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

FÁBIO CÉSAR SCHUARTZ

MÚLTIPLAS ANTENAS COMO ALTERNATIVA PARA AUMENTAR A TAXA DE EXTRAÇÃO DE CHAVES SECRETAS EM REDES VEICULARES COM DESVANECIMENTO LENTO

DISSERTAÇÃO

CURITIBA

2016

FÁBIO CÉSAR SCHUARTZ

MÚLTIPLAS ANTENAS COMO ALTERNATIVA PARA AUMENTAR A TAXA DE EXTRAÇÃO DE CHAVES SECRETAS EM REDES VEICULARES COM DESVANECIMENTO LENTO

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

Coorientador: Prof. Dr. Richard Demo Souza

CURITIBA

2016

Dados Internacionais de Catalogação na Publicação

S383m
2016

Schuartz, Fábio César
Múltiplas antenas como alternativa para aumentar a taxa de extração de chaves secretas em redes veiculares com desvanecimento lento / Fábio César Schuartz.-- 2016.
54 f.: il.; 30 cm

Texto em português, com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Curitiba, 2016.
Bibliografia: f. 46-48.

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

CDD: Ed. 22 -- 621.3

Biblioteca Central da UTFPR, Câmpus Curitiba

Título da Dissertação Nº. 702

Múltiplas Antenas como Alternativa para Aumentar a Taxa de Extração de Chaves Secretas em Redes Veiculares com Desvanecimento Lento

por

Fábio César Schuartz

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

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de MESTRE EM CIÊNCIAS – Área de Concentração: **Telecomunicações e Redes** do Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial – CPGEI – da Universidade Tecnológica Federal do Paraná – UTFPR, às **14**:**00h** do dia **04 de novembro de 2015**. 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. Guilherme Luiz Moritz
(UTFPR)

Visto da coordenação:

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

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

Dedico este trabalho à minha família, a minha mãe Luzmari e minha irmã Taissa, pelo apoio e tranquilidade proporcionados durante este desafio. Dedico ainda a todos meus amigos de coração, que fazem parte da minha família, embora não pelo sangue, mas pela amizade verdadeira. Roberto Chu, Amadeu e Guilherme Beduschi, Rafael Chagas, Renato Gouveia, entre inúmeros outros, vocês são o motivo de sempre seguir em frente, não importam os obstáculos.

AGRADECIMENTOS

Agradeço imensamente aos professores João Luiz Rebelatto e Richard Demo Souza, pela paciência, orientação e ajuda durante o trajeto deste mestrado.

RESUMO

SCHUARTZ, Fábio César. MÚLTIPLAS ANTENAS COMO ALTERNATIVA PARA AUMENTAR A TAXA DE EXTRAÇÃO DE CHAVES SECRETAS EM REDES VEICULARES COM DESVANECIMENTO LENTO. 54 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

A comunicação em redes veiculares *ad hoc* (VANETs) é comumente dividida em dois cenários, chamados veículo-a-veículo (V2V) e veículo-a-infraestrutura (V2I). Objetivando estabelecer uma comunicação segura contra espiões, trabalhos recentes tem proposto a troca de chaves secretas baseado na variação da força do sinal recebido (RSS). Entretanto, o bom desempenho de tal método depende da taxa de variação do canal, sendo mais apropriado a cenários em que o canal varia rapidamente, como geralmente é o caso da comunicação V2V. Já na comunicação V2I, o canal normalmente possui desvanecimento lento. Neste trabalho, é proposta a utilização de múltiplas antenas com o intuito de gerar artificialmente um canal de desvanecimento rápido, permitindo assim a extração de chaves secretas através da RSS em um cenário V2I. Análises numéricas mostram que o modelo proposto pode obter desempenho superior, em termos de taxa de extração de *bits* secretos, do que o modelo de salto em frequência proposto na literatura.

Palavras-chave: Concordância de chave, segurança, redes veiculares, antenas múltiplas, geração de chave secreta, desvanecimento rápido artificial

ABSTRACT

SCHUARTZ, Fábio César. MULTIPLE ANTENNAS AS AN ALTERNATIVE TO INCREASE SECRET KEY EXTRACTION RATE IN VEHICULAR NETWORKS WITH SLOW FADE. 54 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

The communication in vehicular ad hoc networks (VANETs) is commonly divided in two scenarios, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Aiming at establishing secure communication against eavesdroppers, recent works have proposed the exchange of secret keys based on the variation in received signal strength (RSS). However, the performance of such scheme depends on the channel variation rate, being more appropriate for scenarios where the channel varies rapidly, as is usually the case with V2V communication. In the communication V2I, the channel commonly undergoes slow fading. In this work we propose the use of multiple antennas in order to artificially generate a fast fading channel so that the extraction of secret keys out of the RSS becomes feasible in a V2I scenario. Numerical analysis shows that the proposed model can outperform, in terms of secret bit extraction rate, a frequency hopping-based method proposed in the literature.

Keywords: Key agreement, security, vehicular networks, multiple antennas, secret key generation, artificial fast fading

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACK	*do inglês, Acknowledgment*
AFF	*do inglês, Artificial Fast Fading*
CSI	*do inglês, Channel State information*
D-RSS	*do inglês, Differential RSS*
DFH	*do inglês, Dynamic Frequency Hopping*
DSRC	*do inglês, Dedicated Short-Range Communications*
ESPAR	*do inglês, Electronically Steerable Parasitic Array Radiator*
FH	*do inglês, Frequency Hopping*
ITS	*do inglês, Intelligent Transportation System*
KTL	*do inglês, Karhunen-Loeve Transform*
LDPC	*do inglês, Low-Density Parity-Check*
MD-RSS	*do inglês, Multiple Differential Received Signal Strength*
MIMO	*do inglês, Multi-Input Multi-Output*
PKI	*do inglês, Public Key Infrastructure*
RSS	*do inglês, Received Signal Strength*
RSSI	*do inglês, Received Signal Strength Indicator*
RSU	*do inglês, RoadSide Unit*
SNR	*do inglês, Signal-to-Noise Ratio*
TES	*Taxa de extração segura*
TTP	*do inglês, Trusted Third Parties*
V2I	*do inglês, Vehicle-to-Infrastructure*
V2V	*do inglês, Vehicle-to-Vehicle*
VANET	*do inglês, Vehicular Ad hoc Network*
XOR	*do inglês, Exclusive OR*

LISTA DE SÍMBOLOS

A	RSU denominada Alice
B	Veículo legítimo denominado Bob
E	Observador passivo malicioso, denominado Eve
i	Nodo transmissor
j	Nodo receptor
$\mathbf{y}$	Quadro transmitido entre nodos
h_{ij}	Coeficiente de desvanecimento de canal do enlace entre os nodos i e j
$\mathbf{x}_i$	Vetor do sinal transmitido no instante de tempo t
$\mathbf{n}_j$	Ruído Gaussiano complexo de média zero
σ_j^2	Variança do ruído Gaussiano
λ_j	SNR instantânea observada na antena do nodo j
$\bar{\lambda}_j$	SNR média na antena do nodo j
ε	Estimação aproximada da pequena flutuação no canal
d	Número de segmentos utilizados na obtenção da média para remoção de pequenas flutuações
F	Média para remoção de pequenas flutuações
r_k	Valor de cada segmento (RSS) obtido em um instante de tempo distinto
b_s	*Bit* secreto
m	Número total de amostras RSS
T	Tempo de amostragem dos valores de RSS
c	Conjunto de canais disponíveis para comunicação
t_1	Tempo no intervalo 1 para Alice
t_1'	Tempo no intervalo 1 para Eve
p	Probabilidade de Alice e Bob estarem no mesmo canal
p_{ABE}	Probabilidade de Alice, Bob e Eve escolherem o mesmo canal
p_E	Probabilidade de Eve escutar a semente recebida por Bob
s	Número de sementes recebidas por Bob
z	Número de trocas realizadas entre Alice e Bob para formarem a chave secreta
P_Z	Função de probabilidade para Alice e Bob gerarema chave secreta no método FH
$N[Z]$	Número esperado de tentativas de trocas de sementes
p_{EF}	Probabilidade de Eve gerar a chave final
l	Tamanho da semente
h_{ij}^n	Ganho complexo do canal entre os nodos i e j da n-ésima antena
$\alpha_n(t)$	Fração de potência alocada para a n-ésima antena transmissora
$\theta_n(t)$	Deslocamento de fase aplicado ao sinal da n-ésima antena transmissora
$\mathbf{w}$	Sequência de *bits* secretos extraídos das m amostras
$\lvert\mathbf{w}\rvert$	Número total de *bits* secretos extraídos das m amostras
T_{FH}	Tempo total para formação da chave secreta

SUMÁRIO

1 INTRODUÇÃO

Com o aumento no volume de tráfego nas grandes cidades e rodovias, a utilização de um sistema inteligente avançado de informações rodoviárias capaz de monitorar os movimentos dos veículos torna-se importante para minimizar congestionamentos, acidentes e aumentar a segurança nas estradas. Uma rede VANET (*Vehicular Ad hoc Network*) pode ser utilizada para obter dados sobre o trânsito, tais como o volume de tráfego, tipo de veículos e rotas utilizadas por diferentes veículos para controlar o fluxo de tráfego e informar os veículos da rede sobre condições na rodovia, evitando acidentes e congestionamentos (NAFI; KHAN, 2012).

De acordo com Zan et al. (2013), um sistema geral de comunicação entre veículos inclui dois tipos de comunicação: a comunicação V2V (*Vehicle-to-Vehicle*) entre dois veículos e a V2I (*Vehicle-to-Infrastructure*) entre um veículo e uma infraestrutura. Na comunicação V2V, os dados privados são trocados entre dois veículos e na comunicação V2I um veículo estabelece comunicação com uma infraestrutura fixa instalada ao longo da rodovia - RSU (*RoadSide Unit*) - para obter ou enviar informações para um servidor de trânsito remoto. A Figura 1 ilustra uma rede de comunicação veicular. Ambas as comunicações V2V e V2I utilizam dispositivos de rádio com o protocolo DSRC (*Dedicated Short-Range Communications*), baseado no padrão 802.11p, que oferece alta taxa de dados para distâncias até 1000 metros (KENNEY, 2011). Cada RSU possui uma região de operação e quando um veículo atravessa esse limite de alcance, a próxima RSU passa a se comunicar com o veículo. Os carros, entretanto, podem se comunicar livremente entre regiões, respeitando apenas o limite de alcance dos seus dispositivos de rádio.

