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

MARCO ANTÔNIO CHIODI JUNIOR

EMBARALHAMENTO DE PACOTES E SELEÇÃO DE ANTENAS COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA EM REDES SEM FIO

DISSERTAÇÃO

CURITIBA

2016

MARCO ANTÔNIO CHIODI JUNIOR

EMBARALHAMENTO DE PACOTES E SELEÇÃO DE ANTENAS COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA EM REDES SEM FIO

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: Informática Industrial.

Orientador: Prof. Dr. João Luiz Rebelatto

Coorientador: Prof. Dr. Richard Demo Souza

CURITIBA

2016

Dados Internacionais de Catalogação na Publicação

C539e 2016

Chiodi Junior, Marco Antonio
Embaralhamento de pacotes e seleção de antenas como alternativa para aumentar a segurança em redes sem fio / Marco Antonio Chiodi Junior.-- 2016.
47 p. : 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, 2016

1. Redes locais sem fio. 2. Segurança da informação. 3. Antenas – Segurança. 4. 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, inst. IV. Título.

CDD: Ed. 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. ____

Embaralhamento De Pacotes E Seleção De Antenas Como Alternativa Para Aumentar A Segurança Em Redes Sem Fio

por

Marco Antônio Chiodi Junior

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

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 14:**30h** do dia 02 de março de 2016. O trabalho foi aprovado pela Banca Examinadora, composta pelos professores doutores:

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

Prof. Dr. Evelio Martin Garcia Fernandez
(UFPR)

Prof. Dr. Guilherme Luiz Moritz
(UTFPR)

Visto da coordenação:

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

A Folha de Aprovação assinada encontra-se na Coordenação do Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial.

AGRADECIMENTOS

Agradeço a Deus pelo vir-a-ser e pela possibilidade de estar aqui; aos meus pais, Marco Antônio Chiodi e Maria Gorete da Silva Chiodi, por terem sempre me apoiado e acreditado em mim; a minha esposa, Gabriele Regiane Winter Chiodi, por ter me ajudado desde a graduação até aqui; ao meu orientador, Prof. João Luiz Rebelatto, por todo apoio, dedicação e paciência; ao meu coorientador, Prof. Richard Demo Souza, por todo auxílio prestado; ao Prof. Luciano Scandelari e a todos os meus colegas e amigos da Radioenge pela compreensão e apoio neste período de mestrado e também aos meus amigos e colegas do LabSC por toda a ajuda.

RESUMO

CHIODI JUNIOR, MARCO ANTONIO. EMBARALHAMENTO DE PACOTES E SELEÇÃO DE ANTENAS COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA EM REDES SEM FIO. 47 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

Neste trabalho, é proposta a utilização de múltiplas antenas de transmissão juntamente com o embaralhamento de pacotes para aumentar a segurança de uma rede composta por dois nós legítimos (Alice e Bob) e um espião passivo, todos eles providos com múltiplas antenas. Levando em consideração o denominado intervalo de segurança (*Security Gap*) como métrica de desempenho e assumindo um cenário com desvanecimento quase-estático, foi então analisado (analítica e numericamente) o intervalo de segurança em termos de probabilidade de *outage* e de taxa de erro de pacotes (usando códigos convolucionais), mostrando que em ambas as situações é possível atingir níveis negativos de intervalo de segurança com um número praticável de antenas transmissoras. Além disso, mostra-se que usando uma aproximação para o intervalo de segurança baseado na probabilidade de *outage*, é possível estimar com precisão o número de antenas em Alice para se atingir um determinado nível de segurança. Também é mostrado que utilizando o esquema de seleção de antena de transmissão juntamente com o método de combinação de razão máxima na recepção (TAS/MRC) com o embaralhamento de pacote, é possível ter os mesmos resultados, ou muito similares, para um caso real utilizando a FER quando comparado com o caso ideal da probabilidade de *outage*.

Palavras-chave: Segurança em camada física, Intervalo de Segurança, Embaralhamento de Pacotes, TAS/MRC.

ABSTRACT

CHIODI JUNIOR, MARCO ANTONIO. FRAME SCRAMBLING AND ANTENNA SELECTION TO INCREASE WIRELESS NETWORK SECURITY. 47 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

In this work, the use of multiple transmitting antennas with frame scrambling is proposed to increase the security of a network composed by two legitimate nodes (Alice and Bob) and a passive eavesdropper, all of them provided with multiple antennas. Considering the so-called security gap as the performance metric and assuming a quasi-static fading scenario, it was evaluated (analytically and through numerical results) the security gap based on both the outage probability and the frame error rate (using convolutional codes), showing that, in both situations, it is possible to achieve negative values of security gap with a feasible number of transmitting antennas. Moreover, it is showed that using an approximation to security gap based on outage probability, one can accurately estimate the number of antennas in Alice needed to achieve a given level of security. It is also showed that using TAS/MRC with frame scrambling, it is possible to get the same results, or almost the same, in a real case using FER when it is compared to an ideal case with outage probability.

Keywords: Physical-layer Security, Security Gap, Frame Scrambling, TAS/MRC.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

CSI	Informação do Estado do Canal, do inglês *Channel State Information*
SNR	Relação Sinal Ruído, do inglês, *Signal to Noise Ratio*
TAS	Seleção de Antena de Trasmissão, do inglês *Transmit Antenna Selection*
MRC	Combinação de Razão Máxima, do inglês *Maximal-Ratio Combining*
MIMO	Múltiplas Entradas, Múltiplas Saídas, do inglês *Multiple Input and Multiple Output*
FER	Taxa de Erro de Pacote, do inglês *Frame Error Rate*
bpcu	Bits por uso de canal, do inglês *Bits per channel use*
AWGN	Ruído Gaussiano Branco e Aditivo, do inglês *Additive White Gaussian Noise*
BER	Taxa de Erro de Bit, do inglês *Bit Error Rate*

LISTA DE SÍMBOLOS

$\mathscr{O}$	Probabilidade de *outage*
P_f	FER
n_A	Número de antenas em Alice
n_B	Número de antenas em Bob
n_E	Número de antenas em Eve
$\mathbf{y}_j^i$	Sinal recebido no i-ésima antena do nó j
P_t	Potência de transmissão
κ_j	Coeficiente de perda de percurso do transmissor a i-ésima antena do nó j
h_j^i	Desvanecimento visto pela i-ésima antena no nó j
$\mathbf{x}$	Sinal enviado por Alice
n_j^i	Ruído térmico visto pela i-ésima antena do nó j
d_j	Distância entre o transmissor e o nó j
α	Coeficiente de perda de percurso
λ	Comprimento de onda
f_c	Frequência de portadora
γ_j	Relação sinal-ruído instantânea no nó j
N_0	Densidade espectral de potência de ruído
B	Largura de banda utilizada
$\mathscr{R}$	Eficiência espectral em bpcu
γ^{th}	Relação sinal-ruído necessária para atingir uma eficiência espectral $\mathscr{R}$, sendo defina pela seguinte expressão: $2^{\mathscr{R}} - 1$
$\mathscr{O}_E$	Probabilidade de *outage* em Eve
P_{fE}	FER em Eve
$\mathscr{O}_E^*$	Probabilidade de *outage* alvo em Eve
P_{fE}^*	FER alvo em Eve
$\mathscr{O}_B$	Probabilidade de *outage* em Bob
P_{fB}	FER em Bob
$\mathscr{O}_B^*$	Probabilidade de *outage* alvo em Bob
P_{fB}^*	FER alvo em Bob
Δ	Gap de segurança
$\bar{\gamma}_B^*$	Relação sinal-ruído para atingir um desempenho alvo em Bob
$\bar{\gamma}_E^*$	Relação sinal-ruído para atingir um desempenho alvo em Eve
d_B	Distância entre Alice e Bob
d_E	Distância entre Alice e Eve
N	Comprimento do pacote não codificado
$\mathbf{u}_S$	Mensagem embaralhada
$\mathbf{u}$	Mensagem original
$\mathbf{S}$	Matriz de embaralhamento
$P_b^{S-\mathrm{AWGN}}$	BER considerando embaralhamento no canal AWGN
p	BER sem embaralhamento
w	Peso de coluna da matriz $\mathbf{S}^{-1}$

P_f^{S-AWGN}	FER considerando o embaralhamento no canal AWGN
Z	Número de pacotes a serem embaralhados
$P_b^{ZS-\text{AWGN}}$	BER considerando o embaralhamento de pacotes no canal AWGN
$P_f^{ZS-\text{AWGN}}$	FER considerando embaralhamento de pacotes
R	Taxa do código correto de erros
t	Capacidade de correção do código
p_0	BER considerando um código corretor de erros, ou seja, $p_0(\gamma) = p\left(\frac{N}{M}\gamma\right)$
M	Comprimento do pacote codificado
N_c	Tamanho da palavra de entrada do código convolucional
M_c	Tamanho da palavra de saída do código convolucional
K	Comprimento de restrição do código convolucional, do inglês *constraint length*
$P_b^{UB-\text{AWGN}}$	Limite superior da BER de um código convolucional no canal AWGN
δ_{free}	Distância mínima do código
Λ_δ	Peso de uma palavra código que está a uma distância δ da palavra código composta apenas por zeros
f_γ	Função densidade de probabilidade da variável aleatória γ
n_r	Número de antenas de um receptor genérico
$\bar{\gamma}$	Relação sinal-ruído média por antena do receptor
$\Gamma(a,b)$	Função Gama incompleta inferior
$\Gamma(a)$	Função Gama completa
n_t	Número de antenas de uma transmissor genérico
$\Gamma^{-1}(y,a)$	Função inversa da gama incompleta
Δ^{app}	Intervalo de segurança aproximado
n_A^{app}	Número de antenas aproximado em Alice

SUMÁRIO

1 INTRODUÇÃO

Segurança é um assunto crítico atualmente, principalmente no meio sem fio, devida a característica de difusão deste, a qual permite que potenciais espiões (*eavesdroppers*) sejam capazes de interceptar transmissões confidenciais. Tradicionalmente, no modelo de rede de cinco camadas, a segurança é implementada nas camadas superiores, através de criptografia. No entanto, com o aumento do tamanho das redes, a geração e distribuição das chaves criptográficas acaba se tornando inviável, ou ainda, em redes descentralizadas e ad-hoc, tais chaves não podem ser geradas.

O conceito de segurança na camada física, introduzido em (SHANNON, 1949), é uma abordagem promissora no sentido de aumentar a segurança de comunicação, complementando as técnicas clássicas de criptografia. Em (WYNER, 1975), Wyner estendeu o trabalho de Shannon introduzindo o canal chamado *wiretap*, o qual é composto por um par de nós legítimos (normalmente referenciados como Alice e Bob) comunicando na presença de um espião passivo (Eve). Trabalhos recentes aplicam os conceitos de segurança na camada física para comunicações sem fio, mostrando que a aleatoriedade inerente a estes pode melhorar o sigilo de uma rede (GOPALA et al., 2008; BARROS; RODRIGUES, 2006; TANG et al., 2009, 2007).

Entretanto, o projeto de códigos *wiretap* é geralmente desconhecido considerando vários cenários de interesse como é o caso do canal sem fio com desvanecimento quase-estático. Para a utilização dos códigos *wiretap* é necessário uma métrica para a avaliação da segurança do canal, sendo que um dos motivos que impede o desenvolvimento de códigos *wiretap* é a falta de uma métrica simples que possa ser avaliada numericamente (BLOCH; BARROS, 2011). Por exemplo, em (BLOCH et al., 2008), são vistos dois tipos de métricas baseadas na capacidade de canal: a capacidade média de confidencialidade (do inglês, *Average Secrecy Capacity* e a probabilidade de *outage* de confidencialidade (do inglês, *Outage Probability of Secrecy Capacity*. No entanto, em ambos os casos, é necessário certo conhecimento do canal (CSI, do inglês, *Channel State Information*); sendo que no primeiro caso, é necessário total CSI enquanto, no outro, apenas do canal principal.

Uma métrica de segurança mais prática foi introduzida em (KLINC et al., 2011), denominado intervalo de segurança (do inglês, *security gap*), em que a segurança é medida em termos da razão entre as relações sinal-ruído (SNR, do inglês inglês *Signal to Noise Ratio*) requerida em Bob e em Eve para obter uma comunicação com uma taxa de erro baixa o suficiente em Bob e ao mesmo tempo atingir um nível suficiente de segurança na camada física. Isso é, considerando um canal com desvanecimento quase-estático, deve-se garantir: *i) sigilo*, garantindo que a taxa de erro em Eve seja superior a um dado valor alvo; e *ii) confiabilidade*, garantindo que Bob opera com uma taxa de erro abaixo de um limite requerido. A taxa de erro se refere a uma métrica utilizada para medir o desempenho; neste trabalho, foram utilizadas a probabilidade de *outage* ($\mathscr{O}$) e a taxa de erro de pacote (P_f).

