UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E INFORMÁTICA INDUSTRIAL

MARCOS EDUARDO PIVARO MONTEIRO

SISTEMA DE VERIFICAÇÃO DE LOCALIZAÇÃO COM ANTENAS DIRECIONAIS BASEADO EM TEORIA DA INFORMAÇÃO

DISSERTAÇÃO

CURITIBA
2014

MARCOS EDUARDO PIVARO MONTEIRO

SISTEMA DE VERIFICAÇÃO DE LOCALIZAÇÃO COM ANTENAS DIRECIONAIS BASEADO EM TEORIA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de “Mestre em Ciências” – Área de Concentração: Telecomunicações e Redes.

Orientador: Prof. Dr. João Luiz Rebelatto

Co-orientador: Prof. Dr. Richard Demo Souza

CURITIBA
2014

Dados Internacionais de Catalogação na Publicação

M775 Monteiro, Marcos Eduardo Pivaro
2014 Sistema de verificação de localização com antenas direcionais baseado em teoria da informação / Marcos Eduardo Pivaro Monteiro.-- 2014.
69 f.: il.; 30 cm

Texto em português, com resumo em inglês
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Curitiba, 2014
Bibliografia: f. 66-67

1. Redes veiculares ad hoc (Redes de computadores) - Medidas de segurança. 2. Rádio - Antenas. 3. Teoria da informação. 4. Sistemas inteligentes de veículos rodoviários. 5. Sistemas de comunicação sem fio. 6. Métodos de simulação. 7. Engenharia elétrica - Dissertações. I. Rebelatto, João Luiz, orient. II. Souza, Richard Demo, coorient. III. Universidade Tecnológica Federal do Paraná - Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial. IV.Título.

CDD 22 -- 621.3

Biblioteca Central da UTFPR, Câmpus Curitiba

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba

Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial

Título da Dissertação Nº. ____

Sistema de Verificação de Localização com Antenas Direcionais Baseado em Teoria da Informação.

por

Marcos Eduardo Pivaro Monteiro.

Orientador: Prof. Dr. João Luiz Rebelatto
Coorientador: Prof. Dr. Richard Demo Souza

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de MESTRE EM CIÊNCIAS – Área de Concentração: Telecomunicações e Redes do Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial – CPGEI – da Universidade Tecnológica Federal do Paraná – UTFPR, às 14h do dia 27 de agosto de 2014. O trabalho foi aprovado pela Banca Examinadora, composta pelos professores doutores:

Prof. Dr. João Luiz Rebelatto
(Presidente – UTFPR)

Prof. Dr. Marcelo Eduardo Pellenz
(PUCPR)

Prof. Dr. Hermes Irineu Del Monego
(UTFPR)

Visto da coordenação:

Prof. Emilio Carlos Gomes Wille, Dr.
(Coordenador do CPGEI)

AGRADECIMENTOS

Gostaria de expressar meus agradecimentos a todos que, direta ou indiretamente, colaboraram para a realização deste trabalho.

à minha noiva, Cinthya, aos meus pais, João e Solange, e aos meus irmãos, pelo apoio, carinho e compreensão;

a João Luiz Rebelatto, que mostrou-me o caminho a ser tomado, realizando seu papel de orientador de forma exemplar;

a Richard Demo Souza, que com seu apoio ajudou a trilhar o melhor caminho;

a Ohara Kerusauskas Rayel, por ajudar-me a seguir sempre em frente.

RESUMO

MONTEIRO, M. E. P.. SISTEMA DE VERIFICAÇÃO DE LOCALIZAÇÃO COM ANTENAS DIRECIONAIS BASEADO EM TEORIA DA INFORMAÇÃO. 69 f. Dissertação – Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Nesta dissertação, o uso de antenas direcionais em sistemas de verificação de localização é analisado, considerando um cenário realista para redes veiculares. O objetivo é propor um método para a utilização das antenas direcionais nestes sistemas e verificar quais os benefícios proporcionados em termos de desempenho, que representa a capacidade em diferenciar usuários legítimos e maliciosos. Um sistema que utiliza o modelo de propagação log-normal é inicialmente estudado, seguido de uma analise das alterações necessárias para a utilização de um modelo mais realista. Utilizando este modelo, é demonstrado então como o uso de antenas direcionais pode ser introduzido no sistema, adicionando ao processo de verificação uma etapa adicional. Resultados numéricos são obtidos para verificar as expressões analíticas, seguido das comparações entre os desempenhos de cada um dos sistemas apresentados. Através destes resultados, é constatado que a utilização das antenas direcionais proporciona um aumento considerável no desempenho do sistema e, mesmo quando considerado apenas a etapa adicional de verificação, o desempenho é satisfatório. É feita também uma análise da influência do desvanecimento em pequena escala no sistema, demonstrando qual a relação entre o número de amostras e a porcentagem de erro no desempenho do esquema apresentado.

Palavras-chave: Sistema de Verificação de Localização, Antena Direcional, Teoria da Informação, Redes Veiculares Ad Hoc.

ABSTRACT

MONTEIRO, M. E. P.. INFORMATION-THEORETIC LOCATION VERIFICATION SYSTEM WITH DIRECTIONAL ANTENNAS. 69 f. Dissertação – Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

In this master thesis, a performance analysis of an information-theoretic location verification system using directional antennas is performed, considering a vehicular network scenario. Our goal is to develop a method using directional antennas to improve the system performance. First, a recently introduced scheme that uses a simple propagation model is studied, then it is described the modifications needed when a realistic propagation model is considered. Based on the described scheme, it is shown how the use of directional antennas can be introduced into the system, creating a new validation stage called directional verification. Numerical results are used to validate the analytical expressions, showing also the performance differences between the described systems. Using the obtained results, it is shown that the use of directional antennas increase the system performance and that, even when using only the directional verification stage, the performance is satisfactory. An analysis of the relation between the number of samples and the system's error percentage is also performed, when considered a small scale fading model.

Keywords: Location Verification System, Directional Antennas, Information Theory, Vehicular Ad Hoc Networks.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AoA	Ângulo de Chegada, do inglês *Angle-of-Arrival*
BS	Estação Base, do inglês *Base Station*
DA	Antena Direcional, do inglês *Directional Antenna*
DPVAT	Seguro de Danos Pessoais Causados por Veículos Automotores de Vias Terrestres
DV	Verificação Direcional, do inglês *Directional Verification*
FFA	Aproximação para Longas Distâncias, do inglês *Far Field Approximation*
FN	Falso Negativo
FP	Falso Positivo
GPS	Sistema de Posicionamento Global, do inglês *Global Positioning System*
IBGE	Instituto Brasileiro de Geografia e Estatística
IDC	Capacidade de Detecção de Intrusos, do inglês *Intrusion Detection Capability*
IDC	Capacidade de Detecção de Intrusos, do inglês *Intrusion Detection Capability*
ITS	Sistema de Transporte Inteligente, do inglês *Intelligent Transportation System*
LOS	Linha de Visada, do inglês *Line of Sight*
LVS	Sistema de Verificação de Localização, do inglês *Location Verification System*
LVS-DA	Sistema de Verificação de Localização com Antenas Direcionais
LVS-SLOS	Sistema de Verificação de Localização Utilizando o Modelo de Propagação LOS/OLOS
MA	Antena Principal, do inglês *Main Antenna*
MANET	Rede Móvel *Ad-Hoc*, do inglês *Mobile Ad Hoc Network*
NLOS	Sem Linha de Visada, do inglês *Non Line of Sight*
OLOS	Linha de Visada Obstruída, do inglês *Obstructed Line of Sight*
ONSV	Observatório Nacional de Segurança Viária
PC	Centro de Processamento, do inglês *Process Center*
pdf	Função Densidade de Probabilidade, do inglês *Probability Density Function*
ROC	Característica de Operação do Receptor, do inglês *Receiver Operating Characteristic*
RSS	Potência do Sinal Recebido, do inglês *Received Signal Strenght*
SA	Antena Secundária, do inglês *Secondary Antenna*
TDoA	Diferença de Tempo de Chegada, do inglês *Time-Difference-of-Arrival*
ToA	Tempo de Chegada, do inglês *Time-of-Arrival*
VANET	Rede Veicular *Ad-Hoc*, do inglês *Vehicular Ad Hoc Network*
VN	Verdadeiro Negativo
VP	Verdadeiro Positivo

LISTA DE SÍMBOLOS

K	número de estações base
θ_i^{BS}	posição da estação base i
u_i^{BS}	posição no eixo x da estação base i
v_i^{BS}	posição no eixo y da estação base i
ρ	largura ou comprimento da área
x	usuário legítimo $x = 0$ ou malicioso $x = 1$
y	usuário classificado como legítimo $y = 0$ ou como malicioso $y = 1$
θ^r	posição real do veículo
u^r	posição no eixo x do veículo
v^r	posição no eixo y do veículo
θ^c	posição alegada pelo veículo
u^c	posição alegada no eixo x do veículo
v^c	posição alegada no eixo y do veículo
H_0	hipótese o usuário ser legítimo
H_1	hipótese o usuário ser malicioso
D_0	hipótese do sistema identificar o usuário como legítimo
D_1	hipótese do sistema identificar o usuário como malicioso
α	taxa de falso positivo
β	taxa de falso negativo
Pr_0	probabilidade do usuário ser legítimo
Pr_1	probabilidade do usuário ser malicioso
$P(d_0)$	potência do sinal recebido a uma distância de referência d_0
d_0	distância de referência
d	distância entre o transmissor e o receptor
ω_{dB}	variável aleatória gaussiana com média zero e variância σ^2, que representa o sombreamento
σ^2	variância do sombreamento
γ	expoente da perda de percurso
γ_1	expoente da perda de percurso até a distância d_c
γ_2	expoente da perda de percurso entre a distância d_c e d
d_c	distância limiar do modelo de duplo declive
λ	comprimento de onda
h_t	altura da antena transmissora
h_r	altura da antena receptora
$\overline{P}(d)$	potência média recebida
$P_{\mathrm{LOS}}(d)$	potência do sinal recebido a uma distância d para um cenário com linha de visada
$P_{\mathrm{OLOS}}(d)$	potência do sinal recebido a uma distância d para um cenário de com linha de visada obstruída
σ_{LOS}	desvio padrão da RSS a uma distância d para um cenário com linha de visada
σ_{OLOS}	desvio padrão da RSS a uma distância d para um cenário de com linha de visada obstruída

h	envelope do canal
σ_p	desvio padrão do desvanecimento em pequena escala
θ	ângulo entre a antena e a posição real do usuário
$A(\theta)$	ganho da antena (dBi) na direção de θ
υ	parâmetro de sistema relacionado à atenuação da antena
θ_{3dB}	largura de feixe de meia potência
$A_{\max}$	atenuação máxima da antena
C_{id}	capacidade de detecção de intrusos
$I(X;Y)$	informação mútua entre a entrada e a saída do sistema
$H(X\|Y)$	entropia condicional da entrada dado que se conhece a saída do sistema
$H(X)$	entropia da entrada
B	probabilidade de existir um usuário malicioso nos dados observados
$F(m)$	teste estatístico do sistema de verificação de localização
T_F	limiar utilizado pelo sistema de verificação de localização
m	potências dos sinais recebidos pelas estações base referente ao sinal enviado pelo veículo
d_i^c	distância entre a posição alegada pelo usuário e a posição da estação base i
d_i^r	distância real entre o usuário e a estação base i
P_x	ajuste de potência utilizado pelo usuário malicioso para falsificar sua posição
d_i^r	distância entre a posição real do usuário e a posição da estação base i
$\bar{\mu}^c$	média calculada da potência recebida por todas as estações base para a posição onde o usuário afirma estar
μ_i^c	valor calculado da potência recebida pela estação base i para a posição onde o usuário afirma estar, desconsiderando o sombreamento
m_i	amostra da potência do sinal recebido referente a um usuário pela estação base i
Γ	função limiar da regra de decisão do LVS
$N(a,b)$	distribuição normal com média a e variância b
$\Pr(\mathrm{FP_{LVS}})$	probabilidade de falso positivo do sistema de verificação de localização
$\Pr(\mathrm{VP_{LVS}})$	probabilidade de verdadeiro positivo do sistema de verificação de localização
$K_{\min}$	número mínimo de estações base que devem identificar o usuário como malicioso para que ele seja considerado desta forma pelo sistema de verificação de localização
ς	módulo do ângulo máximo da antena direcional
D_m	atenuação na antena principal
D_{s_j}	atenuação na antena secundária j
j	número da antena secundária
D_{f_j}	diferença entre a potência da antena principal e a potência da antena secundária j
p	coeficiente de correlação
r	razão entre a posição no eixo y e a posição no eixo x da estação base
$\mathrm{Mod}(a,b)$	resto da divisão entre a e b
u	ângulo medido em graus
ξ	constante usada devido à conversão entre radianos e graus
θ_{desv_n}	ângulo para onde a antena n está apontada
Σ	matriz de covariância
μ	vetor das médias
$\Pr_{ant}(n)$	probabilidade de falso positivo quando a antena n é considerada a antena principal

$\Pr_{ang}(n,u)$	probabilidade de um ângulo específico
u_n	ângulo na antena n
$\Pr_{\mathrm{BS}}(\mathrm{FP})$	probabilidade de falso positivo de uma estação base

SUMÁRIO

1 INTRODUÇÃO

Veículos automotores são amplamente utilizados ao redor do mundo. Seja para o trabalho, lazer ou qualquer outra necessidade que exija locomoção, estes veículos estão sempre presentes. Nos últimos anos, a frota mundial de veículos cresceu consideravelmente e já passa de 1 bilhão de veículos [WARD 2011]. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), a frota brasileira de veículos já chegou a 65 milhões, com aproximadamente 1 veículo para cada 3 habitantes [IBGE 2013].

Com o aumento no número de veículos, tem-se o crescimento dos problemas relacionados à segurança, logística e mobilidade. Desses problemas, o maior é o da segurança, uma vez que ela está diretamente relacionada à vida. Dentre as causas que prejudicam a segurança, tem-se a imprudência dos motoristas, falta de manutenção nos veículos, problemas na via e outros. De acordo com o Observatório Nacional de Segurança Viária (ONSV) [ONSV 2014], as mortes por acidentes de carro superam as mortes por homicídios ou câncer, com 31,1 vítimas a cada 100 mil habitantes. Segundo o Seguro de Danos Pessoais Causados por Veículos Automotores de Vias Terrestres (DPVAT) [DPVAT 2014], foram contabilizadas 54,767 mil mortes e 444,206 mil sinistros por invalidez permanente em 2013.

Estes números demonstram que, apesar da utilização de veículos automotores ser essencial para a sociedade moderna, estes representam grande risco para os envolvidos. Para ajudar a combater estes e outros problemas, foi criado o conceito de Sistema de Transporte Inteligente (ITS, do inglês *Intelligent Transportation System*). Este sistema utiliza um conjunto de soluções relacionadas à eletrônica, comunicação sem fio e de tecnologia da informação aplicada ao transporte, para melhorar a mobilidade, produtividade e segurança nas vias.

Dentre as tecnologias utilizadas, tem-se a comunicação de veículos com outros veículos e com estações base. Para ajudar na segurança, controle e melhoria dos serviços disponíveis para os nós nas vias, criou-se as Redes Veiculares *Ad-Hoc* (VANETs, do inglês *Vehicular Ad Hoc Networks*). As VANETs são um tipo especial de Redes Móveis *Ad-Hoc* (MANETs, do inglês *Mobile Ad Hoc Network*), que são redes sem fio auto-configuráveis, não

necessitando de uma estrutura física, uma vez que cada nó atua como um roteador. Assim, estas redes podem mover-se em qualquer direção, sendo as redes constantemente reconfiguradas conforme os nós disponíveis no alcance dos membros conectados. Desta forma, cada nó da rede tem que, além de transferir suas próprias informações, retransmitir as informações de outros nós. Além disso, cada nó deve conter informações de roteamento relevantes sobre como transmitir as informações para determinados destinos. O conjunto destas características faz com que estas redes tenham uma topologia altamente dinâmica e autônoma.

No caso das VANETs, cada nó é um veículo capaz de retransmitir as informações de outros veículos da rede. Uma característica importante deste cenário é que, como os próprios veículos são capazes de retransmitir informações, veículos conectados a uma VANET são muitas vezes capazes de enviar informações mesmo quando não existe uma estrutura física na posição atual do veículo. Neste cenário, se o veículo estiver em uma área de sombra, ele pode transmitir sua informação para um segundo veículo. Este, por sua vez, pode retransmitir a informação para outro, até que a informação chegue a um veículo que esteja em uma área de cobertura, encaminhando assim a informação para uma estação base. Neste trabalho, será usado o termo Estação Base (BS, do inglês *Base Station*) para referenciar as estruturas ao longo da via capazes de receber e enviar para o destino final as informações recebidas dos veículos.

Como mencionado, pode-se dizer que o maior benefício trazido pelo ITS e pelas VANETs é a melhoria da segurança nas vias. Em um primeiro cenário, estes sistemas podem ser usados para evitar a colisão de veículos. Dentre os recursos disponíveis para evitar este tipo de situação, tem-se que o sistema pode avisar ao motorista sobre quaisquer situações de perigo na via. Mesmo no caso de uma eventual colisão, o veículo pode enviar uma informação com a sua posição e momento do acidente. Com estes dados, as autoridades responsáveis poderão enviar ambulâncias ou qualquer outro serviço necessário. Neste mesmo cenário, os veículos que receberem a informação do acidente poderão reenviar esta informação para outros veículos, alertando todos os motoristas na região sobre o evento e evitando assim novos acidentes.

Em um segundo cenário, caso um determinado veículo esteja com velocidade excessiva, esta informação poderá ser enviada para outros veículos e para as BSs. Os motoristas então serão alertados sobre o veículo em questão e, caso o excesso de velocidade não tenha uma justificativa plausível (como viaturas e ambulâncias), as autoridades competentes poderão interceptar o veículo evitando assim um possível acidente.

Em uma mesma via, estes sistemas podem auxiliar no envio de ajuda em situações onde um determinado automóvel apresenta defeito. Ainda que o motorista do veículo não tenha como solicitar ajuda diretamente, seu veículo pode informar ao ITS sobre a situação, acelerando

o processo de ajuda.

Outro cenário possível é quando uma ambulância, com uma emergência médica, precisa chegar até o hospital. Veículos no percurso desta ambulância poderão ser avisados, evitando colisões e facilitando o deslocamento. Assim como nos cenários descritos, existem inúmeras outras situações possíveis no qual pode-se facilmente visualizar os benefícios da utilização destes sistemas.

1.1 INTRODUÇÃO AO PROBLEMA

Apesar do ITS e das VANETs representarem potencial para melhoria da segurança e eficiência nas vias, é importante notar que estes sistemas são altamente dependentes das informações sobre o posicionamento dos veículos. Estas posições são normalmente obtidas pelo usuário através da utilização do Sistema de Posicionamento Global (GPS, do inglês *Global Positioning System*). Existem também outras técnicas para se obter a posição do veículo utilizando parâmetros como a Potência do Sinal Recebido (RSS, do inglês *Received Signal Strenght*), o Ângulo de Chegada (AoA, do inglês *Angle-of-Arrival*), o Tempo de Chegada (ToA, do inglês *Time-of-Arrival*) e a Diferença de Tempo de Chegada (TDoA, do inglês *Time-Difference-of-Arrival*) [Gezici 2008]. Embora úteis, a opção mais confiável ainda é o GPS, e as outras técnicas são muitas vezes utilizadas para melhorar a qualidade da posição obtida pelo GPS em situações específicas [Drawil e Basir 2010].

