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

RODRIGO TSUNEYOSHI KAIDO

CODIFICAÇÃO DE REDE COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA NA CAMADA FÍSICA EM *SMART GRIDS*

DISSERTAÇÃO

CURITIBA
2014

RODRIGO TSUNEYOSHI KAIDO

CODIFICAÇÃO DE REDE COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA NA CAMADA FÍSICA EM *SMART GRIDS*

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

K13 Kaido, Rodrigo Tsuneyoshi
Codificação de rede como alternativa para aumentar a segurança na camada física em *smart grids* / Rodrigo Tsuneyoshi Kaido. – 2014.
63 f. : il. ; 30 cm

Orientador: João Luiz Rebelatto.
Coorientador: Richard Demo Souza.
Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial. Curitiba, 2014.
Bibliografia: f. 51-54.

1. Redes elétricas inteligentes. 2. Sistemas de comunicação sem fio – Medidas de segurança. 3. Sistemas de transmissão de dados – Medidas de segurança. 4. Teoria da codificação. 5. Teoria da informação. 6. Sigilo. 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. ed.) 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. 653

"Codificação de Rede como Alternativa para Aumentar a Segurança na Camada Física em Smart Grids."

por

Rodrigo Tsuneyoshi Kaido

Orientador: Prof. Dr. João Luiz Rebelatto

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de MESTRE EM CIÊNCIAS – Área de Concentração: Telecomunicação 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 05 de fevereiro 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. Glauber Gomes de Oliveira Brante
(UTFPR)

Visto da coordenação:

Prof. Ricardo Lüders, Dr.
(Coordenador do CPGEI)

A Folha de Aprovação assinada encontra-se na Coordenação do Programa.

Dedico este trabalho à minha família, ao meu pai Yutaka, à minha mãe Mitica e à minha irmã Beatriz, que sempre proporcionaram a tranquilidade e a disposição necessárias para as muitas horas de estudo nessa longa caminhada.

AGRADECIMENTOS

Agradeço aos professores João Luiz Rebelatto e Richard Demo Souza, pela orientação e incentivo, para a realização do mestrado. Agradeço também ao gerente da COPEL, José Maria Tiepolo, pela autorização dos horários das aulas e pelo incentivo.

RESUMO

KAIDO, Rodrigo Tsuneyoshi. CODIFICAÇÃO DE REDE COMO ALTERNATIVA PARA AUMENTAR A SEGURANÇA NA CAMADA FÍSICA EM *SMART GRIDS*. 62 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Smart grids representam o futuro das redes elétricas. Estes tipos de redes devem ser robustas a flutuações de carga e devem possuir monitoramento e gerenciamento inteligente e em tempo real. Para que essas demandas sejam possíveis, é preciso uma comunicação de dados de alta velocidade, flexível e de baixo custo. Dentro dessas características, muitos autores propõem a utilização de sistemas de comunicação sem fio, os quais possuem um custo de implantação mais baixo que redes ópticas ou cabeadas, além de possuir flexibilidade para rápidas mudanças de topologia, e não apresentarem barreiras em relação aos padrões e equipamentos, o oposto por exemplo ao caso do sistema PLC (*Power Line Communications*). Devido à natureza difusora do canal sem fio, segurança nesse tipo de rede é um dos pontos mais críticos, já que um ataque de qualquer natureza pode provocar perturbações e *blackouts* na rede elétrica, ou gerar problemas de privacidade, na situação em que atacantes passivos (*eavesdroppers*) interceptam mensagens da rede com o intuito de obter algum tipo de benefício. Esta segunda situação, de ataques passivos, será abordada neste trabalho. Além das tradicionais técnicas de criptografia geralmente utilizadas para aumentar a segurança de redes de comunicação, outra área que vem recentemente despertando interesse da comunidade científica é a área de segurança na camada física, a qual é baseada em conceitos da teoria da informação de Shannon. Neste trabalho, utiliza-se as técnicas de codificação de rede para aumentar a segurança na camada física da parte de múltiplo acesso de uma rede de comunicação sem fio, em que dois transmissores possuem informações independentes para um destino em comum, na presença de um *eavesdropper*. Utilizando-se a probabilidade de *outage* com restrições de sigilo como métrica, mostra-se através de resultados analíticos e numéricos que o sigilo pode ser aumentado através da codificação de rede, quando comparada com a transmissão direta e com as técnicas de cooperação tradicionais.

Palavras-chave: Segurança na camada física, codificação de rede, comunicação cooperativa, sigilo, *smart grids*

ABSTRACT

KAIDO, Rodrigo Tsuneyoshi. NETWORK CODING AS A TOOL TO INCREASE THE PHYSICAL-LAYER SECURITY IN SMART GRIDS. 62 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Smart grids represent the future of electrical power systems. These kind of networks must be robust to load fluctuations as well as have smart monitoring and management in a real-time fashion. Based on the aforementioned needs, many authors propose the use of wireless communications systems in order to meet these demands, due to their efficient tradeoff between low-cost and high-speed when compared to wired connections such as optical fibers or metallic cables, and, in addition, they are flexible to topology changes and do not have constraints in terms of standards and devices, the opposite for example to the case of PLC (Power Line Communications). Due to the broadcast nature of the wireless medium, security is one of the critical issues in smart grids since the occurrence of attacks can lead to load fluctuations and blackouts in the electrical system, or generate secrecy problems, in the situation where passive eavesdroppers intercept messages in the network aiming to obtain some kind of benefit. This second case of passive attacks will be addressed in this work. In addition to classical cryptography strategies commonly used to increase the security in communications systems, another area which has been studied by the scientific community is the physical-layer security, which is based on the Shannon's information theory. In this work, we use the network coding technique as a tool to increase the physical-layer security in a multiple access wireless network, where two users have independent information to transmit to a common destination, in the presence of an eavesdropper. By using the secrecy outage probability as the metric, we show through theoretic and numerical results that the network security can be increased through the use of network coding when compared to the direct transmission and traditional cooperative techniques.

Keywords: Physical-layer security, network coding, cooperative communication, secrecy, smart grids

LISTA DE FIGURAS

LISTA DE SIGLAS

PLC	*Power Line Communications*
OSI	*Open Systems Interconnections*
NC	*Network Coding*
DNC	*Dynamic Network Coding*
AF	*Amplify-and-Forward*
DF	*Decode-and-Forward*
SNR	*Signal-to-Noise Ratio*
WLAN	*Wireless Local Area Network*
WSN	*Wireless Sensor Network*
WMN	*Wireless Mesh Network*
LV	*Low-Voltage*
MV	*Medium-Voltage*
DAU	*Data Aggregator Unit*
AMI	*Advanced Metering Infrastructure*
HAN	*Home Area Network*
NAN	*Neighborhood Area Network*
WAN	*Wide Area Network*
SIM	Sistema Inteligente de Medição
GPRS	*General Packet Radio Service*
RF	*Radio-Frequency*
AWGN	*Additive White Gaussian Noise*
bpcu	*bits per channel use*
WTC	*Wire-Tap Channel*
pdf	*probability density function*
MRC	*Maximal Ratio Combining*
XOR	*Exclusive-OR*
GF	*Galois Field*
RLNC	*Random Linear Network Coding*
GDNC	*Generalized Dynamic Network Coding*

LISTA DE SÍMBOLOS

D	Nó destino
e	Nó *eavesdropper*
x_{ij}	Sinal transmitido pelo nó i para o nó j, que possui distribuição Gaussiana
y_{ij}	Sinal recebido pelo nó j, transmitido pelo nó i
h_{ij}	Coeficiente de desvanecimento de canal do enlace entre os nós i e j
P_i	Potência de transmissão do nó i
n_{ij}	Ruído Aditivo Branco e Gaussiano
d_{ij}	Distância entre os nós i e j
γ_{ij}	Relação Sinal-Ruído (SNR) instantânea do enlace entre os nós i e j
σ_{ij}^2	Variância do ruído Gaussiano
$\overline{\gamma}_{ij}$	Relação Sinal-Ruído (SNR) média no enlace entre os nós i e j
I_{ij}	Informação mútua recebida pelo nó j, transmitida pelo nó i
$\mathscr{P}_{o,ij}$	Probabilidade de *outage* do enlace entre i e j
$\mathscr{M}$	Conjunto das mensagens enviadas sem codificação ou criptografia
$\mathscr{X}$	Conjunto de palavras-código obtidas após a codificação com a utilização de uma chave secreta
$\mathscr{K}$	Conjunto de chaves secretas utilizadas para codificar mensagens
$c(M,K)$	Função de codificação da mensagem M usando a chave secreta K
$d(X,K)$	Função de decodificação da mensagem X usando a chave secreta K
$H(M\|X)$	Entropia condicional de M dado X
$H(M)$	Entropia em relação a mensagem M
C_s	Capacidade de sigilo
I_{1D}	Informação mútua recebida pelo nó D que foi enviado pelo nó 1
I_{1e}	Informação mútua que o *eavesdropper* conseguiu interceptar da transmissão do nó 1 para o destino
$p(.)$	Função densidade de probabilidade
$\mathscr{P}_{so}$	Probabilidade de *outage* com restrições de sigilo
R_s	Taxa de sigilo alvo
I_{DF_a}	Informação mútua do esquema DF caso ocorra *outage* no enlace entre os nós 1 e 2
I_{DF_b}	Informação mútua do esquema DF caso não ocorra *outage* no enlace entre os nós 1 e 2
$I_{\mathrm{DF,e}}$	Informação mútua obtida pelo nó *eavesdropper* para o esquema DF
$B(x,y)$	Função Beta (integral de Euler de primeira ordem)

SUMÁRIO

1 INTRODUÇÃO

Smart Grid, ou rede elétrica inteligente, é um termo comumente usado para designar sistemas elétricos de potência que possuem algumas características peculiares que são diferentes dos sistemas de energia tradicionais (WANG; YI, 2011). Essas redes devem ser robustas a flutuações de carga, devem possuir um balanceamento entre fornecimento e demanda de energia, precisam adotar mecanismos inteligentes de controle em tempo real, e devem conseguir contornar situações de falhas em equipamentos, que podem prevenir contra perturbações elétricas e *blackouts* de energia (WANG; YI, 2011). Vários estudos vêm sendo realizados para que estas redes *smart grids* se tornem realidade (WANG et al., 2010; LI; ZHANG, 2011; WANG; YI, 2011; AHMED et al., 2012; LI et al., 2012; NIYATO; WANG, 2012). Dentre as tecnologias de comunicação de dados disponíveis para utilização em *smart grids*, pode-se destacar a comunicação via PLC (*Power Line Communications*). Porém, tal tecnologia pode não ser satisfatória devido a dificuldade em se passar os sinais de dados pelos transformadores, bem como ao fato de não serem flexíveis para atender conexões ponto-a-ponto entre os dispositivos intermediários. Outra possibilidade seria a utilização de comunicação de dados por fibras ópticas, mas os custos para conectar todos os dispositivos são muito elevados e a solução é pouco flexível. Dessa forma, devido principalmente à sua versatilidade e custo relativamente baixo, sistemas de comunicação sem fio vêm surgindo como forte alternativa para aplicação em *smart grids* (WANG; YI, 2011).

Um dos objetivos mais evidentes das *smart grids* é a necessidade de envio de mensagens dos dispositivos elétricos até a central de controle para que se tenha uma estimativa confiável do sistema, e vice-versa, com o envio de mensagens e comandos da central de controle até os dispositivos, sem nenhuma perda de informação (LI; ZHANG, 2011).

Segurança é um dos pontos mais críticos para *smart grids*. Um ataque de qualquer natureza nessas redes pode ter consequências desastrosas. Uma perda de informação pode levar a resultados inesperados como desligamentos de energia não previstos, flutuações de carga e *blackouts* (WANG; YI, 2011). Esse tipo de preocupação é ainda maior em sistemas de comunicação sem fio, devido à característica difusora do canal sem fio.

Os ataques a *smart grids* podem ocorrer de diversas formas. O atacante pode ser ativo, ou seja, pode ser capaz de inserir pacotes errados ou enviar pacotes para destinos diferentes. Como a ideia dessa rede é ser amplamente interligada, um pacote errado pode se espalhar rapidamente por toda a rede e causar grandes estragos. Outra forma de ataque é a presença do atacante passivo, mais comumente conhecido por *eavesdropper*, que fica "escutando" as informações que trafegam pela rede, na tentativa de obter os padrões de tráfego ou decodificar informações importantes, gerando problemas de sigilo das informações. Esse é um dos piores tipos de ataque, já que se tem pouca ou nenhuma informação a respeito do *eavesdropper* (WANG; YI, 2011). Esse tipo de ataque passivo faz parte do escopo deste trabalho.

O uso de criptografia aparece como opção para lidar com esses ataques, como mostrado em (ZHANG et al., 2010), que atua na camada de apresentação do modelo OSI (*Open Systems Interconnections*). Uma outra maneira de proteger a rede é a utilização de um *firewall*, como citado em (WANG; YI, 2011), que atua na camada de aplicação do modelo OSI, que é bastante eficiente em caso de ataques ativos. Poderia ser usada ainda a técnica de *jamming*, que envia um ruído controlado ao atacante (GABRY, 2012), desde que se saiba a localização, o que nem sempre é possível, já que o *eavesdropper* possui a característica de trabalhar exclusivamente em modo de recepção. Vale ressaltar que a preocupação com a segurança existe em todas as camadas do modelo OSI. De maneira complementar às outras técnicas que podem ser adotadas em outras camadas, neste trabalho foi proposta a codificação de rede como alternativa para aumentar a segurança na camada física em *smart grids*.

Em (AHLSWEDE et al., 2000), os autores propuseram uma nova maneira para a disseminação de mensagens em uma comunicação: os nós, que tradicionalmente atuavam como roteadores (apenas retransmitiam informações da maneira como eram recebidas), seriam capazes de retransmitir combinações lineares de diversas mensagens distintas. Com a utilização dessa técnica, denominada codificação de rede (termo em inglês *Network Coding* (NC)), foi mostrado em (AHLSWEDE et al., 2000) que o *throughput* da rede pode ser aumentado. Posteriormente, mostrou-se também que a técnica de codificação de rede, quando aplicada a redes cooperativas, pode prover ganhos em termos de ordem de confiabilidade (XIAO et al., 2007) e ordem de diversidade (XIAO; SKOGLUND, 2010; REBELATTO et al., 2010, 2012). Em (XIAO; SKOGLUND, 2010), os autores propuseram uma codificação de rede denominada DNC (*Dynamic Network Coding*), para uma rede cooperativa formada por dois ou mais usuários que possuíam informações independentes para um destino comum. Foi proposta uma codificação de rede não-binária e determinística para redes dinâmicas, para que a ordem de diversidade obtida fosse maior do que das estratégias tradicionais presentes na literatura. Os

autores consideraram que a rede era dinâmica por causa dos apagamentos de mensagens que podem ocorrer durante as trocas de dados entre os elementos da rede de comunicação. Neste trabalho, considerou-se uma codificação de rede DNC, para o caso particular com dois usuários e um nó destino comum. O que difere da análise em (XIAO; SKOGLUND, 2010) é a presença de um atacante passivo.

Recentemente, diversos autores têm utilizado a codificação de rede para aumentar a segurança de redes sem fio (BHATTAD; NARAYANAN, 2005; CAI; YEUNG, 2006; ZHANG et al., 2010; FRANZ et al., 2012; BLOCH; BARROS, 2011). Em (BHATTAD; NARAYANAN, 2005), foram calculados os limites de probabilidade para uma rede ser fracamente segura quando o *eavesdropper* consegue obter algumas informações. Uma rede fracamente segura significa que o atacante passivo conseguiu obter uma informação do tráfego, sem criptografia, mas não foi capaz de dar significado ao que foi interceptado; o autor considerou ainda que a codificação de rede era feita apenas pelos nós de origem e destino. Em (CAI; YEUNG, 2011), foi apresentada uma rede em grafos, na qual foi proposta uma codificação de rede linear e segura, em que foi incorporada à segurança da informação com a codificação de rede, com o uso de criptografia, e onde o *eavesdropper* podia escutar um subconjunto fixo de enlaces, tudo isso juntamente com a apresentação de provas matemáticas para demonstrar a eficiência da proposição. Em (ZHANG et al., 2010), os autores propuseram um esquema denominado *P-Coding*, que utiliza uma codificação de rede linear e aleatória, para uma rede altamente dinâmica, contra atacantes passivos com muita capacidade de processamento. Os autores relacionaram o tamanho do campo finito com a probabilidade de segurança, e concluíram que quanto maior o tamanho do campo finito mais segura se tornava a rede. Em (FRANZ et al., 2012), a codificação de rede foi proposta em conjunto com a criptografia para evitar ataques de pacotes modificados. Neste caso, o atacante é ativo, já que é capaz de introduzir pacotes alterados na rede. Em (BAO; LI, 2008) foi proposto um esquema de comunicação cooperativa usando codificação de rede adaptativa devido à natureza dinâmica das redes sem fio e à necessidade de adaptação a mudanças rápidas de topologia. Os autores calcularam as taxas alcançadas e a probabilidade de *outage* para os casos assintóticos. Probabilidade de *outage* é a probabilidade de que a SNR instantânea de um enlace seja menor que uma SNR alvo (GOLDSMITH, 2005), ou também a probabilidade de que a informação mútua instantânea transmitida num determinado enlace seja menor que uma taxa alvo.

Em (PHULPIN et al., 2011), os autores justificaram a utilização da codificação de rede para *smart grids*, em termos das trocas de mensagens que devem ser realizadas nesse tipo de rede, e no sentido do aumento da confiabilidade, e concluíram que a ordem de diversidade por nó aumenta quanto maior for o alcance da transmissão, numa rede com 123 nós, tanto para

o sistema PLC quanto para a comunicação sem fio. Essa análise é diferente da que é proposta neste trabalho, primeiro porque não considera a presença de um *eavesdropper*, e segundo porque não considera o sigilo das informações transmitidas, mas apenas o grau de confiabilidade contra a perda de pacotes.

Notou-se ainda que os esquemas de comunicação cooperativa, cuja proposta inicial seria para aumentar a confiabilidade (LANEMAN et al., 2004; NOSRATINIA et al., 2004; GUNDUZ; ERKIP, 2007), também podem ser muito úteis para aumentar o sigilo nestes tipos de redes quando sujeitas à ação de um *eavesdropper* (LAI; GAMAL, 2008; GABRY, 2012), sendo estes conceitos passíveis de extensão para *smart grids* (AHMED et al., 2012; NIYATO; WANG, 2012). Em uma rede de comunicação cooperativa, além de transmitir suas próprias mensagens, os nós auxiliam uns aos outros retransmitindo as mensagens de seus parceiros. Uma vez que a mesma mensagem é transmitida por caminhos distintos (sujeitos a desvanecimentos independentes), o efeito de múltiplas antenas distribuídas é obtido, resultando em um aumento na ordem de diversidade do sistema e consequentemente na sua confiabilidade (LANEMAN et al., 2004; NOSRATINIA et al., 2004).