Em (BALDI et al., 2012), os autores recorrem a uma técnica referida como embaralhamento de pacotes (do inglês, *Frame Scrambling*), onde vários pacotes são embaralhados a fim de diminuir o intervalo de segurança por meio do aumento da propagação de erros residuais. A ideia atrás do embaralhamento é que o erro causado por apenas um bit em qualquer um dos muitos pacotes utilizados no processo é propagado aleatoriamente por todos os pacotes, maximizando assim a incerteza do processo de decodificação; em condições especiais, pode-se aumentar a incerteza de tal forma que metade dos bits recebidos estejam incorretos por conta de apenas um único bit errado.

Além disso, o uso de múltiplas antenas na transmissão foi recentemente mostrado como sendo um meio eficiente de aumentar o sigilo em redes sem fio, pois assim é possível gerar uma vantagem instantânea do canal Alice-Bob sobre o canal espião (ALVES et al., 2012; YANG et al., 2013; CHIODI JUNIOR et al., 2015b; SANAYEI; NOSRATINIA, 2004). Assim, unindo as duas técnicas, embaralhamento de pacotes e diversidade de transmissão, o receptor malicioso poderá cometer mais erros de decodificação do que o legítimo dependendo da geometria do problema, sendo que cada erro será ainda potencializado pelo embaralhamento.

Alguns resultados preliminares com o intervalo segurança baseado na probabilidade de *outage* em um cenário com múltiplas antenas onde Alice utiliza o esquema de Seleção de Antena de Transmissão (TAS, do inglês *Transmit Antenna Selection*) (GOLDSMITH, 2005; SANAYEI; NOSRATINIA, 2004) enquanto ambos, Bob e Eve, operam utilizando o esquema de Combinação de Razão Máxima (MRC, do inglês *Maximal-Ratio Combining*) (GOLDSMITH, 2005) são apresentados em (CHIODI JUNIOR et al., 2015a) e em (CHIODI JUNIOR et al., 2015b), mostrando os benefícios da utilização do TAS juntamente com o embaralhamento para reduzir o intervalo de segurança. Uma característica importante do TAS é requer uma quantidade mínima de realimentação (apenas o índice da melhor antena). Além disso, mesmo que o

espião seja capaz de acessar a mensagem com a informação da antena, a antena selecionada é apenas ótima para o nó legítimo desde que os dois canais sejam independentes. Outro aspecto do TAS é que ele emprega apenas uma cadeia de rádio frequência ao invés de muitas em paralelo, esta característica reduz custo, complexidade, consumo e espaço (ALVES et al., 2012; BRANTE et al., 2011).

1.1 INTRODUÇÃO AO PROBLEMA

Um ponto importante a ser levantado sobre os métodos tradicionais de segurança baseados em criptografia é que suas medidas se baseiam na premissa de que a segurança não pode ser quebrada sem o conhecimento da chave, no entanto, esta não tem comprovação matemática até então (BLOCH; BARROS, 2011). Assim, as análises devem considerar uma limitação na capacidade computacional do espião. No entanto, isso não ocorre quando se implementa a segurança na camada física, onde se pode considerar um espião sem limitações na capacidade computacional ou no conhecimento do canal (MUKHERJEE et al., 2014). Além disso, é possível também utilizar técnicas de segurança implementadas na camada física juntamente com criptografia para melhorar os resultados em comparação com aqueles que utilizam apenas uma solução (BLOCH; BARROS, 2011).

Considerando o canal sem fio com três nós (Alice, Bob e Eve), que será devidamente apresentado no Capítulo 2, onde o canal legítimo é independente do outro, nota-se que não há um canal seguro para envio de chaves criptográficas. Neste modelo, também se considera a utilização de diversidade de transmissão e recepção.

Para garantir o sigilo da comunicação, deve-se fazer com que Eve cometa mais erros do que Bob, para isso, considerando que Bob e Eve estejam utilizando os mesmos esquemas de recepção, o canal de Bob deve estar em melhores condições do que o de Eve. Considerando diferentes métodos na recepção, o problema então é de como criar uma vantagem para o canal Alice-Bob sobre o canal espião. Em (ALVES et al., 2012; YANG et al., 2013; CHIODI JUNIOR et al., 2015b), a utilização de sistemas MIMO é colocada como uma solução para criar tal vantagem, aumentando assim o sigilo na comunicação.

Outro requisito para a segurança é garantir a confiabilidade da informação em Bob, para isto, pode-se utilizar códigos corretores de erros; no entanto, em (BALDI et al., 2012), é mostrado que a utilização de códigos sistemáticos deve ser evitada, assim, os autores fazem uso da técnica de embaralhamento de pacotes, para adicionar incertezas no processo de decodificação, fazendo com que o erro residual na palavra seja espalhado aleatoriamente.

Portanto, neste trabalho de mestrado, buscou-se analisar do ponto de vista de segurança na camada física o esquema de transmissão e recepção TAS/MRC juntamente com a técnica de embaralhamento de pacotes, em um cenário prático onde não há conhecimento dos canais legítimo e ilegítimo por parte de Alice, através da métrica proposta em (KLINC et al., 2011) chamada intervalo de segurança e que será definida mais adiante.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Prover e analisar a segurança no canal *wiretap* através do intervalo de segurança, considerando o caso MIMO, o esquema TAS/MRC com embaralhamento de pacotes sem CSI.

1.2.2 OBJETIVOS ESPECÍFICOS

- Obter expressões analíticas para a intervalo de segurança do TAS/MRC com embaralhamento de pacotes utilizando duas métricas: probabilidade de *outage* e FER;
- Confirmar através de simulações os resultados obtidos analiticamente;

1.3 PUBLICAÇÕES

Dentre as publicações e submissões realizadas no período de mestrado tem-se um artigo publicado em periódico internacional (CHIODI JUNIOR et al., 2015b), um artigo publicado em conferência nacional (CHIODI JUNIOR et al., 2015a) e um artigo submetido para periódico internacional (CHIODI JUNIOR et al., 2015c).

1.4 ESTRUTURA DO DOCUMENTO

O Capítulo 2 apresenta o modelo de canal utilizado, bem como os conceitos preliminares para o desenvolvimento do trabalho, tais como segurança em camada física, embaralhamento de pacotes e intervalo de segurança.

O Capítulo 3 traz a solução proposta para a melhora da segurança, o TAS/MRC com embaralhamento de pacotes, fazendo a dedução analítica do intervalo de segurança utilizando duas métricas, FER e probabilidade de *outage*.

Os resultados numéricos, avaliações e comparações destas estão todos contidos no Capítulo 4. Resultados estes que comprovam a utilização do método proposto para o aumento da segurança na camada física no meio sem fio.

Por fim, o Capítulo 5 apresenta as conclusões e comentários finais da dissertação juntamente com os trabalhos futuros.

2 PRELIMINARES

2.1 MODELO DO SISTEMA

Neste trabalho, considera-se uma rede sem fio composta por um transmissor, Alice (A), comunicando com um receptor, Bob (B), na presença de um espião, chamado Eve (E).

Alice é equipada com n_A antenas e utiliza a técnica TAS para a transmissão, enquanto Bob e Eve tem respectivamente n_B e n_E antenas para a recepção. Neste cenário, Bob e Eve utilizam MRC na recepção, conforme mostrado na Figura 1.

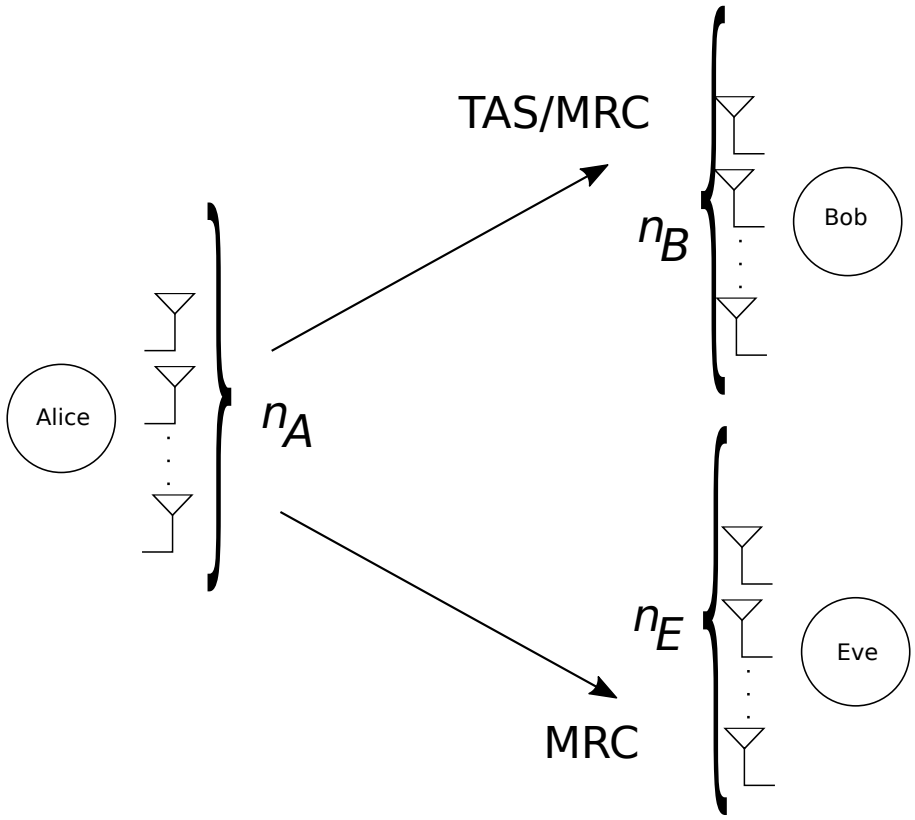

Figura 1: Modelo do sistema

Fonte: Autoria Própria, adaptado de (CHIODI JUNIOR et al., 2015a)

Assim, o pacote transmitido pela antena com melhor qualidade de Alice e recebido na

i-ésima antena do nó $j \in \{B, E\}$ é

$$\mathbf{y}_j^i = \sqrt{P_t\ \kappa_j}\ h_j^i\ \mathbf{x} + n_j^i, \tag{1}$$

com $\mathbf{y}_j^i$ sendo o sinal recebido na i-ésima antena do receptor j, P_t a potência de transmissão, κ_j é o coeficiente de perda de percurso de Alice até o nó j, h_j^i o coeficiente de desvanecimento do canal, $\mathbf{x}$ o sinal enviado por Alice e n_j^i o ruído na i-ésima antena do nó j. A envoltória do coeficiente de desvanecimento segue uma distribuição Rayleigh (GOLDSMITH, 2005) e muda de valor independentemente a cada pacote transmitido.

O coeficiente de perda de percurso entre Alice e o nó j é modelado matematicamente através da equação (GOLDSMITH, 2005):

$$\kappa_j = \frac{\lambda^2}{(4\pi) d_j^{\alpha}}, \tag{2}$$

sendo d_j a distância entre Alice e o nó j, α o coeficiente de perda de percurso e λ o comprimento de onda que neste caso é definido como $\frac{3 \cdot 10^8}{f_c}$ m, onde f_c é a frequência de portadora utilizada na modulação.

Devido à presença de múltiplos percursos, a potência instantânea no receptor apresentará flutuações em relação ao nível médio, assim, pode-se escrever a SNR instantânea como

$$\gamma_j = \bar{\gamma}_j |h_j^i|, \tag{3}$$

com $\bar{\gamma}_j = \frac{P_t \kappa_j}{N_0 B}$, sendo N_0 a densidade espectral de potência de ruído e B a largura de banda utilizada.