Como a posição dos veículos obtida por GPS é enviada pelo próprio veículo, o funcionamento adequado do sistema depende fortemente da legitimidade da posição alegada pelos nós. Assim, posições falsificadas informadas pelos usuários podem comprometer o sistema como um todo.

Uma forma de se resolver este problema é através do uso de um Sistema de Verificação de Localização (LVS, do inglês *Location Verification System*) [Leinmuller et al. 2006, Song et al. 2008, Yan et al. 2009, Yan e Weigle 2010, Abumansoor e Boukerche 2012], que tem o propósito de verificar se a posição informada pelo nó é legítima ou não. Assim, o LVS deve ter duas saídas básicas, as quais são geralmente conflitantes: *i)* uma baixa taxa de Falso Positivo (FP), definida como a situação onde o LVS de forma incorreta classifica um usuário legítimo como malicioso; e *ii)* uma alta taxa de Verdadeiro Positivo (VP), que representa a capacidade do LVS em classificar um usuário malicioso de forma correta.

Uma maneira tradicional de determinar se um usuário é malicioso ou não é configurar um limiar de operação para o LVS, levando ao *trade-off* entre maximizar o VP e minimizar

o FP [Yan et al. 2012]. Nesta abordagem, é possível encontrar um limiar que otimiza a performance do sistema dada uma determinada métrica. Existem diferentes formas de se encontrar este limiar [Xiao et al. 2006, Liu e Lin 2008]. Um possível método é de se procurar por um *trade-off* entre o VP e o FP de acordo com a curva de Característica de Operação do Receptor (ROC, do inglês *Receiver Operating Characteristic*) [Xiao et al. 2006]. Esta curva é uma relação entre as taxas de VP e FP do sistema e cada ponto da curva representa o desempenho de um ponto de operação específico. Quando comparado o desempenho de dois sistemas através das curvas ROC para diversos pontos de operação, se as curvas ROC não se cruzarem, então o melhor desempenho é aquele representado pela curva que está sempre acima. Entretanto, se elas cruzarem entre si, então a curva ROC não é uma métrica ideal para comparar os desempenhos [Chen et al. 2010]. Além disso, este método não determina de forma direta qual é o limiar otimizado para o sistema [Gu et al. 2005].

Outra abordagem é otimizar o limiar do LVS através do uso de dados previamente obtidos de forma empírica [Liu e Lin 2008], que minimiza funções específicas das duas taxas (FP e VP) para encontrar o limiar otimizado. Embora esta abordagem seja válida em diversos cenários, esta técnica não é viável em cenários como longas rodovias pois as medições variam de acordo com as circunstâncias das vias [Yan et al. 2012]. Uma alternativa é o uso de um método que utiliza o teste de hipótese Bayesiano [Chen et al. 2010], mas este método é subjetivo, uma vez que é necessário que seja associado custos para cada tipo de classificação incorreta.

Em [Yan et al. 2014], um LVS baseado em RSS e teoria da informação foi proposto. Este sistema considera o conceito de informação mútua e entropia para definir um método capaz de fazer o *trade-off* entre as taxas de FP e VP, utilizando a métrica de desempenho Capacidade de Detecção de Intrusos (IDC, do inglês *Intrusion Detection Capability*) apresentada em [Gu et al. 2005]. Quanto maior for a capacidade do LVS em classificar corretamente um usuário como malicioso ou legítimo, maior será o valor do IDC. Entretanto, mesmo considerando um limiar que maximiza o valor do IDC, o modelo de propagação de larga escala considerado em [Yan et al. 2012, Yan et al. 2014] é simplificado, e não representa de forma fiel a RSS recebida pelas BSs em uma VANET [Abbas et al. 2012].

Neste trabalho, primeiro é adaptado o LVS proposto em [Yan et al. 2014] para usar o modelo de propagação em larga escala para VANETs apresentado em [Abbas et al. 2012]. Em seguida, é demonstrado como o uso de Antenas Direcionais (DAs, do inglês *Directional Antennas*) pode melhorar o desempenho do sistema. Este novo esquema, chamado de LVS-DA, acrescenta uma nova etapa anterior à checagem do LVS, no qual o nó é assumido como malicioso ou legítimo utilizando apenas as informações obtidas através das DAs.

A fim de não só validar, mas possibilitar a fácil utilização das antenas no LVS, expressões analíticas para se encontrar a performance do sistema foram obtidas para os cenários onde cada BS tem duas, três e quatro DAs. Conforme demonstrado neste trabalho, o esquema proposto tem um desempenho superior aos outros modelos analisados.

1.2 MOTIVAÇÃO

Problemas relacionados aos transportes são de grande importância para a sociedade moderna. Na busca de melhorá-los, soluções como o ITS e as VANETs foram propostas. Como estes sistemas dependem de forma significativa das posições informadas pelos nós, tem-se a necessidade de um sistema que valide as posições alegadas pelos usuários. Para isto, foram criados os LVSs, que têm como objetivo determinar se a posição informada é válida ou não, os benefícios do aumento no desempenho dos LVSs são claros, ajudando a melhorar a segurança nas vias e, como consequência, resultando em um transporte melhor para todos.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Melhorar o desempenho de um LVS através da utilização de antenas direcionais, considerando modelo de propagação realista.

1.3.2 OBJETIVOS ESPECÍFICOS

- Verificar como o LVS baseado em teoria da informação se comporta utilizando um modelo de propagação realista, através da construção de expressões analíticas que representem as alterações no sistema;
- Definir como utilizar as DAs em um LVS para melhorar o desempenho do sistema e elaborar expressões analíticas para este modelo;
- Comparar os resultados analíticos com numéricos, para confirmar a validade das expressões;
- Apresentar graficamente uma comparação do desempenho dos sistemas apresentados com um número variável de BSs.

1.4 ESTRUTURA DO DOCUMENTO

O Capítulo 2 apresenta o modelo de sistema utilizado, descrevendo os principais conceitos para a elaboração das ferramentas de avaliação dos benefícios trazidos em se utilizar DAs com um modelo de propagação realista. Conceitos preliminares relacionados ao LVS também são apresentados.

No Capítulo 3 é apresentada uma análise de como a utilização de DAs nas BSs pode contribuir para a melhoria no desempenho do LVS. Primeiro, o capítulo traz informações sobre o funcionamento do LVS utilizando um modelo de propagação realista para VANETs. Em seguida, é apresentado como DAs podem ser usadas para aprimorar o desempenho do sistema.

No Capítulo 4, os resultados analíticos obtidos para o esquema apresentado são comparados com resultados numéricos, que demonstram a eficiência da utilização das DAs no sistema. Como o LVS descrito considera apenas o modelo de propagação em larga-escala, é demonstrado também as porcentagens de erro geradas quando considerado também o efeito da propagação em pequena escala para um número variável de amostras. Por fim, o Capítulo 5 apresenta as conclusões finais deste trabalho.

2 PRELIMINARES

2.1 MODELO DO SISTEMA

Neste trabalho, é considerada uma rede veicular composta por múltiplos veículos (legítimos e maliciosos) e K BSs fixas, em que a posição da i-ésima BS ($i \in \{1,\ldots,K\}$) é definida como $\theta_i^{BS} = (u_i^{BS}, v_i^{BS}) \in \mathbb{R}$ com distribuição uniforme em uma área quadrada de $\rho \times \rho$ m^2, de acordo com o ilustrado na Figura 2.1. É assumido que os veículos conhecem sua própria posição (obtida por GPS, por exemplo), assim como a posição de todas as BSs. Como [Yan et al. 2014, Abbas et al. 2012], este trabalho também assume que os veículos estão trafegando por uma rodovia.

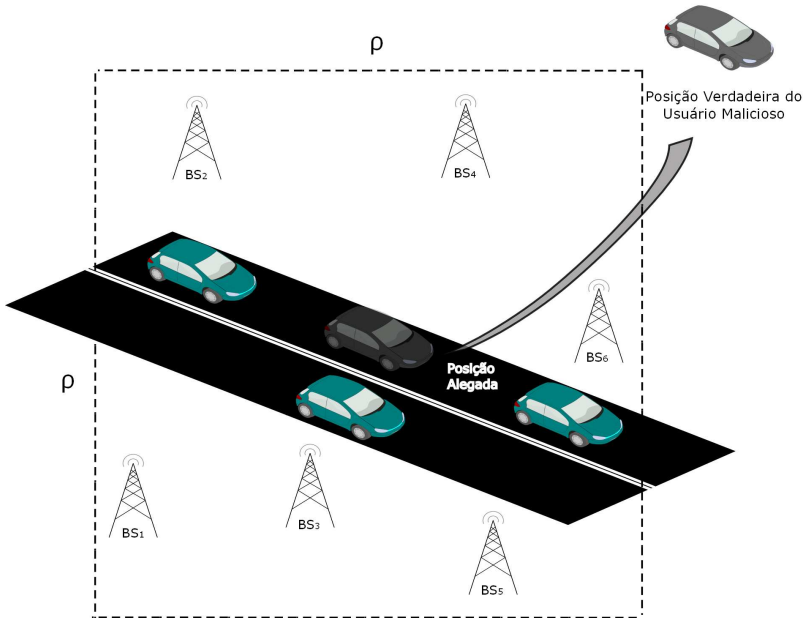

Figura 2.1: Modelo de Sistema para $K = 6$ BSs.

Para o LVS considerado, as informações de entrada (veículos que serão verificados) são representadas por variáveis binárias $X = x$, $x \in \{0,1\}$, em que $x = 0$ representa o usuário legítimo e $x = 1$ representa o usuário malicioso. Da mesma forma, a saída do LVS é indicada por variáveis aleatórias $Y = y$, $y \in \{0,1\}$, onde $y = 0$ e $y = 1$ indica que o sistema classificou,

respectivamente, o usuário como legítimo ou como malicioso. Para cada nó, $\theta^r = (u^r , v^r) \in \mathbb{R}$ representa sua posição real e $\theta^c = (u^c , v^c) \in \mathbb{R}$ representa a posição alegada pelo usuário.

Assim, H_0 e H_1 indicam as hipóteses do usuário ser, respectivamente, legítimo ou malicioso. Da mesma forma, D_0 e D_1 indicam as hipóteses do sistema identificar, respectivamente, que o usuário é legítimo ou malicioso. Este modelo é representado na Figura 2.2. Assim, $\alpha = \Pr(D_1|H_0)$ corresponde à taxa de FP e $\beta = \Pr(D_0|H_1)$ é a taxa de FN. A Tabela 2.1 apresenta de forma resumida a definição da taxa de FP e FN, bem como seus complementos (verdadeiro negativo - VN; verdadeiro positivo - VP).

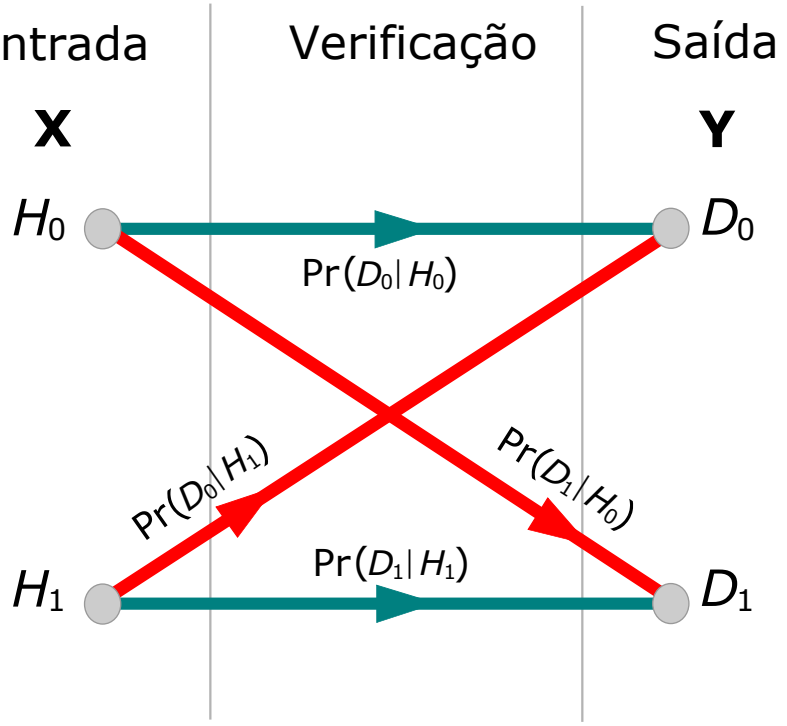

Figura 2.2: Modelo de decisão do sistema.

Tabela 2.1: Descrição das Taxas Utilizadas pelo Sistema

	Usuário Legítimo	Usuário Malicioso
Considerado Legítimo	$\text{VN} = (1-\alpha) = \Pr(D_0\|H_0)$	$\text{FN} = \beta = \Pr(D_0\|H_1)$
Considerado Malicioso	$\text{FP} = \alpha = \Pr(D_1\|H_0)$	$\text{VP} = (1-\beta) = \Pr(D_1\|H_1)$

O funcionamento do sistema está descrito nos passos a seguir, juntamento com as principais suposições realizadas neste trabalho:

1. O usuário (legítimo ou malicioso) informa sua localização alegada para $K \geq 2$ BSs (não necessariamente alinhadas), que estão dentro de seu alcance de comunicação. Uma das BSs será a estação que fará o processamento e é referida como Centro de Processamento

(PC, do inglês *Process Center*), sendo que as outras BSs devem enviar as informações para o PC;

2. É assumido que todos os usuários (incluindo os usuários maliciosos) conhecem as posições das BSs;

3. O usuário legítimo difunde sua posição real θ^r e o usuário malicioso envia uma posição falsa θ^c;

4. O usuário malicioso pode ajustar sua potência de transmissão de forma a alterar a RSS por todas as BSs;

5. É assumido que existe uma probabilidade conhecida do usuário ser legítimo, dada por $\Pr_0 = \Pr(x = 0)$. A probabilidade do usuário ser malicioso é dada por $\Pr_1 = B = 1 - \Pr_0$.

2.1.1 MODELO DE AMEAÇA

Inicialmente, o sistema deve ser capaz de identificar usuários maliciosos que estão em qualquer posição. O problema com esta abordagem é que, na medida que a posição real do usuário malicioso se aproxima da posição falsificada, a taxa de detecção tende a diminuir, aproximando-se de zero. Desta forma, assim como observado em [Yan et al. 2012, Yan et al. 2014], é considerado que o usuário malicioso está a uma distância mínima de sua posição alegada. Desta forma, é assumido que o usuário malicioso está fora da rodovia a uma distância maior que a distância média entre as BSs. Esta consideração é natural, uma vez que é improvável que o usuário malicioso queira falsificar uma posição próxima a sua posição real.

Para que seja possível uma análise deste modelo de ameaça, a exemplo de [Yan et al. 2014], neste trabalho considera-se o modelo de Aproximação para Longas Distâncias (FFA, do inglês *Far Field Approximation*). Nesta aproximação, considera-se que a distância do usuário malicioso para a rodovia é longe o suficiente para que todas as RSSs recebidas pelas BSs de um usuário malicioso sejam aproximadamente iguais. Assim, os sinais transmitidos pelo usuário malicioso são recebidos com uma potência aproximadamente igual por todas as BSs. Embora na prática esta aproximação não seja exata, com ela é possível se ter uma boa estimativa do desempenho do sistema. É importante perceber que diferenças na potência do sinal recebido entre as BSs de um usuário malicioso irá facilitar a detecção do usuário, uma vez que estas diferenças não irão representar as diferenças que ocorrem se ele estivesse na posição alegada e, desta forma, pode-se dizer que a aproximação de FFA, utilizada para tornar os cálculos mais viáveis, favorece o usuário malicioso.

2.2 MODELOS DE PROPAGAÇÃO

Os modelos de propagação são usados para estimar qual a atenuação causada pelos diversos efeitos de um canal sem fio na comunicação entre dois nós. Estes modelos são de extrema importância para o LVS apresentado uma vez que, através deles, é possível prever qual a potência do sinal recebido pelas BSs de acordo com a posição do usuário. Enquanto os modelos de propagação em larga escala tratam dos efeitos causados pelo sombreamento, pela distância entre o transmissor e o receptor e pela frequência de portadora, entre outros fatores, enquanto os efeitos em pequena escala tratam das alterações devido aos diversos percursos percorridos pelo sinal. Nesta seção, dois modelos de larga escala e um modelo de pequena escala são apresentados. É importante notar que, enquanto os modelos em larga escala representam a potência média recebida e são utilizados diretamente, o modelo em pequena escala representa a potência instantânea recebida e é utilizado apenas para encontrar a porcentagem de erro no desempenho estimado do sistema, conforme mostrado no Capítulo 4.

2.2.1 LARGA ESCALA

Neste trabalho, as RSSs recebidas por K BSs são usadas para determinar se o usuário é legítimo ou não. Como o sistema deve ser capaz de prever qual a potência recebida por cada BS, é necessário a utilização de um modelo de propagação que seja capaz de simular as variações na RSS causadas pelo canal. Nos modelos de propagação em larga escala utilizados nesta dissertação, a potência do sinal recebido é afetada pela distância entre a BS e o nó, e pela presença de obstáculos. Com relação à distância, considera-se a atenuação causada pela dissipação da potência do sinal irradiada pelo transmissor. Esta atenuação é chamada de perda de percurso. Outra característica considerada nos modelos utilizados é o sombreamento, que é a atenuação causada devido a obstáculos entre o transmissor e o receptor, e que absorvem, refletem, espalham e causam a difração do sinal transmitido [Goldsmith 2005].

2.2.1.1 LOG-NORMAL

Uma das formas de se estimar a RSS é através do modelo estatístico de log-normal, que descreve a perda de percurso causada pela distância entre o transmissor e o receptor. Desta forma, a potência do sinal recebido pode ser calculada como [Goldsmith 2005, Rappaport 2001]

$$P(d) = P(d_0) - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) + \omega_{dB}, \tag{2.1}$$

onde $P(d_0)$ é a RSS a uma distância de referência d_0, d é a distância entre o transmissor e o receptor, ω_{dB} representa o sombreamento, caracterizado como uma variável aleatória Gaussiana com média zero e variância σ^2, e γ é o expoente da perda de percurso, que pode ser ajustado conforme o cenário considerado. Este foi o modelo utilizado em [Yan et al. 2014].