Um termo bastante comum utilizado quando existe um *eavesdropper*, já citado anteriormente, é o sigilo (*secrecy*). Introduzido primeiramente em (SHANNON, 1949), esse tema vem sendo bastante explorado por diversos autores. Várias técnicas vêm sendo propostas para aumentar o sigilo nas transmissões. Alguns autores propuseram o uso de múltiplas antenas (ALVES et al., 2012; YANG et al., 2013). Outros exploraram os conceitos de comunicação cooperativa com sigilo (LAI; GAMAL, 2008; GABRY, 2012). Já em (BARROS; RODRIGUES, 2006), os autores definiram os conceitos de capacidade de sigilo em termos de probabilidade de *outage* para a transmissão direta e trouxeram uma caracterização da taxa de transmissão máxima em que o *eavesdropper* não era capaz de decodificar nenhuma informação. Em (GABRY, 2012), o autor mostrou expressões fechadas para a probabilidade de *outage* com restrições de sigilo para os esquemas amplifica-e-encaminha (AF) e decodifica-e-encaminha (DF), tanto para o caso de o transmissor possuir conhecimento dos coeficientes de desvanecimento dos canais, como para o caso de não possuir nenhuma informação da condição instantânea dos canais. O autor mostrou que os melhores resultados são obtidos para o esquema DF. Foram analisados alguns casos de posicionamentos diferentes tanto para o nó *relay* quanto para o *eavesdropper*, cuja conclusão foi que a melhor situação para os nós legítimos é quando o nó *relay* está posicionado exatamente no meio dos nós de origem e destino, e o *eavesdropper* está mais afastado do nó transmissor do que do nó de destino. O autor considerou que a única informação conhecida a respeito do atacante passivo era a sua localização (conhecimento da SNR média), mas não tinha conhecimento da condição instantânea do canal. Por último,

Gabry considerou ainda a cooperação através de *jamming*, em que o nó cooperativo envia ruído controlado para o *eavesdropper*, na tentativa de prejudicar a captura dos sinais.

Neste trabalho, foi considerada a comunicação cooperativa usando o esquema DF para fins de comparação em termos de sigilo, em relação ao esquema de codificação de rede proposto.

1.1 MOTIVAÇÃO

Segurança é um dos pontos críticos para *smart grids* pois ataques de qualquer natureza e perdas de mensagens podem provocar perturbações e *blackouts* na rede elétrica, bem como gerar problemas quanto ao sigilo das informações, na situação em que *eavesdroppers* interceptem as mensagens transmitidas nessa rede. Vale lembrar que esse problema de segurança é acentuado devido à natureza difusora das redes sem fio. Por isso, é proposta a utilização da codificação de rede como alternativa para aumentar a segurança na camada física, que pode ser vantajosa para sistemas cooperativos com a presença de um *eavesdropper* (FRAGOULI; SOLJANIN, 2007b). Este esquema de segurança deve ser encarado como um complemento às tradicionais técnicas de segurança presentes na literatura, como por exemplo, o *firewall*, que atua na camada de aplicação do modelo OSI, ou da criptografia clássica, que atua na camada de apresentação deste mesmo modelo. Um ponto negativo para a criptografia clássica é a necessidade de trocas periódicas de chaves de segurança, que precisam ocorrer através de uma comunicação segura, o que pode ser dificultada em *smart grids*, já que os nós da rede estão espalhados geograficamente. Adicionalmente, a codificação de rede pode ser capaz de aumentar a confiabilidade da rede (em termos de diminuição de taxa de erro), o que demonstra mais um benefício para *smart grids*, que necessitam uma rede com alta confiabilidade.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Propor um esquema de transmissão cooperativa, utilizando codificação de rede, que seja mais eficiente em termos de sigilo na camada física que os esquemas de transmissão presentes na literatura.

1.2.2 OBJETIVOS ESPECÍFICOS

- Calcular a probabilidade de existência da capacidade de sigilo;

- Calcular a probabilidade de *outage* com restrições de sigilo;
- Verificar a influência de parâmetros, tais como a taxa de sigilo alvo e a SNR média do *eavesdropper*, no desempenho do esquema proposto.

1.2.3 RESULTADOS OBTIDOS

Para o modelo proposto, os melhores resultados em relação ao sigilo das informações foram obtidos utilizando o esquema de codificação de rede, quando comparado com os esquemas tradicionais descritos na literatura, como por exemplo a transmissão direta, ou ainda a transmissão cooperativa DF. A probabilidade de existência da capacidade de sigilo alcançou 100% de probabilidade de existência usando o esquema de codificação de rede para valores de SNR média bem menores que dos outros esquemas. A utilização da codificação de rede também proporcionou melhores resultados para a probabilidade de *outage* com restrições de sigilo, neste caso, para a região de alta SNR média do esquema como um todo, quando há necessidade de uma probabilidade de *outage* de sigilo inferior a 10^{-3}.

O artigo relacionado a este trabalho, chamado *Network-Coded Cooperation for a Two-User Wiretap Channel*, foi submetido e aceito na conferência ICASSP (*International Conference on Acoustics, Speech and Signal Processing*) que ocorrerá na cidade de Florença, na Itália, nos dias 4 a 9 de Maio de 2014.

2 *SMART GRIDS*

As redes de energia elétrica tradicionais são complexas e possuem baixa eficiência no seu gerenciamento, isso desde a geração da energia até a distribuição ao consumidor final (AHMED et al., 2012). Uma das maneiras buscadas para enfrentar esses problemas são as redes *smart grids*, que visam integrar tecnologias de sensores para coletar dados da rede e usar métodos de controle desde a geração até a distribuição de energia. Para que essas demandas sejam atendidas é preciso uma comunicação de dados eficiente para que os dispositivos elétricos possam enviar medições, receber mensagens sobre tarifação e fornecer informações adicionais aos consumidores (AHMED et al., 2012).

As *smart grids* diferem das redes tradicionais de energia, pois devem ser robustas a flutuações de carga, devem possuir balanceamento inteligente entre fornecimento e demanda, além de ter mecanismos inteligentes de comando e controle em tempo real (WANG; YI, 2011). Como resultado, precisam prevenir que a ocorrência de uma simples falha em um dispositivo cause perturbações e *blackouts* na rede elétrica. Essas redes inteligentes devem permitir a integração com sistemas elétricos que possuam geração de energia distribuída, provenientes, por exemplo, da energia solar e de turbinas eólicas. Neste caso, a potência não irá fluir necessariamente em uma única direção, do gerador ao dispositivo elétrico, mas em várias direções, já que as fontes de geração de energia estarão distribuídas pela malha elétrica. Por último, em consequência desse gerenciamento inteligente, preços variáveis durante o dia passariam a funcionar, pois poderiam ser estabelecidos alguns critérios de tarifação, que devem levar em consideração a carga, a estabilidade do sistema e a qualidade dos serviços.

Para atender a todas essas demandas de troca de informações, torna-se necessário um sistema de comunicação eficiente e seguro. Existem várias alternativas de sistemas de comunicação para *smart grids*. Uma delas, que vêm ganhando força na comunidade científica, é a comunicação sem fio em *smart grids* (WANG; YI, 2011; LI; ZHANG, 2011; PHULPIN et al., 2011; LI et al., 2012; AHMED et al., 2012; NIYATO; WANG, 2012), pois tem menor custo de implantação, fornece enlaces com alta velocidade e é mais flexível para atender as rápidas mudanças de topologia que uma rede elétrica pode sofrer devido à uma pane no sistema.

Além disso, suporta a inclusão de mais dispositivos no modo *"plug-and-play"*, o que facilita a expansão da rede sem grandes custos. Uma outra alternativa, não tão atraente é o sistema PLC, que possui um custo de implantação relativamente baixo, já que utiliza a própria rede elétrica como canal de comunicação; porém, não é flexível para suportar comunicação ponto-a-ponto entre os dispositivos elétricos, o *throughput* pode não ser suficiente para atender as trocas frequentes de informações entre os dispositivos e a central de comando, já que os sinais de alta velocidade podem não conseguir passar pelos transformadores (WANG; YI, 2011), além de possuir restrições quanto aos padrões e equipamentos (GALLI et al., 2011). Uma outra opção seria a utilização de fibras ópticas, que embora sejam mais seguras e confiáveis, possuem um custo elevado para a implantação, além de serem pouco flexíveis a ampliações e mudanças de topologia (WANG; YI, 2011). Por esses motivos, a comunicação sem fio faz parte do escopo deste trabalho.

Devido à natureza difusora das comunicações sem fio, um dos pontos mais críticos dessas redes é a segurança, uma vez que as mesmas podem sofrer diversos tipos de ataques, dentre as quais podem ser destacadas (WANG; YI, 2011):

- *Jamming*: Um nó malicioso gera interferência de forma proposital na mesma banda de frequência de comunicação da *smart grid*, tendo como objetivo reduzir ou até mesmo eliminar a confiabilidade da transmissão;
- Nó *eavesdropper* fora da rede: Um nó malicioso pode capturar informações de um sistema de comunicação sem fio sem ser autorizado a acessar a rede. Como trabalha exclusivamente em modo de recepção, não emite nenhum sinal, ou seja, torna-se difícil saber de sua localização e sua capacidade. Este nó *eavesdropper* tenta decodificar os pacotes recebidos ou analisar os padrões de tráfego dos nós legítimos. Uma das maneiras de lidar com este tipo de adversário são as técnicas de segurança na camada física (FRAGOULI; SOLJANIN, 2007b; GOEL; NEGI, 2009; BLOCH; BARROS, 2011);
- Nó *eavesdropper* dentro da rede: São os nós maliciosos que não seguem as regras de segurança ou que conseguiram passar pelos procedimentos de autenticação;
- Ataques ativos feitos por nós maliciosos: Estes nós maliciosos podem, por exemplo, descartar pacotes, redirecioná-los para destinos errados, mudar o conteúdo dos pacotes e inundar a rede com pacotes sem significado.

Em (WANG; YI, 2011), os autores fizeram uma descrição detalhada do funcionamento de uma *smart grid*, sob o ponto de vista dos tipos de mensagens trocadas para cada caso,

justificando a utilização de sistemas de comunicação sem fio, e propondo o uso de um sistema de *firewall* denominado *smart tracking firewall*, proveniente dos sistemas de informação. Os autores analisaram o tempo de resposta para controlar um ataque, o *throughput* e o atraso na transmissão, e concluíram que o mecanismo proposto era eficiente contra atacantes ativos se comparado aos métodos individuais de mitigação dos ataques. Além dessa análise, os autores explicaram que as redes WLAN (*Wireless Local Area Network*) e redes de sensores WSN (*Wireless Sensor Network*) não são aplicáveis a *smart grids* distribuídas, principalmente devido à relação de desempenho entre taxa e distância entre os dispositivos. Sugeriu ainda que seja usada uma rede *mesh* WMN (*Wireless Mesh Network*).

Uma rede de medição pode ser implementada com diferentes níveis de inteligência. Em geral, parte-se de uma rede em que se realiza a leitura de dispositivos de maneira automatizada, passa por um gerenciamento de medição até chegar aos medidores inteligentes, que incorporam as funcionalidades descritas anteriormente e acrescentam capacidades de controle e gerenciamento (DECONINCK, 2008), permitindo a implementação de tarifas diferenciadas ao longo do dia e comandos para balancear a carga em caso de incidentes na rede elétrica.

Em (DECONINCK, 2008), o autor apresentou uma tabela com algumas características de tempo de resposta adotadas na prática, bem como a criticidade em cada um dos casos, numa *smart grid* implantada na cidade de Flanders, na Bélgica. Nas situações referentes aos comandos e ao balanceamento da carga o tempo foi considerado crítico. Em situações de leitura de medições, ajuste de parâmetros e envio de alarmes foram considerados como tempo não crítico.

De acordo com (PHULPIN et al., 2011), as *smart grids* precisam de 4 tipos de comunicação principais, sendo duas aplicações em dois sentidos distintos. As aplicações são divididas como funcionalidades gerais (medições inteligentes, informações sobre tarifas, etc.) e gerenciamento avançado. As redes foram separadas em duas partes principais, com uma estação-base para cada região para atender consumidores finais (LV - *Low-Voltage*) e de cada estação-base para a central de controle (MV - *Medium-Voltage*).

Em relação às funcionalidades gerais, a troca de informações pode ocorrer periodicamente de 15 em 15 minutos (PHULPIN et al., 2011). Em Flanders, na Bélgica, esse tempo de troca de informações pode ocorrer com um tempo de resposta que pode variar de 5 minutos até 1 dia, pois neste caso, as mensagens trocadas não são críticas (DECONINCK, 2008). Em (PHULPIN et al., 2011), os autores separaram esse tipo de mensagens não críticas em dois serviços distintos, com duas formas de comunicação diferentes:

- Serviço A1: cada nó na rede distribuída envia suas medições (como por exemplo, consumo médio e carga máxima) para a estação-base. O tipo de comunicação requerida neste caso é de muitos nós para um;
- Serviço A2: A estação-base envia informações diárias gerais, como por exemplo o preço das tarifas. O tipo de comunicação é de um para muitos.

Já o gerenciamento avançado exige troca de mensagens em tempo quase real. Em (IEC 62056-21, 2002), o padrão prevê que o tempo de reação de um dispositivo que está sendo monitorado deve estar entre 200 ms e 1500 ms, já que envolvem serviços técnicos de operação e gerenciamento da rede inteligente (DECONINCK, 2008; PHULPIN et al., 2011). Também foi separado em duas categorias de serviços (PHULPIN et al., 2011):

- Serviço B1: A estação-base recebe os status de monitoramento, medidas de tensão, corrente e demanda de carga, por exemplo. A comunicação necessária é de muitos para um;
- Serviço B2: Inclui o controle e comando com o envio de alertas e operações de controle da estação-base aos nós. A comunicação nesse caso é de um para muitos ou de um para um.

Entretanto, em situações reais, como mostrado em (DECONINCK, 2008), esses tempos de resposta para o gerenciamento avançado podem ser diferentes, com valores que podem variar do tempo previsto em norma, para valores de 5 minutos a 1 hora.

Em (PHULPIN et al., 2011), os autores apresentaram uma estimativa de taxa de dados requerida para cada categoria de serviços. Para a troca de informações gerais periódicas (supondo ocorrer a cada 15 minutos) a taxa de dados não ultrapassaria 10 kbps. O exemplo para o cálculo leva em conta 200 transformadores, cada uma atendendo 50 residências. Cada dispositivo elétrico inteligente não gastaria mais que algumas dezenas de bits por segundo para cada estação-base, e da estação-base para a central de controle não ultrapassaria 1 kbps.

Ainda em (PHULPIN et al., 2011), para estimar a taxa de dados requerida para gerenciamento, os autores consideraram que os status e as estimativas eram obtidas em intervalos menores que 10 segundos. Consequentemente a taxa de informação requerida seria aproximadamente da ordem de 1 kbps na LV e alguns kbps da MV para a central de controle.

É importante ressaltar que para o gerenciamento avançado é necessário uma comunicação com alta confiabilidade.

Em (NIYATO; WANG, 2012), são descritos os dispositivos elétricos principais que formam uma *smart grid*:

- Eletrodomésticos: São dispositivos que consomem energia. A potência consumida por esses dispositivos pode ser enviada para um medidor inteligente;
- Medidor inteligente (*Smart Meter*): Dispositivo usado para coletar os dados sobre a potência consumida em cada residência;
- Unidade de agregação de dados (DAU - *Data Aggregator Unit*): Responsável por coletar as informações transmitidas pelos medidores inteligentes. Esses dados são enviados para a central de controle;
- Gerador de potência: É o equipamento responsável pelo fornecimento de potência ao sistema. Em uma *smart grid*, este equipamento deve enviar relatórios sobre o seu status e capacidade à central de controle;
- Transmissão e distribuição de energia: São usadas para transferir potência elétrica do gerador aos consumidores. Informações de status e capacidade também devem ser enviadas para a central de controle;
- Sistema de gerenciamento dos dados coletados: É a central de controle, que fornece o armazenamento, gerenciamento e processamento dos dados coletados.

Em termos de infraestrutura, as *smart grids* podem ser divididas da seguinte maneira (NIYATO; WANG, 2012):

- Sistema de gerenciamento de energia de residências: Monitora e controla diferentes dispositivos elétricos usando vários tipos de tecnologias de comunicação. São capazes de monitorar e controlar de maneira eficiente e em tempo-real;
- Sistema de medição de grandes áreas: Monitora e controla simultaneamente várias medidas fornecidas pelos medidores inteligentes (tensão, fase, corrente, frequência, potência, etc.) para oferecer proteção e ser tolerante a falhas;
- Infraestrutura de medição avançada (AMI - *Advanced Metering Infrastructure*): É um componente-chave na arquitetura de comunicação de dados entre os medidores inteligentes e a central de controle. É responsável ainda por transferir dados medidos em tempo real para a central de controle;

- Rede de atuadores e sensores: Monitora e controla as características operacionais das redes, em caso de falta de energia e distúrbios. Podem ser usados em transformadores, subestações e em residências.

Em termos de comunicação de dados, podem ser caracterizados por três tipos distintos (NIYATO; WANG, 2012):

- Rede residencial (HAN - *Home Area Network*): Onde pode ser utilizada a transmissão sem fio de curto alcance (Zigbee, por exemplo). Podem ser transmitidos, por exemplo, o consumo médio e máximo dos dispositivos elétricos para os medidores inteligentes;
- Rede incluindo a vizinhança (NAN - *Neighborhood Area Network*): Engloba as múltiplas redes residenciais (HAN). Podem ser interligadas por redes WiFi;
- WAN (*Wide Area Network*): Usado para a conexão de todos os sistemas de gerenciamento de longa distância (central de controle, AMI, etc.). Geralmente utilizam redes 3G, satélites,WiMax e fibras ópticas.