O modelo matemático que descreve o desvanecimento para o canal sem fio utilizado neste trabalho é sem linha de visada e é chamado de desvanecimento Rayleigh (GOLDSMITH, 2005). Assim, a função densidade de probabilidade de γ_j,$f_\gamma\left(\gamma_j\right)$, pode ser escrita como (GOLDSMITH, 2005; PROAKIS, 2001)

$$f_y\left(\gamma_j\right) = \begin{cases} \frac{1}{\bar{\gamma}_j} \exp\left(-\frac{\gamma_j}{\bar{\gamma}_j}\right), \gamma \geq 0 \\ 0, \text{ caso contrário.} \end{cases} \tag{4}$$

De (3) e (4), é possível definir a probabilidade de *outage*, ou seja, a probabilidade de falha de comunicação sob desvanecimento Rayleigh como (GOLDSMITH, 2005)

$$\mathscr{O}\left(\mathscr{R}, \gamma_j\right) \triangleq \Pr\left[\gamma_j < \gamma^{th}\right] = 1 - \exp\left(-\frac{\gamma^{th}}{\gamma_j}\right), \tag{5}$$

sendo $\mathscr{R}$ a eficiência espectral utilizada medida em bits por uso de canal (bpcu, do inglês *bits per*

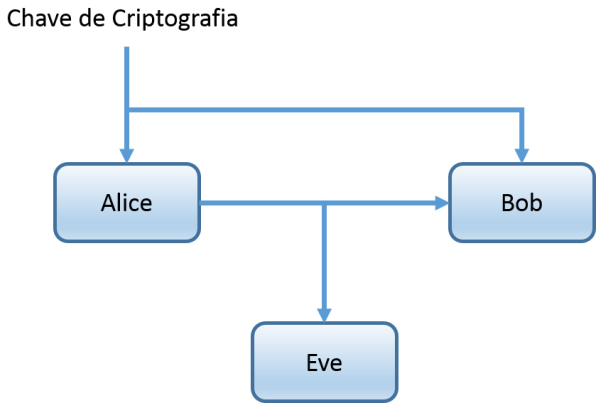

Figura 2: Esquema proposto em (SHANNON, 1949) que modela o efeito do espião no canal de comunicação.

Fonte: Autoria Própria

channel use), γ^{th} a relação sinal-ruído mínima necessária para se atingir $\mathscr{R}$, com $\gamma^{th} = 2^{\mathscr{R}} - 1$.

2.2 SEGURANÇA NA CAMADA FÍSICA

Observando a infraestrutura de redes implementadas atualmente, nota-se a elegância da abordagem por camadas. Com o crescimento das redes no mundo, os problemas fundamentais de transmissão, roteamento, alocação de recursos, entre outros foram distribuídos em protocolos implementados em diferentes camadas. Entretanto, tratando-se de segurança, esta distribuição não ocorre efetivamente (BLOCH; BARROS, 2011).

A prática de incluir autenticação e criptografia em protocolos existentes nas camadas levou a algo que pode ser corretamente classificado como "uma miscelânea de mecanismos de segurança" (BLOCH; BARROS, 2011). Já que a segurança da informação é um assunto de suma importância, é razoável imaginar que ela seja implementada em todas as camadas. No entanto, existe uma que foi ignorada: a camada física.

Em (SHANNON, 1949), a ideia de segurança é baseada única e exclusivamente em criptografia, onde as chaves criptográficas são geradas e compartilhadas para Alice e Bob através de canais sem erros, sendo que Eve recebe a palavra criptografada enviada por Alice também sem erros, isto é, considera-se o pior cenário. Esta suposição da existência de canais livre de erros, na prática, se refere a um código corretor de erros muito eficiente, o qual permite que a mensagem seja recuperada com uma taxa de erros arbitrariamente pequena (BLOCH; BARROS, 2011). O modelo de Shannon pode ser visto na Figura 2.

Neste cenário, para garantir a segurança, Alice e Bob devem gerar e armazenar as

chaves criptográficas, sendo que cada uma delas só deve ser utilizada uma vez para impedir que Eve, através de esforço computacional, recupere a informação da mensagem. Shannon formalizou o tratamento matemático tratando a mensagem original e a palavra codificada como variáveis aleatórias, mostrando que a segurança é obtida quando entropia condicional de uma mensagem dada uma palavra codificada é igual à entropia da mensagem, isso é atingido quando a entropia da chave de criptografia é maior ou igual a da mensagem. Esta suposição implica que a palavra código é estatisticamente independente da mensagem original, isto é a garantia de que nenhum espião consiga extrair informações sobre a mensagem (BLOCH; BARROS, 2011).

Neste mesmo modelo, ainda há o problema de compartilhamento destas chaves, pois o modelo de Shannon supõe um enlace seguro para isso e ainda livre de erros, o que não ocorre na prática em muitos casos. Considerando este modelo, se Eve não tiver capacidade computacional suficiente para quebrar a criptografia, garante-se a segurança (BLOCH; BARROS, 2011).

Em (WYNER, 1975), foi proposto um novo modelo chamado canal *wiretap* degradado, onde, diferentemente daquele mostrado na Figura 2, o ruído térmico se encontra presente em Bob e também em Eve. Além disso, não há mais o canal seguro utilizado na distribuição das chaves de criptografia para os nós legítimos. Neste modelo, Eve recebe apenas uma versão degradada da mensagem recebida no nó legitimo. Infelizmente, Eve acaba sendo explicitamente modelada estando sempre em desvantagem quando é comparada com Bob (BLOCH; BARROS, 2011), limitando assim os cenários para a utilização do modelo, conforme pode ser visto na Figura 3.

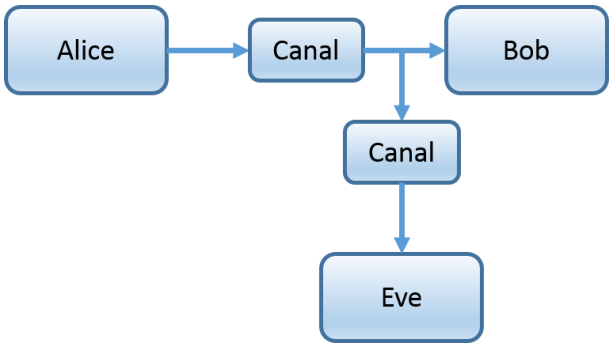

Figura 3: Canal *wiretap* degradado proposto em (WYNER, 1975), onde se pode ver que Eve observa uma versão distorcida da mensagem recebida por Bob.

Fonte: Autoria Própria

Como o modelo da Figura 3 apenas considera Eve em desvantagem, ele se torna limitado para representar o canal sem fio, pois neste Eve não recebe uma versão degradada da mensagem de Bob. Assim, assumindo o meio sem fio e sua propriedade de difusão, passa a existir um canal que liga diretamente Alice a Eve (CSISZAR; KORNER, 1978). Desta forma,

pode-se mudar o modelo da Figura 3 para se adequar ao meio sem fio, obtendo assim o canal *wiretap* (BLOCH; BARROS, 2011; CSISZAR; KORNER, 1978), conforme indicado na Figura 4.

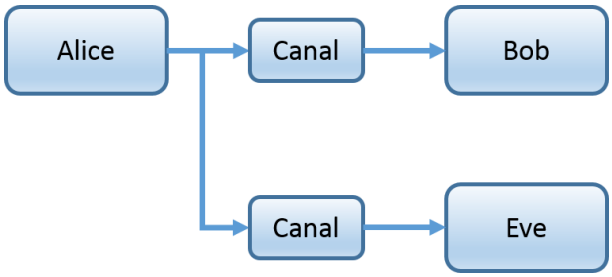

Figura 4: Canal *wiretap* proposto em (CSISZAR; KORNER, 1978).
Fonte: Autoria Própria

2.3 INTERVALO DE SEGURANÇA

Intervalo de segurança é uma métrica definida como a razão entre as SNRs requeridas em Bob e em Eve para que, em Bob, se tenha um determinado nível de confiança na comunicação, enquanto atinge um nível suficiente de segurança na camada física (BALDI et al., 2012, 2010, 2013b). Em outras palavras, quando se considera um canal com desvanecimento constante durante a transmissão de um pacote, deve-se assegurar *i) segurança*, garantindo que a métrica de desempenho, probabilidade de *outage* em Eve ($\mathscr{O}_E$) ou a FER em Eve (P_{fE}), estejam acima de seus respectivos alvos, a probabilidade de *outage* alvo em Eve ($\mathscr{O}_E^*$) e a FER alvo em Eve (P_{fE}^*) respectivamente; *ii) confiança*, assegurando a probabilidade de *outage* em Bob ($\mathscr{O}_B$) ou a FER em Bob (P_{fB}) fiquem abaixo da probabilidade de *outage* alvo em Bob ($\mathscr{O}_B^*$) ou a FER alvo em Bob (P_{fB}^*). Assim, o intervalo de segurança é definido como

$$\Delta \triangleq \frac{\bar{\gamma}_B^*}{\bar{\gamma}_E^*}, \tag{6}$$

ou ainda, pode-se re-escrever (6) em dB como

$$\Delta \triangleq \bar{\gamma}_B^* - \bar{\gamma}_E^* \qquad \text{(dB)}, \tag{7}$$

com $\bar{\gamma}_B^*$ e $\bar{\gamma}_E^*$ sendo a relações sinal-ruído necessárias para que Bob e Eve, respectivamente, atinjam os alvos. A Figura 5 mostra de forma gráfica o que foi expresso em (7).

De acordo com a definição em (7), é possível notar que, quanto mais segura for uma comunicação, menor será o valor de Δ. Como a SNR é função da distância entre os nós, um in-

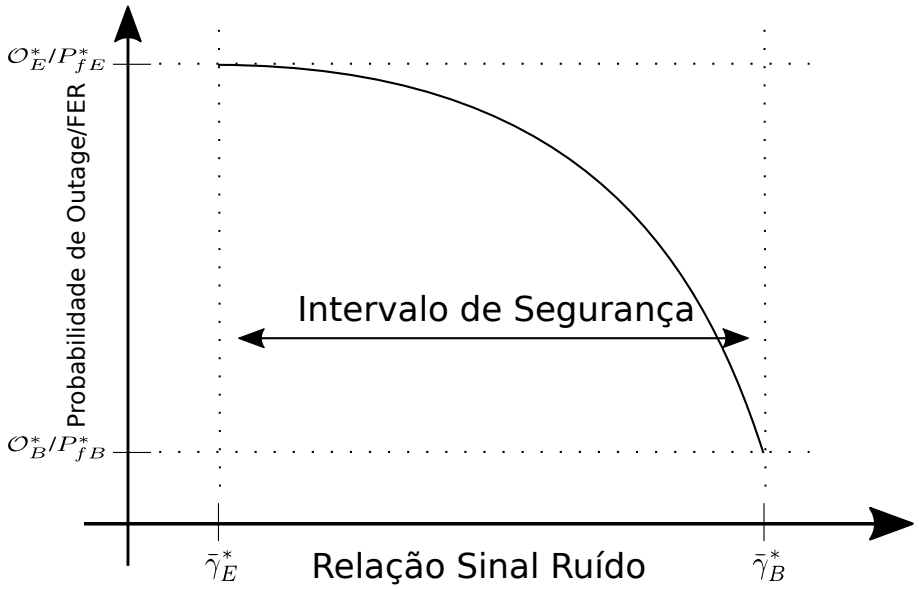

Figura 5: Exemplo de Intervalo de segurança, mostrando os valores limites para Bob e Eve. Fonte: Autoria Própria, adaptado de (CHIODI JUNIOR et al., 2015a)

tervalo pequeno implica que Bob e Eve podem estar muito próximos de Alice e mesmo assim a comunicação se manter segura; no caso de valores negativos, Eve poderia estar até mesmo mais perto de Alice do que Bob. Considerando (2) e (6), pode-se relacionar a razão das distâncias de Bob e Eve até Alice, d_B e d_E respectivamente, com o intervalo de segurança, o resultado pode ser visto na Figura 6.

2.4 EMBARALHAMENTO DE PACOTES

Como visto, o intervalo de segurança deve ser mantido o mais baixo possível para assegurar uma comunicação confiável. Para tal, pode-se utilizar códigos na transmissão; por exemplo, em (KLINC et al., 2011), é proposto o uso de um código LDPC para dificultar a decodificação da mensagem em Eve, os autores ainda mostram que é possível diminuir consideravelmente o intervalo quando comparado com códigos sistemáticos. Outra forma é utilizar embaralhamento como mostrado em (BALDI et al., 2010). No entanto, em ambos os artigos, o tamanho do pacote é limitado ao tipo do código. Neste trabalho, optou-se por utilizar códigos convolucionais para permitir vários tamanhos de pacotes nas análises. Caso contrário, seria necessário utilizar um código diferente para cada valor de profundidade de embaralhamento.