2.2.1.2 DUPLO DECLIVE LOS/OLOS

No esquema proposto nesta dissertação, é utilizado o modelo de propagação em larga escala apresentado em [Abbas et al. 2012], que é direcionado para o uso em VANETs e foi obtido a partir de medidas reais em ambientes urbanos e em rodovias. Este modelo é baseado no modelo de duplo declive proposto em [Cheng et al. 2007], adicionando o impacto do sombreamento causado por outros veículos. Desta forma, foi introduzido o conceito de Linha de Visada Obstruída (OLOS, do inglês *Obstructed Line of Sight*), além das possibilidades de Linha de Visada (LOS, do inglês *Line of Sight*) e Sem Linha de Visada (NLOS, do inglês *Non Line of Sight*). Este modelo é referenciado como LOS/OLOS, sendo a potência recebida a uma distância d do transmissor dada por

$$P(d) = \begin{cases} P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d}{d_0}\right) + \omega_{dB}, & \text{se } d_0 \leq d \leq d_c \\ P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d_c}{d_0}\right) - 10\gamma_2 \log_{10}\left(\frac{d}{d_c}\right) + \omega_{dB} & \text{se } d > d_c, \end{cases} \tag{2.2}$$

em que γ_1 e γ_2 são os expoentes da perda de percurso. De acordo com [Abbas et al. 2012], o valor da distância limiar d_c em (2.2) é dado por

$$d_c = \frac{4h_t h_r}{\lambda} - \frac{\lambda}{4}, \tag{2.3}$$

em que λ é o comprimento de onda e h_t e h_r são, respectivamente, as alturas das antenas transmissora e receptora. Os valores de γ_1, γ_2 e σ^2 são definidos de acordo com a Tabela 2.2, que foi obtida empiricamente em [Abbas et al. 2012] considerando uma frequência de portadora de 5.9 GHz de acordo com o padrão IEEE 802.11p. No modelo de LOS/OLOS , as probabilidades de ocorrência de LOS e OLOS são funções da distância d, e podem ser escritas como

$$\Pr(\text{LOS}|d) = \exp(-d/145), \tag{2.4a}$$

$$\Pr(\text{OLOS}|d) = 1 - \Pr(\text{LOS}|d). \tag{2.4b}$$

Desta forma, a potência média recebida $\bar{P}(d)$ é estimada por

$$\bar{P}(d) = \Pr(\text{LOS}|d) P_{\text{LOS}}(d) + \Pr(\text{OLOS}|d) P_{\text{OLOS}}(d), \tag{2.5}$$

Tabela 2.2: Parâmetros para o modelo LOS/OLOS.

	γ_1	γ_2	$P(d_0)$	σ
LOS	1.66	2.88	-66.1	3.95
OLOS	1.66	3.18	-76.1	6.12

onde $P_{\mathrm{LOS}}(d)$ e $P_{\mathrm{OLOS}}(d)$ são, respectivamente, as RSSs a uma distância d para cenários de LOS e OLOS, obtidas da equação (2.2). Da mesma forma, o desvio padrão médio é dado por

$$\overline{\sigma}(d) = \Pr(\mathrm{LOS}|d)\sigma_{\mathrm{LOS}} + \Pr(\mathrm{OLOS}|d)\sigma_{\mathrm{OLOS}}, \tag{2.6}$$

onde σ_{LOS} e σ_{OLOS} são, respectivamente, os desvios padrão a uma distância média d para cenários de LOS e OLOS, obtidos da Tabela 2.2. Embora a potência média recebida descrita pela equação (2.5) possa ser utilizada pelo LVS, esta deve ser usada apenas quando não se conhece o estado LOS ou OLOS do usuário. Uma alternativa é utilizar diretamente a equação (2.2), identificando previamente se o usuário encontra-se em LOS ou não. Uma vez que o modelo tem valores diferentes para o desvio padrão do sombreamento em LOS e OLOS, é possível se obter o estado atual do usuário comparando o desvio padrão médio com os dois desvios apresentados na Tabela 2.2, selecionando assim o estado que mais se aproxima do desvio apresentado.

A Figura 2.3 faz a comparação entre o modelo de propagação de log-normal utilizado em [Yan et al. 2014], o modelo de duplo declive apresentado em [Cheng et al. 2007] e os modelos de LOS, OLOS e LOS/OLOS apresentados em [Abbas et al. 2012] considerando uma frequência de portadora de 5.9 GHz. Note que, para o modelo LOS/OLOS, é utilizada a equação 2.5 para o cálculo do ganho.

2.2.2 PEQUENA ESCALA

Além dos efeitos causados pela propagação do sinal em larga escala, a RSS é afetada também pelas variações em pequena escala. O desvanecimento em pequena escala é causado pela dispersão temporal devido aos diversos percursos percorridos pelo sinal até o receptor. Esta é uma modelagem estatística e descreve a potência instantânea recebida, sendo descrita por uma Função Densidade de Probabilidade (pdf, do inglês *Probability Density Function*). Embora os conceitos apresentados nesta subseção não entrem diretamente nas equações relacionadas ao LVS proposto, eles são de importância para determinar a relação entre o número de amostras da RSS e a porcentagem de erro no desempenho estimado do sistema.

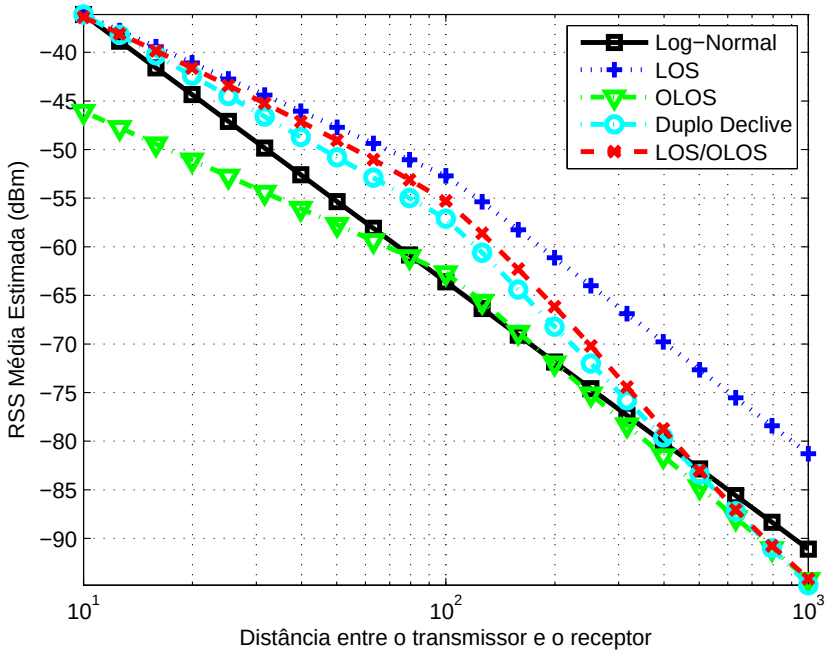

Figura 2.3: RSS média estimada para os modelos de propagação apresentados em função da distância, com $\omega_{dB} = 0$.

2.2.2.1 RAYLEIGH

O desvanecimento Rayleigh é usado em cenários onde o sinal pode ser considerado disperso entre o transmissor e receptor. Desta forma, não existe um caminho do sinal que seja dominante, e um modelo estatístico é necessário para se determinar a natureza geral do canal. Assim, este modelo descreve um cenário onde a propagação por multi percurso é predominante, não existindo LOS entre o transmissor e o receptor. Com estas considerações, tem-se que o desvanecimento Rayleigh por ser descrito pela pdf [Goldsmith 2005]

$$\Pr(h) = \frac{h}{\sigma_p^2} e^{-\frac{h^2}{2\sigma_p^2}}, \tag{2.7}$$

onde h é o envelope do canal e σ_p é o desvio padrão do desvanecimento em pequena escala.

2.3 ANTENAS DIRECIONAIS (DA)

Neste trabalho, sugere-se a utilização de antenas direcionais para melhorar o desempenho do sistema. Antenas direcionais utilizadas na recepção de sinais têm a característica de obter um ganho maior quando o ângulo entre o sinal recebido e a direção da antena aproxima-se de zero, e esta atenuação depende do padrão de ganho da antena. Assim,

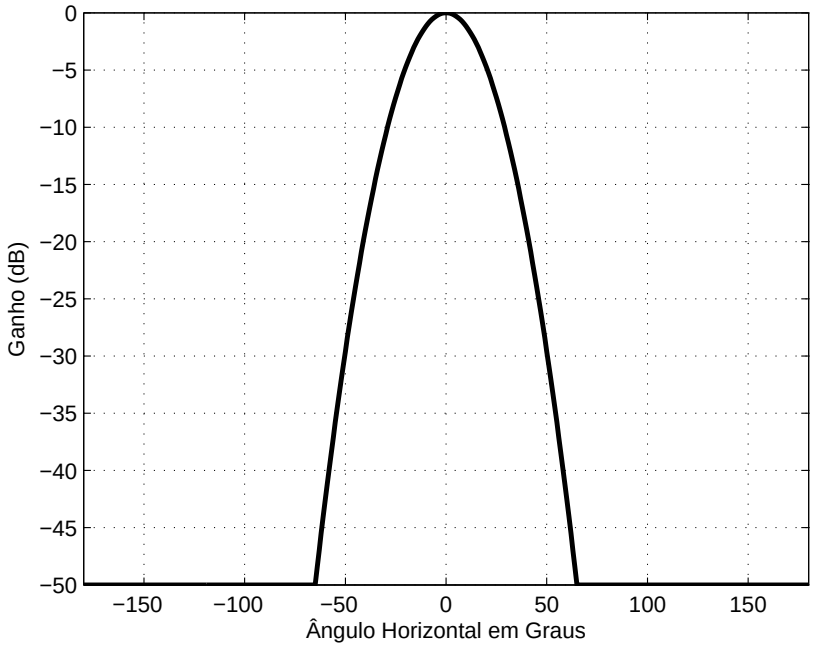

Figura 2.4: Atenuação da antena em função do ângulo.

é utilizado o padrão de ganho da antena dado por [Raman et al. 2011]

$$A(\theta) = -\min\left(\upsilon\left(\frac{\theta}{\theta_{3dB}}\right)^2, A_{\max}\right), \tag{2.8}$$

onde θ é o ângulo entre a antena e a posição real do usuário, $A(\theta)$ é o ganho da antena (dBi) na direção de θ, υ é um parâmetro de sistema que pode ser ajustado conforme necessário, θ_{3dB} é a largura de feixe de meia potência e $A_{\max}$ é a atenuação máxima. Um exemplo com $\upsilon = 12$ é apresentado na Figura 2.4.

2.4 SISTEMA DE VERIFICAÇÃO DE LOCALIZAÇÃO BASEADO EM TEORIA DE INFORMAÇÃO (LVS)

Com o aumento da utilização das posições dos usuários em redes sem fios, e com a constante utilização das posições obtidas pelo nó nestas aplicações, torna-se necessário verificar se as posições informadas pelos usuários são verdadeiras ou não. Neste aspecto, é importante a utilização de um sistema que tenha seu desempenho otimizado, uma vez que a classificação incorreta dos usuários pode ter consequências graves, como é o caso nas VANETs. Desta forma, nesta seção é apresentado o LVS baseado na teoria da informação proposto em [Yan et al. 2014] que, com o objetivo de identificar se as posições informadas são verdadeiras, classifica cada usuário como malicioso ou legítimo. Um LVS deve ter uma alta taxa de VP e, ao mesmo

tempo, uma baixa taxa de FP.

Nesta seção, a descrição do LVS é organizada da seguinte forma:

1. É feita uma análise do parâmetro de desempenho utilizado pelo sistema, que é baseado em teoria da informação;
2. Apresenta-se uma regra de decisão que maximize a informação mútua entre a entrada e a saída do sistema;
3. Utilizando como base a RSS, é descrito o funcionamento do LVS.

2.4.1 CAPACIDADE DE DETECÇÃO DE INTRUSOS (IDC)

Uma vez que taxas de VP e FP são conflitantes, é necessário se obter uma métrica que, baseada nestas duas taxas, possa medir a eficiência do LVS. Utilizando conceitos de teoria da informação, em [Gu et al. 2005] foi proposta a métrica Capacidade de Detecção de Intrusos (IDC, do inglês *Intrusion Detection Capability*), que é definida como

$$C_{id} = \frac{I(X;Y)}{H(X)}, \tag{2.9}$$

sendo C_{id} a capacidade de detecção de intrusos, $I(X;Y) = H(X) - H(X|Y)$ a informação mútua entre a entrada e a saída do sistema, $H(X|Y)$ a entropia condicional da entrada dado que se conhece a saída, e $H(X)$ a entropia da entrada, que são definidas como [Gu et al. 2005]

$$\begin{aligned} H(X) &= -\sum_{x} \Pr(X)\log_2 \Pr(X) \\ &= -B\log_2 B - (1-B)\log_2(1-B); \end{aligned} \tag{2.10a}$$

$$\begin{aligned} H(X|Y) = &-\sum_{x}\sum_{y} \Pr(X)\Pr(Y|X)\log_2\left(\frac{\Pr(X)\Pr(Y|X)}{\Pr(Y)}\right) \\ = &-B(1-\beta)\log_2\left(\frac{B(1-\beta)}{B(1-\beta)+(1-B)\alpha}\right) \\ &-B\beta\log_2\left(\frac{B\beta}{B\beta+(1-B)(1-\alpha)}\right) \\ &-(1-B)(1-\alpha)\log_2\left(\frac{(1-B)(1-\alpha)}{(1-B)(1-\alpha)+B\beta}\right) \\ &-(1-B)\alpha\log_2\left(\frac{(1-B)\alpha}{(1-B)\alpha+B(1-\beta)}\right), \end{aligned} \tag{2.10b}$$

onde B é a probabilidade de existir um usuário malicioso nos dados observados e que, conforme [Yan et al. 2014], é um parâmetro de sistema previamente definido. Conforme

descrito em [Gu et al. 2005], a informação mútua mede a redução da incerteza relacionada à entrada do sistema ao se conhecer a saída. Assim, a informação mútua é normalizada utilizando a entropia da entrada, fazendo com que o valor do parâmetro C_{id} varie entre 0 e 1. Utilizando estes conceitos, o LVS deve ser configurado de forma que os valores de α e β sejam aqueles que maximizem o valor do C_{id}.

2.4.2 REGRA DE DECISÃO

Para o LVS analisado, é utilizada uma regra de decisão para classificar o usuário como legítimo (a saída do sistema é D_0 de acordo com o ilustrado na Figura 2.2) ou malicioso (saída D_1). Desta forma, tem-se uma comparação entre um teste estatístico, $F(m)$, e um limiar correspondente T_F, na forma

$$F(m) \underset{D_0}{\overset{D_1}{\gtrless}} T_F. \tag{2.11}$$

Para um dado valor de $F(m)$, é necessário encontrar um valor de T_F que maximize a informação mútua $I(X;Y)$. Ainda sim, precisa-se definir $F(m)$ de forma que este também maximize a informação mútua. Baseado no lema de Neyman-Pearson [Neyman e Pearson 1933], em [Yan et al. 2014] foi mostrado que a forma funcional de $F(m)$ é dada por $\Lambda(m)$, definida como

$$\Lambda(m) = \frac{\Pr(m|H_1)}{\Pr(m|H_0)}, \tag{2.12}$$

onde m representa o vetor $m = [m_1, m_2, ...m_K]$ de todas as RSSs obtidas por K BSs do sinal enviado pelo veículo, $\Pr(m|H_1)$ e $\Pr(m|H_0)$ são, respectivamente, as funções de verossimilhança para os usuários maliciosos e legítimos, considerando a potência recebida por todas as BSs. Estas funções estão descritas em detalhes na próxima subseção.

2.4.3 DESCRIÇÃO DO SISTEMA UTILIZANDO A POTÊNCIA DO SINAL RECEBIDO

Para que seja possível descrever corretamente o LVS em questão, é necessário determinar as funções de verossimilhança para o usuário legítimo e malicioso. Assim como no LVS proposto neste trabalho, embora seja possível construir um sistema utilizando outras métricas, como ToA ou TdoA, é preferível formular o sistema utilizando a RSS, visto que esta pode ser facilmente obtida, enquanto outros parâmetros dependem do hardware utilizado. No LVS analisado nesta seção, seguindo [Yan et al. 2014], é assumido que tanto as BSs como os usuários têm apenas uma antena cada. Desta forma, o sinal enviado pelo veiculo será propagado em todas as direções, não podendo ser amplificado ou atenuado para apenas um conjunto de

ângulos.

O sistema de [Yan et al. 2014] utiliza o modelo de log-normal descrito na Subseção 2.2.1.1 para calcular as RSSs recebidas de veículos legítimos (H_0) e maliciosos (H_1). Assim, é possível definir a realização da RSS para o usuário legítimo como

$$h_0(d_i^c) = P(d_0) - 10\gamma \log_{10}\left(\frac{d_i^c}{d_0}\right) + \omega_{dB}, \tag{2.13}$$

sendo d_i^c a distância entre a posição alegada pelo usuário e a posição da BS, e o valor de ω_{dB} varia de acordo com a BS. Note que para o caso do usuário legítimo, a distância para a estação base, que é calculada usando a posição alegada pelo usuário, é igual a distância real d_i^r. A distância entre a i-ésima BS e a posição alegada pelo usuário pode ser obtida utilizando

$$d_i^c = \sqrt{(u^c - u_i^{BS})^2 + (v^c - v_i^{BS})^2}. \tag{2.14}$$

Para o usuário malicioso, este tenta configurar sua potência de modo que o sinal coletado pelas BSs seja o mais semelhante possível com o sinal coletado se ele estivesse num local que afirma estar. Desta forma, a potência recebida do usuário malicioso é dada por

$$h_1(d_i^r) = P(d_0) + P_x - 10\gamma \log_{10}\left(\frac{d_i^r}{d_0}\right) + \omega_{dB}, \tag{2.15}$$

sendo P_x o ajuste de potência utilizado pelo usuário malicioso para falsificar sua posição e d_i^r a distância calculada entre a posição real do usuário θ^r e a posição da BS θ_i^{BS}.

