100 segundos de simulação, o sistema DANTE empregado pelo nó **A**, obteve valores constantes de 1% em média para a saída MCAV, considerando 1 e 5 agentes artificiais. Já a saída MCAV do sistema DANTE, empregado

pelo nó **B**, não sofreu variação ao longo do tempo. Como o nó **A** é vizinho do *jammer* e sofre de maneira direta as colisões, a saída MCAV para 1 e 5 agentes artificiais atinge o seu valor máximo, que é de 1%. A saída MCAV dos nós legítimos tende a se tornar estável quando o número de agentes aumenta.

A Figura A.12 ilustra a saída K do sistema DANTE ao longo do tempo diante do ataque *jamming* aleatório no cenário 2. A Figura A.12(a) mostra as saídas K do sistema, utilizado pelos nós **A** e **B**, que considera 1 agente artificial. Já a Figura A.12(b) ilustra as saídas K do sistema usando 5 agentes artificiais.

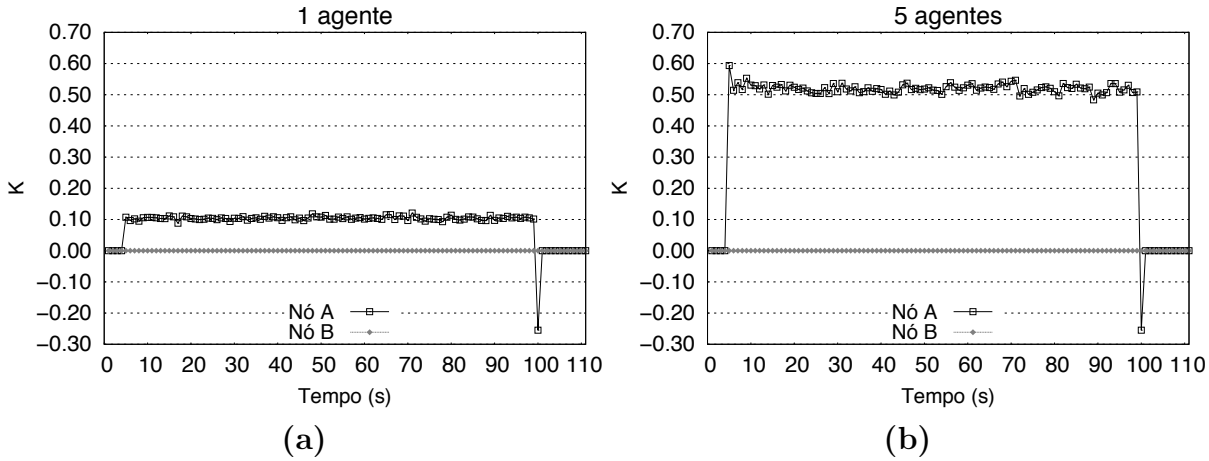

Figura A.12: Saída K do sistema diante do ataque *jamming* reativo no cenário 2

Entre 5 e 100 segundos de simulação quando o *jammer* realiza o ataque na rede, o sistema considerando 1 e 5 agentes artificiais, empregado pelo nó **A**, obteve valores para a saída K que alcançam 0.11 e 0.52 em média, respectivamente. Já a saída K do sistema DANTE usado pelo nó **B** não sofreu variação durante o ataque. Como explicado anteriormente, essa saída apresenta valores que aumentam de forma proporcional ao aumento do número de agentes, por ser calculada a partir do somatório do parâmetro da anomalia observada pelos agentes artificiais.

Síntese da análise inicial do sistema DANTE

A Tabela A.1 resume os melhores resultados para a acurácia e a precisão obtidos pelo sistema DANTE diante dos ataques *jamming* no cenário 2. Da mesma forma como explicado na análise inicial do sistema DANTE no cenário 1, o número de iterações do

algoritmo dDCA é diretamente proporcional ao número de agentes artificiais e multiplicadores informações. Portanto, é interessante escolher valores para esses dois parâmetros que reduzam o número de iterações e simultaneamente obtenham um alto desempenho. A partir dos resultados demonstrados, é possível concluir que o sistema DANTE consegue o melhor desempenho empregando um número de agentes artificiais e multiplicadores de informações igual a 10 e 1, respectivamente.