Pode-se dividir a análise do embaralhamento de pacotes em duas, o desempenho sem a utilização de códigos corretores de erro e fazendo o uso deles. Como a ideia do embaralhamento é misturar os bits da palavra código antes da codificação, assim, na recepção, serão necessários

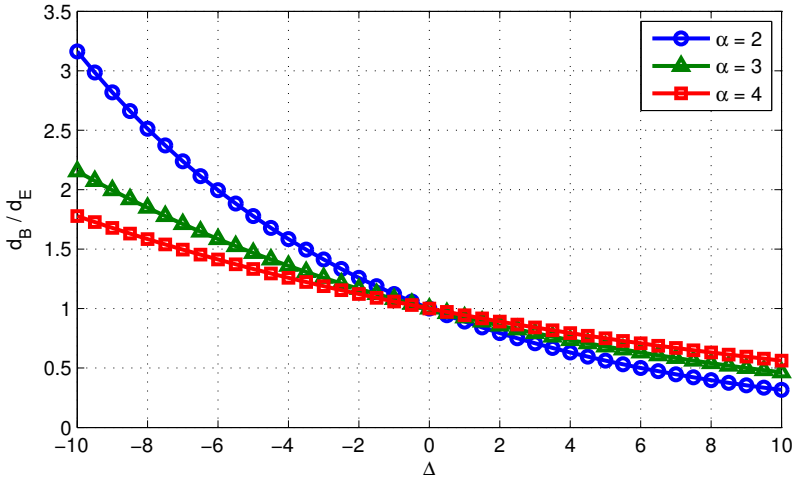

Figura 6: Relação entre distâncias dos nós em relação a Alice com o intervalo de segurança, considerando $\alpha \in [2,3,4]$.

todos os N bits decodificados corretamente (BALDI et al., 2012) para se obter a mensagem novamente, caso um bit seja decodificado erroneamente, o erro é propagado de forma aleatória por toda a palavra, fazendo com que a BER aumente.

Nesta subseção, toda a análise será feita no canal AWGN, pois posteriormente será utilizada a função de erro médio para variar o canal, sem a necessidade de derivar todas as funções novamente.

2.4.1 SEM CÓDIGOS CORRETORES DE ERRO

Conforme dito, o embaralhamento da informação é representado matematicamente como:

$$\mathbf{u}_S = \mathbf{u} \cdot \mathbf{S}, \tag{8}$$

sendo a mensagem original ($\mathbf{u}$) representada na forma matricial com dimensões $(1 \times N)$ e a matriz de embaralhamento ($\mathbf{S}$) com dimensões $(N \times N)$ (BALDI et al., 2010, 2012). Considerando apenas um pacote, pode-se escrever a BER como (BALDI et al., 2012)

$$P_b^{S-\text{AWGN}} = \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} \sum_{\substack{i=1 \\ \text{i ímpar}}}^{\min(j,w)} \frac{\binom{j}{i}\binom{N-j}{w-i}}{\binom{N}{w}}, \tag{9}$$

sendo p a BER sem considerar o embaralhamento, $\binom{N}{j} p^j (1-p)^{N-j}$, a probabilidade de receber j erros em N bits, $\binom{j}{i}\binom{N-j}{w-i}/\binom{N}{w}$, a probabilidade de i dos j erros sejam selecionados no desembaralhamento (BALDI et al., 2012) e w, o peso de coluna da matriz $\mathbf{S}^{-1}$. Enquanto a

FER é a probabilidade que a nenhum bit tenha sido recebido errado:

$$P_f^{S-AWGN} = 1 - (1-p)^N . \tag{10}$$

Ainda é possível estender o mesmo processo para vários pacotes, onde Z pacotes são embaralhados e enviados individualmente, essa técnica é denominada embaralhamento de pacotes. Para isso, as mensagens devem ser concatenadas em $\mathbf{u}' = [\mathbf{u_1}|\mathbf{u_2}|...|\mathbf{u_Z}]$, sendo que a nova matriz $\mathbf{S}$ tem dimensões $(NZ \times NZ)$. Assim, o desempenho da decodificação dependerá da densidade de coluna da matriz $\mathbf{S}^{-1}$, ou seja, $w/(NZ)$. Quando a densidade é 0.5 ou próxima deste valor, é possível aproximar o efeito ao do embaralhamento perfeito (do inglês, *perfect scrambling*), onde um simples erro gera o máximo de incerteza (BALDI et al., 2010, 2012).

Assim, para gerar a matriz de embaralhamento e sua inversa, deve-se definir primeiramente uma matriz inversível com a densidade escolhida. Para exemplificar, considerando $N = 5$, $Z = 2$ e $w = 3$, pode-se utilizar como matriz inversa de embaralhamento

$$\mathbf{S^{-1}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix},$$

e como matriz de embaralhamento propriamente dita como a sua inversa:

$$\mathbf{S} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Assim, considerando duas mensagens de entrada

$$\mathbf{u_1} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ e}$$

$$\mathbf{u_2} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

logo, de (8), o vetor de saída será:

$$\mathbf{u_S} = [\mathbf{u_1}|\mathbf{u_2}] \cdot \mathbf{S} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Depois de passar pelo processo de desembaralhamento, cada bit recebido pode ser visto como a soma dos Z bits recebidos depois do desembaralhamento de um único pacote. Desta forma, a BER do sistema pode ser escrita em função de (9) como (BALDI et al., 2012)

$$P_b^{ZS-\text{AWGN}} = \sum_{\substack{i=1 \\ \text{i ímpar}}}^{Z} \binom{Z}{i} \left(P_b^{S-\text{AWGN}}\right)^i \left(1 - P_b^{S-\text{AWGN}}\right)^{Z-i}. \tag{11}$$

Para o caso da FER utilizando embaralhamento de pacotes, sabe-se que um erro em qualquer um dos Z pacotes é espalhado de tal forma que os demais pacotes também sejam decodificados de forma incorreta. Assim, pode-se escrever a FER utilizando embaralhamento como

$$P_f^{ZS-\text{AWGN}} = 1 - \left(1 - P_f^{S-AWGN}\right)^Z. \tag{12}$$

2.4.2 COM CÓDIGOS CORRETORES DE ERRO

Uma análise matemática geral do desempenho utilizando códigos corretores é demasiadamente difícil (se possível) de ser feita, pois dependerá do tipo de código (código de bloco ou código convolucional) e das suas particularidades.

Supondo um código de bloco com taxa R e com capacidade de correção t, pode-se escrever a BER utilizando embaralhamento em apenas um pacote como (BALDI et al., 2012)

$$P_b^{S-\text{AWGN}} = \sum_{j=0}^{N} \binom{N}{j} \sum_{i=t+1}^{M} \binom{M-N}{i-j} {p_0}^i (1-p_0)^{M-i} \sum_{\substack{i=1 \\ \text{i ímpar}}}^{\min(j,w)} \frac{\binom{j}{i}\binom{N-j}{w-i}}{\binom{N}{w}}, \tag{13}$$

sendo que M é o comprimento do pacote codificado e p_0, a BER considerando um código corretor de erros antes do decodificador, podendo ser escrita como $p_0(\gamma) = p\left(\frac{\gamma}{R}\right)$. Isto se deve ao gasto de energia na transmissão que, devido ao aumento da quantidade de bits na palavra codificada, aumentou para manter a mesma taxa líquida de informação, comparando com o não codificado. A comparação justa ocorre então diminuindo a SNR na proporção do aumento do tamanho da palavra codificada em relação à não codificada, ou seja, $R = \frac{N_c}{M_c}$ (GOLDSMITH, 2005), onde a cada N_c bits de entrada têm-se M_c bits de saída do código convolucional.

A FER, para o código em questão, pode ser entendida como a probabilidade de se errar mais bits do que a capacidade de correção do código. Logo, a FER pode ser escrita como (BALDI et al., 2012)

$$P_f^{S-\text{AWGN}} = \sum_{i=t+1}^{M} \binom{M}{i} p_0^i (1-p_0)^{M-i}. \tag{14}$$

Supondo agora um código convolucional, a análise de BER e FER com embaralhamento se torna consideravelmente mais complexa que no caso com códigos de bloco. Para tornar os cálculos mais simples, optou-se por considerar o embaralhamento perfeito que pode ser obtido com matrizes inversas de embaralhamento com densidade próxima de 0.5. Além disso, devido à complexidade de se obter a expressão exata da BER para um código convolucional, foram utilizados para os cálculos os limites teóricos do código, mais precisamente, o pior caso que é o limite superior.

Assim, considerando um código convolucional com taxa R e comprimento de restrição K, pode-se definir a limite superior da curva de BER como (GOLDSMITH, 2005)

$$P_b^{UB-\text{AWGN}} \leq \frac{1}{N_c} \sum_{\delta=\,\delta_{\text{free}}}^{\infty} \Lambda_\delta P_2(\delta), \tag{15}$$

com δ_{free} sendo a distância mínima do código, Λ_δ o peso de uma palavra código que está a uma distância δ da palavra código com apenas zeros e

$$P_2(\delta) = \begin{cases} \sum_{i=\frac{\delta+1}{2}}^{\delta} \binom{\delta}{i} \frac{p_0^i}{(1-p_0)^{i-\delta}} & \text{, se } \delta \text{ for ímpar;} \\ \sum_{i=\frac{\delta}{2}+1}^{\delta} \binom{\delta}{i} \frac{p_0^i}{(1-p_0)^{i-\delta}} + \binom{\delta}{\delta/2} \frac{(1/2)\, p_0^{\delta/2}}{(1-p_0)^{-\delta/2}} & \text{, se } \delta \text{ for par.} \end{cases} \tag{16}$$

Partindo do limite superior para a BER apresentado em (15), pode-se escrever a FER para este tipo de código como

$$P_f^{S-\text{AWGN}} = 1 - \left(1 - P_b^{UB-\text{AWGN}}\right)^N. \tag{17}$$

Sob a condição de embaralhamento perfeito, quando há um erro em um pacote, metade de seus bits são decodificados de forma errada (BALDI et al., 2012). Assim, de acordo com (17), pode-se então escrever a BER utilizando códigos convolucionais e embaralhamento, como:

$$P_b^{S-\text{AWGN}} = \frac{1}{2} P_f^{S-\text{AWGN}}. \tag{18}$$

Considerando embaralhamento de pacotes, onde Z pacotes são embaralhados, (11) e (12) podem ser utilizadas para o cálculo da BER e da FER, apenas levando em conta (13) e (14) para códigos de bloco e (17) e (18) para códigos convolucionais.

Pode-se calcular a FER para o canal sem fio a partir de (12), que considera o canal AWGN, utilizando a função de erro médio juntamente com a função densidade de probabilidade que modela o desvanecimento do canal. Isto é (GOLDSMITH, 2005)

$$P_f(\bar{\gamma}) = \int_0^\infty f_\gamma(\gamma)\, P_f^{ZS-\text{AWGN}}(\gamma)\, \mathrm{d}\gamma. \tag{19}$$

Para este trabalho, onde consideram-se o TAS, o MRC e o TAS/MRC, tem-se os valores para $f_\gamma(\gamma)$ definidos na Tabela 1. Estes valores foram obtidos derivando as equações de probabilidade de *outage*. Pode-se ver a comparação entre eles na Figura 7 (GOLDSMITH, 2005).

Utilizando o código convolucional padrão NASA $(1, 2, 7)$ com polinômio gerador em octal $[133,\ 171]$ e com distância mínima igual a 10 (PROAKIS, 2001, Tabela 8-2-1), foram traçadas as curvas de BER e FER com embaralhamento de pacotes no canal Rayleigh, os resultados são mostrados nas Figuras 8 e 9.

Tabela 1: Funções densidade de probabilidade para TAS, MRC e TAS/MRC

TAS	$f_\gamma(\gamma) = \frac{n_A}{\bar{\gamma}}\left[1-\exp\left(-\frac{\gamma}{\bar{\gamma}}\right)\right]^{n_A}$
MRC	$f_\gamma(\gamma) = \frac{\gamma^{n_E-1}\exp\left(\frac{-\gamma}{\bar{\gamma}}\right)}{\bar{\gamma}^{n_E}(n_E-1)!}$
TAS/MRC	$f_\gamma(\gamma) = \frac{n_A}{\Gamma(n_B)}\Gamma\left(n_B,\frac{\gamma}{\bar{\gamma}}\right)^{n_A-1}\left[\left(\frac{\gamma}{\bar{\gamma}}\right)^{n_B-1}\exp\left(-\frac{\gamma}{\bar{\gamma}}\right)\right]$

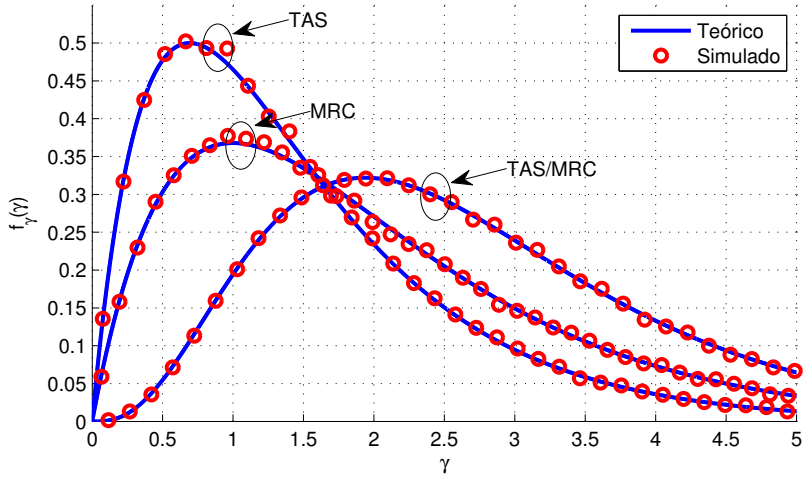

Figura 7: Comparação das funções de densidade de probabilidade do desvanecimento do TAS, MRC e TAS/MRC juntamente com os valores simulados, considerando um sistema com $n_A = n_B = n_E = 2$ e $\bar{\gamma} = 0$ dB.