Conforme descrito em [Yan et al. 2014], é possível considerar uma situação extrema (e favorável ao nó malicioso) onde o usuário ilegítimo está longe o suficiente de todas as BSs de forma que as estações recebam uma potência de sinal aproximadamente igual. Esta abordagem foi descrita na Subseção 2.1.1 e é chamada de FFA, sendo utilizada também no esquema proposto por este trabalho. De forma geral, o usuário malicioso irá tentar configurar P_x de modo a evitar sua detecção, alterando as medições feitas pelas BSs. Conforme descrito em [Yan et al. 2014], o valor otimizado do ponto de vista do usuário malicioso para a potência recebida pelas BSs é definido como

$$h_1(d_i^c) = \bar{\mu}^c + \omega_{dB}, \tag{2.16}$$

sendo $\bar{\mu}^c$ a média calculada da potência recebida por todas as BSs para a posição onde o usuário afirma estar. Esta média é dada por

$$\bar{\mu}^c = \frac{1}{K}\sum_{i=1}^{K} \mu_i^c, \tag{2.17}$$

sendo μ_i^c o valor calculado da potência recebida pela BS i para a posição onde o usuário afirma estar, desconsiderando o sombreamento. Este valor é dado por

$$\mu_i^c = P(d_0) - 10\gamma \log_{10}\left(\frac{d_i^c}{d_0}\right). \tag{2.18}$$

Como tanto $h_1(d_i^c)$ quanto $h_0(d_i^c)$ variam apenas conforme o sombreamento ω_{dB}, que tem uma distribuição normal, ambas as variáveis também têm distribuição normal. Assumindo que as medições das RSSs no vetor m por todas as BSs sejam independentes umas das outras, pode-se definir a função de verossimilhança para o usuário legítimo como [Yan et al. 2014]

$$\begin{aligned} \Pr(m|H_0) &= \prod_{i=1}^{K} \Pr(m_i|H_0) \\ &= \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma} \exp\left(\frac{-(m_i-\mu_i^c)^2}{2\sigma^2}\right), \end{aligned} \tag{2.19}$$

sendo m_i a potência do sinal recebido pela BS i. Assim como para o usuário legítimo, deve-se definir a função para o usuário ilegítimo. Utilizando a FFA, pode-se definir a função de verossimilhança para um usuário ilegítimo como

$$\Pr(m|H_1) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma} \exp\left(\frac{-(m_i-\bar{\mu}^c)^2}{2\sigma^2}\right). \tag{2.20}$$

Utiliza-se então estas duas funções para se formar um teste de comparação capaz de identificar se o usuário é legítimo H_0 ou malicioso H_1. Assim, substituindo (2.19) e (2.20) em (2.12), tem-se que

$$\Lambda(m) = \frac{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\bar{\mu}^c)^2}{2\sigma^2}\right)}{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\mu_i^c)^2}{2\sigma^2}\right)}. \tag{2.21}$$

Para definir um teste de comparação, substitui-se T_F por T_Λ na equação (2.11), resultando em

$$\Lambda(m) = \frac{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\bar{\mu}^c)^2}{2\sigma^2}\right)}{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\mu_i^c)^2}{2\sigma^2}\right)} \underset{D_0}{\overset{D_1}{\gtrless}} T_\Lambda. \tag{2.22}$$

Desta forma, este teste é uma comparação entre as duas funções de verossimilhança, verificando quantas vezes mais provável um usuário está na distribuição de H_1 do que de na distribuição de H_0. Com a equação (2.22) e utilizando de dados empíricos, pode-se encontrar o desempenho do sistema para um dado valor de T_Λ. Para encontrar o desempenho de forma analítica, é necessário encontrar a média e a variância da distribuição para o usuário legítimo e ilegítimo, reescrevendo

a equação (2.22) como

$$F(m) \underset{D_0}{\overset{D_1}{\gtrless}} \Gamma, \tag{2.23}$$

sendo Γ e $F(m)$ duas funções que devem ser determinadas. Com base na equação (2.22), tirando o ln dos dois lados da função e reorganizando os termos, pode-se reescrever as funções como

$$F(m) = \sum_{i=1}^{K} m_i(\bar{\mu}^c - \mu_i^c), \tag{2.24}$$

$$\Gamma = \frac{1}{2}\left(2\sigma^2 ln T_\Lambda - \sum_{i=1}^{K}((\mu_i^c)^2 - (\bar{\mu}^c)^2)\right). \tag{2.25}$$

Com base nas equações (2.24) e (2.19) tem-se que, para o usuário legítimo, a pdf $\Pr(F(m)|H_0)$ tem distribuição normal, e é dada por

$$\Pr(F(m)|H_0) = N\left(\sum_{i=1}^{K}\mu_i^c(\bar{\mu}^c - \mu_i^c), \sum_{i=1}^{K}(\bar{\mu}^c - \mu_i^c)^2\sigma^2\right), \tag{2.26}$$

onde $N(a,b)$ representa uma distribuição normal com média a e variância b. Para o usuário malicioso, considerando as equações (2.24) e (2.20), pode-se ver que a pdf $\Pr(F(m)|H_1)$ também tem distribuição normal, sendo definida como

$$\Pr(F(m)|H_1) = N\left(\sum_{i=1}^{K}\bar{\mu}^c(\bar{\mu}^c - \mu_i^c), \sum_{i=1}^{K}(\bar{\mu}^c - \mu_i^c)^2\sigma^2\right). \tag{2.27}$$

Para encontrar a probabilidade do usuário legítimo ser considerado ilegítimo, basta calcular a área da pdf Gaussiana. Para este cálculo, pode-se usar a função Q, dada por [Stark e Woods 1986]

$$Q(v) = \left(\frac{1}{\sqrt{2\pi}}\right)\int_v^\infty e^{\frac{-t^2}{2}}dt, \tag{2.28}$$

em que v é o valor a ser testado. Assim, utilizando as equações (2.28), (2.25) e (2.26), tem-se que a taxa de FP= α é dada por

$$\begin{aligned}\Pr(\mathrm{FP_{LVS}}) &= \Pr(\Lambda(m) > T_\Lambda|H_0) = \Pr(F(m) > \Gamma|H_0)\\ &= Q\left(\frac{\Gamma - \sum_{i=1}^{K}\mu_i^c(\bar{\mu}^c - \mu_i^c)}{\sqrt{\sum_{i=1}^{K}(\bar{\mu}^c - \mu_i^c)^2\sigma^2}}\right),\end{aligned} \tag{2.29}$$

em que $\Pr(\mathrm{FP_{LVS}})$ é a probabilidade de FP do sistema. Da mesma forma, utilizando as equações

(2.28), (2.25) e (2.27), tem-se que a taxa de VP$= 1-\beta$ é dada por

$$\begin{aligned}\Pr(\mathrm{VP_{LVS}}) &= \Pr(\Lambda(m) > T_\Lambda | H_1) = \Pr(F(m) > \Gamma | H_1) \\ &= Q\left(\frac{\Gamma - \sum_{i=1}^{K} \bar{\mu}^c(\bar{\mu}^c - \mu_i^c)}{\sqrt{\sum_{i=1}^{K}(\bar{\mu}^c - \mu_i^c)^2\sigma^2}}\right).\end{aligned} \tag{2.30}$$

onde $\Pr(\mathrm{VP_{LVS}})$ é a probabilidade de VP do sistema.

Uma vez determinados os valores de α e β considerando FFA, pode-se usá-los para encontrar a entropia condicional definida em (2.10). Para este LVS proposto em [Yan et al. 2014], o valor de T_Λ que maximiza a informação mútua entre a entrada e saída do sistema $I(X;Y) = H(X) - H(X|Y)$ é obtido numericamente. Assim, para cada valor de T_Λ testado deve-se encontrar α e β através das equações (2.29) e (2.30). Em seguida, basta substituir estes valores em (2.10) e em (2.9). O limiar otimizado é aquele que apresenta maior C_{id}. Uma vez definido o limiar, este pode ser usado para decidir se o usuário é malicioso ou legítimo, através da equação (2.22).

Para facilitar a compreensão do método proposto em [Yan et al. 2014] e descrito nesta seção, segue uma visão rápida dos principais pontos apresentados:

- Foram definidas as funções $h_0(d_i^c)$ e $h_1(d_i^r)$ nas equações (2.13) e (2.15), que descrevem, respectivamente, as realizações das RSSs para usuários legítimos e maliciosos;
- Utilizando estas funções e considerando o comportamento estatístico do sombreamento, foram definidas as funções de verossimilhança em $\Pr(m|H_0)$ e $\Pr(m|H_1)$ em (2.19) e (2.20), respectivamente, para usuários legítimos e maliciosos;
- Com base nas equações (2.11) e (2.12), foi escrita a regra de decisão apresentada na equação (2.22). Esta regra de decisão depende do limiar T_Λ e pode ser usada para classificar o usuário;
- Com a regra de decisão formulada, é necessário definir qual o limiar T_Λ que maximiza o valor do parâmetro de desempenho C_{id}. Com base na equação (2.22), para um dado valor de T_Λ encontrou-se as equações (2.29) e (2.30), que são usadas para se obter os valores de α e β;
- Utilizando as equações (2.9) e (2.10), é possível determinar o C_{id} do sistema para cada limiar T_Λ, encontrando assim o limiar que maximiza o desempenho do sistema.

O método para a utilização do esquema apresentado é demonstrado na Figura 2.5, seguindo a seguinte ordem:

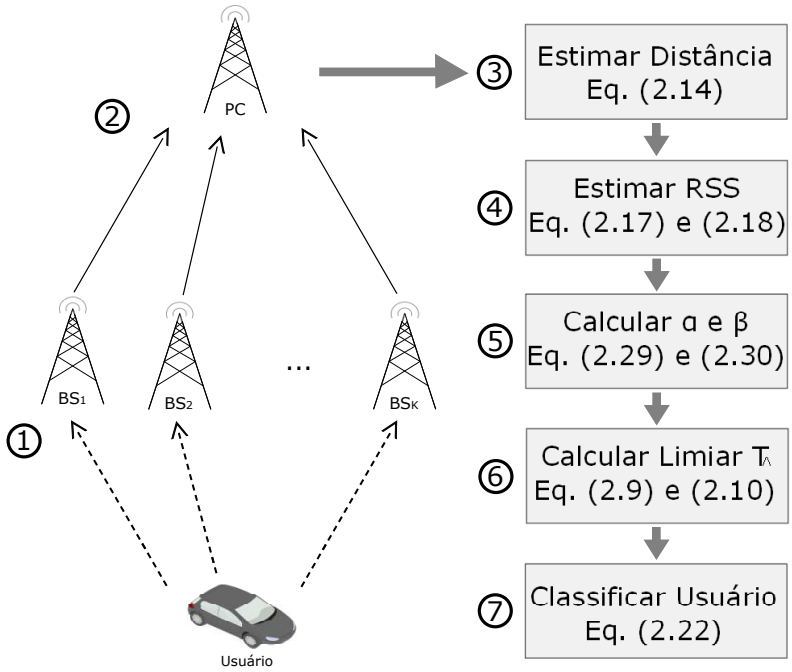

Figura 2.5: Fluxograma da utilização do esquema LVS.

1. As BSs recebem a posição informada pelo usuário e obtém as RSSs a partir dos sinais recebidos;

2. Essas informações são repassadas para o PC;

3. Com base na posição informada, são calculadas as distâncias entre o usuário e as BSs utilizando a equação (2.14);

4. Uma vez calculada estas distâncias, a potência média recebida de um usuário legítimo para cada BS μ_i^c e a potência média recebida por todas as BSs de um usuário ilegítimo $\bar{\mu}^c$ são calculadas utilizando, respectivamente, as equações (2.18) e (2.17);

5. Com estes dados e utilizando as equações (2.29) e (2.30), encontra-se α e β para valores específicos do limiar T_Λ;

6. O desempenho do sistema C_{id} deve ser então determinado para diversos valores do limiar T_Λ através das equações (2.9) e (2.10), obtendo assim o limiar que otimiza o desempenho do sistema;

7. Uma vez obtido o limiar, o usuário é classificado como malicioso ou legítimo utilizando a equação (2.22).

2.5 COMENTÁRIOS

Neste capítulo, o modelo de um sistema de verificação de localização introduzido em [Yan et al. 2014] foi apresentando, tratando os aspectos gerais a serem considerados sobre o sistema. Embora este modelo tenha diferenças consideráveis quando comparado ao LVS-DA proposto neste trabalho e descrito no Capítulo 3, muitos aspectos são compartilhados entre os dois esquemas. Desta forma, para que seja possível compreender a proposta apresentada nesta dissertação, é importante entender com clareza o LVS descrito neste capítulo.

Embora o LVS de [Yan et al. 2014] apresentado tenha diversas qualidades, seu desempenho ainda pode ser melhorado, como mostrado no Capítulo 4. Além disto, o modelo de propagação em larga escala considerado não reflete de maneira satisfatória o cenário de VANETs. No próximo capítulo, é feita uma análise de como adaptar o LVS descrito para um cenário mais realista e, em seguida, é apresentado como antenas direcionais podem ser usadas para aprimorar o desempenho, evitando erros na classificação dos usuários e melhorando assim o desempenho do sistema na detecção de nós maliciosos.

3 SISTEMA DE VERIFICAÇÃO DE LOCALIZAÇÃO COM ANTENAS DIRECIONAIS (LVS-DA)

No capítulo anterior, foram apresentados conceitos básicos relacionados à utilização de um LVS para verificar as posições informadas pelos veículos em uma VANET. Embora o modelo descrito seja bom em muitos aspectos, é importante verificar que o modelo de propagação em larga escala utilizado não corresponde de forma realista ao cenário de uma VANET. Além disso, o desempenho do LVS proposto em [Yan et al. 2014] pode ser melhorado, como será mostrado neste capítulo e ilustrado no Capítulo 4.

Este capítulo aborda como o uso antenas direcionais pode proporcionar melhorias significativas ao desempenho do LVS, considerando um modelo de propagação realista. Primeiro, é descrito quais mudanças são necessárias para que o LVS utilize como base o modelo de propagação em larga escala para VANETs apresentado em [Abbas et al. 2012].

Em seguida, é feita uma análise de como antenas direcionais podem ajudar a melhorar o desempenho do sistema. Além disso, equações analíticas para encontrar o desempenho do sistema são obtidas para um número variável de antenas e estações. Com as informações apresentadas, é possível determinar os benefícios do uso de antenas direcionais no sistema, auxiliando em sua utilização prática.

3.1 MODELO DE PROPAGAÇÃO REALISTA

Conforme descrito no Capítulo 2, o objetivo de um LVS é de identificar usuários maliciosos que informam de maneira incorreta suas posições. Embora o sistema seja otimizado no sentido de maximizar a informação mútua entre a entrada e a saída, o esquema descrito na Seção 2.4 utiliza o modelo de propagação de log-normal, que é simplificado e não reflete de forma correta a RSS em uma VANET [Cheng et al. 2007, Abbas et al. 2012].

Em [Cheng et al. 2007], foi formulado um modelo de duplo declive baseado no modelo de propagação de log-normal e em dados empíricos. Este modelo considera que a variação da atenuação é maior a partir de um certa distância. Posteriormente, utilizando as informações

obtidas em [Cheng et al. 2007], foram feitos novos testes empíricos e constatou-se que, além da variação da atenuação depender da distância, esta também depende da presença ou não de linha de visada entre o transmissor e o receptor. Porém, como em VANETs a linha de visada está geralmente obstruída por veículos, foi introduzido o conceito de OLOS, que representa a linha de visada obstruída, ao invés de NLOS (ausência de linha de visada). Assim, o modelo concentra-se nos estados de LOS, quando existe linha de visada, e do contrário utiliza OLOS.

Nesta seção, é apresentada quais as mudanças necessárias no sistema de verificação de localização proposto em [Yan et al. 2014] para a utilização do modelo de propagação mais realista em VANETs apresentado por [Abbas et al. 2012]. Para diferenciar do sistema original, o LVS que utiliza as alterações no modelo de propagação em larga escala é chamado de LVS-SLOS. A utilização de um modelo de propagação próximo da realidade é importante pois, como o sistema identifica usuários legítimos e maliciosos baseado na probabilidade do usuário pertencer ou não à distribuição correspondente, ao definir uma distribuição de RSS incorreta, tem-se por consequência que a potência do usuário legítimo distancia-se consideravelmente do valor esperado pelo sistema, prejudicando como um todo o desempenho obtido. Assim, o desempenho depende também da capacidade do sistema em estimar a RSS de um usuário legítimo de maneira precisa.

3.1.1 REGRA DE DECISÃO

Embora o cálculo da RSS mude em alguns aspectos para as equações propostas nesta seção, a regra de decisão permanece a mesma da utilizada na Seção 2.4.2, ou seja, é analisada a razão entre a probabilidade da RSS recebida ser de um veículo malicioso ou legítimo. Com isto, pode-se utilizar a regra descrita pelas equações (2.11) e (2.12).

3.1.2 DESCRIÇÃO DO SISTEMA

Baseado no modelo proposto em [Abbas et al. 2012], pode-se calcular a RSS para um usuário legítimo como

$$h_0(d_i^c) = \begin{cases} P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d}{d_0}\right) + \omega_{dB}, & \text{se } d_0 \leq d \leq d_c \\ P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d_c}{d_0}\right) - 10\gamma_2 \log_{10}\left(\frac{d}{d_c}\right) + \omega_{dB} & \text{se } d > d_c, \end{cases}, \qquad (3.1)$$

onde d_c é dado pela equação (2.3) e os valores de γ_1, γ_2 e σ^2 são definidos de acordo com a Tabela 2.2, que foi obtida empiricamente em [Abbas et al. 2012].

Para o usuário malicioso, este irá tentar configurar sua potência de forma que a RSS se

aproxime o mais próximo possível do valor esperado pelas BSs. Usando o mesmo método da Seção 2.4, tem-se que a potência do usuário malicioso é dada pelas equações

$$h_1(d_i^c) = \bar{\mu}^c + \omega_{dB}, \tag{3.2a}$$

$$\bar{\mu}^c = \frac{1}{K}\sum_{i=1}^{K} \mu_i^c, \tag{3.2b}$$

sendo μ_i^c o valor calculado da potência recebida pela BS i considerando o modelo de LOS/OLOS e ω_{dB} uma variável aleatória normal gaussiana que representa o sombreamento. Com base na Equação 2.2, μ_i^c é dado por

$$\mu_i^c = \begin{cases} P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d}{d_0}\right), & \text{se } d_0 \leq d \leq d_c \\ P(d_0) - 10\gamma_1 \log_{10}\left(\frac{d_c}{d_0}\right) - 10\gamma_2 \log_{10}\left(\frac{d}{d_c}\right) & \text{se } d > d_c, \end{cases} . \tag{3.3}$$

Os parâmetros γ_1, γ_2 e σ^2 são utilizados de forma que cada BS faça a seleção entre LOS e OLOS, conforme descrito na Subseção 2.2.1.2. Se LOS for assumido, serão usados os parâmetros LOS da Tabela 2.2. Caso contrário, serão usados os parâmetros de OLOS.

Da mesma forma que no LVS original, uma vez que tanto $h_1(d_i^c)$ quanto $h_0(d_i^c)$ dependem do sombreamento ω_{dB}, que tem uma distribuição normal, ambas as variáveis também têm distribuição normal. Como as medições feitas por cada BS são independentes entre si, a função de verossimilhança do conjunto de medições m é dado pela probabilidade conjunta de todos os elementos de m. Como a probabilidade conjunta de variáveis independentes é dado pelo produto das pdfs de todas as variáveis [Stark e Woods 1986], a função de verossimilhança do conjunto de medições m para o usuário legítimo é dada por

$$\begin{aligned} \Pr(m|H_0) &= \prod_{i=1}^{K} \Pr(m_i|H_0) \\ &= \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(\frac{-(m_i - \mu_i^c)^2}{2\sigma_i^2}\right), \end{aligned} \tag{3.4}$$

sendo a única diferença entre a equação (2.19) e a equação (3.4) o fato de que na segunda equação o desvio pode variar para cada BS, uma vez que este depende do veículo estar em LOS ou OLOS com relação à BS. Assim como para o usuário legítimo, deve-se definir a função de verossimilhança para o usuário malicioso. Utilizando a FFA, pode-se definir esta função como

$$\Pr(m|H_1) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(\frac{-(m_i - \bar{\mu}^c)^2}{2\sigma_i^2}\right). \tag{3.5}$$

sendo, novamente, a única diferença entre a equação (2.20) e a equação (3.5) o fato de que na

segunda equação o desvio depende da BS.