A Figura 1, adaptada de (NIYATO; WANG, 2012), apresenta uma *smart grid*, onde se observa o envio e recebimento das informações periódicas, voltadas aos consumidores finais (serviços A1 e A2), e os serviços de gerenciamento e controle, correspondentes aos serviços B1 e B2, voltados para os elementos de geração, transmissão, distribuição e consumo de energia. Também mostra a disposição das redes de dados HAN, NAN e WAN. As informações de status e comandos para operação da rede devem ser enviados pelos elementos que compõem a geração, transmissão e distribuição de energia. As comunicações desses elementos, em geral, são feitas através de fibras ópticas. A transmissão de dados dos consumidores finais pode ser feita via comunicação PLC ou sem fio, de curto ou longo alcance. Todos os elementos que compõem essa rede formam a infraestrutura AMI. Pelas características da rede, este trabalho pode ser enquadrado aonde existir comunicação de múltiplo acesso, seja na transmissão NAN ou na WAN, pois os elementos intermediários podem recebem dados provenientes de várias entradas, combinar essas informações e transmitir à central de controle, utilizando o esquema de codificação de rede.

No Brasil, o sistema elétrico é muito peculiar e diferente de outras partes do mundo. A matriz energética atinge níveis continentais e é formada em grande parte por energias renováveis, como as hidroelétricas. Logicamente, busca-se eficiência operacional, novas fontes de energia, menor emissão de carbono, tarifas mais ajustadas e maior participação do consumidor final (CPQD, 2013). Aplicações reais vêm sendo implantadas em algumas

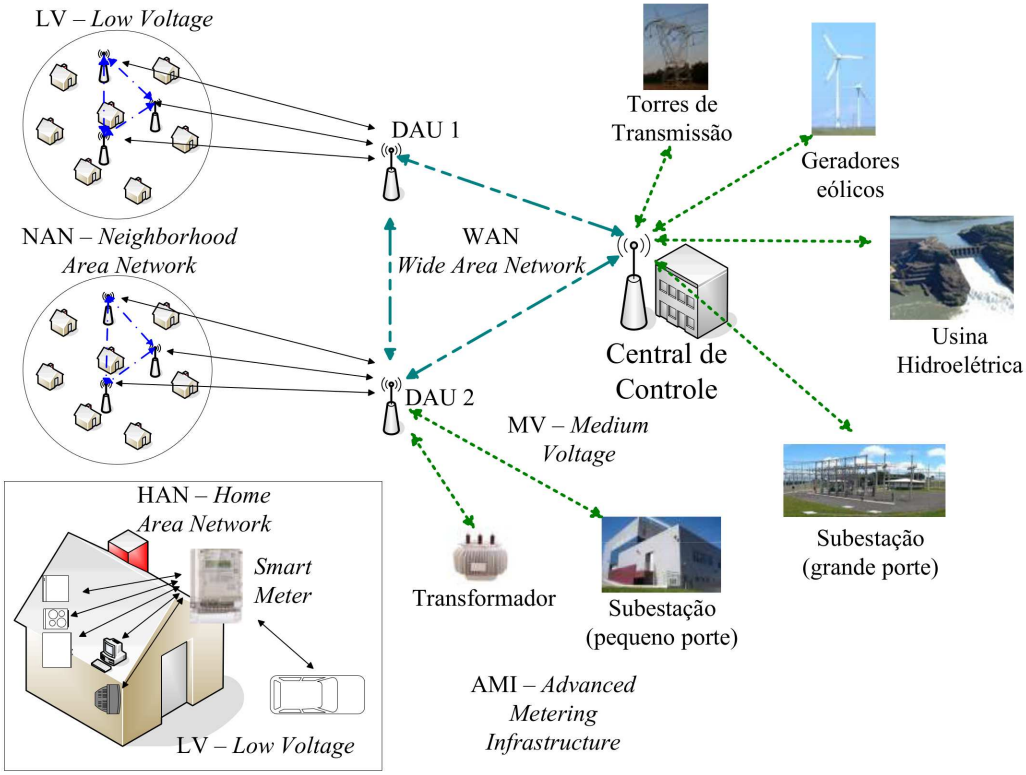


Figura 1: Exemplo de uma *smart grid*.

localidades, como por exemplo na cidade de São Paulo. O sistema adotado é o SIM (Sistema Inteligente de Medição) da empresa Nansen, utilizando sistemas de comunicação sem fio GPRS e RF-*Mesh* (DIGITAL, 2012). Outro projeto, chamado de InovCity, ocorre na cidade de Aparecida, no estado de São Paulo, da empresa EDP, com 13850 medidores inteligentes instalados, cujo foco principal está voltado para a eficiência operacional na coleta de medição de consumo de energia (MARTINS, 2013).

Nos Estados Unidos foram mais de 45 milhões de medidores inteligentes instalados pelo país. Um dos casos de sucesso é o da NV *Energy* (Companhia de Energia do Estado de Nevada, nos Estados Unidos), que está trabalhando em *smart grids* em grandes construções. Até 2015, a perspectiva é economizar 75 MW através desse programa (EASTON, 2013). Em 2011, foram instalados 20 mil termostatos sem fio, que analisam o uso da energia e que possuem controladores de carga que emitem alertas para a redução do consumo de energia em horários de pico de demanda. O sistema pode ainda desligar automaticamente aparelhos de ar-condicionado e outros dispositivos. Esses termostatos funcionam com a tecnologia Zigbee (voltados para as construções) e WiFi (voltados para a central de controle) (CASTLE, 2011).

3 FUNDAMENTAÇÃO TEÓRICA

3.1 MODELO DO SISTEMA

Neste trabalho será considerado a parte de múltiplo acesso de uma rede sem fio, em que duas fontes de informação (referidas como nó 1 e nó 2) possuem informações independentes para transmitir para um destino em comum D. Considera-se também a presença de um nó malicioso passivo (*eavesdropper*) tão próximo ao nó destino D que pode ser considerado sobreposto (com o intuito de facilitar as análises), cujo objetivo é interceptar as mesmas mensagens que são transmitidas para D. Apenas esse posicionamento foi considerado para o *eavesdropper* porque em *smart grids* os outros elementos estão espalhados geograficamente, mas todos devem enviar suas informações para uma central de controle. Em qualquer outro posicionamento o *eavesdropper* estaria limitado a interceptar apenas informações de alguns elementos formadores da rede. Tal modelo está ilustrado na Figura 2, e fornece uma das situações de transmissão que pode ocorrer em *smart grids* para os nós legítimos, onde dois dispositivos elétricos têm informações independentes para transmitir à central de controle.

Considerando $i, j \in \{1, 2, D, e\}$ em referência ao nó 1, nó 2, nó destino D e o nó *eavesdropper e*, para $i \neq j$, e x_{ij} sendo o sinal transmitido pela fonte, que segue uma distribuição Gaussiana com média nula e variância unitária, o sinal recebido por qualquer nó j, y_{ij}, pode ser representado por:

$$y_{ij} = \sqrt{P_i d_{ij}^{-m}} h_{ij} x_{ij} + n_{ij}, \tag{1}$$

onde h_{ij} representa o coeficiente de desvanecimento do canal entre os nós i e j, assumindo possuir distribuição Rayleigh, com média nula e variância unitária, considerando desvanecimento em bloco, P_i é a potência de transmissão do nó i, m é o coeficiente de perda de percurso, n_{ij} representa o ruído aditivo branco e Gaussiano (AWGN) e d_{ij} é a distância entre os nós i e j, a qual, para facilitar a análise, foi considerada como sendo igual a 1 para todos os enlaces da rede, isto é, $d_{ij} = d = 1, \forall i, j$.

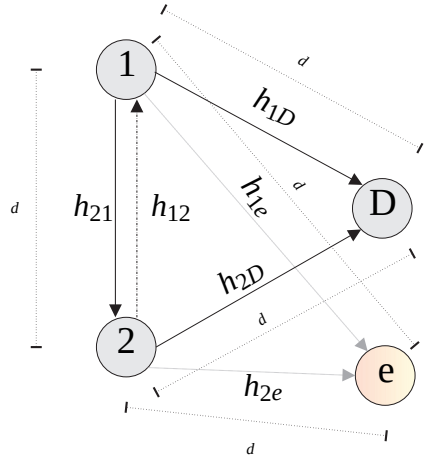


Figura 2: Modelo do sistema, com dois nós transmissores 1 e 2 que possuem informações independentes para um nó destino *D*, na presença de um nó *eavesdropper e* sobreposto ao nó destino *D*.

A SNR instantânea, γ_{ij}, é definida por:

$$\gamma_{ij} = \overline{\gamma}_{ij}|h_{ij}|^2, \tag{2}$$

em que $\overline{\gamma}_{ij} = \frac{P_i}{\sigma_{ij}^2}$ é a SNR média do canal entre os nós *i* e *j*, e σ_{ij}^2 representa a variância do ruído Gaussiano. Neste trabalho, embora a análise seja feita em função da posição do *eavesdropper*, em que foi considerado posicionado sobreposto ao nó destino *D*, com o conhecimento apenas da sua SNR média e sem nenhuma informação da SNR instantânea, na prática, nem a sua localização é conhecida, já que o atacante passivo geralmente não emite nenhum sinal e trabalha em modo de recepção.

Como as distâncias entre os nós são iguais e unitárias, a SNR média, $\overline{\gamma}_{ij}$, é igual para todos os casos, ou seja, $\overline{\gamma}_{1D} = \overline{\gamma}_{2D} = \overline{\gamma}_D$. O mesmo ocorre para o *eavesdropper*, onde $\overline{\gamma}_{1e} = \overline{\gamma}_{2e} = \overline{\gamma}_e$. Uma vez que *h* é assumido possuir distribuição Rayleigh, $|h_{ij}|^2$ possui distribuição exponencial (GOLDSMITH, 2005).

Assume-se também que todos os nós da rede operam no regime *half-duplex*, ou seja, não podem transmitir e receber informações ao mesmo tempo. Também considera-se que as transmissões são ortogonais no domínio do tempo.

Sem considerar as restrições de sigilo, uma *outage* entre dois nós *i* e *j* ocorre quando a informação mútua $I_{ij} = \log_2(1+\gamma_{ij})$, for menor que uma taxa alvo *R* bpcu (*bits per channel use*). A probabilidade desse evento ocorrer é chamada de probabilidade de *outage*, representada

por $\mathscr{P}_{o,ij}$, e é calculada da seguinte maneira:

$$\begin{aligned}\mathscr{P}_{o,ij} &= \Pr\{I_{ij} < R\} \\ &= \Pr\{\log_2(1+\gamma_{ij}) < R\} \\ &= \Pr\{\gamma_{ij} < 2^R - 1\} \\ &= 1 - \exp\left(-\frac{2^R-1}{\overline{\gamma}_{ij}}\right).\end{aligned} \tag{3}$$

3.2 SIGILO (*SECRECY*)

Nesta seção serão definidos os conceitos que envolvem a *Secrecy*, ou o Sigilo, incluindo a capacidade de sigilo, a probabilidade de existência da capacidade de sigilo e a probabilidade de *outage* com restrições de sigilo.

Porém, antes de entrar nessas definições, é importante conhecer os conceitos que envolvem o sigilo propriamente dito. O conceito de nível de sigilo surgiu do trabalho de Shannon para comunicação segura (SHANNON, 1949). A partir desta análise, Wyner criou um modelo denominado *Wire-Tap Channel* (WTC), e deu continuidade aos estudos, na qual considerou que a comunicação do transmissor e do receptor legítimo era livre de ruído, e o *eavesdropper* podia receber uma versão degradada do sinal transmitido (WYNER, 1975). Considerando $\mathscr{M}$ o conjunto de mensagens enviadas pelo transmissor, $\mathscr{X}$ o conjunto de palavras-código obtidas após a codificação com a utilização de uma chave secreta e $\mathscr{K}$ o conjunto de chaves secretas utilizadas para codificar as mensagens, para prevenir que o *eavesdropper* obtivesse a informação, as mensagens $M \in \mathscr{M}$ eram codificadas em palavras-código $X \in \mathscr{X}$, com a utilização de uma chave secreta $K \in \mathscr{K}$, que apenas os nós legítimos conheciam. A codificação era feita por uma função de codificação c (*encoding*) e a decodificação por uma função d (*decoding*), dado que $M = d(X,K)$ se $X = c(M,K)$. No modelo de Shannon, o *eavesdropper* conhecia as funções de codificação $c(M,K)$ e de decodificação $d(X,K)$, mas não tinha nenhuma informação sobre a chave secreta K. Nos termos da teoria da informação[1], o esquema de codificação é dito ser perfeitamente sigiloso (*perfect secrecy*, ou *Shannon secure*) se:

$$H(M|X) = H(M), \tag{4}$$

ou de maneira equivalente $I(M;X) = 0$.

Em outras palavras, esta equação (4) pode ser interpretada como a equivocação do

[1]Mais informações sobre a teoria da informação, consultar (COVER; TOMAS, 1991)

eavesdropper, em termos de entropia condicional $H(M|X) = H(M)$, ou seja, M e X são mutuamente independentes. Ou seja, a quantidade de informação que o *eavesdropper* é capaz de obter é nula ($I(M;X) = 0$), já que não consegue obter a palavra-código M a partir da palavra-código X "escutada".

Uma rede pode ser classificada ainda como sendo fortemente e fracamente segura (SUBRAMANIAN et al., 2010). Uma rede é dita ser fortemente segura se o tamanho das mensagens transmitidas for suficientemente grande, tal que o *eavesdropper* não consiga obter nenhuma informação a partir das mensagens interceptadas (SUBRAMANIAN et al., 2010). Por outro lado, mesmo que o *eavesdropper* consiga interceptar uma informação transmitida pelo nó fonte, se ele não for capaz de dar significado a essa informação, neste caso, caracteriza uma rede fracamente segura (ZHANG et al., 2010).

3.2.1 CAPACIDADE DE SIGILO (*SECRECY CAPACITY*)

A capacidade de sigilo é uma medida de desempenho e significa a máxima taxa de transmissão em que o *eavesdropper* não é capaz de decodificar nenhuma informação (BARROS; RODRIGUES, 2006). Ou seja, é igual a diferença entre as informações mútuas recebidas pelo nó legítimo e pelo *eavesdropper*.

Nos termos da teoria da informação, considerando que X representa as palavras-código enviadas pelo transmissor, Y a versão recebida pelo receptor legítimo e Y_e a versão recebida pelo *eavesdropper*, a capacidade de sigilo, C_s, pode ser escrita da seguinte maneira (LAI; GAMAL, 2008):

$$\begin{aligned} C_s &= \max I(X;Y|Y_e) \\ &= \max(I(X;Y) - I(X;Y_e)). \end{aligned} \tag{5}$$

Essa capacidade de sigilo pode ser escrita em função das nomenclaturas do modelo do sistema proposto neste trabalho, ou seja:

$$C_s = |I_{1D} - I_{1e}|^+, \tag{6}$$

onde I_{1D} representa a informação mútua recebida pelo nó destino D que foi enviado pelo nó 1, e I_{1e} é a informação mútua que o *eavesdropper* conseguiu interceptar e decodificar desta transmissão do nó 1. O símbolo $+$, positivo, significa que o valor de C_s nunca será negativo, pois a informação mútua I_{1e} nunca será maior que I_{1D}, ou seja, o *eavesdropper* nunca conseguirá interceptar mais informações do que foi transmitido pelo nó legítimo 1.

Uma comunicação segura só ocorre se a SNR instantânea do canal entre os nós legítimos 1 e *D*, γ_{1D}, for maior que a SNR instantânea do canal entre o nó 1 e o *eavesdropper*, representado por γ_{1e}.

Outra medida de desempenho é a probabilidade de existência da capacidade de sigilo. Para a transmissão direta, essa probabilidade é dada por (BARROS; RODRIGUES, 2006):

$$\begin{aligned} \Pr\{C_{s,DT} > 0\} &= \Pr(\gamma_{1D} > \gamma_{1e}) \\ &= \int_0^\infty \int_0^{\gamma_{1D}} p(\gamma_{1D}) p(\gamma_{1e}) d\gamma_{1e} d\gamma_{1D} \\ &= \frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D} + \overline{\gamma}_{1e}}, \end{aligned} \tag{7}$$

onde $p(.)$ é a função densidade de probabilidade (pdf).

Como a capacidade de sigilo, em (6), depende da informação mútua do nó 1 com o destino (I_{1D}) e da informação mútua do nó 1 com o *eavesdropper* (I_{1e}), então, a capacidade de sigilo existirá se $\gamma_{1D} > \gamma_{1e}$, ou seja, se a SNR instantânea do canal entre os nós legítimos 1 e *D* for maior que a SNR instantânea do canal do nó 1 com o *eavesdropper e*. Devido ao desvanecimento, a capacidade de sigilo pode existir mesmo quando a SNR média do canal entre os nós 1 e *D*, $\overline{\gamma}_{1D}$, for menor que a SNR média do canal entre o nó 1 e o *eavesdropper*, $\overline{\gamma}_{1e}$, embora com menor probabilidade de ocorrência.

Foi mostrado em (BARROS; RODRIGUES, 2006) que para obter uma capacidade de sigilo com probabilidade de existência não-nula é preciso que $\overline{\gamma}_{1D} > \overline{\gamma}_{1e}$ para $\Pr\{C_s > 0\} > 0,5$. Porém é possível ter $\overline{\gamma}_{1D} < \overline{\gamma}_{1e}$ para $\Pr\{C_s > 0\} < 0,5$. Essa informação é válida para a transmissão direta. Isso mostra que é possível ter uma comunicação segura mesmo quando o *eavesdropper* possui SNR média mais elevada em relação aos nós legítimos, embora com uma probabilidade de existência menor. Para $\overline{\gamma}_{1D} = \overline{\gamma}_{1e}$, a probabilidade de existência é igual a 0,5.

3.2.2 PROBABILIDADE DE *OUTAGE* COM RESTRIÇÕES DE SIGILO

O conceito que envolve a probabilidade de *outage* com restrições de sigilo (do inglês *secrecy outage probability*) foi introduzido do trabalho de (BLOCH et al., 2008) em uma rede com desvanecimento Rayleigh quase-estático, e é bastante semelhante à probabilidade de *outage* sem restrições de sigilo. Um evento de *outage* sem restrições de sigilo ocorre quando a informação mútua instantânea I_{ij} do canal é inferior a uma determinada taxa alvo *R*, conforme mostrado em (3).