Para essas comunicações ocorrerem, são necessários protocolos de comunicação seguros que protejam a confidencialidade das informações. Assim, são gerados dois conjuntos separados de chaves secretas para serem usadas na comunicação V2V e na V2I. Isso permite, por exemplo, um veículo se comunicar com a central de trânsito e obter informações sobre uma faixa da rodovia através de uma chave secreta compartilhada entre o usuário e o servidor, evitando que esta conversa seja decodificada por outros usuários. Por outro lado, um veículo pode desejar informações sobre as condições de trânsito locais sem revelar sua posição exata para um servidor remoto, realizando assim uma comunicação entre veículos.

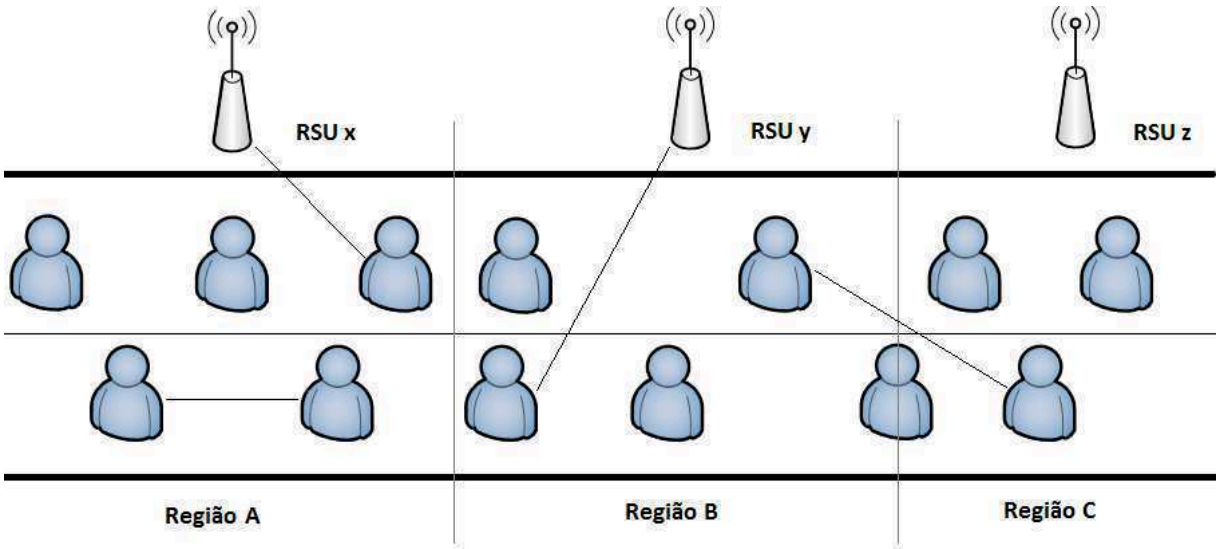

Figura 1: Exemplo da rede de comunicação veicular.
Fonte: (ZAN et al., 2013)

Protocolos tradicionais de concordância de chave incluem criptografia de chave pública e TTP (*Trusted Third Parties*) (PERRIG et al., 2002) para realizar o processo seguramente, tal como os protocolos Kerberos (STEINER; SCHILLER, 1988) e Otway-Rees (OTWAY; REES, 1987). Entretanto, ambos não se encaixam na comunicação V2V e V2I. Por exemplo, na comunicação V2V, não existe essa infraestrutura segura, com autoridade e confiança servindo como central de distribuição, pois a mobilidade dos nodos não é restrita, tornando a topologia da rede imprevisível. Ainda, não é seguro na comunicação V2I, pois mesmo que a infraestrutura esteja conectada a um servidor central de confiança, o procedimento de distribuição das chaves por canal sem fio não é seguro.

A criptografia de chave pública, embora seja um algoritmo forte de segurança, requer aplicações inteligentes e com poder computacional elevado, de alto custo-benifício, para serem utilizados em aplicações embarcadas, e sem considerar os custos energéticos, conforme diversos trabalhos apontam (CHAN, 2004; AL-SHURMAN; YOO, 2006). Outro fator negativo no protocolo de chaves públicas é a necessidade de troca de certificados em grande número.

Em Diffie e Hellman (1976), é apresentado um sistema de distribuição de chave pública que pode ser transformado em um sistema de autenticação de sentido único, onde seja fácil reconhecer o transmissor como autêntico, porém impossível para qualquer outro transmissor que não seja o transmissor legítimo de produzir a mensagem. Existem ainda outros algoritmos de chave pública conhecidos amplamente na literatura, tais como curva elíptica (KOBLITZ, 1998), algorítimo de assinatura digital e RSA. Porém, protocolos de chave pública exigem um

Tabela 1: Trabalhos baseados em criptografia de chave e protocolo de concordância de chaves, com suas principais características e desvantagens

TRABALHO	CARACTERÍSTICAS	DESVANTAGENS
Kerberos (STEINER; SCHILLER, 1988)	protegido contra *eavesdropping*	requer servidor central TTP pode ser comprometido requer conta de usuários
Otway-Rees (OTWAY; REES, 1987)	protegido contra *eavesdropping* detecta modificações	requer servidor central TTP pode ser comprometido
Diffie-Hellman (DIFFIE; HELLMAN, 1976)	protegido contra *eavesdropping* não pode ser quebrado computacionalmente	elevado número de certificados a serem trocados requer concordância prévia de certificados
Chan (CHAN, 2004)	não requer infraestrutura de suporte	requer pré-distribuição de chaves
Blom (BLOM, 1985)	utilização de uma chave mestre	requer pré-distribuição da chave mestre TTP pode ser comprometido
Eschennauer;Gligor (ESCHENAUER; GLIGOR, 2002)	protocolo simples de descoberta de chave	requer pré-distribuição da chave mestre

elevado número de certificados que necessitam ser trocados entre transmissor e receptor e os requerimentos para pré-distribuição dos mesmos podem não estar sempre disponíveis.

Ainda em Chan (2004), um método de pré-distribuição de chaves é apresentado, com um algoritmo auto-organizado e completamente distribuído, sem necessidade de qualquer infraestrutura de suporte. Entretanto, em uma rede veicular, os requisitos para pré-distribuição podem não existir, pois os carros podem se encontrar em um local onde não exista um TTP confiável para pré-distibuição de chaves. No trabalho de (BLOM, 1985), um sistema de geração de chave simétrica é apresentado, com cada par de usuários compartilhando uma chave mestre, distribuída de início por uma autoridade geradora de chaves. Em (ESCHENAUER; GLIGOR, 2002), um algoritmo de gerenciamento de chaves é proposto, baseado em chaves compartilhadas entre os nodos de um gráfico aleatório probabilístico, usando um protocolo simples de descoberta de chave compartilhada para a distribuição de chaves. Entretanto, o requesito necessário para pré-distribuição pode não estar sempre disponível. Por exemplo, na rede veicular, os carros (sem informações secretas compartilhadas inicialmente) podem se encontrar em um lugar onde possivelmente não exista um TTP confiável para pré-distribuição da chave.

A Tabela 1 apresenta de forma resumida os trabalhos baseados em criptografia de chave e protocolo de concordância de chaves, com suas principais características e desvantagens.

Nos trabalhos (ZAN et al., 2013; ZAN; GRUTESER, 2009; ZAN et al., 2012) são porpostos métodos não tradicionais para criar chaves secretas para as comunicações V2V e V2I. Os pontos principais das propostas são *reciprocidade* e *diversidade*. Reciprocidade representa o teorema da reciprocidade do canal, que descreve o fenômeno em que os nodos da comunicaçao situados nos dois extremos do canal irão observar características fortemente correlacionadas deste canal e a diversidade inclui as diversidades em frequência, espacial e temporal.

O conceito de usar características da camada física para gerencialmento de chaves foi apresentado inicialmente por (HERSHEY et al., 1995), onde três técnicas são apresentadas para estabelecer chaves criptográficas. Estas técnicas envolvem combinações de processamento

de sinais, codificação e o fenômeno da propagação. A primeira técnica é baseada no sistema criptográfico de chave pública. A segunda propõe utilizar as características de um canal de rádio urbano como uma variável criptográfica e a terceira apresenta um sistema criptográfico de chave pública que não é baseado na aritimética de campos finitos. Em (AONO et al., 2005), utilizou-se uma antena radiadora ESPAR (*Electronically Steerable Parasitic Array Radiator*) para obter o RSSI (*Received Signal Strength Indicator*), criando uma chave secreta baseada no valor médio dos RSSIs medidos. Trabalho complementar pode ser encontrado em (KITAURA et al., 2006). Porém, todos os trabalhos necessitam de medições precisas no receptor e, considerando a diferença entre diversos dispositivos de comunicação individuais, a medição precisa e uniforme não pode ser garantida para todos os receptores, mesmo considerando a teorema da reciprocidade do canal.

Em Ye et al. (2010), é demonstrado como o estado do canal entre um transmissor e um receptor, ambos sem fio, podem ser usados como base para construção de protocolos práticos de geração de chave secreta entre dois participantes. Outro método de extração de chaves secretas através da aleatoriedade inerente nos canais sem fio é proposto por (LIU et al., 2012). Este método utiliza um sistema de geração de chave baseado nos códigos LDPC (*Low-Density Parity-Check*).

Transmissões MIMO (*Multi-Input Multi-Output*) aleatórias, onde o receptor pode detectar sinais sem o conhecimento do canal devido a tarefa de estimar o canal ser realizada pelo transmissor - o qual pode então ajustar a transmissão MIMO, podem atingir a forma mais forte de segurança da informação, conforme (LI; RATAZZI, 2005), onde em seu trabalho é proposto um algoritmo para gerar aleatoriamente coeficientes de transmissão MIMO.

O método *beamforming* aleatório foi proposto para deteriorar o desempenho da taxa de erro de *bit* do espião através da corrupção do seu sinal recebido induzindo um ruído multiplicativo variante no tempo. *Beamforming* é alcançado ao escolher a potência e fase de transmissão de cada antena, resultando em campos de radiação que se superpõem construtivamente em algumas direções e destrutivamente em outras direções (BETTSTETTER et al., 2005). Em seu trabalho, (WANG et al., 2015) denomina a taxa de segredo de tal método como AFF (*Artificial Fast Fading*) e provê uma análise compreensiva da taxa de segredo para a mesma.