Para formar o teste de comparação, deve-se substituir as funções definidas em (3.4), (3.5) e (2.12) em (2.11), com $F(m) = \Lambda(m)$. Assim, tem-se que

$$\frac{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\bar{\mu}^c)^2}{2\sigma_i^2}\right)}{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\mu_i^c)^2}{2\sigma_i^2}\right)} \underset{D_0}{\overset{D_1}{\gtrless}} T_\Lambda. \tag{3.6}$$

Da mesma forma como descrito na Seção 2.4, a equação (3.6) já pode ser usada para encontrar o desempenho do sistema de forma numérica para um dado valor de T_Λ. Porém, seria também conveniente obter o desempenho do sistema de forma analítica. Como o desvio padrão do sombreamento varia de acordo com a BS, algumas das operações matemáticas usadas para se obter as equações (2.24) e (2.25) devem ser alteradas. Assim, utilizando a equação (2.23) para o sistema proposto, Γ e $F(m)$ são dados por

$$F(m) = \sum_{i=1}^{K} \frac{m_i\,(\bar{\mu}^c - \mu_i^c)}{\sigma_i^2}, \tag{3.7}$$

$$\Gamma = \ln \mathrm{T}\lambda - \sum_{i=1}^{K} \frac{(-\mu^c)^2 + (\mu_i^c)^2}{2\sigma_i^2}. \tag{3.8}$$

Com estas definições, tem-se que, para o usuário legítimo

$$\Pr(F(m), H_0) = N\left(\sum_{i=1}^{K} \frac{\mu_i^c\,(\bar{\mu}^c - \mu_i^c)}{{\sigma_i}^2}, \sum_{i=1}^{K} \frac{(\bar{\mu}^c - \mu_i^c)^2}{{\sigma_i}^2}\right), \tag{3.9}$$

e, para o usuário ilegítimo, tem-se que

$$\Pr(F(m), H_1) = N\left(\sum_{i=1}^{K} \frac{\bar{\mu}^c\,(\bar{\mu}^c - \mu_i^c)}{{\sigma_i}^2}, \sum_{i=1}^{K} \frac{(\bar{\mu}^c - \mu_i^c)^2}{{\sigma_i}^2}\right). \tag{3.10}$$

Por fim, fazendo uma análise similar ao método utilizado na Seção 2.4, para encontrar o FP usa-se

$$\Pr(\mathrm{FP_{LVS}}) = Q\left(\frac{\Gamma - \sum_{i=1}^{K} \frac{\mu_i^c(\bar{\mu}^c - \mu_i^c)}{\sigma_i^2}}{\sqrt{\sum_{i=1}^{K} \frac{(\bar{\mu}^c - \mu_i^c)^2}{{\sigma_i}^2}}}\right), \tag{3.11}$$

e, para calcular a probabilidade de VP usa-se

$$\Pr(\mathrm{VP_{LVS}}) = Q\left(\frac{\Gamma - \sum_{i=1}^{K} \frac{\bar{\mu}^c(\bar{\mu}^c - \mu_i^c)}{\sigma_i^2}}{\sqrt{\sum_{i=1}^{K} \frac{(\bar{\mu}^c - \mu_i^c)^2}{{\sigma_i}^2}}}\right). \tag{3.12}$$

Para o sistema proposto nesta seção, o método de utilização segue a mesma fórmula descrita na Seção 2.4.

3.2 ANTENAS DIRECIONAIS

Na seção anterior, foi explicado a importância da utilização de um modelo de propagação realista. Em seguida, foram descritos os passos para se utilizar o modelo LOS/OLOS em um LVS. Como será visto no próximo capítulo, apesar desta abordagem proporcionar um ganho significativo no desempenho do sistema, ainda há espaço para que este desempenho seja melhorado.

A vantagem em se utilizar DAs em um LVS ocorre pois, com elas, a RSS de um usuário que está na direção (ou área de cobertura) de uma determinada DA deverá ser maior do que a RSS recebida pelas outras antenas, que estão apontadas para outras direções. Desta forma, o esquema apresentado é chamado de LVS-DA e utiliza como base o LVS-SLOS apresentado na Seção 3.1.

3.2.1 VERIFICAÇÃO DIRECIONAL

O esquema proposto nesta seção sugere uma etapa adicional de verificação no LVS-SLOS, apresentado na seção anterior. Desta forma, os sinais obtidos pelas DAs serão pré-processados por um módulo adicional, chamado de DV, conforme ilustrado na Figura 3.1. A saída do sistema é a informação se o usuário é malicioso ou legítimo, e a entrada do sistema é composta por:

1. *i)* a posição alegada pelo usuário;
2. *ii)* a RSS do usuário por todas as DAs de todas BSs;
3. *iii)* a posição de cada BS.

A etapa adicional DV, como apresentado na Figura 3.1, pré-processa os sinais recebidos e automaticamente classifica um dado usuário como malicioso sempre que, para ao menos $K_{\min} \leq K$ BSs, a antena que recebeu a maior RSS não é a antena esperada de acordo com a posição afirmada pelo usuário. Assim, o valor de $K_{\min}$ é utilizado nas equações de desempenho, apresentadas mais adiante neste capítulo. Caso o usuário não seja identificado como malicioso pela etapa DV, as informações são repassadas para a etapa LVS, fazendo a verificação conforme

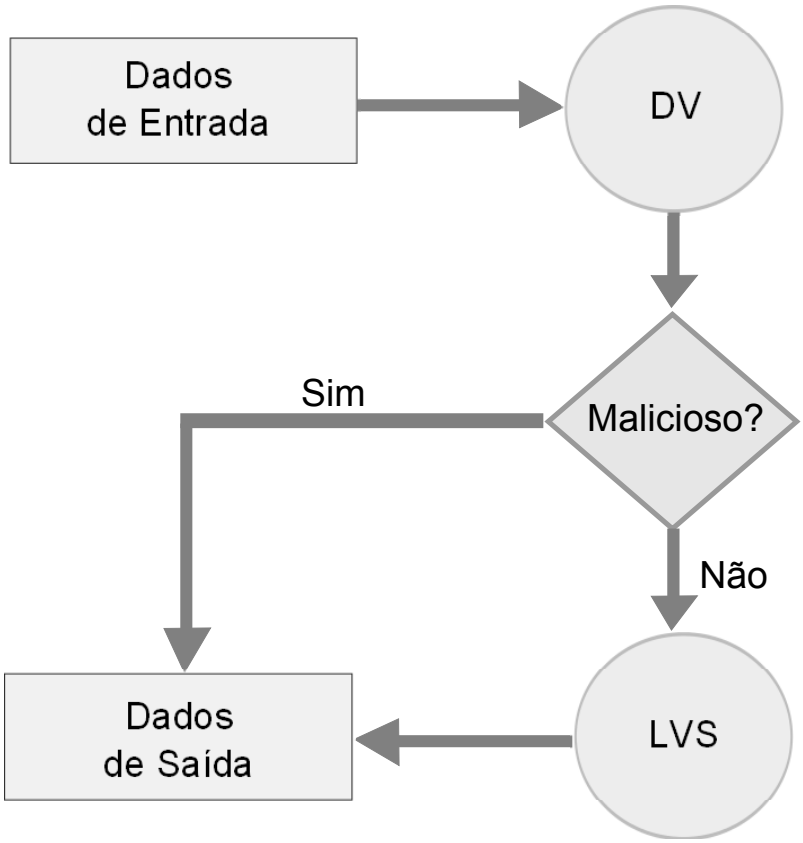

Figura 3.1: Fluxograma do esquema LVS-DA.

descrito na seção 3.1. Desta maneira, a probabilidade de FP e VP do esquema LVS-DA pode ser escrita como

$$\Pr(\mathrm{FP}) = \Pr(\mathrm{FP_{DV}}) + \left[1 - \Pr(\mathrm{FP_{DV}})\right] \Pr(\mathrm{FP_{LVS}}), \tag{3.13a}$$

$$\Pr(\mathrm{VP}) = \Pr(\mathrm{VP_{DV}}) + \left[1 - \Pr(\mathrm{VP_{DV}})\right] \Pr(\mathrm{VP_{LVS}}), \tag{3.13b}$$

onde $\Pr(\mathrm{FP_{LVS}})$ e $\Pr(\mathrm{VP_{LVS}})$ são obtidos utilizando, respectivamente, as equações (3.11) e (3.12), $\Pr(\mathrm{FP_{DV}})$ e $\Pr(\mathrm{VP_{DV}})$ são as taxas de VP e FP obtidas usando apenas a etapa DV, e $\Pr(\mathrm{FP})$ e $\Pr(\mathrm{VP})$ são as taxas finais obtidas pela esquema LVS-DA. Com estas taxas, tem-se os valores de $\alpha = \Pr(\mathrm{FP})$ e $\beta = (1 - \Pr(\mathrm{VP}))$, e pode-se obter o desempenho do sistema através das equações (2.10) e (2.9).

3.2.2 DESCRIÇÃO ANALÍTICA DO SISTEMA

Nesta seção, o desempenho do esquema LVS-DA será avaliado analiticamente dada uma determinada configuração. Esta análise é importante para ajudar na decisão do número necessário de DAs e de BSs para se obter um determinado desempenho, evitando assim a

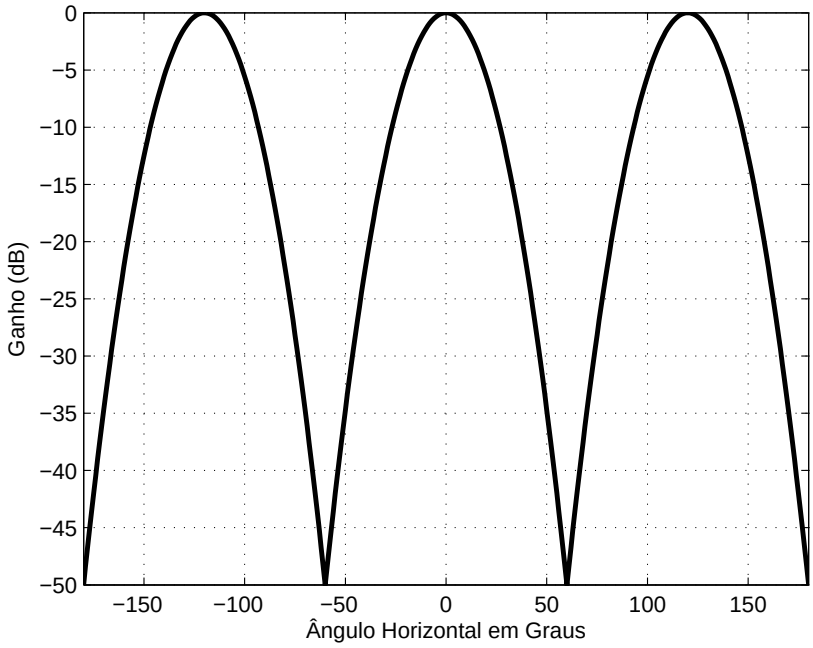

Figura 3.2: Atenuação para um cenário com $N = 3$ DAs.

necessidade de realização de simulações computacionais.

3.2.2.1 MODELO DE UTILIZAÇÃO DAS ANTENAS DIRECIONAIS

Para que seja possível descrever o funcionamento do LVS-DA, é necessário primeiro definir a atenuação causada pelas DAs na RSS. Conforme visto na Seção 2.3, a atenuação pode ser dada pela equação (2.8), que varia de acordo com o ângulo entre o veículo e a antena.

Neste esquema, para um dado valor de θ_{3dB}, o valor υ é ajustado de forma que, para uma determinada posição do usuário, a atenuação causada por cada antena não haja sobreposição. Assim, a Antena Principal (MA, do inglês *Main Antenna*) é a antena que está cobrindo a área onde o usuário afirma estar e tem atenuação entre $-A_{\max}$ e 0_{dB}. As Antenas Secundárias (SAs, do inglês *Secondary Antennas*) representam as outras $N-1$ antenas e têm atenuação média de $-A_{\max}$. Um cenário com $N=3$ DAs é ilustrado na Figura 3.2, em que cada antena cobre 120° e a atenuação causada por cada DA não sobrepõe.

Desta forma, dado o número de antenas N, a atenuação máxima $A_{\max}$ e a largura de feixe de meia potência θ_{3dB}, pode-se definir o valor υ de modo que a atenuação causada por cada antena não sobreponha. Assim, primeiro é necessário encontrar o módulo do ângulo máximo ς de cada DA de acordo com o número de antenas utilizado. Por exemplo, em um cenário com 3 antenas, cada antena deverá cobrir 120°, sendo de $-60°$ a 60°, com módulo do ângulo máximo

equivalente a $\varsigma = 60^\circ$. Este valor é definido pela equação

$$\varsigma = \frac{360}{2N}. \tag{3.14}$$

Uma vez encontrado ς, deve-se encontrar o valor de υ para o esquema LVS-DA de forma que a atenuação máxima de cada DA não sobreponha. Assim, tem-se que o valor de υ pode ser obtido utilizando a equação (2.8) com $\theta = \varsigma$ e $A(\theta) = -A_{\max}$, resultando na equação

$$-A_{\max} = -\upsilon \left(\frac{\varsigma}{\theta_{3dB}} \right)^2, \tag{3.15}$$

e, isolando υ, tem-se que

$$\upsilon = \frac{A_{\max}\theta_{3dB}^2}{\varsigma^2}. \tag{3.16}$$

3.2.2.2 DESCRIÇÃO GERAL DO SISTEMA

Nesta seção, são apresentados os cálculos das taxas de FP e VP para a etapa de DV. Inicialmente, é encontrada a taxa de FP para apenas uma BS, com N DAs. Assim, é necessário verificar qual a probabilidade da MA ter uma RSS menor que a RSS de qualquer uma das SAs. Para a taxa de FP, como esta indica a probabilidade do usuário legítimo ser identificado como falso, a posição alegada pelo usuário é a posição real.

Como visto anteriormente, a potência recebida pela MA tem uma atenuação que varia de acordo com o ângulo entre o usuário e a antena. Para as SAs, a RSS tem atenuação equivalente a $-A_{\max}$. Considera-se que D_m representa a atenuação na MA e D_{s_j} representa a atenuação de uma antena secundária, sendo j o número da antena secundária. É importante notar que ambas as RSSs podem ser vistas como variáveis aleatórias.

Para esta análise, note que apenas a diferença entre as potências recebidas pelas antenas é importante. Com objetivo de facilitar a análise do problema, soma-se $A_{\max}$ ao valor das variáveis D_{s_j} e D_m, fazendo com que D_{s_j} tenha média sempre zero e D_m tenha média maior que zero. Define-se então uma nova variável aleatória para encontrar a diferença entre as duas variáveis, dada como

$$D_{f_j} = D_m - D_{s_j}, \tag{3.17}$$

onde D_{f_j} é a diferença entre a potência da MA e a potência da SA j. A média da nova variável

é a diferença entre as duas médias. Assim, tem-se que

$$\mu_{f_j} = \mu_m - \mu_{s_j}, \tag{3.18}$$

sendo μ_{f_j}, μ_m e μ_{s_j} as médias das variáveis D_{f_j}, D_m e D_{s_j}, respectivamente. A variância da nova variável é a soma das variâncias de D_m e D_{s_j}. Assim,

$$\sigma_{f_j}^2 = \sigma_m^2 + \sigma_{s_j}^2, \tag{3.19}$$

sendo σ_{f_j}, σ_m e σ_{s_j} os desvios das variáveis D_{f_j}, D_m e D_{s_j}, respectivamente. Para uma dada distância média d entre o usuário e a BS, os valores de σ_m e σ_{s_j} devem ser obtidos através de (2.6). No que se segue, as variáveis μ_{f_j} e σ_{f_j} serão representadas omitindo-se o índice j, uma vez que as médias e os desvios são os mesmos para qualquer índice. Note também que, como todas as variáveis D_{f_j} dependem do valor de D_m, existe entre elas um coeficiente de correlação p diferente de zero.

O cálculo da diferença de potência é importante pois a probabilidade de D_m ser menor que D_{s_j} é igual a $\Pr(D_{f_j} < 0)$ [Stark e Woods 1986]. Como a média de D_{f_j} varia conforme o ângulo entre o usuário e a antena, deve-se encontrar uma expressão que indique a probabilidade do usuário estar em um determinado ângulo. Seguindo o modelo descrito em [Yan et al. 2014], é assumido que as BSs estão espalhadas de forma uniforme. Assim, tem-se que a posição da BS i tem seus eixos y e x como variáveis aleatórias com distribuição uniforme. Considerando que a tangente de um ângulo é a razão entre os dois eixos, escolhe-se encontrar a probabilidade dos ângulos através da pdf da razão entre as duas variáveis uniformes $-1 \leq u_i^{BS} \leq 1$ e $-1 \leq v_i^{BS} \leq 1$, que pode ser obtida utilizando [Trott 2007]

$$\begin{aligned} \Pr_{\frac{y}{x}}(r) &= \int_0^\infty x f(x, rx) dx - \int_{-\infty}^0 x f(x, rx) dx \\ &= \begin{cases} \frac{1}{4} & |r| \leq 1 \\ \frac{1}{4r^2} & |r| > 1 \end{cases} \end{aligned}, \tag{3.20}$$

sendo r a razão entre a posição no eixo y e a posição no eixo x da BS, e $\Pr_{\frac{y}{x}}(u)$ a probabilidade da razão entre os dois eixos ser equivalente a u. Antes de encontrar a probabilidade de cada ângulo, é necessário primeiro alterar (3.20) de forma que a equação dependa apenas do ângulo. Para isso, será utilizado um método apresentado em [Stark e Woods 1986], com a pdf de $u = g(r) = \arctan r$ dada por

$$\Pr_u(u) = \frac{\Pr_{\frac{y}{x}}(\tan u)}{g'(\tan u)}, \tag{3.21}$$

onde $g'(r)$ é a primeira derivada da função $g(r)$ com relação a r. É importante notar que, como a tangente não muda quando o ângulo é deslocado em 180°, ângulos a cada 180° têm a mesma probabilidade e, considerando que entre 0 e 360° deve-se ter uma probabilidade de 100%, é necessário dividir por dois a probabilidade descrita em (3.20). Com base nas equações (3.20) e (3.21), considerando que $g'(\tan u) = (\cos u)^2$ e adicionando uma condição de contorno para evitar a divisão por zero, tem-se que

$$\Pr_u(u) = \begin{cases} \frac{1}{8}\xi(\csc u)^2 & \text{Mod}(u,180) \neq 0 \cap \text{Mod}(u,90) = 0 \\ \frac{1}{8}\xi(\sec u)^2 & |\tan u| \leq 1 \\ \frac{1}{8}\xi(\csc u)^2 & |\tan u| > 1 \end{cases}, \tag{3.22}$$

sendo a função $\text{Mod}(a,b)$ o resto da divisão entre a e b, u o ângulo analisado medido em graus e $\xi = \frac{\pi}{180}$ uma constante usada devido à conversão de radianos para graus ao derivar a função. Por fim, para encontrar a probabilidade do usuário estar entre o ângulo mínimo e máximo da antena, deve-se integrar de $-\varsigma$ até ς, resultando na equação

$$\Pr(-\varsigma \leq \theta_{usr} \leq \varsigma) = \int_{-\varsigma}^{\varsigma} \Pr_u(u)\, du. \tag{3.23}$$

Sobre a probabilidade de cada ângulo, tem-se um último detalhe importante. Como cada DA está efetivamente apontando em uma direção diferente, a probabilidade dos ângulos varia de acordo com a posição e o número de antenas na BS. Com o objetivo de definir a direção para onde está apontada cada antena, considera-se então que a MA está apontada para o ângulo $\theta_{\text{desv}_1} = 0°$, e as demais $N-1$ SAs estão apontadas para $\theta_{\text{desv}_n} = 2(n-1)\varsigma$. Desta forma, em um cenário com 3 DAs, por exemplo, elas estariam direcionadas para os ângulos $\theta_{\text{desv}_1} = 0°$, $\theta_{\text{desv}_2} = 120°$ e $\theta_{\text{desv}_3} = 240°$.

Precisa-se então encontrar a probabilidade de qualquer uma das antenas secundárias ter uma potência maior que a antena principal. Primeiro, é importante notar que as variáveis $D_{f_1}, D_{f_2}, ..., D_{f_{N-1}}$ não são independentes, uma vez que todas dependem da variável D_m, relacionada à MA. Uma solução possível é calcular o valor através da probabilidade conjunta entre todas as variáveis. Note que a probabilidade da MA ter a maior RSS é dada por $\Pr(D_{f_1} > 0, D_{f_2} > 0, ..., D_{f_{N-1}} > 0)$. Logo, a probabilidade de qualquer SA ter uma RSS maior que a MA é dada por $1 - \Pr(D_{f_1} > 0, D_{f_2} > 0, ..., D_{f_{N-1}} > 0)$. Assim, a probabilidade conjunta

é dada por [Stark e Woods 1986]

$$\Pr(D_{f_1} > 0, D_{f_2} > 0, ..., D_{f_{N-1}} > 0) = \int_0^{\infty} \frac{1}{\sqrt{(2\pi)^{N-1}|\Sigma|}} \exp\left(-\frac{1}{2}(x-\mu)^T \Sigma^{-1}(x-\mu)\right) dx, \tag{3.24}$$

sendo Σ a matriz de covariância, $|\Sigma|$ a determinante de Σ, μ o vetor das médias e x o vetor das variáveis de integração. Embora (3.24) não tenha uma forma fechada, foram encontradas expressões para 2, 3 e 4 DAs, que serão definidas na próxima seção.