De maneira semelhante, a probabilidade de *outage* com restrições de sigilo, $\mathscr{P}_{so}$, pode ser definida como a probabilidade de que a capacidade de sigilo instantânea C_s seja menor que uma taxa de sigilo alvo R_s (LAI; GAMAL, 2008; BLOCH et al., 2008; GABRY, 2012). Matematicamente, é definida por:

$$\mathscr{P}_{so} = \Pr\{C_s < R_s\}. \tag{8}$$

O uso da probabilidade de *outage* com restrições de sigilo como métrica de desempenho é interessante, já que nem sempre se tem conhecimento da SNR instantânea do canal com o *eavesdropper*, e consequentemente pode não ser possível calcular a capacidade de sigilo instantânea. Também não há outra opção, a não ser fixar uma taxa de sigilo alvo R_s para o cálculo desta probabilidade (BLOCH et al., 2008). Devido a esses fatores, surgiu o interesse de trabalhar com dados probabilísticos, desde que se saiba a distribuição da SNR instantânea dos nós legítimos com o *eavesdropper*.

A definição da probabilidade de *outage* com restrições de sigilo leva a duas possibilidades de ocorrência de uma *outage*: *i*) A mensagem não é recuperada por ambos os nós *D* e *e*; *ii*) A mensagem é corretamente recuperada por *e*, independente do que ocorrer com *D*.

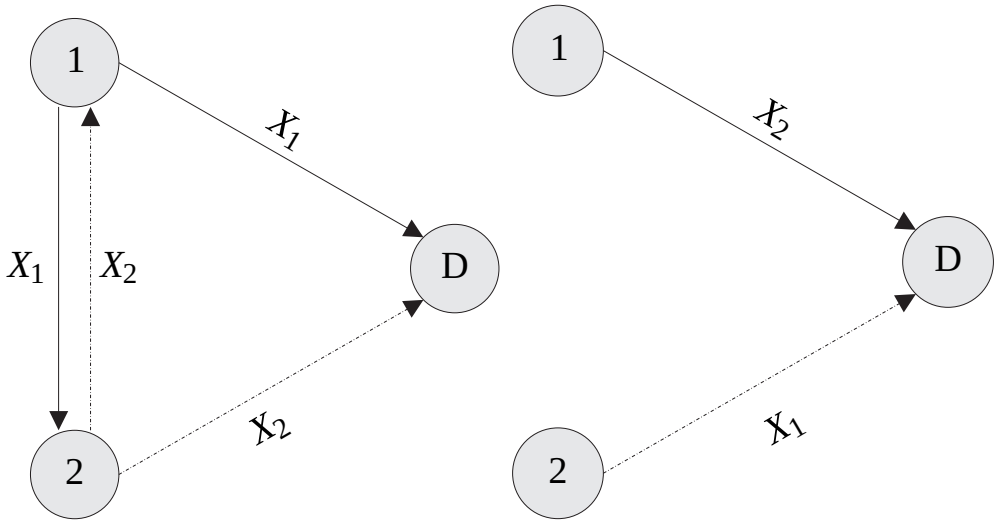
Logo, a probabilidade de *outage* com restrições de sigilo para a transmissão direta é dada por (BARROS; RODRIGUES, 2006):

$$\begin{aligned}\mathscr{P}_{so,\mathrm{DT}} &= \Pr\{C_{s,DT} < R_s\} \\ &= \int_0^{\infty}\int_0^{\gamma_U} p(\gamma_{1D})p(\gamma_{1e})d\gamma_{1e}d\gamma_{1D} \\ &= 1 - \frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D} + 2^{R_s}\overline{\gamma}_{1e}} \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_{1D}}\right),\end{aligned} \tag{9}$$

onde $\gamma_U = 2^{R_s}(1+\gamma_{1e}) - 1$.

3.3 COMUNICAÇÃO COOPERATIVA

A comunicação cooperativa, que inicialmente foi proposta para aumentar a confiabilidade da rede (em termos de diminuição de taxa de erros) (LANEMAN et al., 2004; NOSRATINIA et al., 2004), também pode ser útil para aumentar o sigilo das informações (LAI; GAMAL, 2008; GABRY, 2012). Em uma rede dessa natureza, além de transmitir suas próprias mensagens, os nós auxiliam uns aos outros retransmitindo as mensagens de seus parceiros. Uma



(a) Fase de Difusão (b) Fase de Cooperação

Figura 3: Esquema de comunicação cooperativa, formado pelas fases de (a) difusão e (b) cooperação.

vez que a mesma mensagem é transmitida por caminhos distintos (sujeitos a desvanecimentos independentes), o efeito de múltiplas antenas distribuídas é obtido, resultando em um aumento na ordem de diversidade do sistema e consequentemente na sua confiabilidade (LANEMAN et al., 2004; NOSRATINIA et al., 2004). Com esse auxílio dos outros nós nas transmissões, surgiu o conceito de nó *relay*, do trabalho de Van der Meulen em (MEULEN, 1971). Os nós *relays* são os responsáveis pelo reencaminhamento dos pacotes recebidos do transmissor para o destino. Isto só é possível devido à natureza difusora da comunicação sem fio, já que a transmissão ocorre em todas as direções, ou seja, para o nó de destino e para o nó *relay*, que pode decodificar e retransmitir o mesmo sinal recebido, conforme mostrado na Figura 3. A comunicação cooperativa ocorre em duas fases. Na primeira fase, chamada de difusão ou *broadcast*, ilustrada na Figura 3(a), os nós 1 e 2 irradiam as próprias informações X_1 e X_2, respectivamente. Na segunda fase, ou fase de cooperação, ilustrada na Figura 3(b), os nós irradiam as informações que foram obtidas dos outros nós.

Os protocolos de comunicação cooperativa de maior destaque são o “amplifica-e-encaminha” (AF) e o “decodifica-e-encaminha” (DF), adotado em (LANEMAN et al., 2004; NOSRATINIA et al., 2004; GUNDUZ; ERKIP, 2007), dentre outros.

Esses conceitos de comunicação cooperativa podem ser estendidos para as *smart grids*, como citado em (AHMED et al., 2012; NIYATO; WANG, 2012). Em (AHMED et al., 2012), os autores descreveram a cooperação como uma maneira de aumentar a diversidade e o *throughput* da rede. Já em (NIYATO; WANG, 2012), os autores relacionaram a probabilidade de perda de pacotes em função da utilização dos nós *relays* e também em relação à composição dos custos da energia, quanto mais forem utilizados os nós *relays*. Em (GABRY, 2012), o autor mostrou

que a cooperação também pode ser muito útil quando são envolvidos os conceitos de sigilo, já que obteve um aumento da capacidade de sigilo para o esquema DF e uma menor probabilidade de *outage*, quando comparada com a transmissão direta, e também concluiu que o esquema DF obteve um melhor desempenho para a probabilidade de *outage* com restrições de sigilo do que o esquema AF, em um cenário semelhante ao apresentado na Figura 2, em que a rede legítima está sujeita à presença de um *eavesdropper*. Porém em (GABRY, 2012), o autor não considerou a ocorrência de *outage* entre os nós legítimos 1 e 2.

A informação mútua do esquema DF deve levar em consideração a ocorrência de *outage* no enlace entre os nós legítimos 1 e 2. Vale lembrar que uma *outage* ocorre quando a informação mútua I_{12} for menor que uma taxa alvo R. I_{12} é dada por:

$$I_{12} = \frac{1}{2}\log_2(1+\gamma_{12}), \tag{10}$$

onde o termo $\frac{1}{2}$ é devido à perda de multiplexação, ou seja, a transmissão entre os nós legítimos ocorre apenas durante metade do *time-slot* (durante a fase de difusão). A outra metade do *time-slot* é utilizada na fase de cooperação.

Consequentemente, a probabilidade de *outage* no enlace entre os nós 1 e 2, $\mathscr{P}_{o,12}$ é dada por:

$$\begin{aligned}
\mathscr{P}_{o,12} &= \Pr\{I_{12} < R\} \\
&= \Pr\left\{\frac{1}{2}\log_2(1+\gamma_{12}) < R\right\} \\
&= \Pr\{\gamma_{12} < 2R-1\} \\
&= 1 - \exp\left(-\frac{2^{2R}-1}{\overline{\gamma}_{12}}\right),
\end{aligned} \tag{11}$$

onde R é a taxa alvo. Neste trabalho, considerou-se o caso particular em que $R = R_s$.

Para calcular a informação mútua recebida pelo nó destino D, devem ser seguidos alguns passos, conforme descrito a seguir.

Se ocorrer *outage* no enlace entre os nós 1 e 2, então é considerada a transmissão direta do nó 1 ao nó destino D multiplicada por $\frac{1}{2}$. A informação mútua, representada por I_{DF_a} nessa etapa é dada por:

$$I_{\mathrm{DF}_a} = \frac{1}{2}\log_2(1+\gamma_{1\mathrm{D}}). \tag{12}$$

Se não ocorrer *outage* no enlace entre os nós 1 e 2, e assumindo que o destino faz MRC (*Maximal Ratio Combining*, ou combinação por máxima verossimilhança) após receber as duas

cópias do mesmo sinal (GOLDSMITH, 2005), a informação mútua I_{DF_b}, é dada por:

$$I_{\mathrm{DF}_b} = \frac{1}{2}\log_2(1+\gamma_{1D}+\gamma_{2D}). \tag{13}$$

A informação mútua vista pelo *eavesdropper*, $I_{\mathrm{DF,e}}$, é obtida de forma semelhante, também condicionada à ocorrência ou não de *outage* no enlace entre os nós 1 e 2, ao se substituir o índice D pelo índice e em (12)-(13).

Tendo a informação mútua dos nós legítimos e a informação mútua obtida pelo *eavesdropper*, é possível calcular a probabilidade de existência da capacidade de sigilo ($\Pr\{C_s > 0\}$) e a probabilidade de *outage* com restrições de sigilo ($\Pr\{C_s < R_s\}$).

Seguindo a análise de existência da capacidade de sigilo, conforme explicado em (BARROS; RODRIGUES, 2006), e levando-se em consideração que possa ou não ocorrer *outage* no enlace entre os nós 1 e 2, tem-se que:

$$\begin{aligned}
\Pr\{C_{s,\mathrm{DF}} > 0\} &= (|I_{\mathrm{DF}} - I_{\mathrm{DF,e}}|^+ > 0) \\
&= \left(|I_{\mathrm{DF}_a} - I_{\mathrm{DF},e_a}|^+ > 0\right)\mathscr{P}_{o,12} + \left(|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}|^+ > 0\right)(1-\mathscr{P}_{o,12}) \\
&= \left(\frac{1}{2}\left[\log_2(1+\gamma_{1D}) - \log_2(1+\gamma_{1e})\right] > 0\right)\mathscr{P}_{o,12} + \\
&\left(\frac{1}{2}\left[\log_2(1+\gamma_{1D}+\gamma_{2D}) - \log_2(1+\gamma_{1e}+\gamma_{2e})\right] > 0\right)(1-\mathscr{P}_{o,12}) \\
&\approx \left(\frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D}+\overline{\gamma}_{1e}}\right)\left[1-\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right] + \\
&\left[\frac{3\kappa_e+1}{(\kappa_e+1)^3}\right]\left[\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right],
\end{aligned} \tag{14}$$

onde $\kappa_e = \frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}$. A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$ e $\overline{\gamma}_{1e}$.

Demonstração. Apresentada no Apêndice A.1. □

A probabilidade de *outage* com restrições de sigilo segue o mesmo raciocínio, só que neste caso, tem-se um valor de taxa de sigilo alvo R_s. Uma *outage* ocorrerá se a capacidade de sigilo C_s for menor que este valor de R_s. Separa-se em duas partes, levando-se em consideração a ocorrência ou não de *outage* no enlace entre os nós 1 e 2:

$$\begin{aligned}
\mathscr{P}_{so,\mathrm{DF}}(R_s) &= \Pr(|I_{\mathrm{DF}} - I_{\mathrm{DF,e}}|^+ < R_s) \\
&= \Pr\left(|I_{\mathrm{DF}_a} - I_{\mathrm{DF},e_a}| < R_\mathrm{s}\right)\mathscr{P}_{\mathrm{o},12} + \\
&\Pr\left(|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}| < R_\mathrm{s}\right)(1-\mathscr{P}_{\mathrm{o},12}).
\end{aligned} \tag{15}$$

A probabilidade de *outage* com restrições de sigilo para o esquema DF é dada por:

$$\mathscr{P}_{so,\mathrm{DF}}(R_s) \approx \left[1 - \frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D} + 2^{2R_s}\overline{\gamma}_{1e}} \exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}\right)\right]\left[1 - \exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right] + \left[\frac{-3\kappa_e 2^{2R_s}-1}{\left(\kappa_e 2^{2R_s}+1\right)^3} + 1\right]\left[\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right]. \tag{16}$$

A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$ e $\overline{\gamma}_{1e}$.

Demonstração. Apresentada no Apêndice A.2. □

3.4 CODIFICAÇÃO DE REDE

Em (AHLSWEDE et al., 2000), os autores propuseram uma nova maneira para a disseminação de dados em redes de comunicação: os nós, que tradicionalmente atuavam como roteadores (apenas retransmitiam informações da maneira como eram recebidas), numa rede cabeada e *multicast*, seriam capazes de retransmitir combinações lineares de diversas mensagens distintas. Com a utilização dessa técnica, denominada codificação de rede, foi mostrado em (AHLSWEDE et al., 2000) que o *throughput* da rede pode ser aumentado. Posteriormente, mostrou-se também que a técnica de codificação de rede, quando aplicada a redes cooperativas, pode prover ganhos em termos de confiabilidade (XIAO et al., 2007) e ordem de diversidade (XIAO; SKOGLUND, 2010; REBELATTO et al., 2010, 2012).

Conforme explicado em (BLOCH; BARROS, 2011), os nós intermediários passaram a "misturar" fluxos de diferentes origens utilizando combinações algébricas. A maneira mais simples de codificação de rede é utilizar as operações de XOR (*Exclusive-OR*, Ou-exclusivo), que podem inclusive ser estendidas para mais nós da rede. Porém, as aplicações mais sofisticadas realizam tais combinações lineares sobre um campo finito não-binário GF(q) (Campo de Galois), onde $q = 2^m$, para m inteiro.

A Figura 4 mostra um exemplo típico em que a técnica de codificação de rede pode apresentar benefícios, denominado "*two-way relay channel*", ou canal com nó *relay* bi-direcional. Neste exemplo, a rede é formada por um nó intermediário S e dois nós A e B que tem informações independentes para transmitir e para receber. É feita uma operação simples de XOR entre os bits a e b no nó intermediário S, que encaminha a mensagem combinada. Como o nó A conhece o bit a, então é possível recuperar o bit b. Da mesma maneira, o nó B conhece o bit b e pode identificar o bit a. Outro ponto interessante que também é mostrado na Figura 4 é que, neste caso, há uma transmissão a menos feita pelo nó S, já que é enviada a mesma informação $a \oplus b$ em apenas uma transmissão, aproveitando-se da natureza difusora das redes sem fio, o

que já demonstra um dos benefícios que pode ser obtido da codificação de rede.

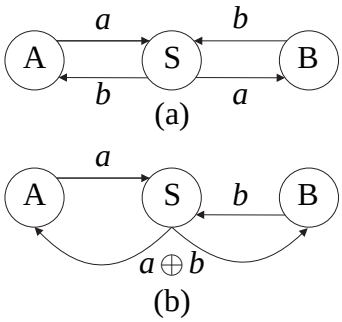


Figura 4: Exemplo clássico de codificação de rede. Em (a) a transmissão ocorre sem codificação de rede. Em (b) tem-se a codificação de rede, com o envio de $a \oplus b$.

A codificação de rede pode ajudar na segurança já que o *eavesdropper* terá que interceptar as informações de diversos enlaces para descobrir a codificação de rede na camada física (FRAGOULI; SOLJANIN, 2007a). A Figura 5, obtida de (FRAGOULI; SOLJANIN, 2007a), mostra como a segurança é obtida pela codificação de rede. O nó A tem informações para enviar ao destino D. Sem codificação de rede, o nó A envia as informações x_1 e x_2 pelos nós intermediários B e C, respectivamente. Se o *eavesdropper* conseguir "escutar" qualquer um dos enlaces, ele facilmente descobrirá as informações. Por outro lado, se o nó A combinar as informações x_1 e x_2 e enviar para os nós B e C combinações diferentes, além de prover redundância das informações, trará dificuldades para o atacante passivo, já que ele precisará interceptar várias informações para tentar identificar os coeficientes usados na codificação da rede para obter alguma informação relevante. Neste exemplo, o nó A envia $x_1 + x_2$ para o nó B, e $x_1 + 2x_2$ para o nó C, antes da informação chegar em D.

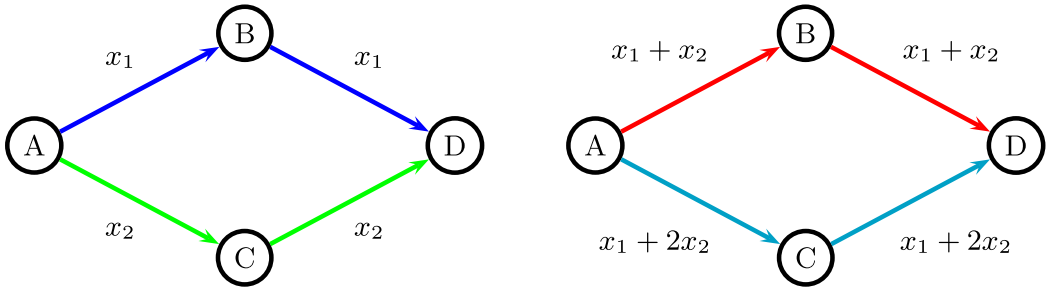


Figura 5: Codificação de rede simples, que proporciona segurança na camada física, com a rede, neste exemplo, formada por 4 nós, com o nó A realizando a codificação de rede e enviando a combinação $x_1 + x_2$ para o nó B e $x_1 + 2x_2$ para o nó C, antes de chegar ao destino D.

Se as combinações lineares forem realizadas sobre um campo finito suficientemente grande, foi mostrado em (XIAO; SKOGLUND, 2010) que o ganho em termos de diversidade são superiores aos encontrados no esquema de cooperação DF.

Outro protocolo que é bastante utilizado em redes sem fio é a RLNC (*Random Linear Network Coding*) (ZHANG et al., 2010), codificação de rede linear e aleatória, usada em redes bastante grandes e muito dinâmicas, com nós entrando e saindo da rede a todo momento, o que não faz parte do escopo deste trabalho.