Em Zan et al. (2013), são propostos dois métodos de concordância de chaves, para os modelos V2V e V2I. O modelo apresentado para o V2V utiliza a extração de chave secreta utilizando a variação na força do sinal recebido. Neste ambiente, a taxa de bits secretos extraídos depende da taxa de variação do canal, que é grande o suficiente. A segurança neste método é garantida pela suposição que a correlação entre o transmissor e o receptor legítimo é maior

Tabela 2: Trabalhos baseados em concordância de chaves utilizando a camada física, com suas principais características e desvantagens

TRABALHO	CARACTERÍSTICAS	DESVANTAGENS
Hershey (HERSHEY et al., 1995)	uso de sistema criptográfico de chave pública	requer medições precisas no receptor
Aono (AONO et al., 2005)	utilização de antena radiadora ESPAR	requer medições precisas no receptor
Ye (YE et al., 2010)	utilização do CSI para geração de chaves	requer medições precisas no receptor
Liu (LIU et al., 2012)	geração de chaves baseado nos códigos LDPC	requer medições precisas no receptor
Li;Ratazzi (LI; RATAZZI, 2005)	transmissor estima o canal garante a segurança da informação	múltiplas antenas no receptor
Bettstetter (BETTSTETTER et al., 2005)	reduz o desempenho de extração de *bits* pelo nodo espião ao introduzir ruídos destrutivos no canal	necessário cálculos pesados de potência e fase de transmissão de cada antena
Zan (ZAN et al., 2013)	uso de salto em frequência aleatório	baixa taxa de geração de chaves

que a correlação entre o transmissor e um receptor espião, resultando na vantagem do receptor legítimo sobre o receptor espião. No modelo V2I, um dos participantes (RSU) é fixo e o ambiente de desvanecimento de múltiplos caminhos (Rayleigh) pode não existir (a característica do canal pode ser dominada pela propagação com linhas de visada), resultando que o método de extração da chave secreta proposto no V2V não é adequado por se tratar de um canal variando lentamente. Assim, os autores propõem o método FH (*Frequency Hopping*) como solução para o ambiente V2I. Neste método, o transmissor e o receptor legítimo selecionam um canal aleatoriamente para enviar e receber, respectivamente. Se ambos escolherem o mesmo canal, um pedaço da informação da chave é transmitida. Após vários segmentos enviados com sucesso, a chave secreta é formada. Entretanto, se o receptor espião escolher corretamente os mesmos canais que o transmissor e o receptor legítimo todas as vezes, o receptor espião também consegue recuperar a chave secreta.

Os trabalhos baseados em concordância de chaves utilizando a camada física, com suas principais características e desvantagens, são apresentados de forma resumida na Tabela 2.

Em Viswanath et al. (2002), é proposto o uso de múltiplas antenas transmissoras em um ambiente com pouco espalhamento ou desvanecimento lento para induzir flutuações rápidas e grandes no canal, objetivando o aumento na diversidade de multiusuários. A quantidade de diversidade depende da taxa e da faixa dinâmica das flutuações do canal e, em ambientes onde as flutuações do canal são pequenas, o ganho de diversidade é incrementado ao induzir flutuações maiores e mais rapidamente. A utilização de múltiplas antenas transmissoras na estação base, preservando a potência total transmitida, é transparente ao receptor e o ambiente é artificialmente transformado em um ambiente de desvanecimento rápido, com a taxa de flutuação do canal aumentada.

1.1 MOTIVAÇÃO

Um sistema de comunicação veicular pode ser muito efetivo na prevenção de acidentes e congestionamento de trânsito quando cada veículo tenta resolver esses problemas individualmente. Hoje em dia, uma atenção especial é dada em tecnologias que podem reduzir os acidentes de trânsito, tais como as redes VANETs e o ITS (*Intelligent Transportation System*), que inclui controle automático para aviso e desvio de colisões (DORLE et al., 2009). Entretanto, embora existam inúmeras vantagens em uma rede VANET, problemas de segurança na transmissão de informações devem ser resolvidos para assegurar que a identidade, posição e informações sobre o movimento de um veículo em específico não possa ser obtido por terceiros (ZHANG et al., 2008). Vários métodos tradicionais de concordância de chaves existem, porém os mesmos apresentam restrições que os tornam impraticáveis no cenário V2I, devido a necessidade de trocas periódicas de chaves de segurança através de uma comunicação segura e a infraestrutura necessária para tal pode não existir ao longo de uma rodovia. Por isso, é proposto um método de concordância de chaves secretas através da informação da força do sinal recebido, utilizando múltiplas antenas, como uma alternativa ao método de *frequency hopping*, proposto em (ZAN et al., 2013), resultando em uma taxa maior de extração de *bits* secretos seguros em um sistema de comunicação veicular V2I.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Propor um esquema de extração de chaves secretas, utilizando a força do sinal recebido e múltiplas antenas no transmissor, que seja mais eficiente em termos de taxa de extração de *bits* secretos seguros que o esquema FH proposto na literatura (ZAN et al., 2013), para o ambiente V2I.

1.2.2 OBJETIVOS ESPECÍFICOS

- Obter a taxa de extração de *bits* secretos seguros através da RSSI, com múltiplas antenas no transmissor.
- Demonstrar a maior eficiência na taxa de extração de *bits* secretos seguros, comparando os resultados obtidos pelo método proposto com o método FH.
- Verificar a influência de parâmetros, tais como o número de antenas no transmissor e o tamanho da chave secreta, no desempenho do esquema proposto.

1.2.3 RESULTADOS OBTIDOS

Neste trabalho foram considerados diversos parâmetros para a avaliação dos métodos de concordância de chaves secretas em um ambiente de comunicação V2I. Para o esquema proposto, foram analisadas as influências causadas pelo número de antenas no transmissor e a correlação entre os canais transmissor e receptor, obtendo-se diferentes taxas de extração. No esquema FH, variaram-se o número de canais, o número de sementes utilizadas para compor a chave secreta e o tamanho das sementes. Resultados simulados mostram que em todos os cenários considerados, o modelo proposto, quando comparado ao modelo FH, apresenta uma taxa maior de extração de *bits* secretos seguros.

O artigo abaixo foi elaborado com os resultados deste mestrado e apresentado no XXXIII Simpósio Brasileiro de Telecomunicações (SBrT'15).

(SCHUARTZ, F. C. ; REBELATTO, J. L. ; SOUZA, R. D. Artificial Fast Fading-Aided Key Agreement Algorithm for Vehicle-to-Infrastructure Networks. In: **XXXIII Simpósio Brasileiro de Telecomunicações (SBrT'15)**, 2015, Juiz de Fora, MG.).

2 PRELIMINARES

2.1 MODELO DO SISTEMA

A comunicação V2V pode ocorrer quando dois veículos estão dentro da área de alcance um do outro. Um veículo realiza a comunicação V2I através das RSUs, sendo que cada RSU cobre apenas um segmento da rodovia, chamado de *região*. Quando os veículos estão na mesma região, eles se comunicam com a mesma RSU.

Assumem-se dois tipos de adversários na comunicação veicular. O primeiro está interessado em conhecer o conteúdo da comunicação privada entre dois veículos. Este adversário pode ser qualquer outro veículo na rodovia desde que não seja um dos veículos trocando informações. Pode ainda ser o servidor de tráfego, controlando todas as RSUs para monitorar a comunicação entre dois veículos. O segundo tipo de adversário está interessado em escutar o conteúdo da comunicação entre um veículo e o servidor. Neste caso, o espião não pode ser nem o carro envolvido na comunicação nem o servidor ou as RSUs controladas por este servidor. Ambos os adversários serão demominados *Eve* para fins de simplificação. Por último, nenhum dos adversários está interessado em interromper o processo de concordância das chaves.

Neste trabalho, considera-se o cenário V2I composto de três nodos: uma RSU (chamada de Alice - A), um veículo legítimo (chamado Bob - B) e um observador passivo malicioso (denominado Eve - E), conforme ilustrado na Figura 2. Todos os dispositivos participantes podem comunicar em canais múltiplos sem interferência, mas somente em um único canal, em um tempo determinado. Considera-se que o equipamento do veículo espião é similar aos equipamentos da RSU e do veículo legítimo, pois devido a geração de chaves secretas usando a aleatoriedade do canal alcançar o *information-theoretical secrecy* (DIFFIE; HELLMAN, 1976), a segurança não depende do poder computacional de Eve. Ainda, a RSU e o veículo legítimo desejam estabelecer uma chave secreta sem nenhuma informação anterior compartilhada.

O quadro transmitido pelo nodo $i \in \{A,B\}$ e recebido pelo nodo $j \in \{A,B,E\}, i \neq j$ é dado por:

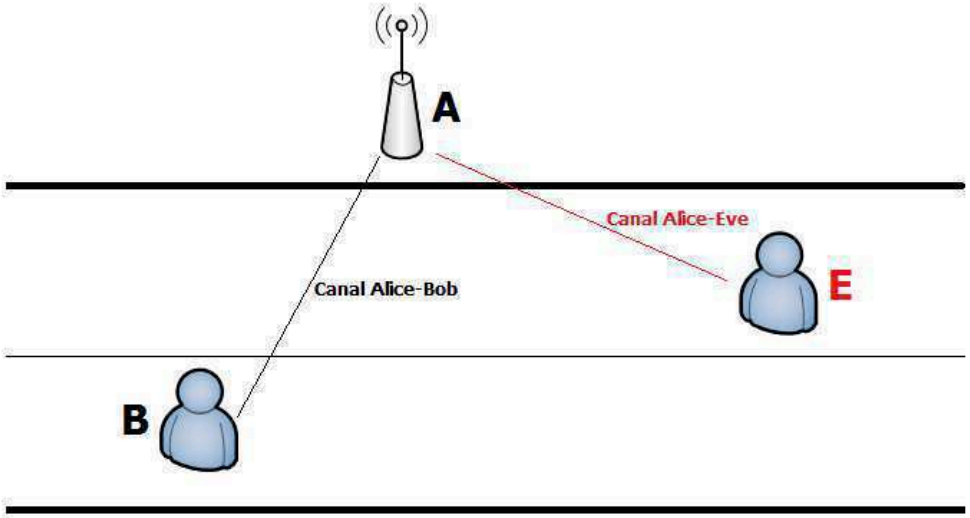

Figura 2: Ambiente V2I composto de três nodos: uma RSU (A), um veículo legítimo (B) e um observador passivo malicioso (E).

Fonte: Autoria própria

$$\mathbf{y}_j(t) = h_{ij}(t)\,\mathbf{x}_i(t) + \mathbf{n}_j(t), \tag{1}$$

em que $h_{ij}(t)$ é o coeficiente de desvanecimento, cuja envoltória é modelada como uma variável aleatória com distribuição Rayleigh independente e identicamente distribuída e que muda independentemente de quadro a quadro; $\mathbf{x}_i(t)$ é o vetor do sinal transmitido no instante de tempo t; e $\mathbf{n}_j(t)$ é o ruído gaussiano complexo de média zero com variança σ_j^2.