Fonte: Autoria Própria

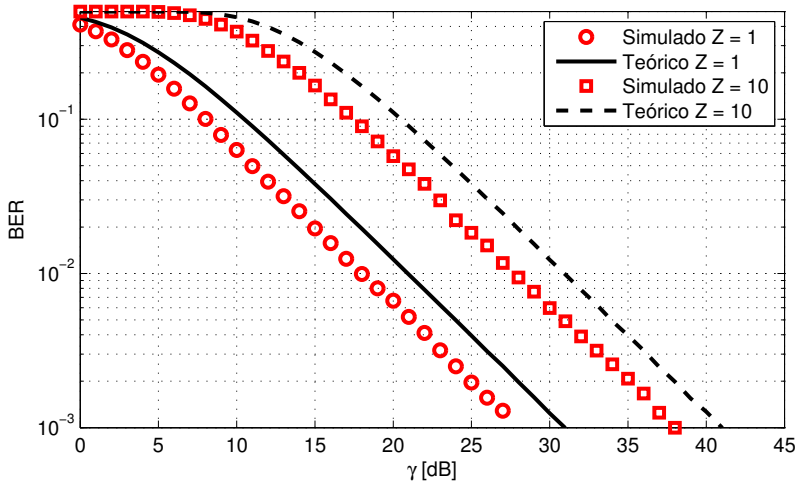

Figura 8: BER com embaralhamento de pacotes considerando o canal Rayleigh, $N = 256$, $w/(NZ) = 0.5$ e o código convolucional padrão NASA (1,2,7) (PROAKIS, 2001, Tabela 8-2-1).

Fonte: Autoria Própria

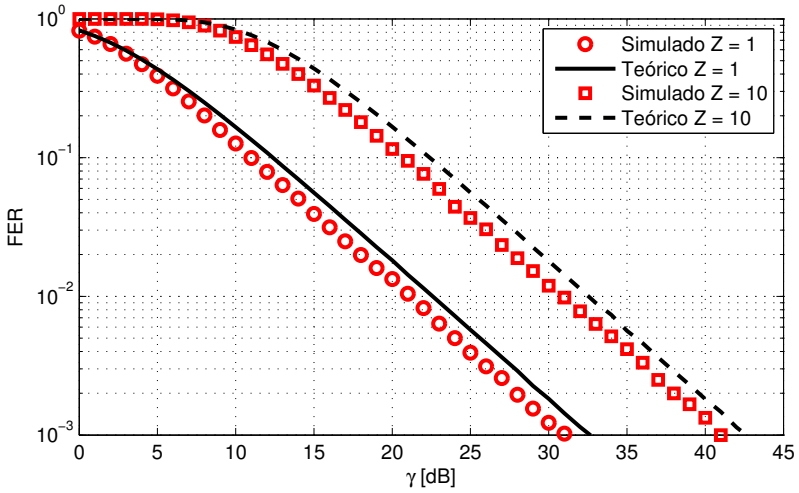

Figura 9: FER com embaralhamento de pacotes considerando o canal Rayleigh, $N = 256$**,** $w/(NZ) = 0.5$ **e o código convolucional padrão NASA (1,2,7) (PROAKIS, 2001, Tabela 8-2-1).**

Fonte: Autoria Própria

3 ESQUEMA PROPOSTO

3.1 INTERVALO DE SEGURANÇA

Quando considerado um canal em que o coeficiente de desvanecimento permanece constante durante a transmissão de um pacote, a análise do intervalo de segurança pode ser feita com duas métricas, a probabilidade de *outage* e a FER. A primeira considera um código robusto o suficiente que consiga recuperar a mensagem enviada pelo transmissor sempre que a capacidade de canal for maior do que a taxa de transmissão; a outra, considera um código real e dependerá das características individuais deste. Assim, pode-se relacionar a probabilidade de *outage* como o limite teórico para a FER; logo, a análise considerando probabilidade de *outage* e FER consiste em comparar o quão próxima do limite teórico a segurança de uma rede pode chegar utilizando um código prático.

3.1.1 PROBABILIDADE DE *OUTAGE*

Partindo do modelo proposto, deve-se primeiro encontrar a equação da probabilidade de *outage* para um receptor operando sob MRC em um canal com desvanecimento Rayleigh, assim, é possível escrever esta equação como (GOLDSMITH, 2005)

$$\mathscr{O}_{MRC} = \Gamma\left(n_r, \frac{\gamma^{th}}{\bar{\gamma}}\right), \tag{20}$$

sendo n_r o número de antenas de um receptor genérico, $\bar{\gamma}$ a relação sinal-ruído média por antena do receptor e $\Gamma(a,b)$ a função gama incompleta inferior

$$\Gamma(a,b) = \frac{\int_0^b \exp(-t)\, t^{a-1}\, \mathrm{d}t}{\Gamma(a)}. \tag{21}$$

O TAS escolhe sempre a melhor antena de transmissão em relação ao receptor legítimo, assim, quando este método é aplicado com n_t antenas transmissoras, a probabilidade de *outage* será a probabilidade de falhar simultaneamente a comunicação nas n_t antenas, ou seja, o produtório das probabilidades de falha individual, sob a suposição de que todas as antenas estão

devidamente espaçadas estando sujeitas a desvanecimento independentes. Como todos os canais tem os mesmos parâmetros de desvanecimento, pode-se escrever a probabilidade de *outage* do TAS/MRC como (CHEN et al., 2005, 2008)

$$\mathscr{O}_{\text{TAS/MRC}}(n_t, n_r) = \Gamma\left(n_r, \frac{\gamma^{th}}{\bar{\gamma}}\right)^{n_t}, \tag{22}$$

com n_t sendo o número de antenas de um transmissor genérico.

Como visto, a propriedade do embaralhamento de pacotes é distribuir o erro de um único pacote em todos os Z pacotes utilizados, logo, considerando que Bob trabalha sob o TAS/MRC e Eve apenas sob o MRC, pode-se escrever as probabilidades de *outage* alvo desejadas para Bob e Eve respectivamente como

$$\mathscr{O}_B^* = 1 - \left[1 - \mathscr{O}_{\text{TAS/MRC}}(n_A, n_B)\right]^Z \text{ e} \tag{23a}$$

$$\mathscr{O}_E^* = 1 - \left[1 - \mathscr{O}_{\text{MRC}}(n_E)\right]^Z, \tag{23b}$$

onde * indica a probabilidade alvo do sistema.

Assim, as probabilidades de *outage* de apenas um pacote podem ser desenvolvidas de (23a) e (23b) para Bob e Eve como

$$\mathscr{O}_{\text{TAS/MRC}}(n_A, n_B) = 1 - (1 - \mathscr{O}_B^*)^{\frac{1}{Z}} \text{ e} \tag{26a}$$

$$\mathscr{O}_{\text{MRC}}(n_E) = 1 - (1 - \mathscr{O}_E^*)^{\frac{1}{Z}}. \tag{26b}$$

De (6), é necessário isolar os valores de SNR que atingem os requisitos de confiabilidade ($\mathscr{O}_B^*$ e $\mathscr{O}_E^*$) das equações de probabilidade de *outage* para então obter o intervalo de segurança. Ou seja, encontrar a solução para (26a) e (26b). Isso implica na inversão da função gama incompleta ($\Gamma^{-1}(y, a)$), a qual não tem forma analítica, no entanto, esta dificuldade pode ser resolvida com soluções numéricas.

Assim, isolando $\bar{\gamma}_B^*$ e $\bar{\gamma}_E^*$ respectivamente de (26a) e (26b), o intervalo de segurança baseado na probabilidade de *outage* é

$$\Delta = \frac{\Gamma^{-1}\left(\left[1 - (1 - \mathscr{O}_E^*)^{1/Z}\right], n_E\right)}{\Gamma^{-1}\left(\left[1 - (1 - \mathscr{O}_B^*)^{1/Z}\right]^{1/n_A}, n_B\right)}. \tag{29}$$

Para evitar que a equação do intervalo de segurança fique em função da inversa da função gama incompleta é possível aproximar esta para os casos onde o nível de ruído é irrisório quando comparado com a potência do sinal recebido, ou seja, quando $\bar{\gamma} \gg 1$. Assim, pode-se

aproximar a função gama incompleta como (CHEN et al., 2005)

$$\Gamma\left(n_r, \frac{\gamma^{th}}{\bar{\gamma}}\right) \approx \frac{\left(\frac{\gamma^{th}}{\bar{\gamma}}\right)^{n_r}}{\Gamma(n_r+1)}. \tag{30}$$

Logo, aplicando (30) em (29), tem-se que o intervalo de segurança aproximado é

$$\Delta^{\text{app}} = \frac{\left[\left(1-[1-\mathscr{O}_E^*]^{1/Z}\right)\Gamma(n_E+1)\right]^{1/n_E}}{\left[\left(1-[1-\mathscr{O}_B^*]^{1/Z}\right)\Gamma(n_B+1)^{n_A}\right]^{1/(n_A n_B)}}, \bar{\gamma} \gg 1. \tag{31}$$

Por causa da diversidade de transmissão e recepção, a condição para que (31) se aproxime de (29), $\bar{\gamma} \gg 1$, dependerá também da quantidade de antenas no receptor e no transmissor. Quanto maior o grau de diversidade, menos qualidade de canal é necessária para se atingir um determinado valor de intervalo, não satisfazendo a condição para a qual a aproximação é válida, resultado em um distanciamento das curvas.

Pode ser do interesse prático obter o número de antenas em Alice para se atingir um valor pré-definido de segurança em camada física, o qual pode ser obtido isolando n_A de (29) que resulta em

$$n_A = \left\lceil \frac{\log\left(1-(1-\mathscr{O}_B^*)^{1/Z}\right)}{\log\left(\Gamma\left(\frac{\Gamma^{-1}\left(1-[1-\mathscr{O}_E^*]^{1/Z}, n_E\right)}{\Delta}, n_B\right)\right)} \right\rceil, \tag{32}$$

sendo que $\lceil\cdot\rceil$ corresponde à operação de arredondamento para o inteiro acima.

Assim como no caso de (31), para se evitar deixar n_A em função da inversa da função gama incompleta, pode-se aplicar (30) em (32), assim, o número de antenas aproximado de Alice é

$$n_A^{\text{app}} = \left\lceil \frac{\frac{1}{n_B}\log\left(1-(1-\mathscr{O}_B^*)^{\frac{1}{Z}}\right)}{\frac{1}{n_E}\left[\log\left(1-(1-\mathscr{O}_E^*)^{\frac{1}{Z}}\right)+\log(\Gamma(n_E+1))\right]-\left[\frac{1}{n_B}\log(\Gamma(n_B+1))+\log(\Delta)\right]} \right\rceil \tag{33}$$

Nota-se que o caso especifico sem embaralhamento de pacotes pode ser obtido fazendo $Z=1$ em (29), (31), (32) e (33).

3.1.2 FER

Considerando códigos convolucionais, resolver (19) não é uma tarefa trivial mesmo em posse de $f_\gamma(\gamma)$. Uma solução para este problema é utilizar uma abordagem semi-analítica

que simula o efeito do desvanecimento através de integração de Monte Carlo (MACKEOWN, 1997), onde a FER é calculada a partir da média da probabilidade de erro para cada realização do canal.

O intervalo de segurança baseado na FER é então obtido através das funções inversas de P_{fB} e P_{fE}, em outras palavras, obter $\bar{\gamma}$ em função da FER para Bob e Eve. No entanto, assim como (19), para códigos convolucionais esta tarefa também apresenta grande dificuldade, tendo de ser realizada numericamente através de uma busca exaustiva dos valores de SNR.