Ataque *jamming*	**Acurácia**	**Precisão**	**Número de agentes artificiais**	**Multiplicadores de informações**
Deceptivo	100%	100%	1, 5, 10, 50, 100	1, 5, 10, 25, 50
Aleatório	82%	44%	10	1, 10, 50
Reativo	100%	100%	10, 50, 100	1, 5, 10, 25, 50

Tabela A.1: Síntese dos melhores resultados da acurácia e da precisão obtidos pelos sistemas DANTE diante dos ataques *jamming* no cenário 2

A.1.2 Comparação dos sistemas DANTE e CLADE

Nesta seção são apresentadas as análises comparativas dos sistemas DANTE e CLADE empregando o cenário 2. Esse cenário representa aquele ilustrado na Figura 4.1(b). Os parâmetros utilizados nas simulações são os mesmos exibidos na Tabela 4.1.

Assim como na análise comparativa no cenário 1, os valores dos patamares de detecção avaliados para os sistemas DANTE e CLADE são 0.0, 0.25, 0.50, 0.75 e aleatório, respectivamente. Além disso, foram fixados os seguintes parâmetros do sistema DANTE, o número de agentes artificiais e o número multiplicadores de informações. A partir das análises iniciais realizadas no cenário 2, concluiu-se que o sistema DANTE obtém os melhores resultados empregando um número de agentes artificiais e multiplicadores de informações igual a 10 e 1, respectivamente. Também foram utilizados os mesmos valores para os pesos de normalidade e anormalidade, exibidos na Tabela 4.2.

De forma similar ao cenário 1, na comparação do cenário 2 também é avaliado o período de coleta dos sistemas. Isso é feito para investigar a latência necessária para os sistemas detectarem os *jammers* no meio de transmissão sem fio. Os valores estocásticos dos períodos de detecção são 0.25, 0.50, 0.75 e 1 segundo. As métricas consideradas na

comparação dos sistemas são a acurácia e a precisão, explicadas na Seção 4.4.

Ataque *jamming* deceptivo

As Figuras A.13 e A.14 ilustram a acurácia e a precisão obtidas pelos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo. O sistema DANTE tem o seu desempenho melhorado de acordo com o aumento do período de coleta. A redução do período de coleta dos quadros afeta o desempenho do sistema DANTE. Isso ocorre devido à redução do número de quadros coletados que sofreram interferência, tendo como consequência o aumento de erros na detecção do ataque pelos agentes artificiais. Além disso, a alteração do valor do patamar de detecção não modificou o desempenho do sistema DANTE. Apesar do sistema DANTE não ter alcançado resultados relevantes para a acurácia em alguns períodos de coleta, como nos períodos iguais a 0.25 e 0.50, esse sistema obteve resultados significantes para a precisão, por exemplo, ao alcançar a precisão maior que 85% com o período de coleta igual a 0.25.