A relação sinal-ruído (SNR, do inglês *Signal-to-Noise Ratio*) instantânea observada na antena do nodo j é $\lambda_j = \bar{\lambda}_j |h_j|^2$, onde $\bar{\lambda}_j = P/(d_j^{\alpha}\sigma_j^2)$ é a SNR média na antena do nodo j.

2.2 METODOLOGIA PARA GERAÇÃO DE CHAVES SECRETAS

Devido suas características atrativas de simplicidade e devido à segurança depender apenas da teoria da informação (DIFFIE; HELLMAN, 1976), a geração de chaves na camada física ganhou grande atenção nos últimos anos (ZENG, 2015). O processo típico de geração de chaves inclui:

- Análise do canal;

- Extração aleatória;
- Quantização;
- Reconciliação;
- Amplificação de privacidade.

A *análise do canal* é o primeiro passo no processo de geração da chave secreta, onde medidas da RSS do canal são coletadas por Alice e Bob. No segundo passo, *extração aleatória*, Alice e Bob extraem a aleatoriedade causada pelo desvanecimento do canal. A fase de *quantização* é o processo de converter uma sequência de medidas da RSS em uma sequência de *bits*. No quarto passo, chamado *reconciliação*, Alice e Bob trocam informações de paridade para localizar e corrigir quaisquer erros na sequência de *bits* quantizados, causados por ruídos, interferências, variações na construção dos equipamentos, natureza da comunicação *half-duplex*, etc. A última fase, *amplificação de privacidade*, utiliza funções matemáticas para gerar sequências de *bits* menores, com o objetivo de aumentar a entropia da comunicação (PREMNATH et al., 2013, 2014; ZENG, 2015). Uma descrição mais detalhada da metodologia é apresentação no apêndice A.

Neste trabalho, as fases de análise do canal e de extração aleatória são substituídas por um conjunto de valores da RSS geradas aleatoriamente, conforme o grau de similaridade estipulado entre os canais Alice-Bob e Alice-Eve. A fase de reconciliação é realizada em duas transmissões. Inicialmente Alice informa Bob quais *bits* puderam ser extraídos por ela e Bob retorna à Alice a lista final de quais *bits* ambos concordam na extração. Os *bits* que não puderam ser extraídos por Alice e Bob são descartados, reduzindo, assim, a sobrecarga durante a fase de reconciliação. A fase de amplificação de privacidade não é utilizada neste modelo proposto, pois não são trocadas informações adicionais de paridade durante a fase de reconciliação (os *bits* errados na sequência serão descartados e não corrigidos).

2.3 ALGORITMO DE CONCORDÂNCIA DE CHAVE NA COMUNICAÇÃO V2V

O modelo para concordância de chaves D-RSS, proposto em (ZAN et al., 2013), é baseado no teorema da reciprocidade do canal e na propriedade da descorrelação espacial. O teorema da reciprocidade do canal define que $h_{ij}(t)$ é altamente correlacionada com $h_{ji}(t)$ e a descorrelação espacial é a propriedade em que $h_{ij}(t)$ é descorrelacionado de $h_{iz}(t)$, desde que $j \neq z$. Com o passar do tempo, a característica do canal sofre variação, resultando em uma força do sinal recebido diferente a cada instante de tempo. Realizando medições da força do sinal

recebido a cada instante, é possível extrair um *bit* secreto 0 ou 1 de acordo com uma diminuição ou aumento do valor do sinal a cada dois instantes de tempo distintos. A taxa de extração de chaves depende da taxa de variação do canal, que, neste caso, é rápida. Esta rápida variação do canal ocorre devido ao movimento dos veículos e pela propagação de múltiplos caminhos causando grande desvanecimento, resultando em um modelo de canal que não é puramente de desvanecimento *Rayleigh* (WEIXIN et al., 2006).

A reciprocidade do canal descreve o fenômeno no qual os nodos de comunicação em cada extremidade do canal observam características semelhantes do canal, tais como a resposta ao impulso do canal ou o valor da força do sinal recebido (RSS). A Figura 3 mostra um período onde o RSS foi coletado dentro de um ambiente de múltiplos caminhos (ZAN et al., 2013).

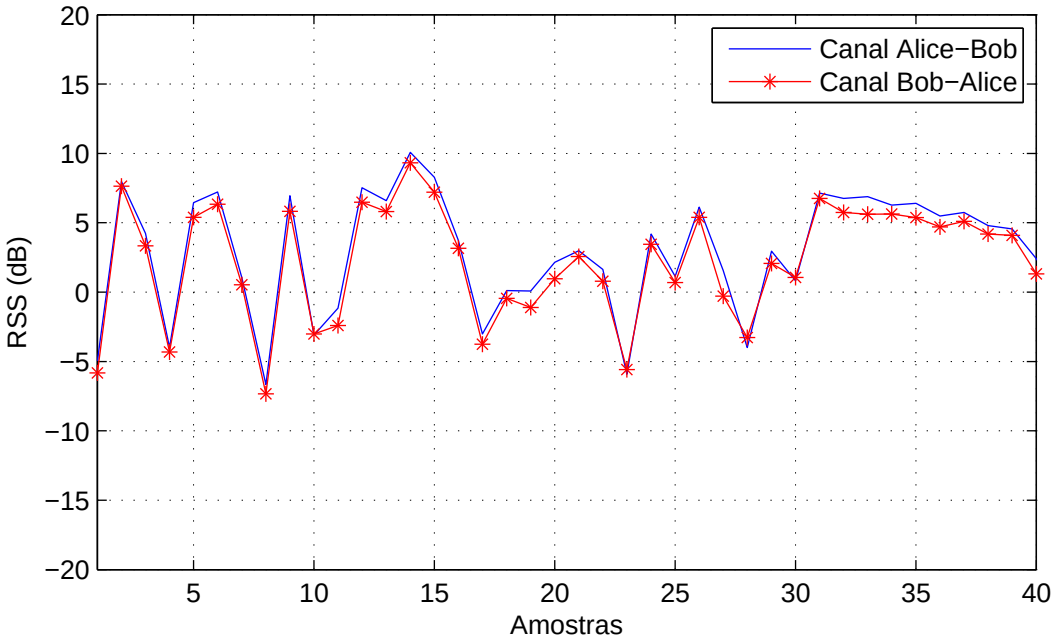

Figura 3: Exemplo da reciprocidade do canal.

Fonte: (ZAN et al., 2013)

Neste exemplo, Alice e Bob transmitem alternadamente sinais sem fio para cada um em um ambiente de múltiplos caminhos enquanto se movimentam em baixa velocidade (cerca de um metro por segundo). Ambos Alice e Bob verificam o canal e realizam medições do valor do RSS com uma taxa de amostragem igual a quarenta vezes por segundo. Devido a reciprocidade do canal, os valores observados por Alice e Bob, em cada valor amostrado do canal, são altamente correlacionados (aproximadamente 0,9120) (ZAN et al., 2013).

Entretanto, Eve, que está em uma localização diferente de Bob, observa valores diferentes de RSS do canal Alice-Eve, comparado aos obervados por Bob no canal Alice-Bob,

conforme ilustrado na Figura 4. Observa-se que as curvas são altamente descorrelacionados (aproximadamente 0,1937) devido a propriedade da descorrelação espacial em um canal de desvanecimento Rayleigh de múltiplos caminhos.

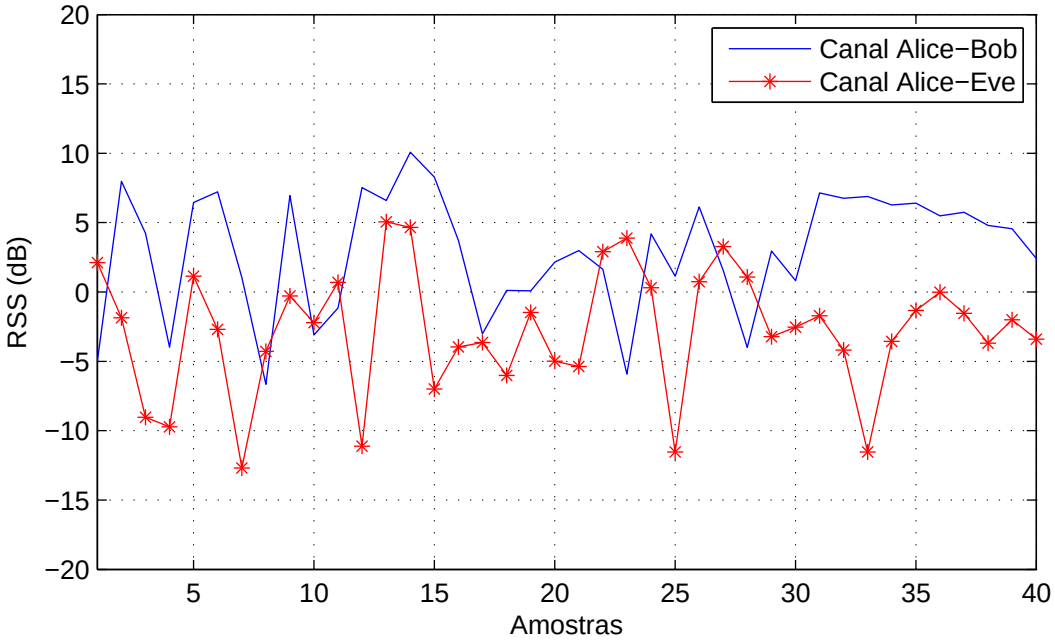

Figura 4: Exemplo da descorrelação espacial.

Fonte: (ZAN et al., 2013)

A Figura 5 mostra o modelo da comunicação V2V. Por causa da reciprocidade do canal, dois veículos - Alice e Bob - observam características semelhantes do canal. Assim, através de uma aproximação diferencial, eles podem extrair uma sequência de *bits* do canal em cada lado do mesmo. Esta sequência única de *bits* podem ser usadas para formar uma chave secreta.