Como todas as variáveis D_f têm a mesma média e o mesmo desvio, basta calcular a covariância entre duas variáveis quaisquer para se obter a matriz de covariância. Para calcular a covariância, tem-se que

$$\begin{aligned}
\text{Cov} &= E[D_{f_1} D_{f_2}] - \mu_{f_1}\mu_{f_2} \\
&= E[(D_m - D_{s_1})(D_m - D_{s_2})] - \mu_{f_1}\mu_{f_2} \\
&= E[D_m^2 - D_m D_{s_1} - D_m D_{s_2} + D_{s_1} D_{s_2}] - \mu_{f_1}\mu_{f_2} \\
&= E[D_m^2] - E[D_m D_{s_1}] - E[D_m D_{s_2}] + E[D_{s_1} D_{s_2}] - \mu_{f_1}\mu_{f_2} \\
&= E[D_m^2] - \mu_m\mu_{s_1} - \mu_m\mu_{s_2} + \mu_{s_1}\mu_{s_2} - \mu_{f_1}\mu_{f_2} \\
&= E[D_m^2] - \mu_{f_1}\mu_{f_2},
\end{aligned} \tag{3.25}$$

onde D_m e D_{s_j} são variáveis independentes e o valor de μ_{s_j} é sempre zero para qualquer valor do índice j, conforme descrito no início desta subseção. Note que as simplificações feitas em (3.25) são possíveis pois o primeiro momento conjunto de duas variáveis independentes é igual ao produto das médias [Stark e Woods 1986].

Como a probabilidade de FP é dividida entre as N antenas e o usuário legítimo pode estar em qualquer uma delas, precisa-se calcular a probabilidade para cada uma das DAs e depois somá-las. Isto ocorre pois a probabilidade do usuário estar em um determinado ângulo varia de antena para antena e, como qualquer uma das antenas pode ser a antena principal, é necessário somar as probabilidades individuais. Desta forma, tem-se que

$$\Pr_{ant}(n) = \int_{-\varsigma}^{\varsigma} \Pr_{ang}(n,u)du, \tag{3.26}$$

onde $\Pr_{ant}(n)$ é a probabilidade de FP quando a antena n é considerada MA e $\Pr_{ang}(n,u)$ é a

probabilidade dos ângulos e é dada por

$$\Pr_{ang}(n,u) = \begin{cases} \frac{1}{8}^{\circ}(\csc u_n)^2 & \text{Mod}(u_n,180) \neq 0 \cap \text{Mod}(u_n,90) = 0 \\ \frac{1}{8}^{\circ}(\sec u_n)^2 & |\tan u_n| \leq 1 \\ \frac{1}{8}^{\circ}(\csc u_n)^2 & |\tan u_n| > 1 \end{cases} , \cdot (1 - \Pr(D_{f_1} > 0, D_{f_2} > 0, ..., D_{f_{N-1}} > 0)) \tag{3.27}$$

sendo $u_n = (u + \theta_{\text{desv}_n})$ o ângulo na antena n. Na literatura pesquisada, não foi possível encontrar uma forma genérica fechada para a expressão (3.26), uma vez que a equação muda conforme o número total de DAs. Ainda sim, uma simples aproximação pelo método trapezoidal [Stark e Woods 1986] utilizando cada passo igual a um grau é suficiente para se obter ótimos resultados, como será demonstrado no Capítulo 4. Desta forma a equação (3.26), utilizada para se calcular a probabilidade para uma antena, pode ser reescrita utilizando o método trapezoidal como

$$\Pr_{ant}(n) = \frac{\Pr_{ang}(n,-\varsigma)}{2} + \left(\sum_{i=-\varsigma+1}^{\varsigma-1} \Pr_{ang}(n,i) \right) + \frac{\Pr_{ang}(n,\varsigma)}{2}. \tag{3.28}$$

Como a probabilidade para uma BS é a soma das probabilidades para cada antena, tem-se que

$$\Pr_{\text{BS}}(\text{FP}) = \sum_{n=1}^{N} \Pr_{ant}(n), \tag{3.29}$$

onde $\Pr_{\text{BS}}(\text{FP})$ é a probabilidade de FP de uma BS. Como (3.29) representa a probabilidade para apenas uma estação, é necessário ainda calcular a probabilidade de ao menos $K_{\min}$ BSs identificarem o usuário como malicioso. Para isto, é utilizada a distribuição binomial. Para minimizar a quantidade de cálculos, pode-se encontrar a probabilidade de VN, ou seja, a probabilidade de que um número menor que $K_{\min}$ BSs identifiquem que o usuário é malicioso, para depois utilizar a relação $\text{FP} = 1 - \text{VN}$, conforme descrito na Tabela 2.1. Assim, tem-se que a probabilidade final de FP para a etapa DV é dada por

$$\Pr(\text{FP}_{\text{DV}}) = 1 - \sum_{k=0}^{K_{\min}-1} \binom{K}{k} \Pr_{\text{BS}}(\text{FP})^k (1 - \Pr_{\text{BS}}(\text{FP}))^{K-k}. \tag{3.30}$$

Resta apenas encontrar a probabilidade de VP, que é a probabilidade da antena principal não ser a antena que recebe a potência máxima. Neste caso, diferente da probabilidade de FP, onde o usuário está sempre na região da MA, o veículo pode estar em qualquer uma das DAs e a MA pode ser qualquer antena. Desta forma, a probabilidade de VP para uma BS é simplesmente a probabilidade do usuário malicioso estar em qualquer uma das SAs considerando cada

antena com probabilidade igual, e é dada pela equação $\Pr_{\mathrm{BS}}(\mathrm{VP}) = \frac{N-1}{N}$, conforme resultados apresentados no Capítulo 4. Para o cálculo da probabilidade com K BSs utiliza-se novamente a mesma abordagem da equação (3.30), ou seja, calcular a probabilidade de FN para depois utilizar a relação $\mathrm{VP} = 1 - \mathrm{FN}$. Assim, tem-se que a probabilidade final de VP para a etapa DV é dada por

$$\Pr(\mathrm{VP}_{\mathrm{DV}}) = 1 - \sum_{k=0}^{K_{\min}-1} \binom{K}{k} \Pr_{\mathrm{BS}}(\mathrm{VP})^k (1 - \Pr_{\mathrm{BS}}(\mathrm{VP}))^{K-k}. \tag{3.31}$$

Para o caso onde são utilizadas apenas antenas direcionais, sem a verificação do LVS proposto na seção anterior, o valor de C_{id} pode ser obtido diretamente através das equações (3.30), (3.31), (2.9) e (2.10). Porém, quando as antenas direcionais são usadas em conjunto com o LVS proposto, é necessário utilizar as equações (3.11), (3.12), (3.30), (3.31), (3.13a) e (3.13b) para encontrar os valores finais do FP e do VP, e por fim utilizar as equações (2.9) e (2.10) para encontrar o valor de C_{id}.

3.2.3 PROBABILIDADES RELACIONADAS AO NÚMERO DE ANTENAS DIRECIONAIS

Como descrito na seção anterior, a função de probabilidade descrita pela equação (3.24) varia de acordo com o número de DAs. Nesta seção, será feita uma análise de como se obter a probabilidade para 2, 3 e 4 antenas.

3.2.3.1 DUAS ANTENAS DIRECIONAIS

Para duas antenas, tem-se apenas uma variável normal aleatória D_{f_1} com média igual a diferença de potência entre a MA e a SA. Desta forma, a probabilidade pode ser descrita como [Stark e Woods 1986]

$$\begin{aligned} \Pr(D_{f_1} > 0) &= \int_0^{\infty} \frac{1}{\sqrt{2\pi}\sigma_f} \exp\left(-\frac{(x-\mu_f)^2}{2\sigma_f^2}\right) dx \\ &= \frac{1}{2}\mathrm{Erfc}\left(-\frac{\mu_f}{\sqrt{2}\sigma_f}\right) \end{aligned}, \tag{3.32}$$

onde $\mathrm{Erfc}(a)$ corresponde à função de erro complementar, dada por [Stark e Woods 1986]

$$\mathrm{Erfc}(a) = \frac{2}{\sqrt{\pi}} \int_a^{\infty} \exp(-x^2) dx. \tag{3.33}$$

3.2.3.2 TRÊS ANTENAS DIRECIONAIS

Para o caso com 3 DAs, tem-se duas variáveis aleatórias. Desta forma, a função torna-se uma integral de uma distribuição normal bivariada com coeficiente de correlação diferente de zero. Assim, tem-se que [Stark e Woods 1986]

$$\Pr(D_{f_1} > 0, D_{f_2} > 0) = \int_0^\infty \int_0^\infty \frac{1}{2\pi\sigma_f^2\sqrt{(1-p^2)}} e^{\frac{x^2+y^2-2xyp+2(-1+p)\left(x+y-\mu_f\right)\mu_f}{2\left(-1+p^2\right)\sigma_f^2}} dxdy. \quad (3.34)$$

Para encontrar uma forma analítica para a equação (3.34), pode-se utilizar a função T de Owen, definida em [Owen 1956]. Quando $a > 0$ e $b > 0$, a função T calcula a área entre $y = 0$ e $y = bx$ e de $x = a$ até $x = \infty$, para uma distribuição normal com coeficiente de correlação igual a zero e com médias e variâncias unitárias. Esta função é definida como

$$T(a,b) = \frac{1}{2\pi} \int_0^b \frac{e^{-\frac{a^2}{2}\left(1+x^2\right)}}{1+x^2} dx. \quad (3.35)$$

A importância desta função está no fato de que ela é conhecida e tabelada, podendo ser usada para calcular a integral de uma distribuição normal bivariada com coeficiente de correlação diferente de zero [Owen 1956]. Para isto, é necessário definir uma segunda função B que é capaz de encontrar áreas de retângulos, dada como [Owen 1956]

$$\begin{aligned} B(a,b,c) = {} & \frac{1}{4}\mathrm{Erfc}\left[-\frac{b}{\sqrt{2}}\right] + \frac{1}{4}\mathrm{Erfc}\left[-\frac{c}{\sqrt{2}}\right] - \mathrm{T}\left[b, \frac{-a+\frac{c}{b}}{\sqrt{1-a^2}}\right] \\ & - \mathrm{T}\left[c, \frac{-a+\frac{b}{c}}{\sqrt{1-a^2}}\right] \end{aligned}, \quad (3.36)$$

sendo $B(a,b,c)$ a probabilidade de $x < b$ e $y < c$ com coeficiente de correlação a. Como para o problema proposto $b = c$, pode-se simplificar a equação resultando em

$$B(a,b) = \frac{1}{2}\mathrm{Erfc}\left[-\frac{b}{\sqrt{2}}\right] - 2\mathrm{T}\left[b, \frac{-a+1}{\sqrt{1-a^2}}\right]. \quad (3.37)$$

Utilizando a equação (3.37), pode-se calcular enfim a probabilidade da equação (3.24) para 3 antenas, que é dada por

$$\Pr(D_{f_1} > 0, D_{f_2} > 0) = B\left(p, \frac{\mu_f}{\sigma_f}\right). \quad (3.38)$$

3.2.3.3 QUATRO ANTENAS DIRECIONAIS

Para quatro DAs, é utilizado um método proposto em [Steck 1958]. Este método utiliza as funções G, T de Owen, C, e a função S proposta no próprio artigo para encontrar o volume que define a probabilidade da MA ter uma potência maior que todas as SAs. Primeiro é necessário definir a função $G(a)$, que é a probabilidade de uma variável normal gaussiana com média a e variância unitária ser maior que zero. Esta equação é definida como [Steck 1958]

$$G(a) = \frac{1}{2}\text{Erfc}\left(-\frac{a}{\sqrt{2}}\right). \tag{3.39}$$

A função T de Owen é definida pela equação (3.35). Para $a > 0$, $b > 0$ e $c > 0$, $S(a,b,c) - \frac{1}{4\pi}\text{ArcTan}\left[\frac{c}{\sqrt{\left(1+b^2+b^2c^2\right)}}\right]$ é a probabilidade de três variáveis normais padronizadas independentes estarem na região entre os planos $x = 0$, $x - cz = 0$, $y = 0$, $y = a$, $z - by = 0$ e $z = \infty$. Assim, e a função S é definida como [Steck 1958]

$$S(a,b,c) = \int_0^a \int_{by}^{\infty} \int_0^{cz} \frac{e^{\frac{1}{2}\left(-x^2-y^2-z^2\right)}}{2\sqrt{2}\pi^{3/2}} dxdzdy + \frac{1}{4\pi}\text{ArcTan}\left[\frac{c}{\sqrt{(1+b^2+b^2c^2)}}\right]. \tag{3.40}$$

A última equação necessária é a função C descrita em [Steck 1958]. Para este trabalho, utiliza-se uma forma simplificada da função, considerando que as médias das três variáveis são equivalentes a μ_f e têm coeficiente de correlação igual a p. Assim, a função $C(a,b)$ descreve a probabilidade de $x \leq b$, $y \leq b$ e $z \leq b$ com coeficiente de correlação a, e é definida como [Steck 1958]

$$C(a,b) = \frac{3}{2}(G[b]) - 3\left(\text{T}\left[b, \frac{-a+1}{\sqrt{1-a^2}}\right]\right) - 6\left(S\left[b, \frac{-a+1}{\sqrt{1-a^2}}, \frac{\left(1-a^2\right)-\left(a-a^2\right)}{\sqrt{\left(1-3a^2+2a^3\right)}}\right]\right). \tag{3.41}$$

Utilizando a equação (3.41), pode-se obter enfim a probabilidade da MA ter uma potência maior que qualquer uma das 3 SAs através da equação

$$\Pr(D_{f_1} > 0, D_{f_2} > 0, D_{f_3} > 0) = C\left(p, \frac{\mu_f}{\sigma_f}\right). \tag{3.42}$$

3.3 COMENTÁRIOS

Neste capítulo, foram obtidas inicialmente as equações para a utilização de um LVS baseado em teoria da informação com um modelo de propagação realista. Em seguida, foi feita uma análise de como a utilização de antenas direcionais pode melhorar o desempenho do

sistema. A proposta do esquema apresentado é melhorar o desempenho do sistema comparando a RSS recebida por cada DA, adicionando uma etapa chamada de DV ao processo de verificação. Assim, quando mais de K_{min} BSs verificarem que a RSS máxima não é aquela recebida pela DA que está cobrindo a região onde o veículo alega se encontrar, o usuário é considerado malicioso. Expressões analíticas para o desempenho do sistema também foram obtidas.

4 RESULTADOS NUMÉRICOS

Após a apresentação de um LVS baseado em teoria da informação no Capítulo 2, foi feita uma análise no Capítulo 3 de como este sistema poderia ser aprimorado utilizando um modelo de propagação realista e, em seguida, foi proposto a utilização de DAs, que têm como objetivo aprimorar o desempenho do sistema.

Neste capítulo, são apresentados resultados numéricos para confirmar as equações analíticas obtidas e para comparar o desempenho dos sistemas. Primeiro, os esquemas de LVS, LVS-SLOS e LVS-DA serão analisados em um mesmo cenário, comparando os resultados analíticos com os resultados simulados. Em seguida, serão verificadas as alterações no desempenho do sistema quando utilizado o modelo LOS/OLOS, que representa de forma mais realista o cenário de VANETs.

São comparados então os esquemas de LVS-SLOS e LVS-DA, de forma que seja possível identificar as melhorias no desempenho relacionadas ao uso de antenas direcionais, sem intervenção de aspectos relacionados ao modelo de propagação em larga escala, ou seja, a diferença de desempenho é relacionada apenas às DAs. Por fim, será verificado qual a relação entre o número de amostras e a porcentagem de erro no desempenho do sistema, considerando um desvanecimento em pequena escala.

4.1 PARÂMETROS UTILIZADOS

As simulações apresentadas nesta seção foram feitas utilizando a média de 10000 amostras. Os valores do desvio padrão referente ao sombreamento, expoente da perda de percurso e potência recebida a uma distância de 10 metros são utilizados conforme dados da Tabela 2.2. Considera-se que o usuário legítimo está viajando em uma rodovia e é assumido que a posição alegada pelo usuário legítimo é sempre sua posição real. As K BSs estão uniformemente distribuídas em uma área quadrada e é considerado o modelo de propagação em larga escala LOS/OLOS. Outros parâmetros serão informados conforme necessário.

4.2 COMPARAÇÃO ENTRE RESULTADOS ANALÍTICOS E SIMULADOS

Inicialmente, serão verificadas as equações analíticas obtidas neste trabalho. Com este objetivo, as Figuras 4.1, 4.2, 4.3 apresentam os valores de C_{id}, FP e VP em função do limiar T_Λ, com $K = 10$ BSs distribuídas de forma uniforme em uma área de $\rho \times \rho\ m^2$, com $\rho = 200$ m.

A Figura 4.1 demonstra um cenário em que é utilizado o LVS proposto em [Yan et al. 2014], considerando assim o modelo de propagação em larga escala log-normal. Como pode-se perceber, os valores de C_{id}, FP e VP obtidos de forma analítica estão de acordo com os valores obtidos através da simulação. Ainda conforme as equações analíticas, o valor de C_{id} depende de α e β.

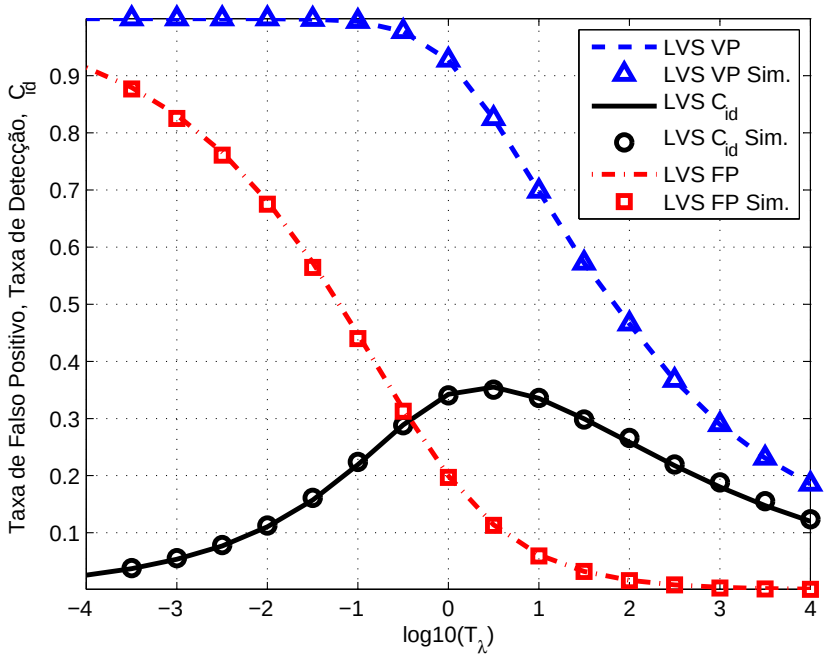

Figura 4.1: C_{id}, VP e FP em função de T_Λ para o esquema LVS com $K = 10$ BSs e $\rho = 200$m.