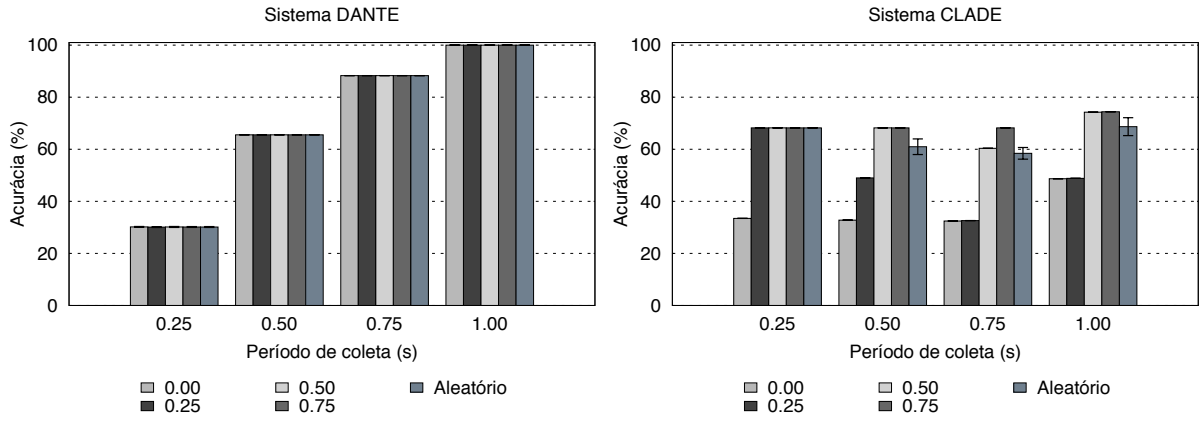

Figura A.13: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo no cenário 2

No que diz respeito ao sistema CLADE, existe a necessidade de encontrar um ponto de equilíbrio o qual permita que tanto a acurácia quanto a precisão alcancem resultados relevantes. Esse ponto de equilíbrio é encontrado quando o sistema CLADE emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50. No entanto, de um modo geral, o sistema CLADE obteve um pior desempenho que o sistema DANTE diante do ataque *jamming* deceptivo no cenário 2.

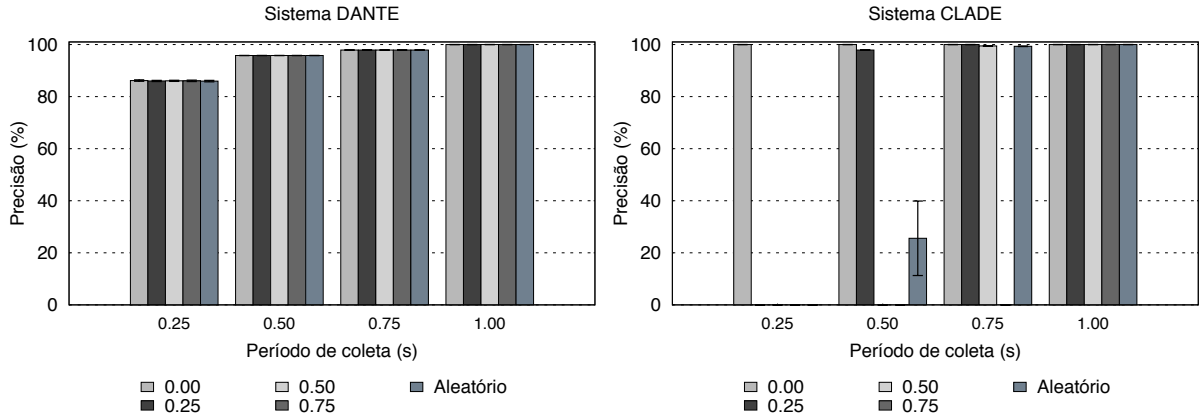

Figura A.14: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* deceptivo no cenário 2

Ataque *jamming* aleatório

As Figuras A.15 e A.16 ilustram a acurácia e a precisão obtidas pelos sistemas DANTE e CLADE diante do ataque *jamming* aleatório no cenário 2. Da mesma forma como avaliado no ataque *jamming* deceptivo, o sistema DANTE tem o seu desempenho melhorado de acordo com o aumento do período de coleta. Isso ocorre devido à necessidade dos agentes artificiais coletarem uma certa quantidade de quadros que sofreram colisão. No entanto, apesar do sistema DANTE obter valores relevantes para acurácia, o mesmo não ocorre com a precisão. O sistema DANTE não lidou de forma eficiente com a aleatoriedade do ataque, alcançando resultados pouco relevantes. A aleatoriedade do ataque acarretou num aumento do número de falsos-positivos produzidos pelo sistema, reduzindo a precisão do sistema.