O método de aproximação diferencial, proposto em (ZAN et al., 2013), determina o *bit* secreto baseado na diferença entre dois valores vizinhos do RSS. Neste método, ilustrado na Figura 6, quando um aumento entre dois valores do RSS é observado, um *bit* 1 é gerado e quando é observado um decrécimo, um *bit* 0 então é gerado. Esse aumento ou decréscimo deve ser maior que ε/d, onde ε é uma estimação aproximada da pequena flutuação no canal e d é o número de segmentos utilizados para se obter uma média para remoção de pequenas flutuações. (2) representa o cálculo da média:

$$F = (1/d)\sum_{k=1}^{d} r_k, \tag{2}$$

em que F é o valor médio para remoções de pequenas flutuações, utilizando d segmen-

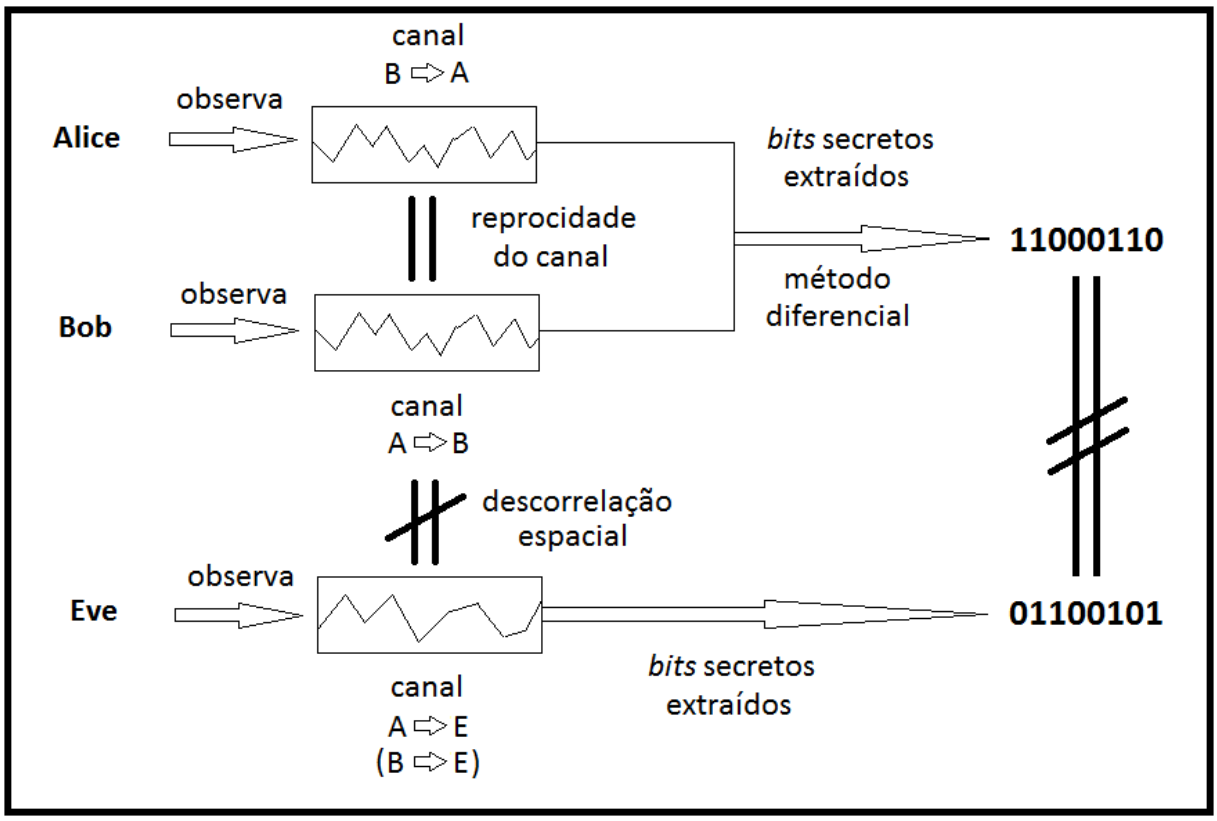

Figura 5: Modelo de concordância de chaves na comunicação V2V.

Fonte: (ZAN et al., 2013)

tos, e r_k, para $k = 1, 2, \ldots, d$, é o valor de cada segmento (RSS) obtido em um instante de tempo distinto.

Um *bit* secreto b_s é gerado por um nodo baseado na diferença entre os valores RSS de duas amostras consecutivas h_t e h_{t+1}, com $t = 1, 2, \ldots, m-1$, onde m é o número total de amostras RSS. O método para extração de *bits* é dado por:

$$b_s(t) = \begin{cases} 1, \text{ if } h_{t+1} - h_t > \varepsilon/d \\ 0, \text{ if } h_t - h_{t+1} > \varepsilon/d \\ \text{indeterminado, caso contrário} \end{cases} \tag{3}$$

Inicialmente, ambos Alice e Bob coletam, durante um período T, os valores do RSS usando sua taxa de amostragem máxima. Estas amostras coletadas são divididas em segmentos para melhorar a taxa de concordância de *bits*. O *bit* secreto é gerado ao comparar uma amostra do RSS de cada segmento. Se existir um aumento maior que um valor pré-determinado, será gerado um *bit* 1. Se o decréscimo for maior que este valor, será gerado um *bit* 0. Caso a variação

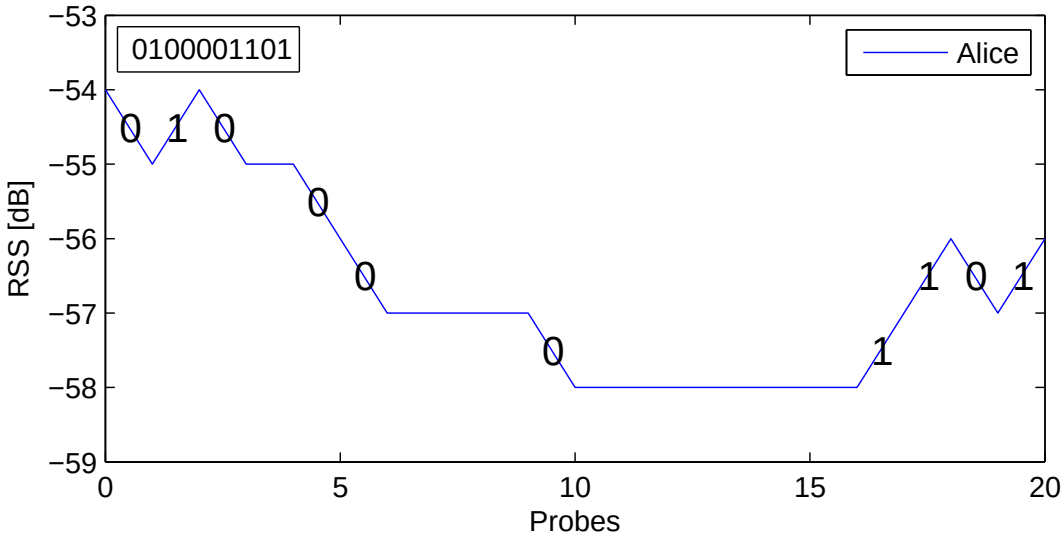

Figura 6: Exemplo de aproximação diferencial.

Fonte: (ZAN et al., 2013)

não seja suficientemente grande para gerar um *bit* 0 ou 1, nenhum valor pode ser inferido e será gerado um valor indefinido para este instante de tempo (representado pelo símbolo '?'). Na última fase, Alice manda para Bob somente as posições onde as amostragens foram utilizadas para gerar seus *bits* secretos. A partir destas posições, Bob escolhe as posições onde ele também conseguiu extrair *bits* secretos e responde à Alice.

Um exemplo deste método é ilustrado na Figura 7. Observa-se que Alice obtém uma sequência de *bits* 010?1?0??010 comparando o primeiro valor do RSS de cada segmento. Ela não está segura dos valores dos *bits* nas posições 4, 6, 8 e 9, na sequência. Então, ela envia para Bob uma mensagem com esta informação. Por outro lado, Bob obtém a sequência de *bits* 0?0?1?01?010. Em adição ao que Alice não tem certeza, Bob coloca a posição 2 na lista de *bits* incertos e informa Alice. Após remover os *bits* incertos, ambos Alice e Bob obtém a sequência final de *bits* 0010010. Mesmo obtendo as posições que serão utilizadas para formar esta sequência final de *bits*, Eve não conseguirá formar a mesma chave secreta, pois a sequência obtida por ela será composta por valores de *bits* diferentes dos observados por Alice e Bob, devido a alta descorrelação do canal Alice-Eve.

Eve, entretanto, deve obter os mesmos valores que Alice e Bob nas mesma posições escolhidas por ambos para compor a chave secreta. Falhar em extrair um único *bit* secreto impossibilita compor a chave necessária para comprometer a segurança na comunicação entre Alice e Bob. Assim, aumentando o número de *bits* necessários para compor a chave secreta, diminui a chance de Eve obter todos os *bits* nos instantes de tempo selecionados por Alice e

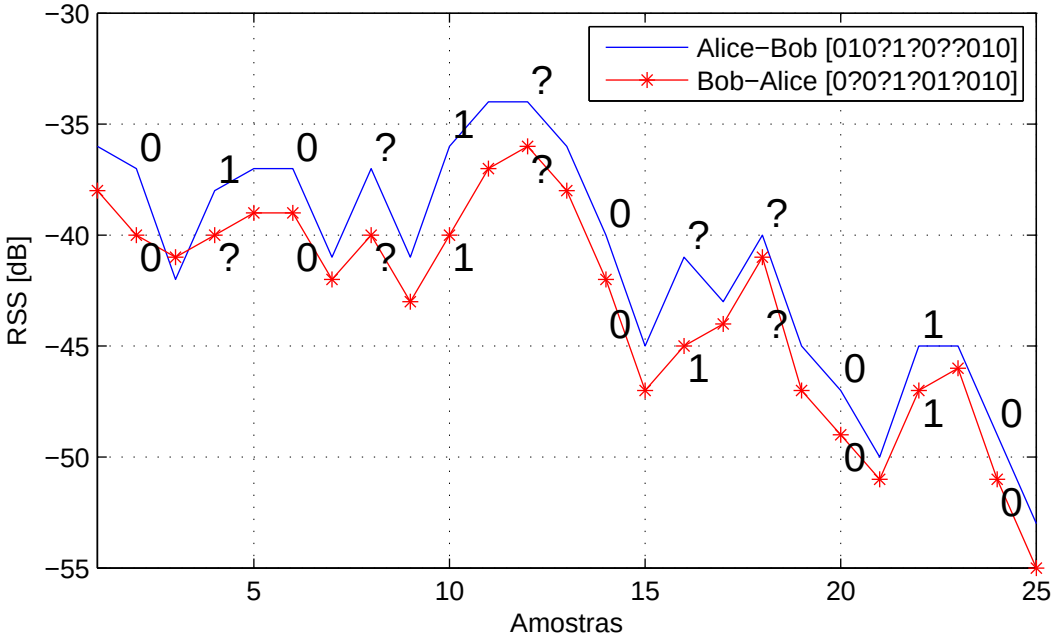

Figura 7: Exemplo do método de concordância de chaves.

Fonte: (ZAN et al., 2013)

Bob, reduzindo a probabilidade de obter a chave secreta.