4 ANÁLISE DA CODIFICAÇÃO DE REDE EM *SMART GRIDS*

Conforme explicado em (PHULPIN et al., 2011), a codificação de rede se adapta perfeitamente às necessidades das *smart grids*. Como a rede é integrada, pode-se aproveitar da natureza difusora da comunicação sem fio, pois os sinais enviados por uma estação-base podem ser escutados por outras estações-base. Consequentemente, os nós podem operar de maneira oportunística e armazenar todos os pacotes, mesmo que não sejam destinados a ele. Esse comportamento aumenta a robustez e a flexibilidade da rede pois:

- Como cada estação-base transmite um pacote na rede de acordo com os envios periódicos, explicados anteriormente no Capítulo 2, pode-se aproveitar quando a qualidade do canal esteja acima de um limiar (evitando a *outage*);
- Cada nó pode escutar o meio e armazenar as combinações lineares dos pacotes recebidos de outras estações-base;
- As estações-base podem compartilhar as combinações lineares armazenadas provenientes de outros nós, utilizando a difusão;
- Após receber uma requisição de uma estação-base, um nó pode enviar pacotes com as combinações lineares e os coeficientes para a estação-base e/ou para a central de controle, que será capaz de recuperar os dados.

A segurança proporcionada pela codificação de rede difere dos outros protocolos já que os pacotes são misturados ao longo da rede através de operações algébricas.

Vale destacar que segurança é um dos pontos fundamentais e mais críticos nesse tipo de rede. Erros em um simples pacote, provocado por um atacante ativo de qualquer natureza, pode propagar uma sequência de pacotes com erros, o que pode dificultar a decodificação do pacote no destino. Para tentar minimizar os efeitos de ataques ativos, são descritas duas maneiras diferentes (PHULPIN et al., 2011):

- Os nós legítimos podem introduzir bits de redundância no fluxo de informação para reduzir os estragos provocados por um atacante;
- Poderiam utilizar funções *hash* para detectar pacotes modificados. Neste caso, os nós legítimos conseguiriam identificar de onde vem estes pacotes e poderiam isolar os nós maliciosos.

Para o caso de ataques passivos, que faz parte do escopo deste trabalho, foi utilizada a codificação de rede para aumentar a segurança na camada física. Porém, para que os protocolos de segurança funcionem adequadamente, principalmente os de codificação de rede, deseja-se um conjunto de regras que devem ser atendidos pelos nós participantes (BLOCH; BARROS, 2011):

- Os nós precisam codificar corretamente os pacotes;
- Os nós intermediários precisam encaminhar corretamente os pacotes codificados;
- Se for seguir os critérios de confidencialidade, os nós participantes devem ignorar os dados que não são destinados a eles. Porém, como se busca aumentar a robustez da rede, é preferível que os nós armazenem os dados que são destinados a outros nós, já que estes podem ser recombinados e retransmitidos em caso de falhas na rede.

Os ataques passivos podem ser classificados em três mais comuns (BLOCH; BARROS, 2011): “nós bons mas curiosos”, “atacantes com acesso a alguns enlaces” (*Dumb*) e o “pior caso de *eavesdropper*” que tem acesso a todos os enlaces da rede:

- “Nós bons mas curiosos”: este tipo de nó apresenta comportamento adequado, mas tenta adquirir tantas informações quantas forem possíveis de acordo com o fluxo de pacotes. Como os níveis de segurança dependem do tamanho dos blocos de pacotes e da topologia da rede, poderiam ser adotados critérios de segurança algébricos, por exemplo, protegendo partes dos pacotes, o que aumenta a complexidade na decodificação;
- “Atacantes com acesso a alguns enlaces” (*Dumb*): a dificuldade, neste caso, é encontrar códigos capazes de serem transmitidos a diferentes enlaces, que dificultem ou impossibilitem a reconstrução pelo *eavesdropper*, dos bits que trafegam na rede, e desde que o *eavesdropper* não tenha acesso a todos os enlaces da rede;
- O pior caso é quando o *eavesdropper* tem acesso a todos os pacotes que são transmitidos na rede. Como ele escuta todos os enlaces, ele pode conseguir descobrir a codificação de rede utilizada e obter algum tipo de informação relevante.

Neste trabalho, foram considerados apenas os dois últimos tipos de atacantes passivos. O primeiro deles, chamado de *Dumb*, não é capaz de identificar os coeficientes da codificação de rede, e o segundo, o atacante passivo que tem acesso às informações de todos os enlaces e conhece os coeficientes usados na codificação de rede do sistema.

4.1 CODIFICAÇÃO DE REDE DINÂMICA (DNC)

Neste trabalho, foi considerada a codificação de rede DNC (*Dynamic Network Coding*), similar ao descrito em (XIAO; SKOGLUND, 2010), onde os autores comprovaram a existência de códigos determinísticos para redes dinâmicas com ordem de diversidade igual $2M-1$, sendo M o número de usuários da rede cooperativa. Entretanto, para atingir essa ordem de diversidade, é necessário que a codificação de rede seja não-binária. Os autores consideraram ainda a possibilidade de ocorrer erros na transmissão entre os usuários. A diferença de análise feita em (XIAO; SKOGLUND, 2010) para este trabalho é a presença de um atacante passivo localizado em sobreposição ao nó destino D.

A taxa alvo R considerada foi igual a $\frac{1}{2}$, ou seja, para cada bit transmitido, transmite-se um bit de redundância.

A Figura 6, de (XIAO; SKOGLUND, 2010), mostra como as mensagens são recebidas e encaminhadas para o nó destino D. É usada uma codificação de rede não-binária, realizada num campo finito de Galois GF(4), já que o tamanho mínimo do alfabeto para a codificação de rede é três. As mensagens trocadas por essa rede cooperativa são X_1, X_2, $X_1 \boxplus X_2$ e $X_1 \boxplus 2X_2$. O símbolo $\boxplus$ representa uma soma binária em um campo finito. Como essas quatro mensagens estão sujeitas a desvanecimentos independentes, se o nó destino conseguir recuperar duas das quatro mensagens, é possível recuperar as mensagens originais X_1 e X_2. Do ponto de vista do nó 1, se a mensagem X_1 não for recuperada na transmissão direta, basta recuperar quaisquer duas mensagens dentre as três enviadas (X_2, $X_1 \boxplus X_2$ e $X_1 \boxplus 2X_2$), ou seja, só ocorrerá erros nessa rede se 3 ou mais mensagens não puderem ser decodificadas corretamente. Caso ocorra *outage* no enlace entre o nó 1 e D ($\gamma_{1D} < \gamma_{th}$, onde γ_{th} representa uma SNR limiar) e não ocorra *outage* entre os nós 1 e 2, ou seja, $\gamma_{12} > \gamma_{th}$, então, a probabilidade de *outage*, para esta situação é representada por (XIAO; SKOGLUND, 2010):

$$\begin{aligned} \Pr\{\gamma_{1D} < \gamma_{th} | \gamma_{12} \geq \gamma_{th}\} &= \mathscr{P}_o \left[\binom{3}{2} \mathscr{P}_o^2 (1-\mathscr{P}_o) + \mathscr{P}_o^3 \right] \\ &\approx 3\mathscr{P}_o^3, \end{aligned} \tag{17}$$

onde $\mathscr{P}_o = 1 - \exp\left(-\frac{2^R-1}{\overline{\gamma}_{1D}}\right)$. O primeiro $\mathscr{P}_o$ da equação corresponde a *outage* ocorrida na

transmissão direta. A combinação $\binom{3}{2}$ representa a combinação das três mensagens restantes combinadas duas a duas, de tal maneira que se ocorrer *outage* em duas mensagens ($\mathscr{P}_o^2$), mesmo que a terceira seja recuperada ($1-\mathscr{P}_o$), não é possível recuperar as mensagens originais X_1 e X_2, ocasionando uma condição de *outage*. O terceiro termo, $\mathscr{P}_o^3$ corresponde a *outage* das três mensagens, além da ocorrida com a transmissão direta.

Caso não ocorra *outage* na transmissão direta ($\gamma_{1D} > \gamma_{th}$) mas ocorra *outage* entre os nós 1 e 2 ($\gamma_{12} < \gamma_{th}$), o nó 1 transmitirá a mesma informação X_1, durante a segunda fase (cooperação). Em outras palavras, o nó destino D recebe duas cópias de X_1, e supondo que faça MRC, a probabilidade de *outage*, para esse caso é igual a (LANEMAN; WORNELL, 2003):

$$\Pr\{\gamma_{1D} < \gamma_{th} | \gamma_{12} < \gamma_{th}\} \approx 0.5\mathscr{P}_o^2, \tag{18}$$

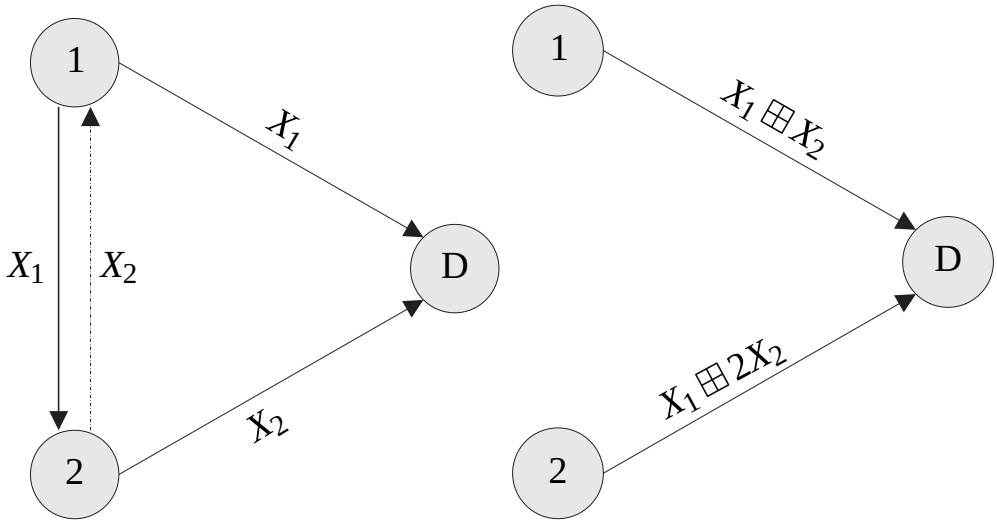
A probabilidade de *outage* da rede DNC é obtida combinando os resultados das equações (17) e (18), que é dada por (XIAO; SKOGLUND, 2010):

$$\begin{aligned}\mathscr{P}_{o,\text{DNC}} &= \Pr\{\gamma_{1D} < \gamma_{th} | \gamma_{12} \geq \gamma_{th}\}(1-\mathscr{P}_o) + \\ &\quad \Pr\{\gamma_{1D} < \gamma_{th} | \gamma_{12} < \gamma_{th}\}\mathscr{P}_o \\ &\approx 3,5\mathscr{P}_o^3.\end{aligned} \tag{19}$$

Esse resultado mostrado na equação (19), leva em consideração que os canais entre os nós 1 e 2 são recíprocos, ou seja, que $\gamma_{12} = \gamma_{21}$ (realização instantânea). Se considerar $\gamma_{12} \neq \gamma_{21}$, basta adicionar ao resultado mais um termo $0,5\mathscr{P}_o$ (XIAO; SKOGLUND, 2010) (não considerada neste trabalho). Além disso, esse resultado mostra que a ordem de diversidade é igual a três, que é melhor se comparado ao esquema DF, cuja ordem de diversidade é igual a dois.

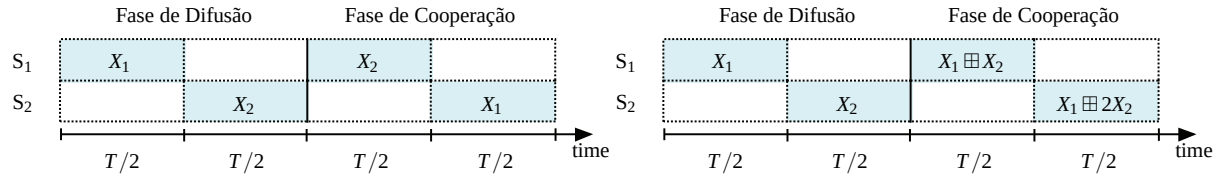
A Figura 7 mostra a transmissão dos pacotes no domínio do tempo, apontando as diferenças fundamentais do esquema de cooperação DF (Figura 7(a)) com a codificação de rede (Figura 7(b)). No esquema DF, observa-se que na fase de cooperação os nós apenas encaminham os pacotes X_1 e X_2 recebidos pelos outros nós. Já no esquema DNC, os pacotes X_1 e X_2 são combinados antes de serem enviados ao destino ($X_1 \boxplus X_2$ e $X_1 \boxplus 2X_2$).

Caso a codificação de rede seja binária, não é possível atingir a ordem de diversidade $2M-1$, pois, se os blocos transmitidos forem X_1, X_2, $X_1 \boxplus X_2$ e $X_1 \boxplus X_2$, do ponto de vista do nó 1, caso a informação X_1 não seja recuperada pelo nó D pela transmissão direta, recuperar duas das três mensagens do conjunto $\{X_2, X_1 \boxplus X_2, X_1 \boxplus X_2\}$ não é garantia de recuperar X_1, pois, se o nó D receber duas vezes a mesma informação $X_1 \boxplus X_2$ não é possível recuperar X_1. Neste



(a) Fase de Difusão (b) Fase de Cooperação

Figura 6: Esquema DNC, formado pelas fases de (a) difusão e (b) cooperação, na qual são transmitidas as combinações lineares $X_1 \boxplus X_2$ e $X_1 \boxplus 2X_2$.



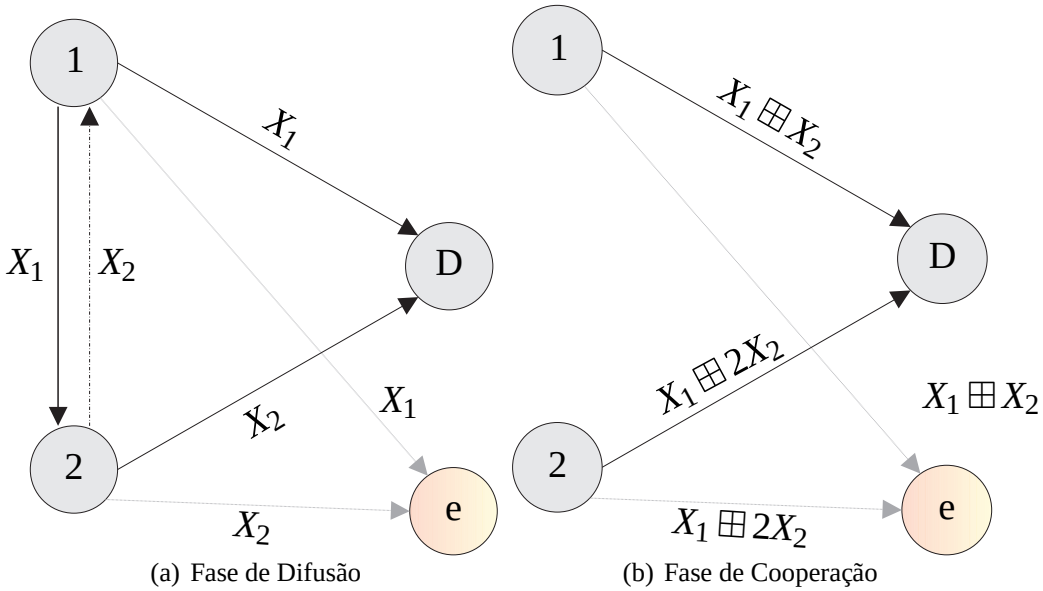
(a) Decodifica-e-Encaminha (DF) (b) Codificação de Rede Dinâmica (DNC)

Figura 7: Alocação do canal no domínio do tempo considerando o esquema (a) Decodifica-e-Encaminha (DF); (b) Codificação de Rede Dinâmica (DNC). T representa a duração do time-slot.

caso a ordem de diversidade obtida é igual a dois (XIAO; SKOGLUND, 2010), o mesmo obtido considerando apenas uma rede cooperativa tradicional sem codificação de rede.

Neste trabalho, foi considerada uma rede cooperativa DNC com o uso de codificação de rede não-binária, para o caso particular para $M = 2$ usuários, considerando que os canais inter-usuários são recíprocos (realização instantânea), e considerando a presença de um nó *eavesdropper* próximo ao nó destino *D*. Esse *eavesdropper* está interessado em todas as informações transmitidas pelos nós legítimos 1 e 2, mostrado na Figura 8, adaptada de (XIAO; SKOGLUND, 2010).

Foram considerados dois tipos de *eavesdroppers*: O primeiro, que tem acesso a todas as informações, tanto da fase de difusão quanto da cooperação, e inclusive tem acesso aos coeficientes da codificação de rede (esse atacante foi chamado neste trabalho apenas de *eavesdropper*), e o segundo, que consegue interceptar apenas informações da fase de difusão, e não consegue, por algum motivo (por exemplo, algum tipo de criptografia utilizada nos coeficientes) obter os coeficientes utilizados na codificação de rede (chamado neste trabalho de "*Dumb*"). As duas fases de transmissão são ilustradas pelas Figuras 8(a) e 8(b), com a presença do nó *eavesdropper*, *e*.



(a) Fase de Difusão (b) Fase de Cooperação

Figura 8: Esquema DNC, com a presença do nó *eavesdropper*, *e*.

4.2 ANÁLISE DA CODIFICAÇÃO DE REDE COM RESTRIÇÕES DE SIGILO

Para calcular a probabilidade de *outage* com restrições de sigilo para o esquema DNC, como não se tem conhecimento da informação mútua recebida pelo nó destino *D* e nem a obtida pelo *eavesdropper*, foi utilizada uma outra técnica, diferente dos esquemas mostrados anteriormente (DT e DF), partindo-se da probabilidade de *outage* da codificação de rede sem restrições de sigilo, mostrada na equação (19).

Nesta parte são descritos os passos para se obter o resultado numérico da pdf da SNR dos nós legítimos. Para obter o resultado analítico da pdf basta derivar a CDF, ou seja, derivar a probabilidade de *outage*, que nada mais é do que a CDF da SNR (GOLDSMITH, 2005). Embora a probabilidade de *outage* do esquema DNC (equação (19)) tenha sido calculada em função de uma SNR limiar (γ_{th}), ela também foi escrita em função da probabilidade de *outage* de um enlace simples. Por essa razão, foi considerada que a CDF da SNR instantânea é igual a probabilidade de *outage* do esquema DNC. Neste caso, tem-se que a SNR instantânea γ_{1D} corresponde a SNR instantânea equivalente do esquema DNC.