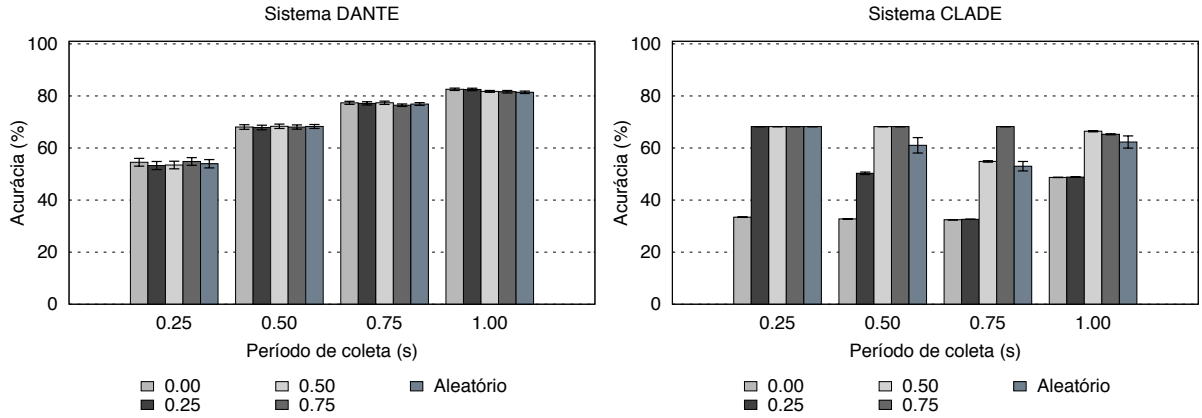

Figura A.15: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* aleatório no cenário 2

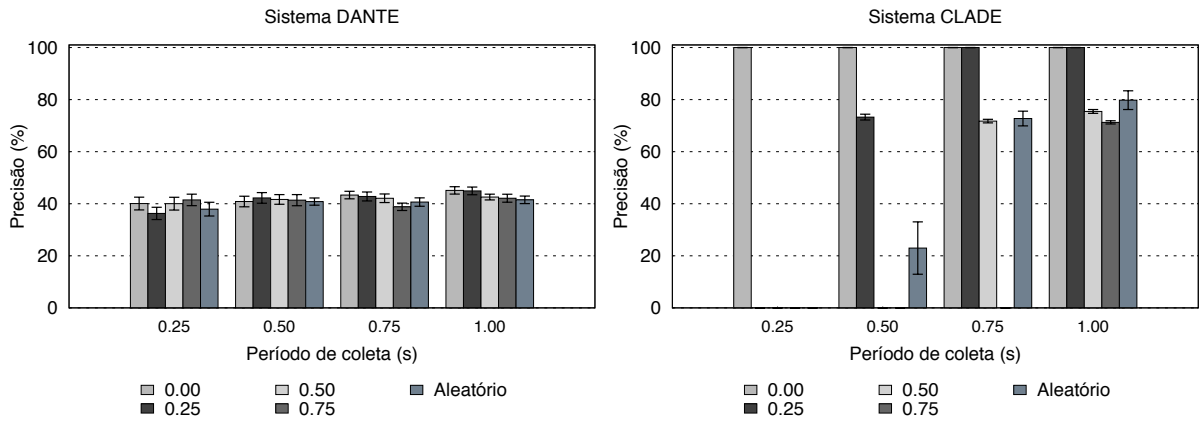

Figura A.16: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* aleatório no cenário 2

No sistema CLADE existe a necessidade de encontrar um ponto de equilíbrio o qual permita que tanto a acurácia quanto a precisão alcancem resultados relevantes. No ataque *jamming* aleatório, esse ponto de equilíbrio é verificado quando o sistema CLADE emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50. Considerando esse ponto de equilíbrio, apesar do sistema CLADE obter um valor para a acurácia 12% menor que aquele alcançado pelo sistema DANTE, o sistema CLADE obteve um valor para a precisão 32% maior que o alcançado pelo sistema DANTE. Com base nesses resultados, conclui-se que o sistema CLADE obteve resultados significantes tanto quanto aqueles alcançados pelos sistema DANTE na tarefa de detecção do ataque *jamming* aleatório.

Ataque *jamming* reativo

As Figuras A.17 e A.18 ilustram a acurácia e a precisão obtidas pelos sistemas DANTE e CLADE diante do ataque *jamming* reativo. Da mesma forma como avaliado nos ataques *jamming* deceptivo e aleatório, o mesmo comportamento ocorre no ataque *jamming* reativo, no qual o desempenho do sistema DANTE melhora conforme o período de coleta é aumentado. Como mencionado anteriormente, quanto maior o número de colisões capturadas, maior é a probabilidade do sistema acertar a ocorrência de um ataque na rede. Além disso, a modificação do valor do patamar de detecção não alterou o desempenho do sistema DANTE. O mesmo comportamento pode ser observado na métrica precisão, a qual é diretamente proporcional ao período de coleta.

Em alguns períodos de detecção, como nos períodos iguais a 0.25 e 0.50, o sistema DANTE não alcançou resultados relevantes para a acurácia. Contudo, ao se comparar os melhores valores da acurácia dos dois sistemas, é possível concluir que o sistema DANTE alcançou uma acurácia 28% maior que o sistema CLADE. Portanto, o sistema DANTE obteve um desempenho mais relevante que o sistema CLADE na tarefa de detecção do ataque *jamming* reativo. Concernente à precisão, ambos os sistemas alcançaram acurácia máxima de 100%.