Assim, é definido como **taxa de extração segura**, em *bits* por segundo, a máxima taxa que um método pode extrair *bits* secretos que são seguros de Eve, isto é, os *bits* que ambos Alice e Bob podem simultaneamente obter, mas Eve não. Cada chave secreta, ou semente, que foi obtida por Eve deve ser descartada, porém o tempo gasto para gerar a mesma possui impacto na taxa de extração.

2.4 ALGORITMO DE CONCORDÂNCIA DE CHAVE NA COMUNICAÇÃO V2I: SALTO EM FREQUÊNCIA

Os métodos tradicionais de concordância de chaves não servem para a comunicação segura V2I, conforme citado anteriormente. O método de concordância de chaves proposto no modelo V2V (ZAN et al., 2013) também não é adequado, pois requer um ambiente de desvanecimento rápido.

- O método requer um ambiente de desvanecimento Rayleigh de multiplos caminhos, o qual pode não existir na comunicação V2I. Por exemplo, quando um RSU for instalado em uma posição muito mais alta que os veículos na rodovia, a característica do canal é dominada pela propagação com linha de visada;

- Os RSUs são instalados em localizações fixas e podem não ser vistoriadas por pessoas durante longos períodos, permitindo um espião instalar algum dispositivo de escuta muito próximo do dispositivo da RSU por muito tempo antes de ser detectado;
- Se um adversário comprometer a RSU, a chave secreta não é mais um segredo. Assim, confiar em um RSU para gerar a chave secreta entre um veículo e o servidor não é uma maneira segura.

Neste cenário, a extração de *bits* secretos somente se torna possível em certos intervalos de tempo, quando o canal varia. Porém, a taxa de variação do canal é lenta, tornando o método D-RSS proposto para o ambiente V2V não eficiente em um cenário V2I.

Como alternativa, o modelo estudado por (ZAN et al., 2013) é baseado no método FH (*frequency hopping*). Neste modelo, ambas as partes do processo de concordância de chaves - Alice e Bob - aleatoriamente selecionam um canal para enviar e escutar, respectivamente, dentro do conjunto de c canais disponíveis para comunicação. Qualquer nodo pode comunicar em múltiplos canais sem sofrer interferência, porém cada nodo pode apenas escutar um único canal em um dado instante de tempo. Caso Alice e Bob estejam no mesmo canal, a informação chave, denominada como *semente*, é transferida com sucesso e Bob envia um sinal de reconhecimento (ACK) para Alice. Caso contrário, ocorre um *timeout*. Alice e Bob selecionam outros canais e repetem o processo, onde Alice utiliza diferentes sementes, para cada tentativa de transmissão. Se Alice receber um ACK, ela sabe que aquela semente será usada. Se não, a semente será descartada.

A Figura 8 descreve o método de concordância de chave para o V2I. Alice recebe uma semente de um RSU:x dentro da sua região pelo canal 1 no tempo t_1. Devido às diversidades de frequência, espaço e tempo, Eve pode não receber esta semente. Por exemplo, Eve pode não estar escutando o canal 1 no instante t_1 ou ela não está no alcance da comunicação do RSU:x que enviou a semente para Alice (regiões diferentes). Mais tarde, Eve pode receber uma semente do mesmo RSU:x que enviou uma semente para Alice anteriormente, mas no canal 3 e no tempo t_1' (tempo no intervalo 1 para Eve). Entretanto, estas sementes são completamente independentes.

A probabilidade que Alice e Bob estejam no mesmo canal é dada por:

$$p = \frac{1}{c}, \tag{4}$$

enquanto a probabildade de Alice, Bob e Eve escolherem o mesmo canal é:

$$p_{ABE} = \frac{1}{c^2}, \tag{5}$$

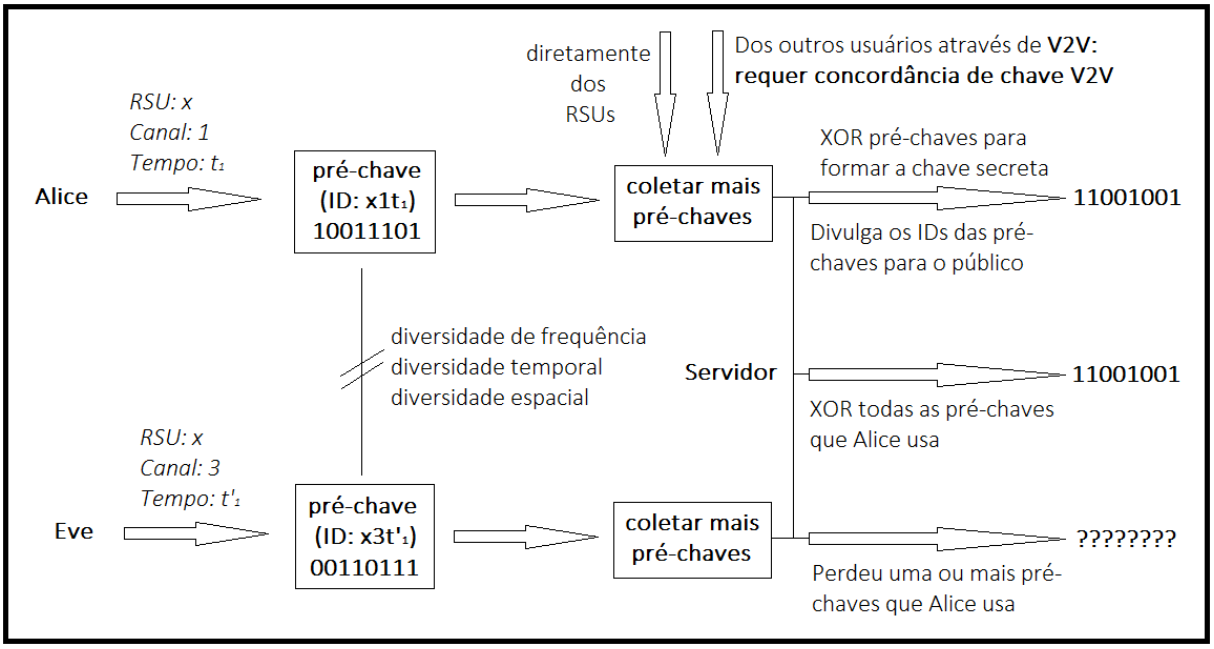

Figura 8: Modelo de concordância de chaves na comunicação V2I.

Fonte: (ZAN et al., 2013)

Para Eve obter a semente, ela necessita apenas escolher o mesmo canal que Bob (ZAN; GRUTESER, 2009; ZAN et al., 2013). A probabilidade de Eve escutar a semente é:

$$p_E = \frac{1}{c}, \tag{6}$$

De acordo com Zan et al. (2013), para obter um nível alto de segurança, o método necessita de um número grande de canais, o que é impraticável devido às restrições de equipamento, e o tempo necessário para uma semente ser trocada com sucesso aumenta com o número de canais. Para resolver este problema, é introduzido um método de múltiplas concordâncias, onde Alice e Bob repetirão a concordância de semente múltiplas vezes. O processo termina quando Bob recebe s sementes. No final, Bob seleciona todas as sementes e utiliza uma operação XOR para formar a chave secreta. Quais sementes foram utilizadas é conhecido pelo servidor, permitindo o mesmo executar uma operação XOR no mesmo conjunto de sementes e recuperar a chave. Por outro lado, se Eve perder uma única semente, ela não pode formar a mesma chave.

A segurança no FH é determinada pelo número de canais c disponíveis para transmissão e o número de sementes s usadas para compor a chave secreta. A função de probabilidade para Alice e Bob gerarem a chave secreta depois de z tentativas de trocas torna-se uma distribuição Pascal (ZAN; GRUTESER, 2009), dada por:

$$P_Z(z) = \binom{z-1}{s-1} (1/c)^s (1-(1/c))^{z-s}, \tag{7}$$

onde o número esperado de tentativas de trocas de sementes é:

$$N[Z] = \frac{s}{(1/c)} = s.c, \tag{8}$$

A probabilidade de Eve gerar a chave final é dada por:

$$p_{EF} = (1/c)^s, \tag{9}$$

Ainda, o tamanho da semente l determina a taxa de extração de *bit*, pois a semente inteira é transmitida em cada tentativa. A semente contendo mais *bits* irá gerar uma chave secreta com mais *bits*, logo, mais segura. Entretanto, mesmo quando Eve não consegue escutar a semente inteira, ela ainda pode obter alguma informação dos dados incompleto, conforme (ZAN; GRUTESER, 2009). Assim, quando mais longo for o tempo de transmissão, mais exposta estará a semente.

Alice continua coletando sementes ao longo da rodovia, assim como trocando sementes com outros veículos legítimos quando possível. No final, Alice seleciona algumas das sementes e utiliza uma operação XOR para formar a chave secreta. Quais sementes foram utilizadas é de conhecimento do servidor, permitindo ele executar uma operação XOR no mesmo conjunto de sementes e recuperar a chave. Por outro lado, se Eve perder uma única semente, ela não pode formar a mesma chave. Cada índice das sementes é único, o qual é a combinação do ID da RSU, o número do canal e do tempo (por exemplo, índice x_1t_1 e x_3t_1').

3 MODELO PROPOSTO

O trabalho proposto em Zan et al. (2013) para o sistema V2I utiliza o método FH devido às propriedades de diversidade espaço-temporal. Porém, a taxa de obtenção de chaves de segurança depende da probabildade da Alice e Bob estarem no mesmo canal, do tamanho da semente e do número de sementes utilizadas para gerar a chave. O modelo presume um ambiente onde as flutuações no canal são pequenas.

Este trabalho propõe utilizar múltiplas antenas no RSU para induzir artificialmente o desvanecimento rápido no ambiente V2I. O método proposto, o qual será referido como MD-RSS, adota o conceito de múltiplas antenas "*dumb*", conceito introduzido em (VISWANATH et al., 2002). O termo *dumb* vem do fato que as múltiplas antenas são completamente transparentes aos usuários (neste caso, os veículos). A Figura 9 mostra um exemplo de um canal de desvanecimento lento, antes e depois de ser aplicado o método MD-RSS.

Considerando um sistema com N antenas transmissoras na estação base e $h_{ij}^{n}(t)$ o ganho complexo do canal entre os nodos i e j da n-ésima antena, em um intervalo de tempo t. A RSU transmite o mesmo quadro $\mathbf{x}_i(t)$ para todas as antenas, depois de multiplicá-lo por um número complexo $\sqrt{\alpha_n(t)}e^{j\theta_n(t)}$ na antena n, para $n = 1, ..., N$, de tal forma que $\sum_{n=1}^{N} \alpha_n(t) = 1$, preservando o total de potência transmitida. Um exemplo é ilustrado na Figura 10, para o caso particular com $N = 2$.