Assim como em (26a) e (26b), a FER de Bob e Eve vista em apenas um pacote para se atingir o desempenho alvo em Z pacotes podem ser derivadas respectivamente como

$$P_{fB} = 1 - \left(1 - P_{fB}^{*}\right)^{\frac{1}{Z}}, \tag{34a}$$

$$P_{fE} = 1 - \left(1 - P_{fE}^{*}\right)^{\frac{1}{Z}}. \tag{34b}$$

Assim, de (6), (34a) e (34b), pode-se escrever o intervalo de segurança baseado na FER como

$$\Delta = \frac{P_{fB}^{-1}\left(1 - \left(1 - P_{fB}^{*}\right)^{\frac{1}{Z}}\right)}{P_{fE}^{-1}\left(1 - \left(1 - P_{fE}^{*}\right)^{\frac{1}{Z}}\right)}. \tag{37}$$

Assim como em (32) e (33), onde o número de antenas em Alice foi determinado para se obter um determinado nível de segurança em camada física, pode-se obter também para o caso da FER. No entanto, como em (37), não é possível obter uma expressão analítica devido à utilização de códigos corretores de erro, logo, n_A deve ser extraído através de uma busca exaustiva. Isto é feito incrementando n_A e calculando o intervalo de segurança até atingir os valores requeridos. Este processo de busca utilizado em (37) e também para determinar n_A inclui um erro que deve ser definido nos parâmetros de projeto; sendo que este erro é definido como a diferença absoluta entre os resultados de duas iterações (MACKEOWN, 1997; CHEN; FENG, 2010).

4 RESULTADOS NUMÉRICOS

Neste capítulo, serão apresentados da análise do modelo proposto no Capítulo 3. Todas as simulações assumem que Eve e Bob trabalham com diversidade de recepção, sendo que o limite de confiabilidade para Bob ($\mathscr{O}_B^*$ ou P_{fB}^*) foram escolhidos arbitrariamente como sendo iguais a 0.01, enquanto para Eve, este limite ($\mathscr{O}_E^*$ ou P_{fE}^*) é 0.9.

O código adotado foi o convolucional padrão NASA $(1,2,7)$ com taxa $1/2$, seu polinômio gerador em octal é $[133, 171]$ e $\delta_{free} = 10$ (PROAKIS, 2001, Tabela 8-2-1). Neste trabalho, adotou-se um erro máximo associado ao método de Monte Carlo de até 1^{-6}. A eficiência espectral foi definida em $\mathscr{R} = 1$ bpcu.

A Figura 10 apresenta a probabilidade de *outage* e FER para Bob e Eve, sem embaralhamento de pacotes ($Z = 1$), obtidos através da análise e validados por resultados numéricos. A curva de Eve não aparece em função de n_A justamente por conta do método TAS que sempre escolhe a melhor antena para Bob, a qual é uma escolha aleatória do ponto de vista de Eve. Isso acarreta em uma melhora de desempenho quando n_A aumenta. Além disso, pode-se notar que os resultados analíticos tem boa precisão em relação às simulações.

4.1 INTERVALO DE SEGURANÇA

Como o tamanho do pacote influencia a FER, ele também implica em alterações no intervalo de segurança. No entanto, como o cálculo da métrica de segurança leva em consideração a diferença das SNRs necessárias para se atingir o valor alvo de desempenho para Bob e Eve, esta influência de N no intervalo de segurança é atenuada. Assim, mesmo considerando pacotes de tamanho infinito, os resultados obtidos baseados na probabilidade de *outage* são muito próximos daqueles obtidos pela FER, os quais consideram um tamanho de pacote finito e códigos que não atingem a capacidade de canal.

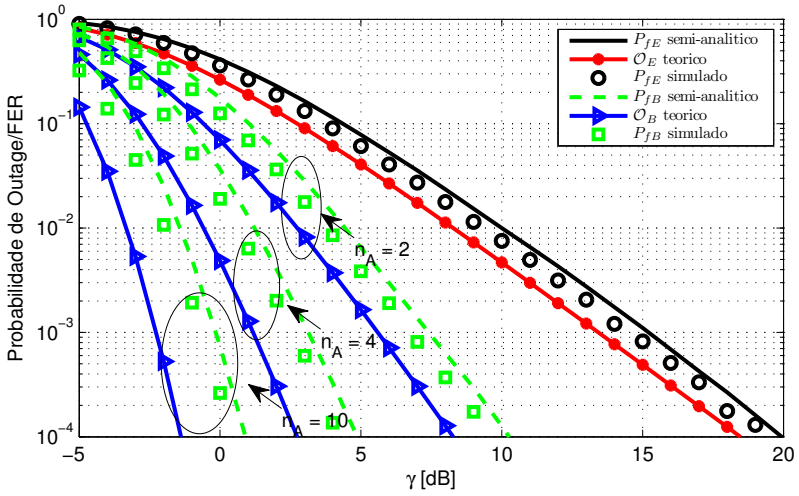

Figura 10: Comparação entre probabilidade de *outage* e o limite superior da FER para Eve e Bob, considerando $n_A \in [2,4,10]$.

Fonte: Autoria Própria

4.1.1 INTERVALO EM FUNÇÃO DA PROFUNDIDADE DE EMBARALHAMENTO DE PACOTES

Pode-se analisar o comportamento do intervalo de segurança em relação ao embaralhamento de pacotes alterando a quantidade de pacotes no embaralhamento e mantendo os demais parâmetros constantes. Os resultados do intervalo de segurança baseado na FER e na probabilidade de *outage* podem então ser visto na Figura 11.

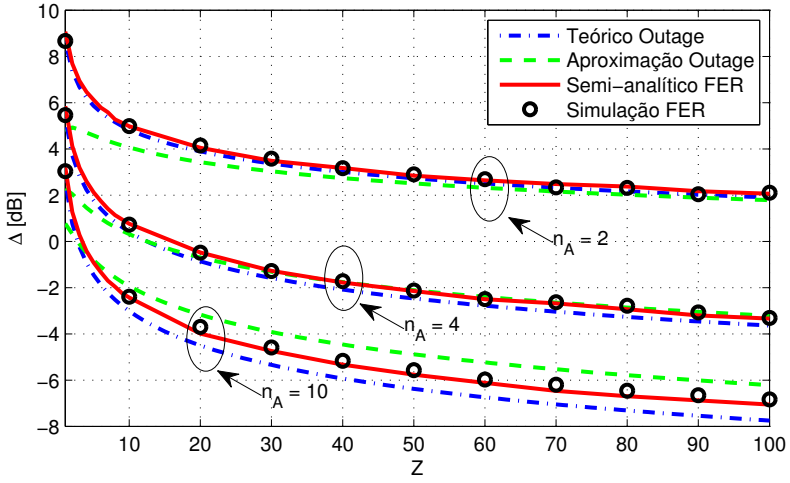

Figura 11: Intervalo de segurança baseado na FER e na probabilidade de *outage*, considerando o código convolucional padrão NASA, com $N = 256$ bits, $n_B = n_E = 2$ e $n_A \in [2,4,10]$.

Fonte: Autoria Própria.

Nota-se a proximidade entre os valores de intervalo independentemente da origem destes, mas principalmente dos valores simulados e daqueles obtidos pelo método semi-analítico. Isto mostra que é possível obter resultados próximos aos reais mesmo utilizando aproximações como o limite superior da FER. Também é possível observar que o número de antenas em Alice influencia no comportamento do intervalo em relação a Z. Para o caso onde $n_A = 2$, a inclinação da curva é menos acentuada do que as demais curvas.

Um resultado importante é obtenção de valores de intervalo de segurança menores do que 0 dB com um número praticável de antenas de transmissão e recepção, bem como com poucos blocos de embaralhamento. Isto significa que mesmo com um canal em média pior do que o espião, os nós legítimos podem se comunicar de forma segura.

4.1.2 INTERVALO EM FUNÇÃO DO NÚMERO DE ANTENAS NOS NÓS

A seguir, foi investigado o comportamento do intervalo de segurança em função do número de antenas em Alice e Eve. As Figuras 12, 13 e 14 mostram o intervalo de segurança em função de n_A e n_E considerando, respectivamente, a probabilidade de *outage* exata de (6), a probabilidade de *outage* aproximada extraída de (31) e a FER. Nos três casos citados, assumiu-se o uso de embaralhamento de pacotes com profundidade igual a $Z = 10$ pacotes devido a facilidade de se gerar a matriz de embaralhamento para este valor, além disso, como se verá mais adiante, o aumento de Z não implica em ganhos lineares nos resultados.

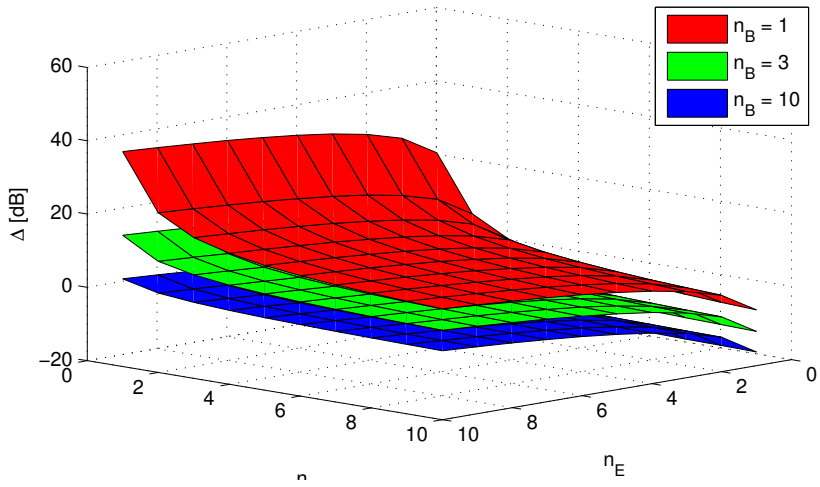

Figura 12: Intervalo de Segurança baseado na probabilidade de *outage* exata de (29) **em função de** n_A **e** n_E **para** $n_B \in [1,3,10]$**.**

Fonte: Autoria Própria.

Comparando as Figuras 12 e 13, observa-se que a diferença entre as curvas exata e

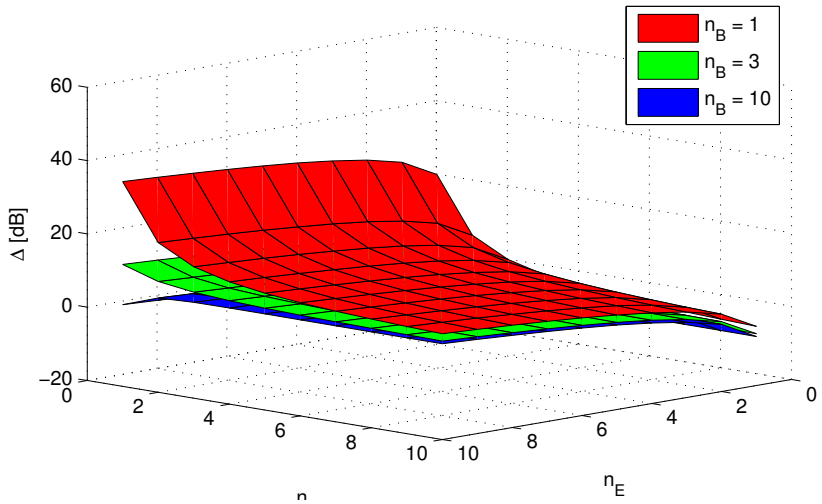

Figura 13: Intervalo de Segurança baseado na probabilidade de *outage* aproximada de (31) **em função de n_A e n_E para $n_B \in [1,3,10]$.**

Fonte: Autoria Própria.

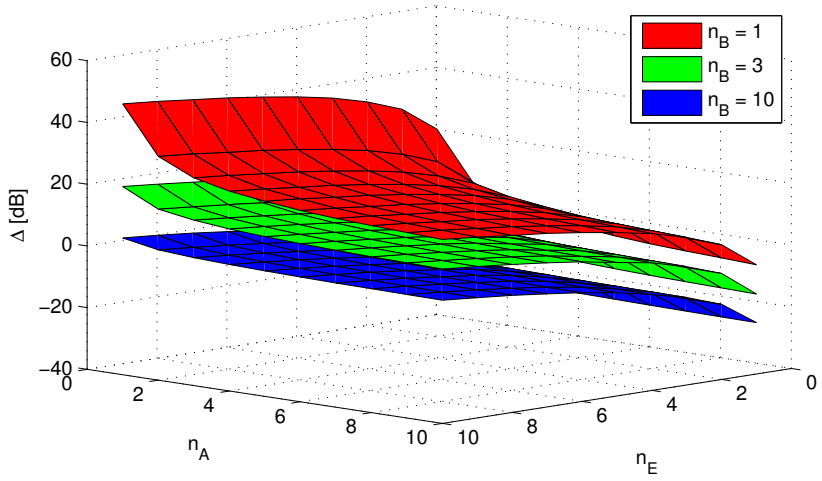

Figura 14: Intervalo de Segurança baseado no limite superior da FER de (37) **em função de n_A e n_E para $n_B \in [1,3,10]$.**

Fonte: Autoria Própria.

aproximada aumenta com n_A e n_B, assim como na Figura 11. Este comportamento pode ser explicado pela aproximação em alta SNR usada em (31). Como n_A ou n_B aumenta, menos qualidade no enlace é necessária para atingir o mesmo desempenho, fazendo com que a aproximação seja menos precisa. Isso significa que os resultados atuais (em termos de intervalo de segurança requerido) podem ser até mesmo menores do que aqueles encontrados em (CHIODI JUNIOR et al., 2015b). Os resultados na Figura 14, na qual se considera um código real que não atinge a capacidade de canal, mostram melhores valores para o intervalo de segurança do que os apre-

sentados na Figura 12. Isto implica que o canal legítimo pode estar em uma situação muito pior do que foi anteriormente calculado, quando comparado com o ilegítimo e mesmo assim apresentar um intervalo de segurança adequado.