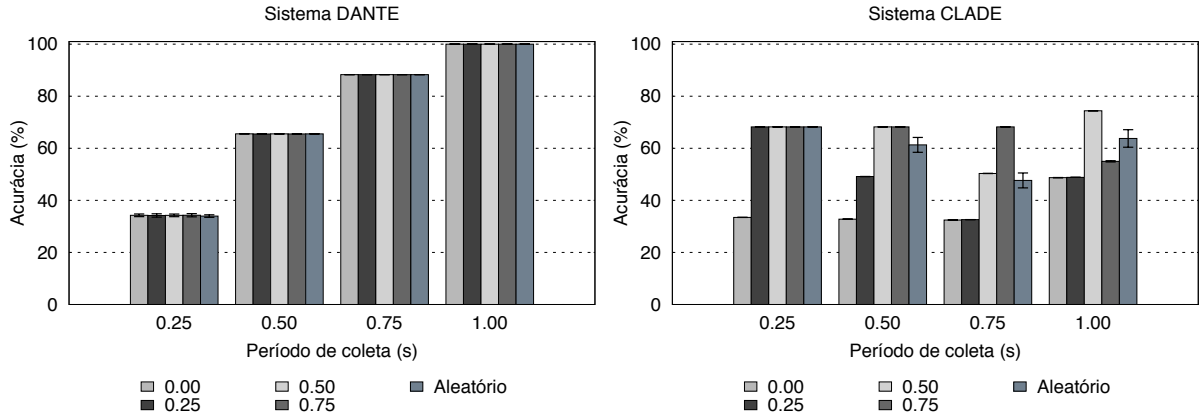

Figura A.17: Acurácia dos sistemas DANTE e CLADE diante do ataque *jamming* reativo no cenário 2

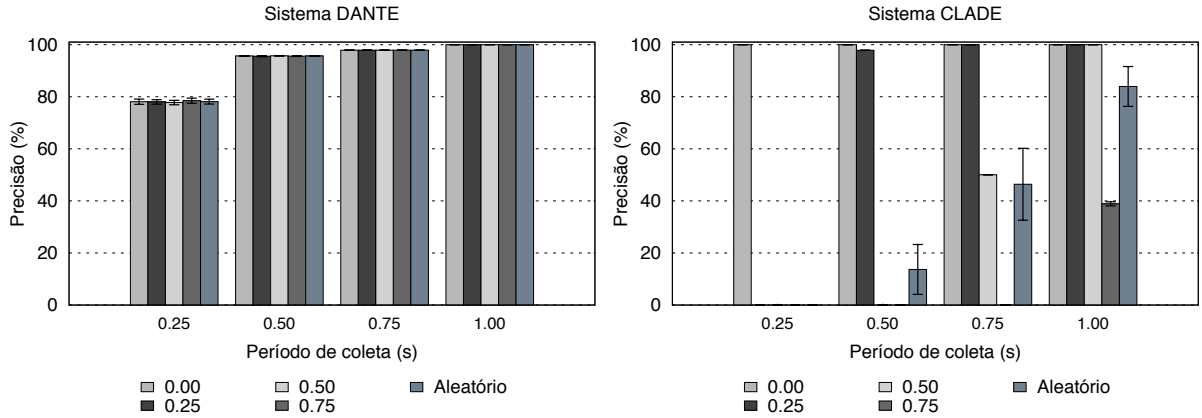

Figura A.18: Precisão dos sistemas DANTE e CLADE diante do ataque *jamming* reativo no cenário 2

Como observado nas análises anteriores, o sistema CLADE necessita de um ponto de equilíbrio. Esse ponto possibilita que tanto a acurácia quanto a precisão alcancem resultados relevantes. No ataque *jamming* reativo, o ponto de equilíbrio é verificado quando o sistema CLADE emprega o período de coleta igual a 0.25 ou 0.50 segundo e o

patamar de detecção igual a 0.25. Considerando os gráficos da acurácia e da precisão nesse ponto de equilíbrio, é possível concluir que, apesar do sistema CLADE ter alcançado a precisão de 100%, esse sistema não conseguiu valores relevantes para a acurácia diante do ataque *jamming* reativo no cenário 2. Isso ocorreu devido ao número de falsos-negativos obtidos pelo sistema, o qual produz um impacto direto na métrica de acurácia.