O sinal recebido pelo usuário j é então dado por:

$$\mathbf{y}_j(t) = \left(\sum_{n=1}^{N} \sqrt{\alpha_n(t)} e^{j\theta_n(t)} h_{ij}^{n}(t) \right) \mathbf{x}_i(t) + \mathbf{n}_j(t), \tag{10}$$

onde $\alpha_n(t)$ representa as frações de potência alocadas para cada antena transmissora e $\theta_n(t)$ representa os deslocamentos de fase aplicados ao sinal, em cada antena, distribuídos uniformemente. O ganho do canal médio, visto pelo receptor j é:

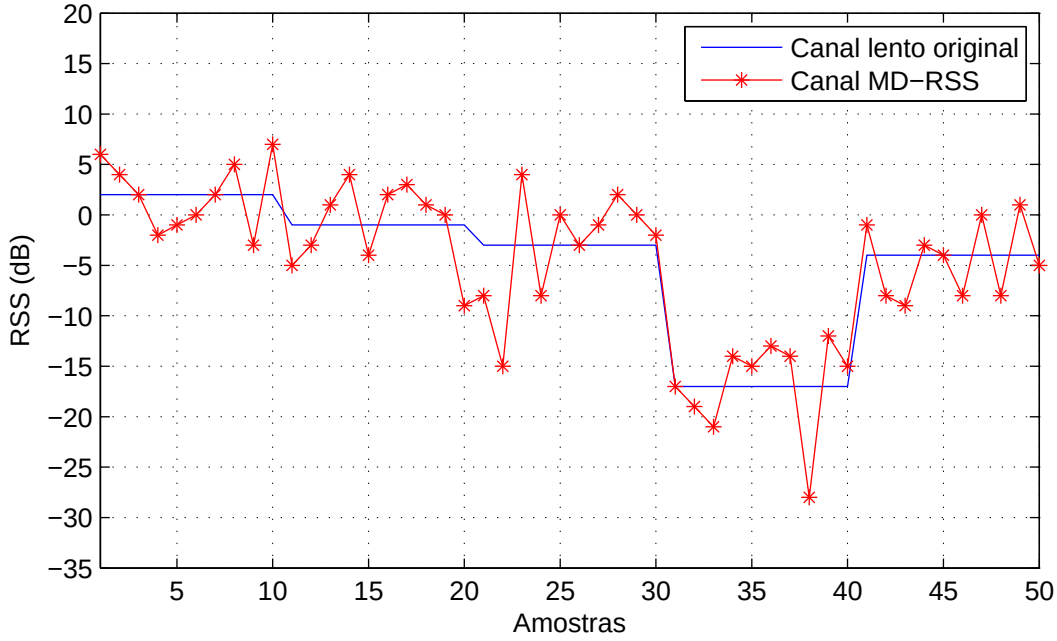

Figura 9: Exemplo de um canal, antes de depois de ser aplicado o método MD-RSS para transformar um canal lento em um canal de desvanecimento rápido.

Fonte: Autoria própria

$$h_{ij}(t) = \sum_{n=1}^{N} \sqrt{\alpha_n(t)} e^{j\theta_n(t)} h_{ij}^n(t). \tag{11}$$

Assim, variando os valores de $\alpha_n(t)$ e $\theta_n(t)$ durante o tempo - $\alpha_n(t)$ varia entre 0 e 1 e $\theta_n(t)$ entre 0 e 2π, pode-se induzir flutuações no canal médio mesmo se as flutuações dos ganhos de canal $h_{ij}(t)$ forem muito pequenas. A taxa de variação de $\alpha_n(t)$ e $\theta_n(t)$ no tempo é definida na especificação do sistema, devendo ser suficientemente lenta e acontecendo em uma escala de tempo que permita o canal ser estimado confiavelmente pelos usuários e com o SNR realimentado. Não é necessária a medição dos ganhos de canal $h_{ij}(t)$ individualmente - fase ou magnitude, pois a existência de múltiplas antenas transmissoras é completamente transparente ao receptor, onde um único sinal piloto é necessário para medição do canal. Os símbolos pilotos são repetidos por cada antena transmissora, exatamente como os símbolos de dados.

Fatores influenciando a segurança no modelo RSS com múltiplas antenas são os níveis de correlação do canal entre Alice e Bob e entre Alice e Eve, o tamanho, em *bits*, da chave secreta e o nível de segurança da privacidade. A correlação do canal entre Alice e Bob determina a taxa de extração dos *bits* secretos. No método RSS com múltiplas antenas, a correlação do canal entre Alice e Eve irá determinar em quais pontos de tempo Eve pode extrair *bits* secretos

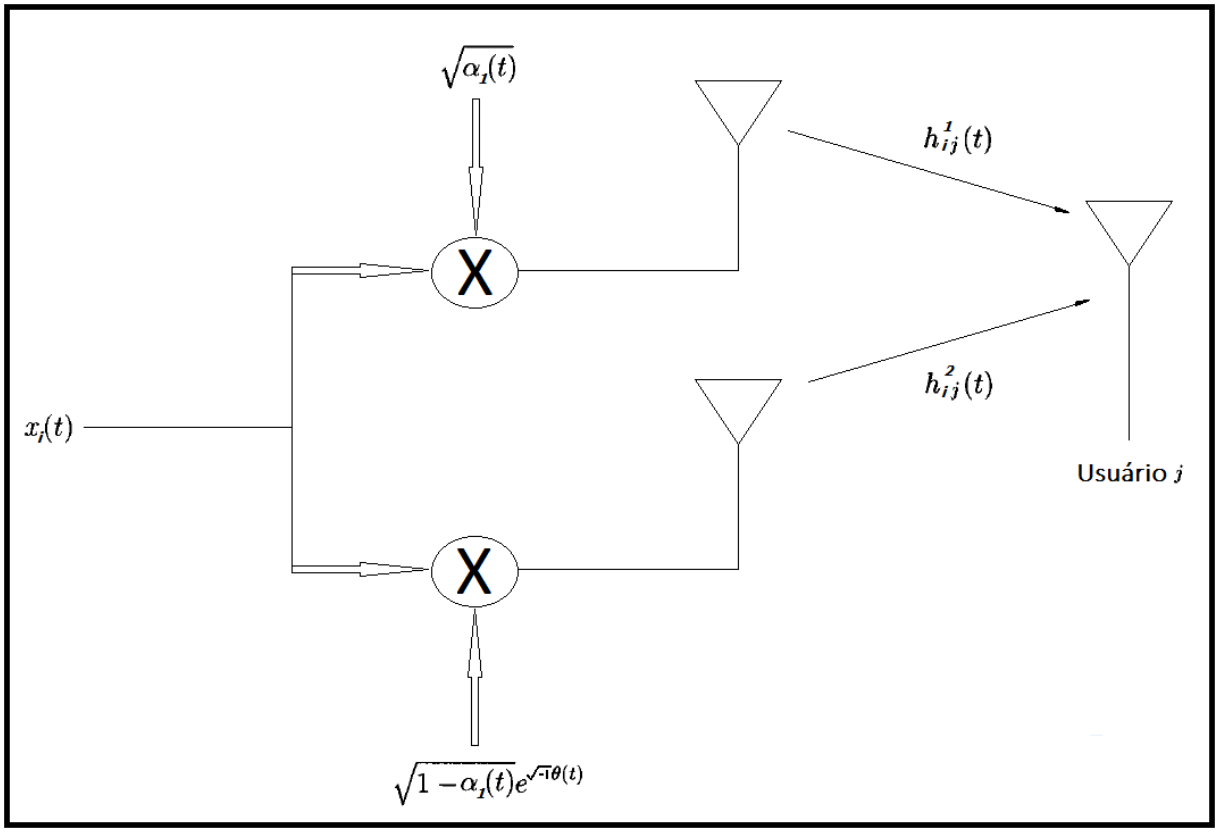

Figura 10: Modelo de duas antenas transmitindo o mesmo sinal com fase e potência variantes no tempo.

Fonte: (VISWANATH et al., 2002)

do sinal recebido. Entretanto, estes *bits* somente têm valor quando ambos Alice e Bob também podem extraí-los propriamente. Assim, quanto mais correlacionado for o canal entre Alice e Eve, maior será a chance, em um dado momento, que Alice, Bob e Eve extraiam todos o mesmo *bit* secreto. O tamanho da chave secreta irá influenciar no nível de segurança da extração de chaves, isto é, na probabilidade de Eve conseguir extrair a mesma chave secreta que Alice e Bob. Aumentar o tamanho da chave, em número de *bits*, reduz a chance de Eve extrair todos os *bits* que Alice e Bob concordaram em utilizar para formar a chave, pois a correlação Alice-Bob é maior que a correlação Alice-Eve.

No modelo FH, proposto em (ZAN et al., 2013), os fatores que influenciam na taxa de extração de *bits* são o número de canais c disponíveis, o número de sementes s utilizadas, o tamanho da semente l, em *bits*, e o nível de segurança da privacidade. Aumentar o número de canais reduz a chance de Bob e Eve acertarem o canal em que Alice se encontra. Isso reduz a taxa de extração de *bits*, porém também reduz a probabilidade de Eve não obter a semente trocada entre Alice e Bob. Utilizar um número maior de sementes reduz a taxa de extração de *bits*, porém Eve necessita obter mais sementes para formar a chave secreta, reduzindo sua

chance de extrair a mesma. Aumentar o tamanho da semente, ou seja, transmitir mais *bits* cada vez que Alice e Bob acertam o mesmo canal, aumenta a taxa de extração de *bits*. Porém, transmissões muito longas podem comprometer a segurança da semente, pois Eve pode obter informações parciais da semente se o tamanho da mesma for muito longa (ZAN et al., 2013). O nível de segurança da privacidade, isto é, a chance de Eve conseguir extrair a chave secreta, tem influência na relação entre os parâmetros c e s, conforme por (9).

Para realizar uma comparação na taxa de extração de *bits* do esquema proposto com o modelo FH, é definida a *Taxa de Extração Segura* (TES) como a máxima taxa no qual Alice pode enviar informação confiável para Bob, de tal maneira que a probabilidade de Eve obter esta informação é arbitrariamente pequena. Um *bit secreto seguro* é um *bit* extraído por Alice e Bob, mas não por Eve. Se Alice ou Bob não conseguir extrair um *bit* com sucesso - resultando em um valor indeterminado, no instante de tempo t, este *bit* é descartado por ambos. Caso contrário, este é considerado um *bit* secreto seguro e será utilizado na formação da chave secreta.