4.2 NÚMERO DE ANTENAS EM ALICE

Os resultados desta seção foram obtidos considerando o intervalo de segurança alvo como $\Delta = 0$ dB. Pode-se calcular os valores exatos de n_A necessário para atingir um certo desempenho a partir de (32), variando o número de pacotes utilizado no embaralhamento de pacotes e a probabilidade de *outage* alvo em Eve, como podem ser vistos na Tabela 2.

Tabela 2: Número de antenas transmissoras, n_A, obtido de (32) **variando $\mathscr{O}_E^*$ e Z, para $\Delta = 0$ dB, $\mathscr{O}_B^* = 0.01$ e $n_B = n_E = 2$.**

Z	$\mathscr{O}_E^*$				
	0.1	0.3	0.5	0.7	0.9
1	2	4	7	13	44
10	2	3	3	4	5
100	2	2	2	3	3

Ou ainda, é possível extrair o número de antenas em Alice da equação aproximada do intervalo de segurança, (33), conforme a Tabela 3.

Tabela 3: Número de antenas transmissoras, n_A, obtido de (33) **variando $\mathscr{O}_E^*$ e Z, para $\Delta = 0$ dB, $\mathscr{O}_B^* = 0.01$ e $n_B = n_E = 2$.**

Z	$\mathscr{O}_E^*$				
	0.1	0.3	0.5	0.7	0.9
1	2	4	7	13	44
10	2	3	3	4	5
100	2	2	2	3	3

Para o caso pratico utilizando códigos corretores de erros, na Tabela 4, são apresentados as quantidades mínimas de antenas em Alice para se atingir o mesmo nível de segurança em camada física, agora considerando a FER como métrica de desempenho.

Tabela 4: Número de antenas transmissoras, n_A, em função de Δ, P_{fE}^* e Z, para $P_{fB}^* = 0.01$, $N = 256$ e $n_B = n_E = 2$.

Z	P_{fE}^*				
	0.1	0.3	0.5	0.7	0.9
1	3	5	8	18	94
10	2	3	3	4	5
100	2	2	2	3	3

Das Tabelas 2 e 3, percebe-se que, mesmo com as diferenças encontradas nos intervalos de segurança do valor exato e da aproximação, vistos na Figura 11; os valores para n_A são os mesmos. Isto ocorre porque o arrendamento para cima presente em (32) e (33) anulando esta diferença.

É possível notar, observando as Tabelas 2 e 4, que, na total falta da técnica de embaralhamento de pacotes, ou seja, as colunas onde $Z = 1$, o número de antenas de transmissão necessárias para se atingir um intervalo de segurança igual a 0 dB é maior para todos os valores alvo de Eve considerando a FER como métrica do que quando considera-se a probabilidade de *outage*. Entretanto, quando o profundidade do embaralhamento aumenta, ambos os cenários (FER e probabilidade de *outage*) convergem para os mesmos resultados. Quando $Z = 100$, por exemplo, é possível atingir um intervalo de segurança igual a zero, com Bob operando com um FER/probabilidade de *outage* de 0.01 e Eve, com 0.9, enquanto Alice usa um número realizável de antenas (três) para transmitir.

Portando, pode-se dizer que as previsões teóricas para o número de antenas de Alice para se obter um determinado nível de segurança através da probabilidade de *outage* são precisas o suficiente para fornecer uma aproximação muito razoável do resultado prático com a FER, especialmente quando o número de pacotes utilizado no embaralhamento aumenta. Este é um resultado desejado, aumentando Z, aumenta-se também a segurança em camada física para esta abordagem.

4.2.1 INTERVALO EM FUNÇÃO DOS VALORES ALVO DE FER E PROBABILIDADE DE *OUTAGE*

Aqui foi avaliada a influência dos valores alvos de FER e probabilidade de *outage* de Bob e Eve no intervalo de segurança. Foram considerados todos os nós com duas antenas, usando embaralhamento de pacotes com profundidade igual a $Z \in [1, 5, 10]$. As Figuras 15, 16 e 17 trazem os casos com probabilidade de *outage* exata, probabilidade de *outage* aproximada e FER respectivamente.

Nos três casos, pode-se observar que o intervalo de segurança aumenta consideravelmente com o aumento do valor alvo de Eve, enquanto o comportamento oposto é observado se o alvo de Bob aumentar. Isso acontece por conta de que valores alvo grandes para Eve implicam em mais erros e consequentemente menos qualidade de canal, tornando o intervalo maior. O mesmo acontece no caso de Bob. Nota-se que, quando $Z = 1$, a aproximação se afasta das demais curvas, uma vez que o intervalo na Figura 15 é muito menor do que aquele apresentado na Figura 16. Entretanto, a precisão da aproximação aumenta quando valores maiores de Z são

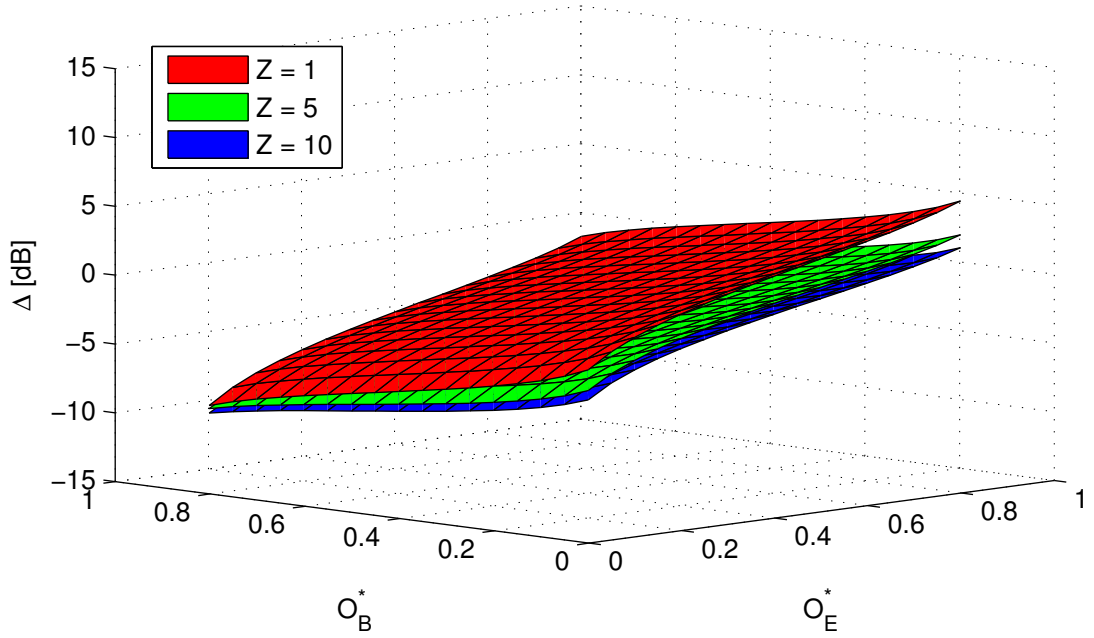

Figura 15: Intervalo de segurança baseado na probabilidade de *outage* exata em função de $\mathscr{O}_B^*$ e $\mathscr{O}_E^*$ considerando $Z \in [1,5,10]$ e $n_A = n_B = n_E = 2$.

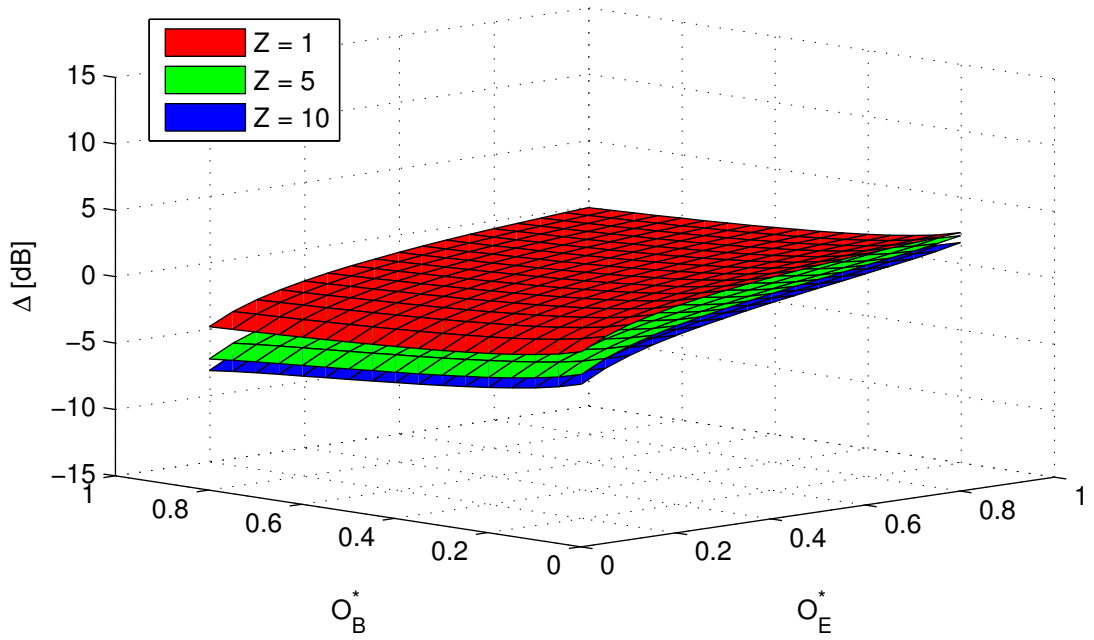

Figura 16: Intervalo de segurança baseado na probabilidade de *outage* aproximada em função de $\mathscr{O}_B^*$ e $\mathscr{O}_E^*$ considerando $Z \in [1,5,10]$ e $n_A = n_B = n_E = 2$.

empregados.

Comparando as Figuras 15 e 17, observam-se valores muito próximos; neste caso, referindo-se a variação dos valores alvos de FER e da probabilidade de *outage*, o intervalo de

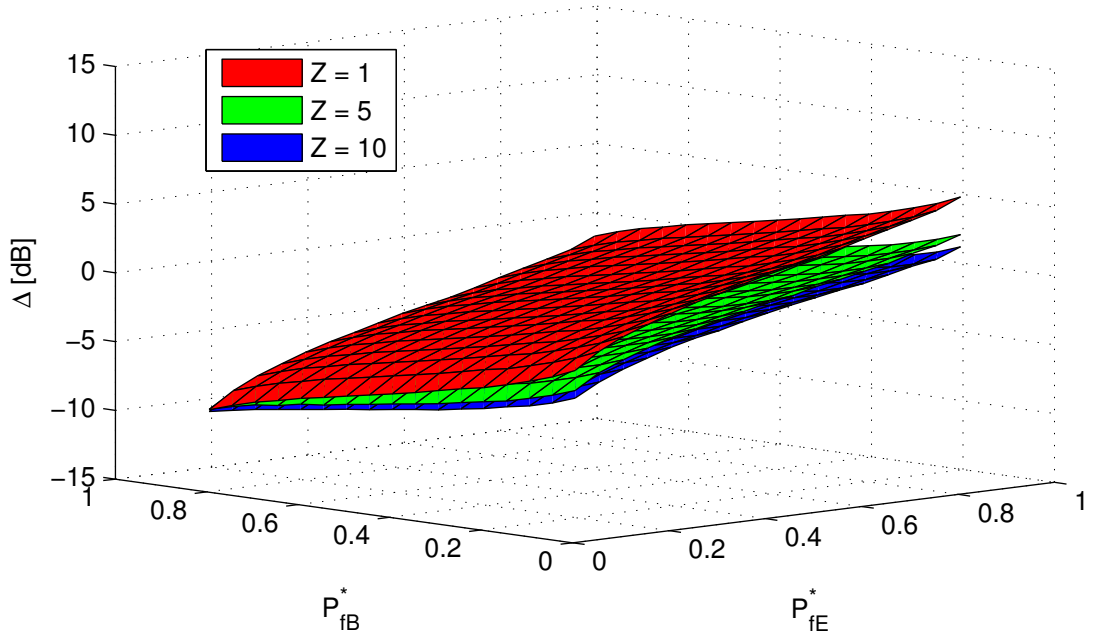

Figura 17: Intervalo de segurança baseado na FER em função de $\mathscr{O}_B^*$ e $\mathscr{O}_E^*$ considerando $Z \in [1,5,10]$ e $n_A = n_B = n_E = 2$.

segurança baseado na probabilidade de *outage* é uma alterativa para estimar a segurança em cenários reais a fim de evitar soluções numéricas.