Além disso, a distância dos nós legítimos até o *jammer* ocasionou impacto no desempenho da precisão do sistema CLADE no cenário 2. Ao comparar os gráficos da precisão do cenário 1 com os gráficos da precisão do cenário 2, nota-se a redução de desempenho do sistema. Uma possível explicação para esse fato está na sensibilidade das medições de detecção empregadas pelo sistema CLADE. Uma vez que os nós legítimos estão mais próximos do *jammer*, a detecção torna-se mais fácil devido às medições de detecção variarem com maior frequência ao ataque.

No entanto, a partir do momento que a distância entre os nós legítimos e o *jammer* aumenta, essas medições tornam-se ineficazes. Embora esse problema ocorra com o sistema CLADE, o mesmo comportamento que causa impacto no desempenho da precisão não é visto no sistema DANTE. Além das medições de normalidade e anormalidade serem sensíveis ao impacto do ataque na rede, o uso de agentes artificiais reduz a probabilidade de erro do sistema DANTE, como verificado nos gráficos.

Síntese da comparação dos sistemas DANTE e CLADE

A Tabela A.2 resume os melhores resultados para a acurácia obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming* no cenário 2. O sistema DANTE alcançou maiores resultados para a acurácia que o sistema CLADE. No ataque *jamming* aleatório o sistema DANTE obteve a acurácia 13% maior que o sistema CLADE, ao que passo que, nos ataques *jamming* deceptivo e reativo, a diferença alcançou 28% e 51%, respectivamente.

A Tabela A.3 exibe os melhores resultados para a precisão alcançados pelos sistemas DANTE e CLADE sob os ataques *jamming* no cenário 2. Em relação à precisão, o sistema CLADE obteve um rendimento superior aquele alcançado pelo sistema DANTE.

Sistema	Ataque *jamming*	Acurácia	Período de coleta	Patamar de detecção
DANTE	Deceptivo	100%	1 segundo	-
	Aleatório	82%	1 segundo	-
	Reativo	100%	1 segundo	-
CLADE	Deceptivo	72%	1 segundo	0.50, 0.75
	Aleatório	69%	0.25 segundo	0.50
	Reativo	49%	1 segundo	0.0, 0.25

Tabela A.2: Síntese dos melhores resultados para a acurácia obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming*

Nos ataques *jamming* deceptivo e reativo, ambos os sistemas alcançaram 100% de precisão. Contudo, no ataque *jamming* aleatório, o sistema CLADE obteve a precisão 31% maior que o sistema DANTE.

Sistema	Ataque *jamming*	Precisão	Período de coleta	Patamar de detecção
DANTE	Deceptivo	100%	1 segundo	-
	Aleatório	44%	1 segundo	-
	Reativo	100%	1 segundo	-
CLADE	Deceptivo	100%	1 segundo	-
	Aleatório	75%	1 segundo	0.50
	Reativo	100%	1 segundo	0.0, 0.25

Tabela A.3: Síntese dos melhores resultados para a precisão obtidos pelos sistemas DANTE e CLADE diante dos ataques *jamming*

A partir das avaliações realizadas é possível expor as seguintes afirmações relativas aos sistemas DANTE e CLADE. O sistema DANTE apresenta o melhor desempenho ao considerar o período de coleta igual a 1 segundo. A alteração do valor do patamar de detecção não altera o desempenho do sistema DANTE nos ataques *jamming* deceptivo e reativo e não existe modificação significante no desempenho desse sistema no ataque *jamming* aleatório. Referente ao sistema CLADE, o ponto de equilíbrio é encontrado quando o sistema emprega o período de coleta igual a 1 segundo e o patamar de detecção igual a 0.50.

Por fim, é concluído que o sistema DANTE possui um desempenho superior ao sistema CLADE no cenário 2. O sistema DANTE obteve a precisão de 100% nos ataques *jamming* deceptivo e reativo. Além disso, o sistema DANTE alcançou os melhores resultados para a acurácia em todos os três ataques *jamming* analisados.