Na Figura 4.2, utilizando o mesmo cenário da Figura 4.1, os parâmetros de desempenho são novamente apresentados, agora para o esquema LVS-SLOS. É possível perceber que os valores obtidos de forma analítica através das equações descritas na Seção 3.1 estão de acordo com a simulação, verificando assim a validade das equações apresentadas.

Em seguida, a Figura 4.3 apresenta os resultados analíticos e simulados para o esquema LVS-DA com $N = 3$ DAs, no mesmo cenário utilizado nas Figuras 4.1 e 4.2. Novamente, pode-se perceber que os valores obtidos de forma analítica através das equações apresentadas no capítulo anterior estão de acordo com os resultados da simulação.

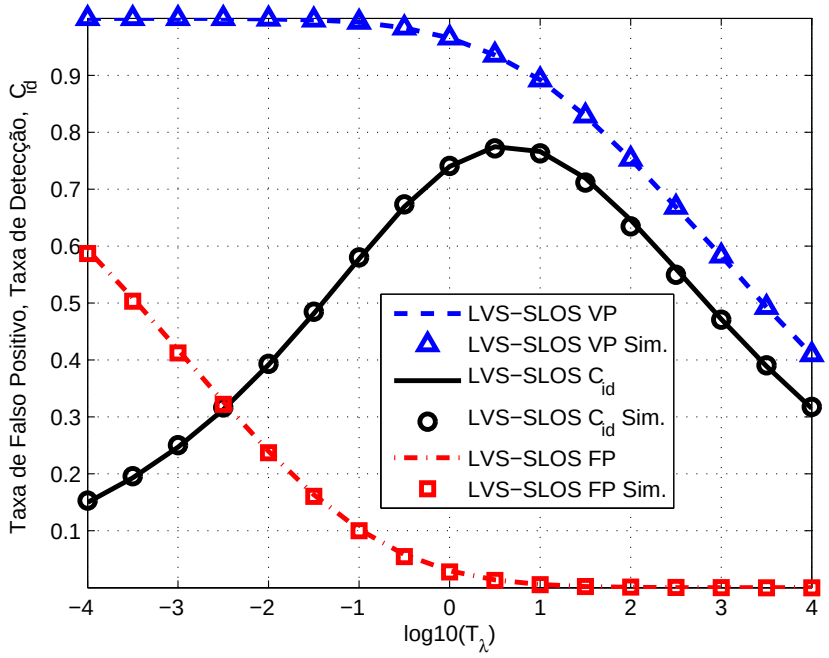

Figura 4.2: C_{id}**, VP e FP em função de** T_Λ **para o esquema LVS-SLOS com** $K = 10$ **BSs e** $\rho = 200$**m.**

Na Figura 4.4, são apresentados resultados analíticos e simulados para um número variável de BSs e de DAs, com $N \in \{2,3,4\}$ DAs. Embora existam diversas considerações relacionadas à figura apresentada, para esta subseção o mais importante é validar as equações utilizadas neste trabalho. Assim, é possível perceber que os valores obtidos de forma analítica estão de acordo com os valores obtidos através de simulação, demonstrando a validade das equações. Outra observação importante é que, para $N = 3$ DAs, o desempenho do sistema pode ser visto como um pouco superior ao desempenho quando o sistema tem uma BS a mais e $N = 2$ DAs. Por exemplo, para $K = 6$ e $N = 3$ tem-se $C_{id} = 0.87$, e quando $K = 7$ e $N = 2$ tem-se $C_{id} = 0.84$.

4.3 DESEMPENHO DOS ESQUEMAS LVS, LVS-SLOS E LVS-DA

Com o objetivo de comparar as melhorias no desempenho devido a utilização de um modelo que melhor corresponde ao cenário de VANETs, a Figura 4.5 apresenta uma comparação entre o esquema de LVS apresentado em [Yan et al. 2014] e o esquema LVS-SLOS apresentado no Capítulo 3.1, que considera o modelo mais realista de LOS/OLOS. Através da figura, pode-se perceber que a taxa de VP do LVS-SLOS é sempre superior a taxa de VP do LVS, demonstrando que o sistema tem uma capacidade melhor de identificar intrusos, uma vez que a potência recebida foi gerada usando o modelo em larga escala realista, e o LVS apresentando em [Yan et al. 2014] considera o modelo log-normal para identificar os usuários. Assim, a taxa

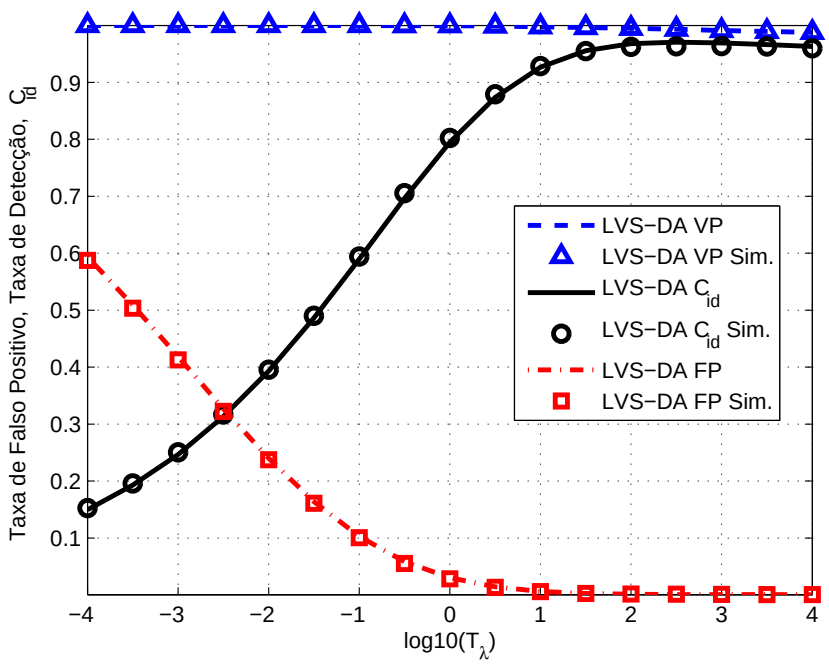

Figura 4.3: C_{id}**, VP e FP em função de** T_Λ **para o esquema LVS-DA com** $K = 10$ **BSs,** $\rho = 200$**m e** $N = 3$ **DAs.**

de FP do novo esquema é sempre inferior, de forma que o sistema tem uma probabilidade muito menor de identificar um usuário legítimo como malicioso. Como consequência, o parâmetro de desempenho tem um valor sempre maior no novo esquema.

Estes resultados são esperados uma vez que, como o esquema LVS-SLOS conhece de maneira mais precisa a potência do sinal recebido pela BS de um veículo, é possível diferenciar usuários maliciosos e legítimos com maior precisão, melhorando o desempenho do sistema. Embora esta análise seja útil para verificar o comportamento do sistema, o mais importante a ser observado é o maior do valor de C_{id} para cada um dos sistemas, uma vez que o LVS usará o limiar que otimize o desempenho.

As próximas análises consideram apenas o cenário em que o sistema utiliza o modelo de propagação LOS/OLOS, eliminando as diferenças de desempenho causadas pelo modelo de propagação em larga escala de forma que seja possível verificar as melhorias proporcionadas pela utilização das DAs. A Figura 4.6 apresenta os valores de C_{id}, FP e VP para os esquemas de LVS-SLOS e LVS-DA. Tendo em mente que o objetivo do LVS é escolher o limiar T_Λ que maximiza o C_{id}, pode-se ver que o valor máximo do C_{id} obtido pelo esquema utilizando as DAs é significativamente superior ao valor obtido utilizando o esquema LVS-SLOS. Pode-se ver também que, para qualquer valor de T_Λ, a taxa de VP do esquema proposto é próxima de 1. Isto ocorre devido a etapa DV, que não depende do limiar T_Λ. Conforme esperado, percebe-se

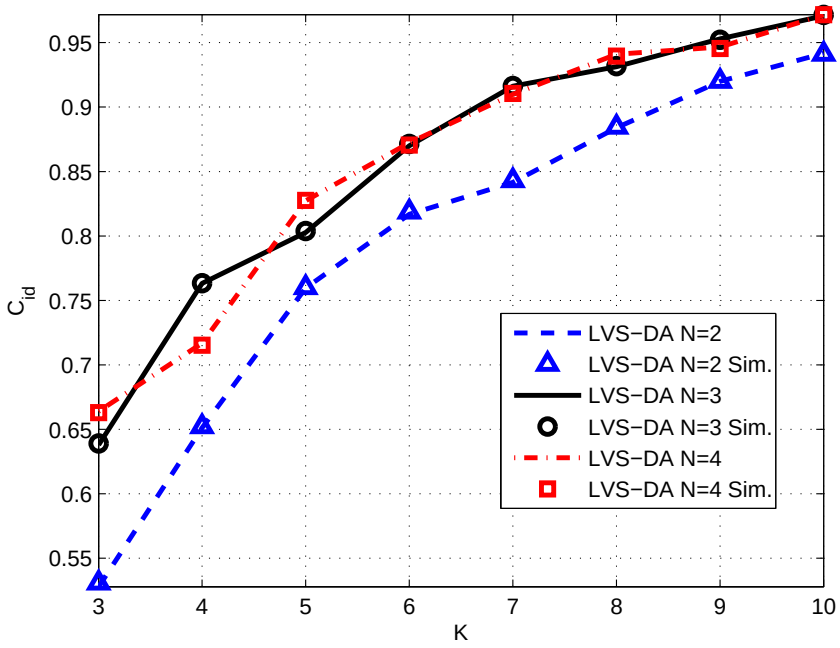

Figura 4.4: C_{id} **em função de** K **para o esquema LVS-DA com** $N \in \{2,3,4\}$ **DAs.**

que o valor de FP diminui conforme o limiar aumenta, seguindo um comportamento similar ao esquema LVS-SLOS.

A Figura 4.7 apresenta o valor de C_{id} em função da distância ρ. Pode-se perceber que o esquema LVS-DA tem um desempenho significativamente melhor que o esquema LVS-SLOS para todas as distâncias verificadas. É possível ver também que ambos os modelos têm um valor ótimo aproximadamente em $\rho = 500$ m. A melhoria no desempenho até 500 m é devido ao fato de que a diferença de RSS em cada BS aumenta conforme a distância aumenta. Porém, conforme a probabilidade SLOS aproxima-se de 1, o usuário malicioso é capaz de prever de forma mais eficaz a potência que deve ser recebida pelas BSs, diminuindo a diferença entre a RSS do usuário legítimo e malicioso.

4.4 NÚMERO ÓTIMO DE K_{MIN}

O desempenho do esquema LVS-DA para diferentes valores de K_{min} é investigado na Figura 4.8, com diferentes valores de DAs $N \in \{2,3,4\}$ e distâncias $\rho \in \{200,800\}$. Pode-se ver que o valor ótimo de K_{min} depende do número de antenas N. Embora aumentar o número de DAs nas BSs aumenta a taxa de VP, também ocorre um aumento na taxa de FP. Isto devido ao fato de que, com mais DAs, a probabilidade da RSS do usuário legítimo ter uma atenuação próxima de $-A_{\text{max}}$ aumenta, causando por consequência o aumento da probabilidade de FP.

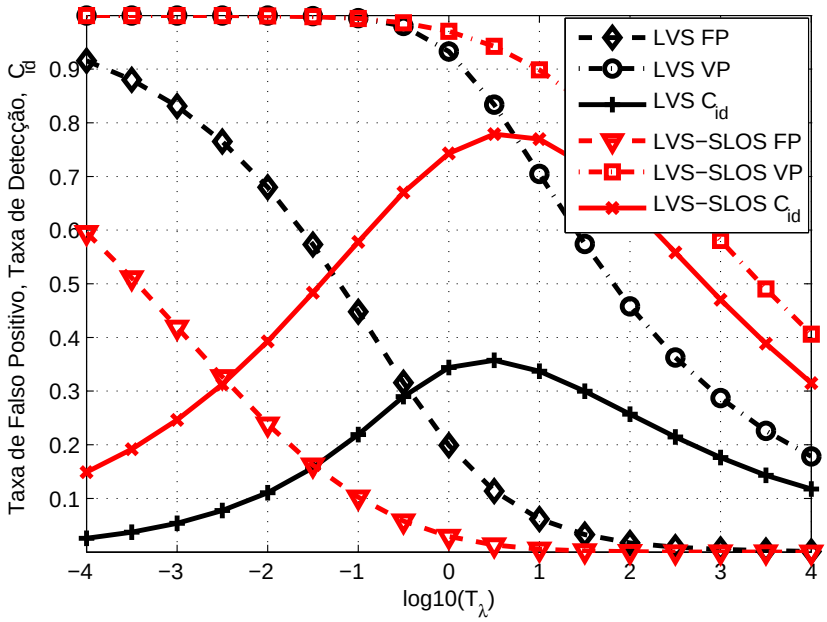

Figura 4.5: C_{id}**, VP e FP em função de** T_Λ **para os esquemas LVS e LVS-SLOS com** $K = 10$ **BSs e** $\rho = 200$**m.**

Com $N \in \{2,3,4\}$, o melhor desempenho é obtido usando, respectivamente, $K_{\min} = 3$, $K_{\min} = 4$ e $K_{\min} = 5$. Assim, o melhor valor de $K_{\min}$ aumenta com o número de DAs. O motivo é que, assim como o aumento do número de DAs gera uma taxa maior de FP, o aumento de $K_{\min}$ diminui a taxa de FP, uma vez que $K_{\min}$ representa o número necessário de estações que devem considerar o usuário como malicioso para que ele seja considerado malicioso pelo sistema. Além disto, a taxa de VP diminui quando $K_{\min}$ aumenta.

Outra observação importante é que, quando $K_{\min} = K$, a etapa DV quase nunca identifica um usuário como malicioso, e a saída do sistema é aproximadamente equivalente a saída de um sistema que não utilize DAs. Este fato também explica a diferença de desempenho entre $\rho = 800m$ e $\rho = 200$m quando $K_{\min} = 10$, uma vez que é esperada uma queda de desempenho quando a probabilidade de OLOS chega próxima de 1. Assim, quando comparado com $N = 3$, usando $N = 2$ tem-se uma taxa de FP e VP menor, e usando $N = 4$ tem-se uma taxa de FP e VP maior. Note que é desejável a menor taxa possível de FP e a maior taxa possível de VP. Uma consideração importante sobre a Figura 4.8 é que são utilizadas $K = 10$ BSs. Obviamente, quando o número K de BSs varia, o valor de $K_{\min}$ também pode variar. A Tabela 4.1 apresenta valores otimizados de $K_{\min}$ de acordo com o número de BSs e DAs, facilitando a escolha de $K_{\min}$ de acordo com o cenário analisado. É possível obter o valor de $K_{\min}$ para outros valores de K através de simulações ou utilizando as equações descritas no Capítulo 3, variando o valor de $K_{\min}$ e comparando os desempenhos obtidos.

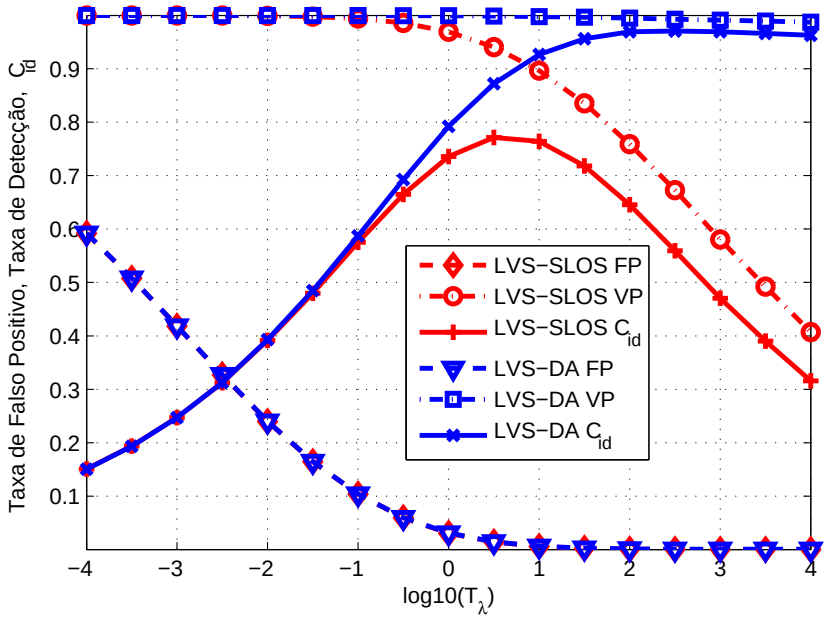

Figura 4.6: C_{id}**, VP e FP em função de** T_Λ **para os esquemas LVS-SLOS e LVS-DA com** $K = 10$ **BSs e** $\rho = 200$**m.**

Tabela 4.1: Número Ótimo de K_{min}

	2 DAs	3 DAs	4 DAs
2 BSs	1	1	2
3 BSs	1	2	2
4 BSs	2	2	2
5 BSs	2	2	3
6 BSs	2	3	3
7 BSs	2	3	4
8 BSs	3	3	4
9 BSs	3	4	4
10 BSs	3	4	5

4.5 COMPARAÇÃO DO DESEMPENHO EM FUNÇÃO DO NÚMERO DE BSS

Conforme descrito na subseção anterior, o número de BSs influencia no número de K_{min} otimizado e no desempenho do sistema. Assim, na Figura 4.9 é comparado o desempenho dos esquemas LVS-DA e LVS-SLOS para diferentes valores de K com $\rho = 500$ m e $N \in \{2,3,4,5,6\}$ DAs. Conforme esperado, percebe-se que o aumento no número de DAs e de BSs tende a aumentar o desempenho do sistema. Entretanto, como estes dois fatores influenciam no valor de K_{min}, a curva de desempenho de cada um dos modelos não é suave, existindo assim configurações específicas que apresentam melhores resultados. Desta forma, ainda que o desempenho quando utilizadas $N = 6$ DAs seja superior aos demais, a configuração utilizando $N = 3$ é aproximadamente equivalente a $N = 4$ e tem desempenho apenas um pouco

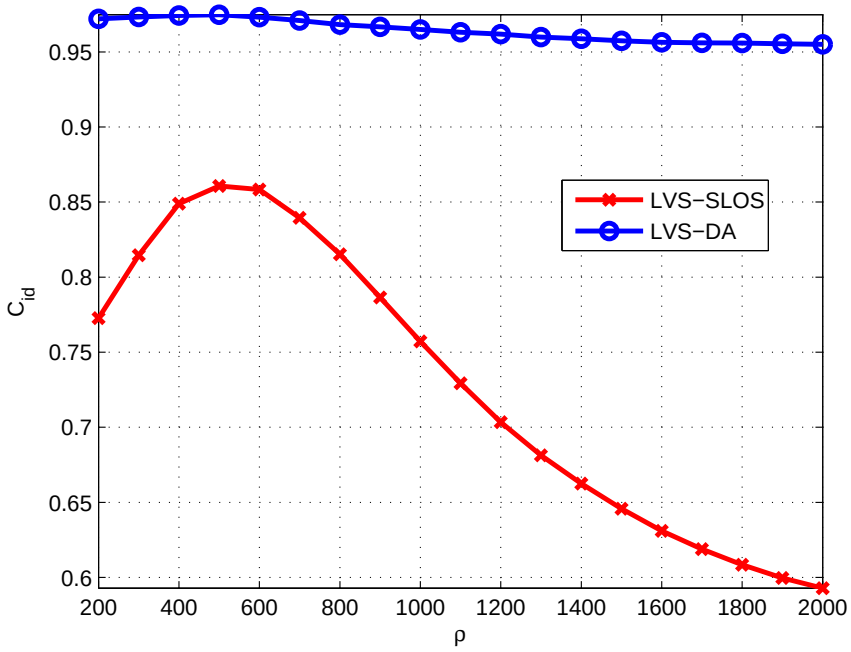

Figura 4.7: C_{id} **em função de** ρ **para os esquemas LVS-SLOS e LVS-DA, com** $K = 10$ **BSs.**

abaixo da configuração $N = 5$ DAs, aproximando conforme o número de BSs aumenta. Assim, a configuração utilizando $N = 3$ DAs é uma boa opção quando comparado com o esquema com $N = 4$ DAs, uma vez que é obtido um resultado semelhante com um número menor de antenas.