5 COMENTÁRIOS FINAIS

5.1 CONCLUSÕES

Considerando uma rede com três nós, dois legítimos e um espião, este trabalho propôs um método prático de transmissão e recepção, o TAS/MRC com embaralhamento de pacotes. Esta abordagem foi avaliada utilizando como métrica o intervalo de segurança levando em consideração duas métricas de desempenho: a probabilidade de *outage* e a FER, este utilizando um código corretor de erros.

Assim, mostrou-se que o intervalo de segurança baseado na FER é fracamente dependente do tamanho do pacote para o código utilizado; após isso, viu-se que o valor do intervalo pode ser aproximado com uma grande precisão a partir da equação do limite superior do código utilizado, ao invés de se usar uma equação exata nem sempre disponível.

Também, como em (CHIODI JUNIOR et al., 2015a), atestou-se que a aproximação da probabilidade de *outage* é apenas válida para poucas antenas em Alice, como também para poucas antenas em Bob. Com o aumento das antenas em Bob, o intervalo aproximado começa a se comportar de forma diferente do exato e do baseado na FER, tendo uma queda de segurança com o aumento das antenas em Alice; enquanto para os outros dois casos, o aumento nas antenas de Alice e Bob traz uma melhora para a segurança (o valor do intervalo se torna menor). No entanto, ao isolar a quantidade de antenas em Alice, o erro referente a aproximação da função Gama incompleta se torna irrisório. Também observa-se que ao se utilizar o embaralhamento de pacotes para a FER, obtém-se os mesmos números de antenas em Alice do caso do intervalo de segurança baseado na probabilidade de *outage*, ou seja, o TAS/MRC com embaralhamento de pacotes pode atingir os mesmo resultados que o caso onde se considera o limite de Shannon.

Observou-se que o aumento da quantidade de pacotes utilizada no embaralhamento tem um efeito positivo no aumento da segurança. Isto se deve ao efeito do TAS/MRC que fornece uma vantagem instantânea do canal legítimo sobre o ilegitimo fazendo com que o embaralhamento piore muito mais a recepção da mensagem em Eve do que em Bob. No entanto, este aumento de Z também influencia no atraso da recepção da mensagem, pois é necessário

receber todos os Z pacotes para efetuar o desembaralhamento.

5.2 TRABALHOS FUTUROS

Como trabalhos futuros, é possível analisar esquemas cooperativos com o intuito de melhorar a segurança em camada física, assim como em (ZOU et al., 2015; CHEN, 2011), porém utilizando o intervalo de segurança como métrica para avaliação da segurança (KOLOKOTRONIS et al., 2015).

Outra proposta mais imediata é expandir a análise de segurança do TAS/MRC deste trabalho para contemplar esquemas com múltiplos espiões, como pode ser visto em (IBRAHIM et al., 2014; WANG et al., 2012; SHRESTHA et al., 2013), podendo também utilizar múltiplos nós legítimos, utilizando o intervalo de segurança ou ainda outras métricas como a capacidade de confidencialidade para avaliar estas abordagens.

Também, pode-se fazer uma análise de segurança com o TAS/MRC com embaralhamento de pacotes em redes ad-hoc (MUCCHI et al., 2014; SUN et al., 2012), onde a ausência de infra-estrutura dificulta a criação e distribuição de chaves de criptografia. Ainda, esta abordagem descentralizada facilitaria a escalabilidade da rede com baixo *overhead*, pois a única informação que os transmissores precisam saber é o índice da antena com melhor SNR. Não apenas nisso, mas também é possível aplicar os princípios de segurança em camada física em redes convencionais, como em (BALDI et al., 2013a), na geração e distribuição de chaves criptográficas; por exemplo, para distribuí-las, pode-se embaralhar a informação em Z pacotes antes de enviar, assim, apenas quem conseguir receber todos os pacotes corretamente poderá utilizar a chave, dificultando o recebimento em Eve.

REFERÊNCIAS

ALVES, H. et al. Performance of Transmit Antenna Selection Physical Layer Security Schemes. **IEEE Signal Process. Lett.**, v. 19, n. 6, p. 372–375, Junho 2012. ISSN 1070-9908.

BALDI, M.; BIANCHI, M.; CHIARALUCE, F. Non-systematic codes for physical layer security. In: **Information Theory Workshop (ITW), 2010 IEEE**. [S.l.: s.n.], 2010. p. 1–5.

BALDI, M.; BIANCHI, M.; CHIARALUCE, F. Coding with scrambling, concatenation and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analisys. **IEEE Trans. Inf. Forensics Security**, v. 7, n. 3, p. 883–894, Junho 2012. ISSN 1556-6013.

BALDI, M. et al. A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks. **IEEE Microw. Wireless Compon. Lett.**, v. 2, n. 2, p. 183–186, Abril 2013. ISSN 2162-2337.

BALDI, M. et al. A practical viewpoint on the performance of LDPC codes over the fast Rayleigh Fading Wire-Tap Channel. In: **Computers and Communications (ISCC), 2013 IEEE Symposium on**. [S.l.: s.n.], 2013. p. 000287–000292.

BARROS, J.; RODRIGUES, M. Secrecy Capacity of Wireless Channels. In: **Information Theory, 2006 IEEE International Symposium on**. [S.l.: s.n.], 2006. p. 356–360.

BLOCH, M.; BARROS, J. **Physical-Layer Security: From Information Theory to Security Engineering**. Cambridge University Press, 2011. ISBN 9781139496292. Disponível em: <https://books.google.com.br/books?id=ov5jYjrrNCIC>.

BLOCH, M. et al. Wireless Information-Theoretic Security. **IEEE Trans. Inf. Theory**, v. 54, n. 6, p. 2515–2534, Junho 2008. ISSN 0018-9448.

BRANTE, G. de O.; KAKITANI, M.; SOUZA, R. D. Energy Efficiency Analysis of Some Cooperative and Non-Cooperative Transmission Schemes in Wireless Sensor Networks. **IEEE Trans. Commun.**, v. 59, n. 10, p. 2671–2677, Outubro 2011. ISSN 0090-6778.

CHEN, C.-Y. et al. Antenna Selection in Space-Time Block Coded Systems: Performance Analysis and Low-Complexity Algorithm. **IEEE Trans. Signal Process.**, v. 56, n. 7, p. 3303–3314, Julho 2008. ISSN 1053-587X.

CHEN, J.; FENG, L. Using Lower and Upper Bounds to Increase the Computing Accuracy of Monte Carlo Method. In: **Computational and Information Sciences (ICCIS), 2010 International Conference on**. [S.l.: s.n.], 2010. p. 630–633.

CHEN, L. Physical layer security for cooperative relaying in broadcast networks. In: **MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011**. [S.l.: s.n.], 2011. p. 91–96. ISSN 2155-7578.

CHEN, Z. et al. Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels. In: **Information Theory, 2003. Proceedings. IEEE International Symposium on**. [S.l.: s.n.], 2005. p. 94–.

CHIODI JUNIOR, M. A. et al. On the Security Gap of Convolutional-Coded Transmit Antenna Selection Systems. In: **XXXIII Simpósio Brasileiro de Telecomunicações 2015 (SBrT2015)**. Juiz de Fora, Brazil: [s.n.], 2015.

CHIODI JUNIOR, M. A. et al. Achieving Negative Security Gap with Transmit Antenna Selection and Frame Scrambling in Quasi-Static Fading Channels. **Electronics Letters**, v. 51, n. 3, p. 200–202, Fevereiro 2015. ISSN 0013-5194.

CHIODI JUNIOR, M. A. et al. Security Gap of Coded Transmit Antenna Selection Systems with Frame Scrambling. **Journal of Communication and Information Systems**, 2015. ISSN 1980-6604.

CSISZAR, I.; KORNER, J. Broadcast channels with confidential messages. **IEEE Trans. Inf. Theory**, v. 24, n. 3, p. 339–348, Maio 1978. ISSN 0018-9448.

GOLDSMITH, A. **Wireless Communications**. Cambridge University Press, 2005. ISBN 9780521837163. Disponível em: <https://books.google.com.br/books?id=n-3ZZ9i0s-cC>.

GOPALA, P. K.; LAI, L.; GAMAL, H. E. On the Secrecy Capacity of Fading Channels. **IEEE Trans. Inf. Theory**, v. 54, n. 10, p. 4687–4698, Outubro 2008. ISSN 0018-9448.

IBRAHIM, D.; HASSAN, E.; EL-DOLIL, S. Improving physical layer security in two-way cooperative networks with multiple eavesdroppers. In: **Informatics and Systems (INFOS), 2014 9th International Conference on**. [S.l.: s.n.], 2014. p. ORDS–8–ORDS–13.

KLINC, D. et al. LDPC codes for the Gaussian Wiretap Channel. **IEEE Trans. Inf. Forensics Security**, v. 6, n. 3, p. 532–540, Setembro 2011. ISSN 1556-6013.

KOLOKOTRONIS, N. et al. A cooperative jamming protocol for physical layer security in wireless networks. In: **Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on**. [S.l.: s.n.], 2015. p. 5803–5807.

MACKEOWN, P. K. Book; Book/Illustrated. **Stochastic simulation in physics**. [S.l.]: Singapore ; New York : Springer, 1997. ISBN 9813083263.

MUCCHI, L. et al. Secrecy capacity of the Noise-Loop secure modulation. In: **Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on**. [S.l.: s.n.], 2014. p. 1–5.

MUKHERJEE, A. et al. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. **IEEE Commun. Surveys Tuts.**, v. 16, n. 3, p. 1550–1573, Março 2014. ISSN 1553-877X.

PROAKIS, J. **Digital Communications**. McGraw-Hill, 2001. (McGraw-Hill Series in Electrical and Computer Engineering. Computer Engineering). ISBN 9780072321111. Disponível em: <https://books.google.com.br/books?id=sbr8QwAACAAJ>.

SANAYEI, S.; NOSRATINIA, A. Antenna selection in MIMO systems. **IEEE Commun. Mag.**, v. 42, n. 10, p. 68–73, Outubro 2004. ISSN 0163-6804.

SHANNON, C. Communication theory of secrecy systems. **The Bell System Technical Journal**, v. 28, n. 4, p. 656–715, Outubro 1949. ISSN 0005-8580.

SHRESTHA, A.; JUNG, J.; KWAK, K. S. Secure wireless multicasting in presence of multiple eavesdroppers. In: **Communications and Information Technologies (ISCIT), 2013 13th International Symposium on**. [S.l.: s.n.], 2013. p. 814–817.

SUN, D. et al. Exploring opportunistic scheduling in ad-hoc network with physical layer security. In: **Network Security and Systems (JNS2), 2012 National Days of**. [S.l.: s.n.], 2012. p. 62–67.

TANG, X.; LIU, R.; SPASOJEVIC, P. On the Achievable Secrecy Throughput of Block Fading Channels with No Channel State Information at Transmitter. In: **Information Sciences and Systems, 2007. CISS '07. 41st Annual Conference on**. [S.l.: s.n.], 2007. p. 917–922.

TANG, X. et al. On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels. **IEEE Trans. Inf. Theory**, v. 55, n. 4, p. 1575–1591, Abril 2009. ISSN 0018-9448.

WANG, C.-L.; CHO, T.-N.; YANG, K.-J. A New Cooperative Transmission Strategy for Physical-Layer Security with Multiple Eavesdroppers. In: **Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th**. [S.l.: s.n.], 2012. p. 1–5. ISSN 1550-2252.

WYNER, A. The wire-tap channel. **The Bell System Technical Journal**, v. 54, n. 8, p. 1355–1387, Outubro 1975. ISSN 0005-8580.

YANG, N. et al. Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels. **IEEE Trans. Commun.**, v. 61, n. 1, p. 144–154, Janeiro 2013. ISSN 0090-6778.

ZOU, Y. et al. Improving physical-layer security in wireless communications using diversity techniques. **IEEE Netw.**, v. 29, n. 1, p. 42–48, Janeiro 2015. ISSN 0890-8044.