Tem-se que a CDF da SNR instantânea γ_{1D} obtida a partir da probabilidade de *outage* do esquema DNC com dois usuários (XIAO; SKOGLUND, 2010) é dada por:

$$F_{\gamma_{1D}}(\gamma_{1D}) = 3,5\left[1 - \exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^3, \tag{20}$$

onde a pdf é obtida através da derivada da CDF, como segue:

$$\begin{aligned} p_{\gamma_{1D}}(\gamma_{1D}) &= 3,5\frac{\partial\left[F_{\gamma_{1D}}(\gamma_{1D})\right]}{\partial\gamma_{1D}} \\ &= \frac{10,5}{\overline{\gamma}_{1D}}\left[1-\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^2\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right) \\ &= \frac{10,5}{\overline{\gamma}_{1D}}\left[1-\exp\left(-|h_{1D}|^2\right)\right]^2\exp\left(-|h_{1D}|^2\right), \end{aligned} \tag{21}$$

Para obter a pdf da SNR instantânea do nó 1 com o *eavesdropper*, basta substituir a letra *D* pela letra *e* na equação (21).

Em termos de simulação, para o esquema DNC, os valores numéricos das SNR instantâneas γ_{1D} e γ_{1e} são obtidos através do método de amostragem da transformação inversa (*Inverse transform sampling method*) (DEVROYE, 1986).

A primeira análise a ser feita é sobre a probabilidade de existência da capacidade de sigilo do modelo, ou seja, da probabilidade de que C_s seja maior que zero ($\Pr\{C_s>0\}$). Parte-se da equação (5) de (BARROS; RODRIGUES, 2006), e usa-se a solução da integral encontrada na equação 3.312.1 de (GRADSHTEYN; RYZHIK, 2007):

$$\begin{aligned} \Pr\{C_{s,\mathrm{DNC}}>0\} &= \Pr\{\gamma_{1D}>\gamma_{1e}\} \\ &= \int_0^{\infty}\int_0^{\gamma_{1D}} p_{\gamma_{1D}}(\gamma_{1D})p_{\gamma_{1e}}(\gamma_{1e})d\gamma_{1e}d\gamma_{1D} \\ &= \frac{10,5\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}\sum_{i=0}^{2}\binom{2}{i}(-1)^i\mathrm{B}\left(\frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}(i+1),4\right), \end{aligned} \tag{22}$$

onde $B(x,y)=\int_0^1 t^{x-1}(1-t)^{y-1}dt$ corresponde à função Beta (ou a integral de Euler de primeira ordem, mostrada na equação 8.380.1 de (GRADSHTEYN; RYZHIK, 2007)). Foi considerado ainda o fato de que $(1-x)^n=\sum_{i=0}^{n}\binom{n}{i}(-1)^i x^i$.

Demonstração. Apresentada no Apêndice A.3. □

A outra análise importante é a probabilidade de *outage* com restrições de sigilo, quando

a capacidade de sigilo instantânea C_s é menor que uma taxa de sigilo alvo R_s, dada por:

$$\begin{aligned}\mathscr{P}_{so,\mathrm{DNC}}(R_s) &= \Pr\{C_s < R_s\} \\ &= \Pr\left\{\gamma_{1D} < 2^{R_s}(1+\gamma_{1e}) - 1\right\} \\ &= \int_0^{\infty}\int_0^{\gamma_U} p_{\gamma_{1D},\gamma_{1e}}(\gamma_{1D},\gamma_{1e})d\gamma_{1D}d\gamma_{1e} \\ &= 36,75\sum_{i=0}^{3}\binom{3}{i}(-1)^i \exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}i\right)\mathrm{B}\left(\frac{2^{2R_s}\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}i+1,3\right).\end{aligned} \tag{23}$$

Demonstração. Apresentada no Apêndice A.4. □

4.3 ANÁLISE DA CODIFICAÇÃO DE REDE COM RESTRIÇÕES DE SIGILO, CASO *DUMB-EAVESDROPPER*

Para o caso de um *eavesdropper* que não conheça os coeficientes usados na codificação de rede (chamado de "*Dumb*", neste trabalho), em que ele somente é capaz de obter informação significativa durante a fase de difusão, a informação mútua obtida pelo *eavesdropper* é menor se comparada ao caso em que o atacante passivo conhece os coeficientes utilizados na codificação de rede.

Para o cálculo da probabilidade de existência da capacidade de sigilo e da probabilidade de *outage* com restrições de sigilo para este esquema, parte-se do mesmo princípio descrito na seção anterior. A pdf da SNR dos nós legítimos é a mesma mostrada na equação (21). A diferença fundamental é que o coeficiente de desvanecimento de canal entre o nó 1 e o *eavesdropper*, h_{1e}, possui distribuição Rayleigh, com média nula e variância unitária. Consequentemente, $|h_{1e}|^2$ possui distribuição exponencial (GOLDSMITH, 2005), com a pdf dada por $p_{\gamma_{1e}}(\gamma_{1e}) = \frac{1}{\overline{\gamma}_{1e}}\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)$.

Então, a probabilidade de existência da capacidade de sigilo, $\Pr\{C_{s,\mathrm{DNC\ Dumb}} > 0\}$ é dada por:

$$\begin{aligned}\Pr\{C_{s,\mathrm{DNC\ Dumb}} > 0\} &= \Pr\{\gamma_{1D} > \gamma_{1e}\} \\ &= \int_0^{\infty}\int_0^{\gamma_{1D}} p_{\gamma_{1D}}(\gamma_{1D})p_{\gamma_{1e}}(\gamma_{1e})d\gamma_{1e}d\gamma_{1D} \\ &= \frac{10,5\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}\sum_{i=0}^{2}\binom{2}{i}(-1)^i\mathrm{B}\left(\frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}(i+1),2\right).\end{aligned} \tag{24}$$

Demonstração. Apresentada no Apêndice A.5. □

A probabilidade de *outage* com restrições de sigilo para o caso "*Dumb*", $\mathscr{P}_{so,\mathrm{DNC\ Dumb}}$,

é dada por:

$$\begin{aligned}\mathscr{P}_{so,\text{DNC Dumb}}(R_s) &= \Pr\{C_s < R_s\} \\ &= \Pr\left\{\gamma_D < 2^{R_s}(1+\gamma_{1e}) - 1\right\} \\ &= \Pr\{\gamma_D < \gamma_U\} \\ &= \int_0^{\infty}\int_0^{\gamma_U} p_{\gamma_{1D},\gamma_{1e}}(\gamma_{1D},\gamma_{1e})d\gamma_{1D}d\gamma_{1e} \\ &= \frac{3,5\overline{\gamma}_{1D}}{2^{2R_s}\overline{\gamma}_{1e}}\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}\right)B\left(\frac{\overline{\gamma}_{1D}}{2^{2R_s}\overline{\gamma}_{1e}},4\right),\end{aligned} \tag{25}$$

em que $\gamma_U = 2^{R_s}(1+\gamma_{1e}) - 1$.

Demonstração. Apresentada no Apêndice A.6. □

5 RESULTADOS NUMÉRICOS

Neste capítulo alguns resultados serão apresentados com o intuito de comprovar os resultados obtidos analiticamente, e também para ilustrar a eficiência do esquema proposto quando comparado aos esquemas DT e DF.

A Figura 9 apresenta a probabilidade de existência da capacidade de sigilo ($\Pr\{C_s > 0\}$) em função da SNR média, $\overline{\gamma}_{1D}$, para os esquemas DT, DF, DNC e DNC-Dumb, considerando $\overline{\gamma}_{1e} = 10$ dB. No caso DNC-Dumb, a probabilidade de existência da capacidade de sigilo é maior que a dos outros esquemas, mesmo para valores de $\overline{\gamma}_{1D}$ baixos. Caso o *eavesdropper* seja capaz de obter todas as informações em todas as transmissões, o esquema DNC apresenta melhores resultados em relação ao DF, para $\overline{\gamma}_{1D} > 2$ dB, e melhor que o esquema DT para $\overline{\gamma}_{1D} > 3$ dB, aproximadamente. Outro resultado interessante ocorre quando a probabilidade de existência da capacidade de sigilo para o esquema DNC chega a 1 (100% de probabilidade de existência), para $\overline{\gamma}_{1D} > 8$ dB. Ou seja, há uma diferença significativa em relação ao DF, cuja probabilidade tende a 1 para $\overline{\gamma}_{1D} \approx 26$ dB (diferença aproximada de 18 dB). Nota-se que para o esquema DNC, a capacidade de sigilo existirá com maior probabilidade que os demais esquemas, a partir de 3 dB, mesmo quando $\overline{\gamma}_{1D} < \overline{\gamma}_{1e}$, o que é interessante já que se torna possível ter uma transmissão com sigilo mesmo quando o *eavesdropper* tenha SNR média maior que os nós legítimos.

A Figura 10 mostra a probabilidade de *outage* com restrições de sigilo ($\Pr\{C_s < R_s\}$) em função da SNR média, $\overline{\gamma}_{1D}$, para os esquemas DT, DF, DNC e DNC-Dumb, para uma taxa de sigilo alvo $R_s = 0,5$ bpcu. Percebe-se que os esquemas com codificação de rede (DNC e DNC-Dumb) apresentam a maior ordem de diversidade (igual a três) em relação aos demais. Essa maior ordem de diversidade contribui quando há necessidade de uma probabilidade de *outage* com restrições de sigilo menor que 10^{-3}, aproximadamente. Para o esquema DNC-Dumb, a partir de $\overline{\gamma}_{1D} \approx 20$ dB, já se pode observar o benefício da codificação de rede em relação aos esquemas DT e DF. Em $\overline{\gamma}_{1D} \approx 31$ dB, pode-se observar o cruzamento das curvas de probabilidade do esquema DF com o DNC quando o *eavesdropper* sabe quais os coeficientes utilizados na codificação de rede, mostrando uma melhora no desempenho a partir desse valor

para o esquema DNC.

Já a Figura 11 mostra a influência da SNR média do *eavesdropper* no desempenho da probabilidade de *outage* com restrições de sigilo para os esquemas DNC e DNC-Dumb. Quanto maior $\overline{\gamma}_{1e}$, mais a probabilidade de *outage* com restrições de sigilo é degradada (curva desloca-se para a direita). Porém a ordem de diversidade mantém-se constante.

A probabilidade de *outage* com restrições de sigilo em função da taxa de sigilo alvo R_s está apresentada na Figura 12, considerando $\overline{\gamma}_{1D} = 35$ dB e $\overline{\gamma}_{1e} = 10$ dB, para os esquemas DT, DF, DNC e DNC-Dumb. Como esperado, pode-se perceber que quanto maior a taxa de sigilo alvo, R_s, maior é a probabilidade de *outage* com restrições de sigilo. Percebe-se também que o esquema DNC apresenta melhor desempenho para taxas de sigilo alvo inferiores 1,2 bpcu, quando comparada ao esquema DF. Para uma taxa de sigilo alvo superior a 1,9 bpcu, o esquema DNC passa a apresentar pior desempenho que a transmissão direta, porém, para esse valor de R_s, a probabilidade de *outage* com restrições de sigilo já está bastante elevada, na casa de 10^{-2}.

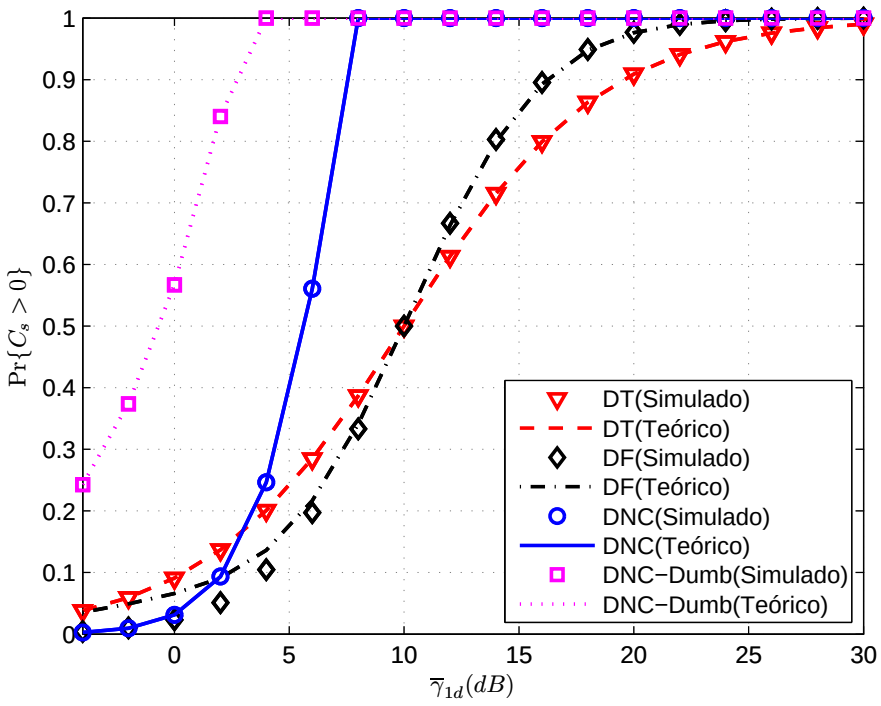


Figura 9: Probabilidade de existência da capacidade de sigilo ($\Pr\{C_s > 0\}$) em função de $\overline{\gamma}_{1D}$, para os esquemas DT, DF, DNC e DNC-Dumb, com a SNR média do *eavesdropper* $\overline{\gamma}_{1e} = 10$ dB.

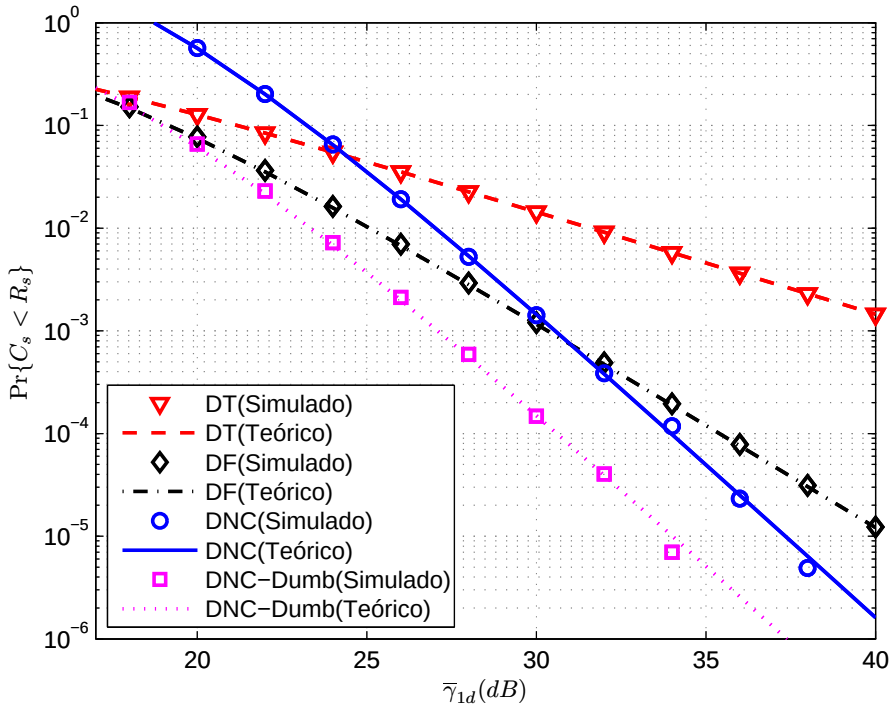


Figura 10: Probabilidade de *outage* com restrições de sigilo ($\Pr\{C_s < R_s\}$) em função de $\overline{\gamma}_{1D}$, para os esquemas DT, DF, DNC e DNC-Dumb, com $R_s = 0,5$ bpcu e SNR média do *eavesdropper* $\overline{\gamma}_{1e} = 10$ dB.

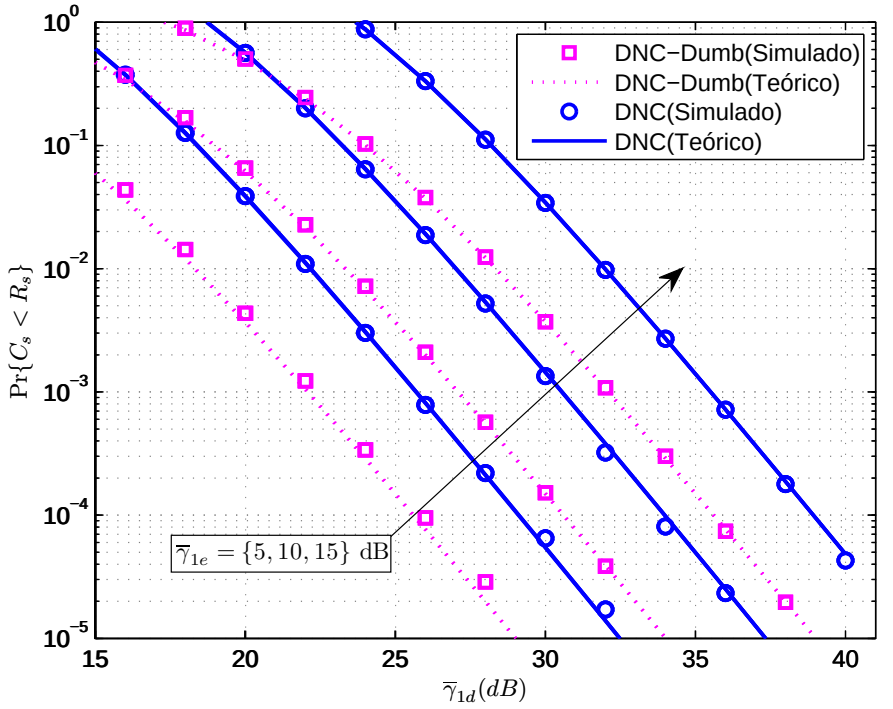


Figura 11: Probabilidade de *outage* com restrições de sigilo ($\Pr\{C_s < R_s\}$) em função de $\overline{\gamma}_{1D}$ para os esquemas DNC e DNC-Dumb, com $R_s = 0,5$ bpcu e SNR média do *eavesdropper* $\overline{\gamma}_{1e} = \{5, 10, 15\}$ dB.