Utilizando o mesmo cenário da Figura 4.9, é comparado o desempenho dos esquemas LVS-DA com $N = 3$ e LVS-SLOS na Figura 4.10, apresentando também o desempenho da etapa de DV quando usada de forma isolada. Conforme a figura, o melhor resultado é obtido quando utilizado o esquema LVS-DA, uma vez que este é baseado tanto na etapa de DV quanto na etapa de LVS. Comparando as Figuras 4.10 e 4.7, percebe-se também que, para outros valores de ρ, a diferença entre o desempenho apresentado pelos esquemas LVS-DA e LVS-SLOS é ainda maior.

Para $\rho = 500$ m, o esquema LVS-DA com $N = 3$ DAs e $K = 3$ BSs tem um desempenho melhor que o esquema LVS-SLOS com $K = 6$ BSs. Como esta diferença de 3 BSs é constante, é possível concluir que mesmo com 3 BSs a menos, o esquema LVS-DA com $N = 3$ tem desempenho melhor que o esquema LVS-SLOS. Pode-se ver também que a etapa DV tem um desempenho próximo do LVS-DA. Para $K = 7$, por exemplo, $C_{id} = 0.920$ para o esquema LVS-DA e $C_{id} = 0.871$ para a etapa de DV. Mesmo que estes resultados sejam próximos, é importante notar que o cenário em questão lida com questões de segurança e qualquer aumento significativo de desempenho deve ser considerado.

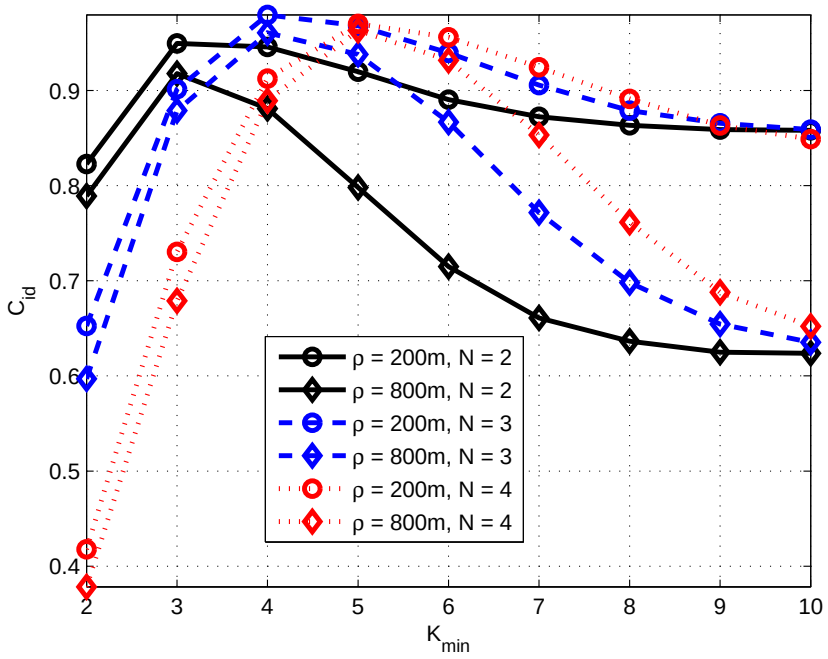

Figura 4.8: C_{id} **em função de** $K_{\mathbf{min}}$ **para o esquema LVS-DA com** $N \in \{2,3,4\}$ **DAs,** $K = 10$ **BSs e** $\rho \in \{200,800\}$ **m.**

4.6 PORCENTAGEM DE ERRO ASSOCIADA AO DESVANECIMENTO EM PEQUENA ESCALA

Todos os resultados apresentados neste trabalho consideram apenas os efeitos da perda de percurso e do sombreamento que representam, respectivamente, a atenuação causada pela dissipação da potência do sinal irradiada pelo transmissor e a atenuação causada devido a obstáculos entre o transmissor e o receptor. Assim, os efeitos de pequena escala descritos na Seção 2.2.2 são desconsiderados, levando em consideração que ao se obter a média de diversas amostras da RSS, pode-se simplesmente utilizar as equações relacionadas à larga escala para estimar a potência do sinal recebido. Embora esta aproximação seja válida, existe uma porcentagem de erro associada a ela e é importante traçar um paralelo entre o número de amostras e esta porcentagem. A Figura 4.11 foi obtida através de simulação para os esquema de LVS-DA e LVS-SLOS, mostrando o erro da métrica C_{id} quando utilizada uma quantidade variável de amostras da RSS. Desta forma, foi comparado o desempenho obtido pelo sistema quando considerado apenas os efeitos em larga escala com o desempenho obtido quando considerado também o desvanecimento em pequena escala Rayleigh, descrito na Seção 2.2.2. Pode-se perceber que o esquema com DAs precisa de uma quantidade menor de amostras para obter a mesma porcentagem de erro que o esquema LVS-SLOS, apresentando assim uma vantagem computacional uma vez que é necessário processar um número menor de amostras.

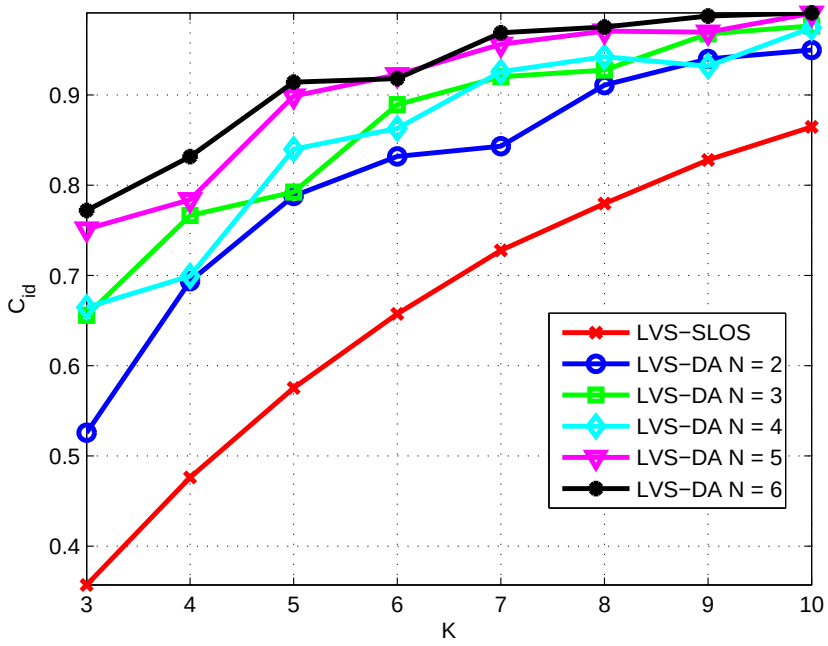

Figura 4.9: C_{id} **em função de** K **BSs para os esquemas LVS-SLOS e LVS-DA com** $N \in \{2,3,4,5,6\}$**.**

Outra observação importante é que a portagem de erro varia de acordo com o número de K BSs. Isto se deve ao fato de que um sistema com mais BSs tem um número de amostras da RSSs maior, diminuindo os efeitos do desvanecimento em pequena escala no desempenho do sistema.

4.7 COMENTÁRIOS

Neste capítulo, inicialmente foram feitas validações das equações descritas nos capítulos anteriores com resultados obtidos através de simulações, para um número variável de BSs e de DAs. Considerando um cenário mais realista para VANETs, posteriormente foi feita uma análise do desempenho do esquema LVS-SLOS. Como previsto, o esquema LVS-SLOS teve desempenho significativamente superior ao do esquema LVS proposto em [Yan et al. 2014]. Foi feita então a comparação com o esquema LVS-DA, proposto no Capítulo 3. Como esperado, a utilização de $N = 3$ antenas direcionais proporciona uma melhora significativa no sistema, tendo um desempenho superior mesmo quando comparado ao esquema LVS-SLOS utilizando 3 BSs a mais, podendo melhorar com o aumento do número de DAs.

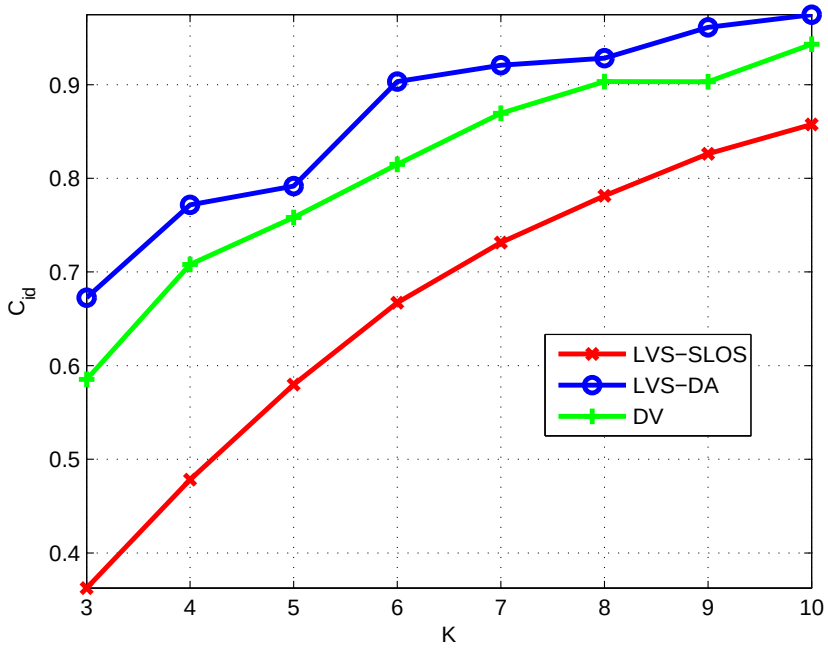

Figura 4.10: C_{id} **em função de** K **BSs para os esquemas de LVS-SLOS, LVS-DA e DV.**

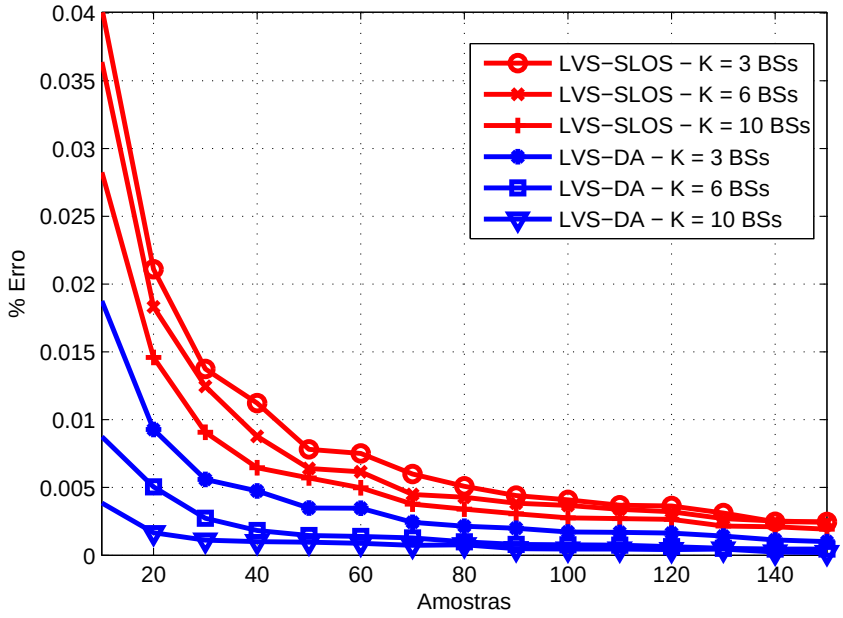

Figura 4.11: Porcentagem de erro em função do número de K **BSs e do número de amostras para os esquemas de LVS-SLOS e LVS-DA.**

5 COMENTÁRIOS FINAIS

Neste trabalho, foi apresentando um método para a utilização de DAs no sistema de verificação de localização baseado em teoria da informação apresentado em [Yan et al. 2014]. O esquema proposto foi chamado de LVS-DA. Verificou-se também como o modelo de propagação realista para VANETs (LOS/OLOS) proposto em [Abbas et al. 2012] influencia nos resultados do sistema.

Primeiro verificou-se como o LVS deve ser modificado para que o modelo de propagação LOS/OLOS pudesse ser usado, permitindo que o sistema classifique melhor os usuários. Este sistema foi chamado de LVS-SLOS. Em seguida, foi constatado que a utilização de DAs pode ser usada nestes sistemas comparando a potência do sinal recebido por cada DA nas BSs. Foi proposto assim a criação de uma etapa adicional de validação chamada de DV, que classifica os usuários baseado na diferença da potência recebida entre as DAs. Assim, o usuário é considerado malicioso sempre que ao menos $K_{\min}$ BSs recebem a maior potência na DA incorreta. Verificou-se também quais os efeitos no desempenho estimado ao considerar apenas a potência média recebida, desprezando os efeitos em pequena escala.

As expressões analíticas obtidas para o sistema proposto foram verificadas com o uso de resultados numéricos, para um número variável de BSs e de DAs. Utilizando o método apresentando, é possível verificar qual o desempenho estimado para uma determinada configuração sem a utilização de simulações, facilitando a tomada de decisões relacionadas ao sistema. Constatou-se que a utilização de três antenas direcionais proporciona um desempenho equivalente a no mínimo três estações a mais quando comparado com o LVS-SLOS, correspondendo a um aumento de 10% a 26%, dependendo do número de BSs utilizadas pelo sistema. Mesmo quando utilizado apenas o estágio de verificação direcional, o desempenho do sistema é superior a utilização do esquema LVS-SLOS, demonstrando a eficiência da utilização de antenas direcionais na verificação de localização.

Trabalhos futuros incluem a investigação de como a utilização das antenas direcionais pode impactar positivamente em outros parâmetros de desempenho, como a taxa máxima de

transmissão entre os veículos e as BSs, e a verificação do comportamento do sistema quando a distribuição das posições das BSs não é uniforme, gerando assim uma probabilidade por ângulo diferente. Por fim, pode ser feita uma análise de como a presença de grandes obstáculos entre os veículos pode alterar o comportamento do sistema.

REFERÊNCIAS

ABBAS, T.; TUFVESSON, F.; KAREDAL, J. A measurement based shadow fading model for vehicle-to-vehicle network simulations. **ArXiv e-prints**, Jan. 2012.

ABUMANSOOR, O.; BOUKERCHE, A. A secure cooperative approach for nonline-of-sight location verification in VANET. **IEEE Trans. Veh. Technol.**, v. 61, n. 1, p. 275–285, Jan. 2012. ISSN 0018-9545.

CHEN, Y. et al. Detecting and localizing identity-based attacks in wireless and sensor networks. **IEEE Trans. Veh. Technol.**, v. 59, n. 5, p. 2418–2434, Jun. 2010. ISSN 0018-9545.

CHENG, L. et al. Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band. **Selected Areas in Communications, IEEE Journal on**, v. 25, n. 8, p. 1501–1516, 2007. ISSN 0733-8716.

DPVAT. **Números sobre acidentes de trânsito**. January 2014. Disponível em: <http://goo.gl/GWA2LU>.

DRAWIL, N.; BASIR, O. Intervehicle-communication-assisted localization. **Intelligent Transportation Systems, IEEE Transactions on**, v. 11, n. 3, p. 678–691, 2010. ISSN 1524-9050.

GEZICI, S. A survey on wireless position estimation. **Wireless Personal Communications**, Springer US, v. 44, n. 3, p. 263–282, 2008. ISSN 0929-6212. Disponível em: <http://dx.doi.org/10.1007/s11277-007-9375-z>.

GOLDSMITH, A. **Wireless Communications**. [S.l.]: Cambridge University Press, 2005.

GU, G. et al. **An Information-Theoretic Measure of Intrusion Detection Capability**. [S.l.], 2005.

IBGE. **Números sobre Industria Automotiva**. August 2013. Disponível em: <http://goo.gl/oO855u>.

LEINMULLER, T.; SCHOCH, E.; KARGL, F. Position verification approaches for vehicular ad hoc networks. **IEEE Wireless Commun.**, v. 13, n. 5, p. 16–21, Oct. 2006. ISSN 1536-1284.

LIU, B.-C.; LIN, K.-H. Wireless location uses geometrical transformation method with single propagation delay: Model and detection performance. **IEEE Trans. Veh. Technol.**, v. 57, n. 5, p. 2920–2932, Sep. 2008. ISSN 0018-9545.

NEYMAN, J.; PEARSON, E. S. On the problem of the most efficient tests of statistical hypotheses. **Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character**, The Royal Society, v. 231, p. 289–337, 1933. ISSN 02643952.

ONSV. **Números sobre acidentes de trânsito**. March 2014. Disponível em: <http://goo.gl/gpN8E4>.

OWEN, D. B. Tables for computing bivariate normal probabilities. April 1956.

RAMAN, C. et al. Half-duplex relaying in downlink cellular systems. **IEEE Trans. Wireless Commun.**, v. 10, n. 5, p. 1396–1404, May. 2011. ISSN 1536-1276.

RAPPAPORT, T. **Wireless Communications: Principles and Practice**. 2nd ed.. ed. [S.l.]: Prentice Hall PTR, 2001.

SONG, J.-H.; WONG, V.; LEUNG, V. C. M. Secure location verification for vehicular ad-hoc networks. In: **Proc. IEEE GLOBECOM**. [S.l.: s.n.], 2008. ISSN 1930-529X.

STARK, H.; WOODS, J. W. (Ed.). **Probability, Random Processes, and Estimation Theory for Engineers**. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1986. ISBN 0-13-711706-X.

STECK, G. P. A table for computing trivariate normal probabilities. Jan 1958.

TROTT, M. **The Mathematica Guidebooks Additional Material: Probability Distribution of a Quotient**. [S.l.]: Springer-Verlag, New York, 2007.

WARD. **Números sobre Industria Automotiva**. August 2011. Disponível em: <http://goo.gl/HsyIRt>.

XIAO, B.; YU, B.; GAO, C. Detection and localization of sybil nodes in VANETs. In: **Proc. Workshop DIWANS**. [S.l.: s.n.], 2006.

YAN, G.; OLARIU, S.; WEIGLE, M. Providing location security in vehicular ad hoc networks. **IEEE Wireless Commun.**, v. 16, n. 6, p. 48–55, Dec. 2009. ISSN 1536-1284.

YAN, S. et al. An information theoretic location verification system for wireless networks. In: **Proc. IEEE GLOBECOM**. [S.l.: s.n.], 2012.

YAN, S. et al. Optimal information-theoretic wireless location verification. **IEEE Trans. Veh. Technol.**, v. 63, n. 7, p. 3410–3422, Sept. 2014. ISSN 0018-9545.

YAN, S. O. G.; WEIGLE, M. Cross-layer location verification enhancement in vehicular networks. In: **Proc. IEEE Intelligent Vehicles Symposium (IV)**. [S.l.: s.n.], 2010. ISSN 1931-0587.

ÍNDICE REMISSIVO