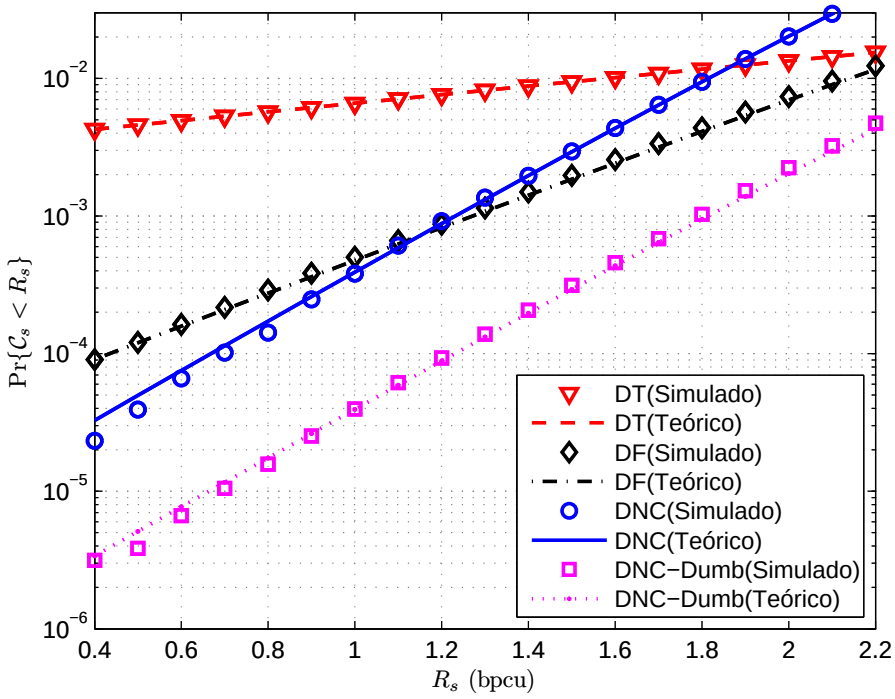


Figura 12: Probabilidade de *outage* com restrições de sigilo ($\Pr\{C_s < R_s\}$) em função da taxa de sigilo alvo, R_s, para os esquemas DT, DF, DNC e DNC-Dumb, com $\overline{\gamma}_{1D} = 35$ dB e $\overline{\gamma}_{1e} = 10$ dB.

6 CONCLUSÃO

Smart grids necessitam de um sistema de comunicação de dados seguro e que seja capaz de atender a todas as trocas de mensagens existentes nessa rede. Segurança é um dos pontos mais críticos, devido à natureza difusora da comunicação sem fio, já que uma falha na comunicação de dados pode provocar perturbações e *blackouts* na rede elétrica, ou gerar problemas de privacidade, na situação em que *eavesdroppers* possam interceptar as informações propagadas na rede na tentativa de obter algum benefício. Para reduzir os efeitos desses atacantes passivos, foi proposta a codificação de rede, como alternativa para aumentar a segurança na camada física, de maneira complementar aos métodos tradicionais de segurança previstos na literatura (*firewall* e criptografia, por exemplo). A vantagem, neste caso, é que não é necessário nenhum mecanismo adicional na camada física. O esquema ainda é vantajoso para sistemas de comunicação cooperativa quando se tem a presença de um atacante passivo.

Os resultados apresentados neste trabalho mostraram que o esquema DNC é capaz de aumentar o sigilo das redes sem fio, quando comparado com os outros esquemas (DT e DF), mesmo com a presença de um *eavesdropper*. Foram analisadas a probabilidade de existência da capacidade de sigilo e a probabilidade de *outage* com restrições de sigilo para uma rede cooperativa de múltiplo acesso (característica de uma rede *smart grid*). Foi mostrado através de resultados teóricos e numéricos que o sigilo pode existir mesmo quando a SNR média dos nós legítimos for inferior à SNR média do *eavesdropper*, com melhores resultados para o esquema DNC a partir de um determinado valor. Adicionalmente, esse esquema mostrou-se capaz de diminuir a probabilidade de *outage* com restrições de sigilo para a região de alta SNR média, ou seja, aumenta o sigilo nas transmissões, se comparado com os esquemas DT e DF. Foi verificado, ainda, que quanto maior a taxa de sigilo alvo, R_s, maior a probabilidade de *outage* com restrições de sigilo. O esquema DNC apresentou melhores resultados para valores de R_s baixos, para o modelo apresentado, com probabilidade de *outage* de sigilo pequena. Foi avaliada também a influência da SNR média do *eavesdropper*, e verificou-se que a probabilidade de *outage* com restrições de sigilo é degradada quanto maior a SNR média do *eavesdropper*. Entretanto, a ordem de diversidade manteve-se constante.

Foi mostrado também que o esquema DNC proporcionou um aumento da ordem de diversidade para três, superior a ordem de diversidade do esquema DF, que é igual a dois, mesmo com a presença de um *eavesdropper*, desde que seja utilizada uma codificação de rede dinâmica e não-binária.

6.1 TRABALHOS FUTUROS

Para o esquema proposto pode-se generalizar as equações de probabilidades, para o caso de M usuários, além de simular as curvas em relação aos outros esquemas.

Outro ponto importante que pode ser explorado é a utilização de outras técnicas de codificação de rede, como por exemplo o GDNC (*Generalized Dynamic Network Coding*), que pode aumentar a ordem de diversidade do esquema, para beneficiar as *smart grids*.

REFERÊNCIAS

AHLSWEDE, R. et al. Network information flow. **IEEE Transactions on Information Theory**, v. 46, n. 4, p. 1204 – 1216, 2000.

AHMED, M. et al. Smart grid cooperative communication with smart relay. **Journal of Communications and Networks**, v. 14, p. 640–652, 2012.

ALVES, H. et al. Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Process. Lett.**, v. 19, n. 6, p. 372–375, June 2012.

BAO, X.; LI, J. Adaptive network coded cooperation (ANCC) for wireless relay networks: Matching code-on-graph with network-on-graph. v. 7, n. 2, p. 574–583, February 2008.

BARROS, J.; RODRIGUES, M. R. D. Secrecy capacity of wireless channels. In: **Proc. of the IEEE Int. Symp. on Inform. Theory, ISIT'06**. Seattle, Washington, U.S.A.: [s.n.], 2006.

BHATTAD, K.; NARAYANAN, K. R. Weakly secure network coding. In: **Proc. First Workshop on Network Coding, Theory, Appl. (NetCod'05)**. Riva del Garda, Itália: NetCod, 2005.

BLOCH, M.; BARROS, J. **Physical-Layer Security: From Information Theory to Security Engineering**. [S.l.]: Cambridge University Press, 2011.

BLOCH, M. et al. Wireless information-theoretic security. **IEEE Trans. on Information Theory**, v. 54, p. 2515–2534, 2008.

CAI, N.; YEUNG, R. Secure network coding on a wiretap network. **IEEE Trans. on Information Theory**, v. 57, p. 424–435, 2011.

CAI, N.; YEUNG, R. W. Network error correction, part II: Lower bounds. **Commun. in Inf. and Systems**, v. 6, n. 1, p. 37–54, 2006.

CASTLE, S. It's not a trial: First smart grid rollout of energy management home networking to take place in june. 2011. Disponível em: <http://greentechadvocates.com/2011/01/31/its-not-a-trial-first-smart-grid-rollout-of-home-energy-management-to-take-place-in-june/>.

COVER, T. M.; TOMAS, J. A. **Elements of Information Theory**. Nova Iorque: John Wiley & Sons, 1991.

CPQD. **Smart Grid: energia eficiente no Brasil**. 2013. Disponível em: <http://www.cpqd.com.br/mercado/smart-grid>.

DECONINCK, G. An evaluation of two-way communication means for advanced metering in Flanders (Belgium). In: **IEEE International Instrumentation and Measurement Technology Conference**. Victoria, CAN: [s.n.], 2008.

DEVROYE, L. **Non-Uniform Random Variate Generation**. [S.l.]: New York: Springer-Verlag, 1986.

DIGITAL, C. **Smart grid: Piloto envolve mil clientes em São Paulo**. 2012. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=30066>.

EASTON, J. **U.S. Smart Grid. Past, Present and Future.** 2013. Disponível em: <http://www.smartgrid.com.br/eventos/smartgrid2013/>.

FRAGOULI, C.; SOLJANIN, E. **Network Coding Applications**. Boston, MA: Foundations and Trends in Networking, Now Publishers Inc., 2007.

FRAGOULI, C.; SOLJANIN, E. **Network Coding Fundamentals**. Boston, MA: Foundations and Trends in Networking, Now Publishers Inc., 2007.

FRANZ, E.; PFENNIG, S.; FISCHER, A. Efficiency of secure network coding schemes. In: **Proc. of 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS)**. Canterbury, UK: [s.n.], 2012.

GABRY, F. **Cooperation for Secrecy in Wireless Networks**. Tese (Doutorado) — KTH, School of Electrical Engineering, Communication Theory Laboratory, September 2012.

GALLI, S.; SCAGLIONE, A.; WANG, Z. For the grid and through the grid: The role of power line communications in the smart grid. In: **Proceedings of the IEEE**. New York, US: IEEE Press, 2011. v. 99, n. 6.

GOEL, S.; NEGI, R. Guaranteeing secrecy using artificlal noise. **IEEE Trans. Wireless Communications**, v. 7, p. 2180–2189, 2009.

GOLDSMITH, A. **Wireless Communications**. Stanford, CA: Cambridge University Press, 2005.

GRADSHTEYN, I.; RYZHIK, I. M. **Table of Integrals, Series, and Products**. San Diego, CA: Academic Press - Elsevier, 2007.

GUNDUZ, D.; ERKIP, E. Opportunistic cooperation by dynamic resource allocation. **IEEE Trans. on Wireless Communications**, v. 6, p. 1446–1454, 2007.

IEC 62056-21. **Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange**. 2002.

LAI, L.; GAMAL, H. E. The relay-eavesdropper channel: Cooperation for secrecy. **IEEE Trans. on Information Theory**, v. 54, n. 9, p. 4005–4019, September 2008.

LANEMAN, J. N.; TSE, D. N. C.; WORNELL, G. W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. **IEEE Trans. on Information Theory**, v. 50, n. 12, p. 3062–3080, December 2004.

LANEMAN, J. N.; WORNELL, G. W. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks. **IEEE Trans. on Information Theory**, v. 49, p. 2415–2425, 2003.

LI, H. et al. Efficient and secure wireless communications for advanced metering infrastructure in smart grids. **IEEE Trans. on Smart Grid**, v. 3, n. 3, p. 1540–1551, September 2012.

LI, L. L. H.; ZHANG, W. Communication requirement for reliable and secure state estimation and control in smart grid. **IEEE Trans. on Smart Grids**, v. 2, n. 3, p. 476–486, September 2011.

MARTINS, J. B. **Projeto InovCity Aparecida - Status de Execução, Principais Aprendizados para o Desenvolvimento Futuro das Smart Grids no Brasil**. 2013. Disponível em: <http://www.smartgrid.com.br/?pagina=177>.

MEULEN, E. C. van der. Three-terminal communication channels. **Advanced Applied Probability**, v. 3, p. 120–154, 1971.

NIYATO, D.; WANG, P. Cooperative transmission for meter data collection in smart grid. **IEEE Communications Magazine**, p. 90–97, 2012.

NOSRATINIA, A.; HUNTER, T.; HEDAYAT, A. Cooperative communication in wireless networks. **IEEE Communications Magazine**, v. 42, p. 74–80, 2004.

PAPOULIS, A. **Probability, Random Variables, and Stochastic Processes**. 2nd. ed. New York: McGraw-Hill, 1984.

PHULPIN, Y.; BARROS, J.; LUCANI, D. Network coding in smart grids. **IEEE SmartGridComm**, p. 49–54, 2011.

REBELATTO, J. L. et al. Generalized distributed network coding based on nonbinary linear block codes for multi-user cooperative communications. In: **Proc. IEEE Int. Symp. Inf. Theory, ISIT'10**. Austin, TX: ISIT, 2010. p. 943–947.

REBELATTO, J. L. et al. Multi-user cooperative diversity through network coding based on classical coding theory. **IEEE Trans. Signal Process.**, v. 60, n. 2, p. 916–926, February 2012.

SHANNON, C. Communication theory of secrecy systems. **Bell System Technical Journal**, v. 28, p. 656–715, 1949.

SNELL, J.; COLLEGE, S. **Introduction to Probability**. Hanover, NH: Dartmouth College, 1997.

SUBRAMANIAN, A. et al. Strong and weak secrecy in wiretap channels. In: **6th Int. Symp. on Turbo Codes and Iterative Information Processing, ISTC'10**. Brest, França: [s.n.], 2010.

WANG, X.; YI, P. Security framework for wireless communications in smart distribution grid. **IEEE Trans. on Smart Grids**, v. 2, n. 4, p. 809–818, December 2011.

WANG, Y.; LIN, W.; ZHANG, T. Study on security of wireless sensor networks in smart grid. In: **Proc. of the 2010 International Conference on Power System Technology**. Hangzhou, CN: [s.n.], 2010.

WYNER, A. D. The wire-tap channel. **The Bell System Technical Journal**, v. 54, p. 1355–1387, 1975.

XIAO, L. et al. A network coding approach to cooperative diversity. **IEEE Trans. on Information Theory**, v. 53, n. 10, p. 3714–3722, October 2007.

XIAO, M.; SKOGLUND, M. Multiple-user cooperative communications based on linear network coding. **IEEE Trans. on Communications**, v. 58, n. 12, p. 3345–3351, December 2010.

YANG, N. et al. Transmit antenna selection for security enhancement in MIMO wiretap channels. **IEEE Trans. on Communications**, v. 61, n. 1, p. 144–154, January 2013.

ZHANG, P. et al. P-coding: Secure network coding against eavesdropping attacks. In: **Proc. IEEE INFOCOM 2010**. San Diego, US: [s.n.], 2010.

APÊNDICE A – PROVA DAS EQUAÇÕES

A.1 PROVA DA EQUAÇÃO (14)

Para o cálculo da probabilidade de existência da capacidade de sigilo do esquema DF, apresentada na equação (14), é necessário dividi-la em duas partes, dependendo da ocorrência ou não de *outage* no enlace entre os nós 1 e 2:

$$\begin{aligned}\Pr(C_{s,\mathrm{DF}} > 0) = \Pr\left(|I_{\mathrm{DF}_a} - I_{\mathrm{DF},e_a}|^+ > 0\right)\mathscr{P}_{o,12} + \\ \Pr\left(|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}|^+ > 0\right)(1-\mathscr{P}_{o,12})\,.\end{aligned} \tag{26}$$

Na primeira parte, quando ocorre *outage* no enlace entre os nós 1 e 2, os nós não podem cooperar entre si, e só ocorre a transmissão direta, multiplicado por $\frac{1}{2}$ (correspondente a metade do *time-slot*). Consequentemente, a probabilidade de existência da capacidade de sigilo é a mesma da equação (7), ou seja:

$$\begin{aligned}\Pr\left(|I_{\mathrm{DF}_a} - I_{\mathrm{DF},e_a}|^+ > 0\right) &= \Pr\left\{\frac{1}{2}\left(\log\left(1+\gamma_{1D}\right) - \log\left(1+\gamma_{1e}\right)\right) > 0\right\} \\ &= \frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D}+\overline{\gamma}_{1e}}.\end{aligned} \tag{27}$$

Na segunda parte, quando não há ocorrência de *outage* no enlace entre os nós 1 e 2,

tem-se que:

$$\begin{aligned}
\Pr\left\{|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}|^+ > 0\right\} &= \Pr\left(|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}|^+ > 0\right) \\
&= \Pr\left\{\frac{1}{2}\left(\log_2\left(1+\gamma_{1D}+\gamma_{2D}\right) - \log_2\left(1+\gamma_{1e}+\gamma_{2e}\right)\right) > 0\right\} \\
&= \Pr\left\{\log_2\left(\frac{1+\gamma_{1D}+\gamma_{2D}}{1+\gamma_{1e}+\gamma_{2e}}\right) > 0\right\} \\
&= \Pr\left\{\frac{1+\gamma_{1D}+\gamma_{2D}}{1+\gamma_{1e}+\gamma_{2e}} > 1\right\} \\
&\approx \Pr\left\{\frac{\gamma_{1D}+\gamma_{2D}}{\gamma_{1e}+\gamma_{2e}} > 1\right\} \\
&= \Pr\left\{\frac{\overline{\gamma}_{1D}\left(|h_{1D}|^2+|h_{2D}|^2\right)}{\overline{\gamma}_{1e}\left(|h_{1e}|^2+|h_{2e}|^2\right)} > 1\right\} \\
&= \Pr\left\{\frac{|h_{1D}|^2+|h_{2D}|^2}{|h_{1e}|^2+|h_{2e}|^2} > \kappa_e\right\},
\end{aligned} \tag{28}$$

onde $\kappa_e = \frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}$. A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$ e $\overline{\gamma}_{1e}$.

Como os coeficientes h_{1D}, h_{2D}, h_{1e} e h_{1e} possuem distribuição Rayleigh, consequentemente $|h_{1D}|^2$, $|h_{2D}|^2$, $|h_{1e}|^2$ e $|h_{2e}|^2$ possuem distribuição exponencial (GOLDSMITH, 2005). Para resolver a equação (28), foi utilizada a chamada distribuição da razão de duas variáveis aleatórias (*ratio distribution*) (PAPOULIS, 1984). Foram consideradas três variáveis aleatórias X, Y e Z, onde $X = |h_{1D}|^2 + |h_{2D}|^2$, $Y = |h_{1e}|^2 + |h_{2e}|^2$ e $Z = \frac{X}{Y}$. Considera-se que a pdf de X é $p_X(x) = \lambda^2 x \exp(-\lambda x)$ e a pdf de Y é $p_Y(y) = \lambda^2 y \exp(-\lambda y)$ (SNELL; COLLEGE, 1997), onde $\lambda = 1$ (representa a média das variáveis aleatórias exponencialmente distribuídas), além de $z = \frac{x}{y}$, ou seja, $x = zy$. A pdf da distribuição da razão, $p_Z(z)$, é calculada da seguinte maneira (PAPOULIS, 1984):

$$\begin{aligned}
p_Z(z) &= \int_0^\infty y p_X(zy) p_Y(y) dy \\
&= z \int_0^\infty y^3 \exp\left(-y(z+1)\right) dy \\
&= \frac{6z}{(z+1)^4}.
\end{aligned} \tag{29}$$

É preciso calcular a CDF de $p_Z(z)$, representada por $F_Z(z)$, que neste caso, para o intervalo de integração $[\kappa_e, \infty]$, corresponde a segunda parte da probabilidade de existência da

capacidade de sigilo do esquema DF:

$$\begin{aligned} F_Z(\kappa_e) &= \Pr\left\{|I_{\mathrm{DF}_b} - I_{\mathrm{DF,e}_b}|^+ > 0\right\} \\ &= \int_{\kappa_e}^{\infty} f_Z(z)dz \\ &= \int_{\kappa_e}^{\infty} \frac{6z}{(z+1)^4}dz \\ &= \frac{3\kappa_e+1}{(\kappa_e+1)^3}. \end{aligned} \tag{30}$$

A equação final da probabilidade de existência da capacidade de sigilo é obtida combinando as equações (27) e (30), que é dada por:

$$\begin{aligned} \Pr\{C_{s,\mathrm{DF}} > 0\} &= \Pr\left\{|I_{\mathrm{DF}_a} - I_{\mathrm{DF},e_a}|^+ > 0\right\} \mathscr{P}_{o,12} + \\ &\quad \Pr\left\{|I_{\mathrm{DF}_b} - I_{\mathrm{DF},e_b}|^+ > 0\right\} (1 - \mathscr{P}_{o,12}) \\ &\approx \left(\frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D}+\overline{\gamma}_{1e}}\right)\left[1 - \exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right] + \\ &\quad \left[\frac{3\kappa_e+1}{(\kappa_e+1)^3}\right]\left[\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right]. \end{aligned} \tag{31}$$

A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$ e $\overline{\gamma}_{1e}$.

A.2 PROVA DA EQUAÇÃO (16)

De forma similar à equação (14), o cálculo da probabilidade de *outage* com restrições de sigilo está condicionado à ocorrência ou não de *outage* no enlace entre os nós 1 e 2. Caso o

referido enlace esteja em *outage*, tem-se:

$$\begin{aligned}
\Pr\left\{|I_{\mathrm{DF}_a}-I_{\mathrm{DF,e}_a}|^+<R_\mathrm{s}\right\} &= \Pr\left\{\frac{1}{2}\log_2(1+\gamma_{1D})-\frac{1}{2}\log_2(1+\gamma_{1e})<R_s\right\}\\
&= \Pr\left\{\log_2\left(\frac{1+\gamma_{1D}}{1+\gamma_{1e}}\right)<2R_s\right\}\\
&= \Pr\left\{\frac{1+\gamma_{1D}}{1+\gamma_{1e}}<2^{2R_s}\right\}\\
&= \Pr\left\{1+\gamma_{1D}<2^{2R_s}(1+\gamma_{1e})\right\}\\
&= \Pr\left\{\gamma_{1D}<2^{2R_s}(1+\gamma_{1e})-1\right\}\\
&= \Pr\left\{\gamma_{1D}<\gamma_U\right\}\\
&= \int_0^\infty\int_0^{\gamma_U}\frac{\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)}{\overline{\gamma}_{1D}}\frac{\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)}{\overline{\gamma}_{1e}}d\gamma_{1D}d\gamma_{1e}\\
&= \frac{1}{\overline{\gamma}_{1D}\overline{\gamma}_{1e}}\int_0^\infty\int_0^{\gamma_U}\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)d\gamma_{1D}d\gamma_{1e}\\
&= \frac{1}{\overline{\gamma}_{1e}}\int_0^\infty\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)d\gamma_{1e}-\frac{1}{\overline{\gamma}_{1e}}\int_0^\infty\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)\exp\left(-\frac{\gamma_U}{\overline{\gamma}_{1D}}\right)d\gamma_{1e}\\
&= 1-\frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D}+\overline{\gamma}_{1e}2^{2R_s}}\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}\right).
\end{aligned} \tag{32}$$

onde $\gamma_U = 2^{2R_s}(1+\gamma_{1e})-1$.

A segunda parte, $\Pr\left\{|I_{\mathrm{DF}_b}-I_{\mathrm{DF,e}_b}|^+<R_\mathrm{s}\right\}$, quando não ocorre *outage* no enlace entre os nós 1 e 2, tem-se que:

$$\begin{aligned}
\Pr\left\{|I_{\mathrm{DF}_b}-I_{\mathrm{DF,e}_b}|^+<R_\mathrm{s}\right\} &= \Pr\left\{\frac{1}{2}\log_2(1+\gamma_{1D}+\gamma_{2D})-\log_2(1+\gamma_{1e}+\gamma_{2e})<R_s\right\}\\
&= \Pr\left\{\log_2\left(\frac{1+\gamma_{1D}+\gamma_{2D}}{1+\gamma_{1e}+\gamma_{2e}}\right)<2R_s\right\}\\
&= \Pr\left\{\frac{1+\gamma_{1D}+\gamma_{2D}}{1+\gamma_{1e}+\gamma_{2e}}<2^{2R_s}\right\}\\
&\approx \Pr\left\{\frac{\gamma_{1D}+\gamma_{2D}}{\gamma_{1e}+\gamma_{2e}}<2^{2R_s}\right\}\\
&= \Pr\left\{\frac{\overline{\gamma}_{1D}\left(|h_{1\mathrm{D}}|^2+|h_{2\mathrm{D}}|^2\right)}{\overline{\gamma}_{1e}\left(|h_{1e}|^2+|h_{2e}|^2\right)}<2^{2R_s}\right\}\\
&= \Pr\left\{\frac{|h_{1D}|^2+|h_{2D}|^2}{|h_{1e}|^2+|h_{2e}|^2}<\kappa_e 2^{2R_s}\right\}\\
&= \Pr\left\{\frac{\left(|h_{1D}|^2+|h_{2D}|^2\right)}{\left(|h_{1e}|^2+|h_{2e}|^2\right)}<\gamma_0\right\},
\end{aligned} \tag{33}$$

onde $\kappa_e = \frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}$ e $\gamma_0 = \kappa_e 2^{2R_s}$. A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$

e $\overline{\gamma}_{1e}$.

A análise é similar ao demonstrado no Apêndice A.1, onde os coeficientes h_{1D}, h_{2D}, h_{1e} e h_{1e} possuem distribuição Rayleigh e, consequentemente, $|h_{1D}|^2$, $|h_{2D}|^2$, $|h_{1e}|^2$ e $|h_{2e}|^2$ possuem distribuição exponencial (GOLDSMITH, 2005). Da mesma maneira, foi utilizada a chamada distribuição da razão de duas variáveis aleatórias (*ratio distribution*) (PAPOULIS, 1984). Portanto, a pdf da distribuição da razão, $p_Z(z)$, é a mesma obtida em (29), ou seja (PAPOULIS, 1984):

$$\begin{aligned} p_Z(z) &= \int_0^\infty y p_X(zy) p_Y(y) dy \\ &= z \int_0^\infty y^3 \exp\left(-y(z+1)\right) dy \\ &= \frac{6z}{(z+1)^4}, \end{aligned} \tag{34}$$

É preciso calcular a CDF de $f_Z(z)$, representada por $F_z(z)$, que neste caso, para o intervalo de integração $[0, \gamma_0]$, corresponde a resposta da segunda parte da probabilidade de *outage* com restrições de sigilo para o esquema DF:

$$\begin{aligned} F_Z(\gamma_0) &= \Pr\left\{ |I_{\mathrm{DF}_b} - I_{\mathrm{DF,e}_b}|^+ < R_\mathrm{s} \right\} \\ &= \int_0^{\gamma_0} f_Z(z) dz \\ &= \int_0^{\gamma_0} \frac{6z}{(z+1)^4} dz \\ &= \frac{-3\gamma_0 - 1}{(\gamma_0+1)^3} + 1. \end{aligned} \tag{35}$$

A equação final da probabilidade de *outage* com restrições de sigilo é obtida

combinando as equações (32) e (35), que é dada por:

$$\begin{aligned}\mathscr{P}_{so,\mathrm{DF}}(R_s) &= \Pr\left\{|I_{\mathrm{DF}_a} - I_{\mathrm{DF,e}_a}|^+ < R_\mathrm{s}\right\}\mathscr{P}_{\mathrm{o},12} + \\ &\Pr\left\{|I_{\mathrm{DF}_b} - I_{\mathrm{DF,e}_b}|^+ < R_\mathrm{s}\right\}(1-\mathscr{P}_{\mathrm{o},12}) \\ &\approx \left[1 - \frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1D}+\overline{\gamma}_{1e}2^{2R_s}}\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}\right)\right]\left[1-\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right] + \\ &\left[\frac{-3\kappa_e 2^{2R_s}-1}{\left(\kappa_e 2^{2R_s}+1\right)^3}+1\right]\left[\exp\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{12}}\right)\right].\end{aligned} \tag{36}$$

A aproximação é válida para a região de alta SNR média para $\overline{\gamma}_{1D}$ e $\overline{\gamma}_{1e}$.

A.3 PROVA DA EQUAÇÃO (22)

Sabendo que a pdf de γ_{1D} e γ_{1e} são dadas respectivamente por:

$$p_{\gamma_{1D}}(\gamma_{1D}) = \frac{10,5}{\overline{\gamma}_{1D}}\left[1-\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^2\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right), \tag{37}$$

$$p_{\gamma_{1e}}(\gamma_{1e}) = \frac{10,5}{\overline{\gamma}_{1e}}\left[1-\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)\right]^2\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right), \tag{38}$$

a probabilidade de existência da capacidade de sigilo é então obtida como segue:

$$\begin{aligned}\Pr\{C_{\mathrm{s,DNC}} > 0\} &= \Pr\{\gamma_{1D} > \gamma_{1e}\} \\ &= \int_0^\infty\int_0^{\gamma_{1D}} p_{\gamma_{1D}}(\gamma_{1D})p_{\gamma_{1e}}(\gamma_{1e})d\gamma_{1e}d\gamma_{1D} \\ &= \int_0^\infty p_{\gamma_{1D}}(\gamma_{1D})\left(\int_0^{\gamma_{1D}} p_{\gamma_{1e}}(\gamma_{1e})d\gamma_{1e}\right)d\gamma_{1D} \\ &= \int_0^\infty p_{\gamma_{1D}}(\gamma_{1D})F_{\gamma_{1e}}(\gamma_{1D})d\gamma_{1D} \\ &= \int_0^\infty \frac{10,5}{\overline{\gamma}_{1D}}\left[1-e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}}\right]^2 e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}}\left[1-e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1e}}}\right]^3 d\gamma_{1D} \\ &= \frac{10,5}{\overline{\gamma}_{1D}}\int_0^\infty\left[\sum_{i=0}^{2}\binom{2}{i}(-1)^i e^{-(i+1)\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}}\right]\left[1-e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1e}}}\right]^3 d\gamma_{1D} \\ &= \frac{10,5\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}\sum_{i=0}^{2}\binom{2}{i}(-1)^i \mathrm{B}\left(\frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}(i+1),4\right),\end{aligned} \tag{39}$$

em que $B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$ corresponde à função Beta (ou à integral de Euler de primeira ordem, definida pela equação 8.380.1 de (GRADSHTEYN; RYZHIK, 2007)). Foi utilizada também a solução da integral encontrada na equação 3.312.1 de (GRADSHTEYN; RYZHIK, 2007). Foi considerado ainda o fato de que $(1-x)^n = \sum_{i=0}^{n}\binom{n}{i}(-1)^i x^i$.

A.4 PROVA DA EQUAÇÃO (23)

Sabendo que a pdf de γ_{1D} e γ_{1e} são dadas respectivamente por:

$$p_{\gamma_{1D}}(\gamma_{1D}) = \frac{10,5}{\overline{\gamma}_{1D}}\left[1-\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^2 \exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right), \tag{40}$$

$$p_{\gamma_{1e}}(\gamma_{1e}) = \frac{10,5}{\overline{\gamma}_{1e}}\left[1-\exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)\right]^2 \exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right), \tag{41}$$

a probabilidade de *outage* com restrições de sigilo para o esquema NC é dada por:

$$\begin{aligned}
\mathscr{P}_{so,\mathrm{DNC}}(R_s) &= \Pr\{C_s < R_s\} \\
&= \Pr\left\{\gamma_{1D} < 2^{R_s}(1+\gamma_{1e})-1\right\} \\
&= \Pr\{\gamma_{1D} < \gamma_U\} \\
&= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1D},\gamma_{1e}}(\gamma_{1D},\gamma_{1e}) d\gamma_{1D} d\gamma_{1e} \\
&= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1D}}(\gamma_{1D}) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1D} d\gamma_{1e} \\
&= \int_0^\infty \left(\int_0^{\gamma_U} p_{\gamma_{1D}}(\gamma_{1D}) d\gamma_{1D}\right) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} \\
&= \int_0^\infty F_{\gamma_{1D}}(\gamma_U) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} \\
&= \int_0^\infty 10,5\left[1-e^{-\frac{\gamma_U}{\overline{\gamma}_{1D}}}\right]^3 \frac{3,5}{\overline{\gamma}_{1e}}\left[1-e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}}\right]^2 e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\
&= \frac{36,75}{\overline{\gamma}_{1e}} \int_0^\infty \left[1-e^{-\frac{\gamma_U}{\overline{\gamma}_{1D}}}\right]^3 \left[1-e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}}\right]^2 e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\
&= \frac{36,75}{\overline{\gamma}_{1e}} \int_0^\infty \left[1-e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}} e^{-\frac{2^{2R_s}\gamma_{1e}}{\overline{\gamma}_{1D}}}\right]^3 \left[1-e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}}\right]^2 e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\
&= \frac{36,75}{\overline{\gamma}_{1e}} \int_0^\infty \left[\sum_{i=0}^{3}\binom{3}{i}(-1)^i e^{\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}} i\right)} e^{\left(-\frac{2^{2R_s}\gamma_{1e}}{\overline{\gamma}_{1D}} i - \frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right)}\right] \left[1-e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}}\right]^2 d\gamma_{1e} \\
&= 36,75 \sum_{i=0}^{3}\binom{3}{i}(-1)^i e^{\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}} i\right)} \mathrm{B}\left(\frac{2^{2R_s}\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}} i + 1, 3\right).
\end{aligned} \tag{42}$$

A.5 PROVA DA EQUAÇÃO (24)

Sabendo que a pdf de γ_{1D} e γ_{1e} são dadas respectivamente por:

$$p_{\gamma_{1D}}(\gamma_{1D}) = \frac{10,5}{\overline{\gamma}_{1D}}\left[1-\exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^2 \exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right), \tag{43}$$

$$p_{\gamma_{1e}}(\gamma_{1e}) = \frac{1}{\overline{\gamma}_{1e}} \exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right), \tag{44}$$

a probabilidade de existência da capacidade de sigilo para o caso DNC-Dumb é então obtida como segue:

$$\begin{aligned}
\Pr\{C_{s,\text{DNC Dumb}} > 0\} &= \Pr\{\gamma_{1D} > \gamma_{1e}\} \\
&= \int_0^\infty \int_0^{\gamma_{1D}} p_{\gamma_{1D}}(\gamma_{1D}) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} d\gamma_{1D} \\
&= \int_0^\infty p_{\gamma_{1D}}(\gamma_{1D}) \left(\int_0^{\gamma_{1D}} p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} \right) d\gamma_{1D} \\
&= \int_0^\infty p_{\gamma_{1D}}(\gamma_{1D}) F_{\gamma_{1e}}(\gamma_{1D}) d\gamma_{1D} \\
&= \int_0^\infty \frac{10,5}{\overline{\gamma}_{1D}} \left[1 - e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}}\right]^2 e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}} \left[1 - e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1e}}}\right] d\gamma_{1D} \\
&= \frac{10,5}{\overline{\gamma}_{1D}} \int_0^\infty \left[\sum_{i=0}^{2} \binom{2}{i} (-1)^i e^{-(i+1)\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}}\right] \left[1 - e^{-\frac{\gamma_{1D}}{\overline{\gamma}_{1e}}}\right] d\gamma_{1D} \\
&= \frac{10,5\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}} \sum_{i=0}^{2} \binom{2}{i} (-1)^i \mathrm{B}\left(\frac{\overline{\gamma}_{1e}}{\overline{\gamma}_{1D}}(i+1), 2\right).
\end{aligned} \tag{45}$$

A.6 PROVA DA EQUAÇÃO (25)

Sabendo que a pdf de γ_{1D} e γ_{1e} são dadas respectivamente por:

$$p_{\gamma_{1D}}(\gamma_{1D}) = \frac{10,5}{\overline{\gamma}_{1D}} \left[1 - \exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right)\right]^2 \exp\left(-\frac{\gamma_{1D}}{\overline{\gamma}_{1D}}\right), \tag{46}$$

$$p_{\gamma_{1e}}(\gamma_{1e}) = \frac{1}{\overline{\gamma}_{1e}} \exp\left(-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}\right), \tag{47}$$

a probabilidade de *outage* com restrições de sigilo para o caso DNC-Dumb é então obtida como segue:

$$
\begin{aligned}
\mathscr{P}_{so,\text{DNC Dumb}}(R_s) &= \Pr\{C_s < R_s\} \\
&= \Pr\left\{\gamma_{1D} < 2^{2R_s}(1+\gamma_{1e}) - 1\right\} \\
&= \Pr\{\gamma_{1D} < \gamma_U\} \\
&= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1D},\gamma_{1e}}(\gamma_{1D},\gamma_{1e}) d\gamma_{1D} d\gamma_{1e} \\
&= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1D}}(\gamma_{1D}) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1D} d\gamma_{1e} \\
&= \int_0^\infty \left(\int_0^{\gamma_U} p_{\gamma_{1D}}(\gamma_{1D}) d\gamma_{1D} \right) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} \\
&= \int_0^\infty F_{\gamma_{1D}}(\gamma_U) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e} \\
&= \int_0^\infty 3,5 \left[1 - e^{\frac{\gamma_U}{\overline{\gamma}_{1D}}}\right]^3 \frac{1}{\overline{\gamma}_{1e}} e^{\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\
&= \frac{3,5}{\overline{\gamma}_{1e}} \int_0^\infty \left[1 - e^{-\frac{2^{2R_s}-1}{-\overline{\gamma}_{1D}}} e^{-\frac{2^{2R_s}\gamma_{1e}}{\overline{\gamma}_{1D}}}\right]^3 e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\
&= \frac{3,5\overline{\gamma}_{1D}}{2^{2R_s}\overline{\gamma}_{1e}} e^{\left(-\frac{2^{2R_s}-1}{\overline{\gamma}_{1D}}\right)} B\left(\frac{\overline{\gamma}_{1D}}{\overline{\gamma}_{1e}2^{2R_s}}, 4\right).
\end{aligned}
\tag{48}
$$