A sequência de *bits* secretos extraídos é dada por $\mathbf{w}$, que contém o conjunto de bits secretos b_s, tal que $b_{s_{A,t}} = b_{s_{B,t}} \neq b_{s_{E,t}}$, para $t = 1, 2, \ldots, m-1$ e $b_{s_{A,t}} \neq indeterminado$, onde $|\mathbf{w}|$ é o número total de *bits* secretos extraídos das m amostras.

A TES é calculada considerando o número de *bits* secretos obtidos durante um intervalo de tempo, dada por:

$$TES_{MD-RSS} = \frac{|\mathbf{w}|}{T} \quad (bits/s) \tag{12}$$

Para o modelo FH, o tempo total para formação da chave secreta T_{FH} será o tempo necessário para trocar s sementes utilizando c canais. A partir de (9), a chave secreta obtida será formada por *bits* secretos seguros e a TES será:

$$TES_{FH} = \frac{l}{T_{FH}} \quad (bits/s) \tag{13}$$

4 RESULTADOS NUMÉRICOS

Neste capítulo são apresentados os resultados numéricos e a discussão do desempenho entre os métodos de concordância de chave MD-RSS e FH. Foram analisados a frequência e os coeficientes do canal amostrado com suas matrizes de correlação e numericamente calculado a extração de *bits* secretos seguros empíricos entre Alice e Bob, baseado em coeficientes do canal no domínio do tempo, para diferentes ambientes do canal.

4.1 NÍVEL DE SEGURANÇA DA PRIVACIDADE

A probabilidade de Eve extrair a chave secreta afeta o número de *bits* secretos necessários para compor a chave no modelo MD-RSS, assim como a relação entre canais c e sementes s no modelo FH. Reduzir a probabilidade de Eve extrair a chave secreta (p_E) implica em aumentar o tamanho da chave secreta no MD-RSS e aumentar o número de sementes, para um mesmo número de canais, no FH. Em (KIM et al., 2011) é discutida a relação custo-benefício entre privacidade e segurança, e o valor de $p_E = 7\%$ é considerado satisfatório. A Figura 11 apresenta a relação entre p_E e o tamanho da semente para a correlação do canal Alice-Eve de 19,37% e 38,74%, no modelo MD-RSS com duas antenas. Ao diminuir a probabilidade de Eve obter a chave secreta, observa-se o aumento necessário no tamanho da mesma, obrigando Eve extrair mais *bits* secretos nos mesmos instantes de tempo que Alice e Bob. A Figura 12, para o modelo FH, apresenta a relação entre p_E e o número de sementes s, considerando o número de canais disponíveis $c \in \{3, 10\}$, conforme a equação 9. Ao reduzir a chance de Eve extrair a chave secreta com sucesso, observa-se o aumento no número de sementes necessárias para compor a chave, pois Eve deve coletar todas as sementes utilizadas por Alice e Bob para também compor a chave secreta.

4.2 CORRELAÇÃO ENTRE CANAIS E TAMANHO DA CHAVE SECRETA

A Figura 13 apresenta a chance de Eve conseguir a chave secreta, utilizando simulação numérica conforme (3), como uma função tanto da correlação Alice e Eve como do tamanho

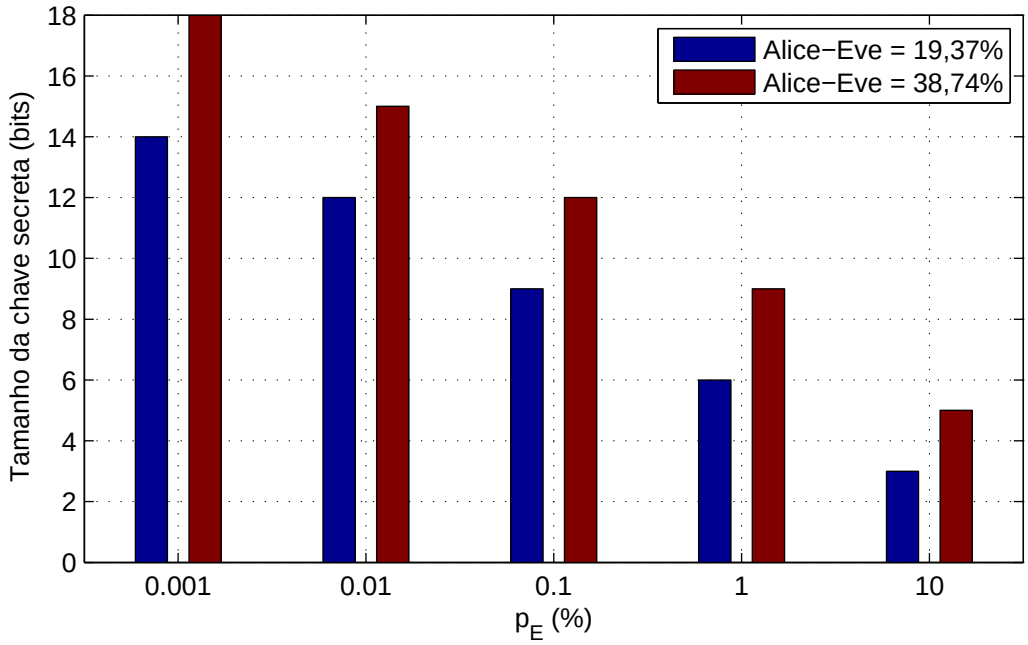

Figura 11: Relação entre p_E e o tamanho necessário da semente, considerando a correlação do canal Alice-Eve de 19,37% e 38,74%, com duas antenas, no modelo MD-RSS.

Fonte: Autoria própria

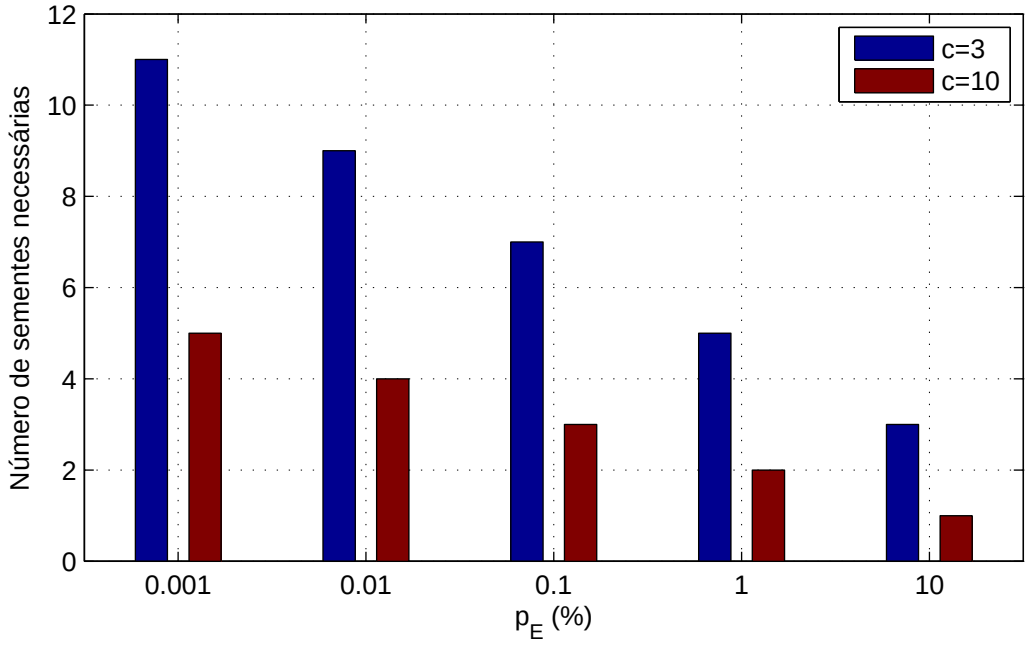

Figura 12: Relação entre p_E e o número de sementes s, para valores de $c \in \{3, 10\}$ canais disponíveis, no modelo FH.

Fonte: Autoria própria

da chave secreta, para valores de correlação Alice-Eve variando entre 0 e 100%, o tamanho da chave secreta variando entre 1 e 15 *bits* de comprimento e considerando $p_E \leq 10^{-5}$. Como esperado, a capacidade de Eve obter a chave secreta é severamente reduzida com a redução na correlação do canal entre Alice e Eve. Ainda, pode-se observar que aumentando o tamanho da chave secreta também reduz a chance de Eve extrair todos os *bits* nos mesmos instantes de tempo que Alice e Bob.

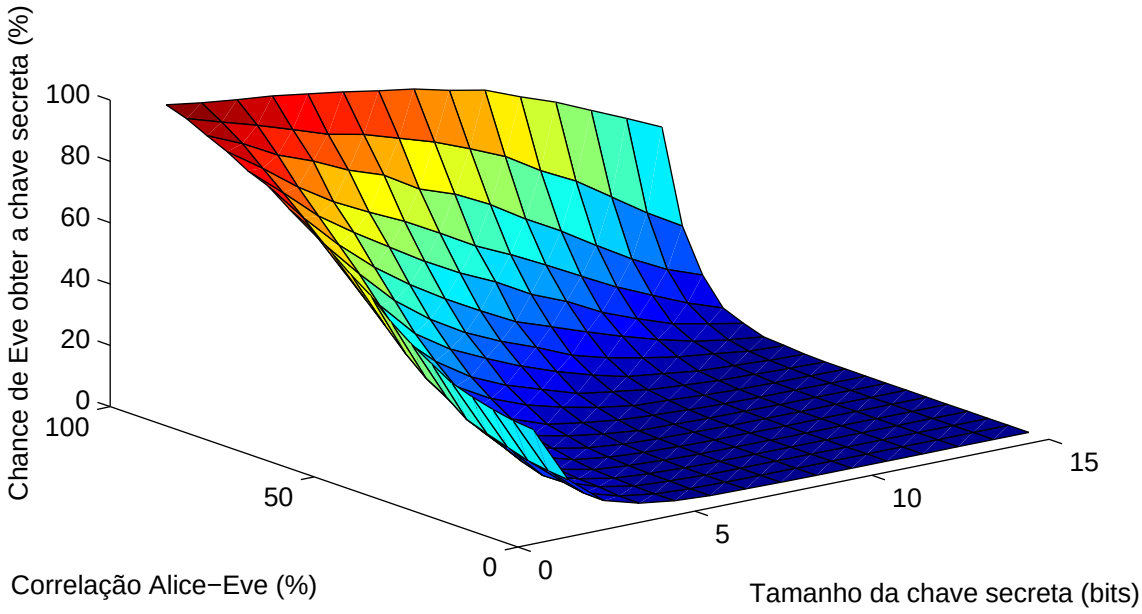

Figura 13: Chance de Eve conseguir a chave secreta como uma função da correlação entre Alice e Eve, e o tamanho da chave secreta, para $\varepsilon = 3$, $d = 1$ e $N = 2$ antenas.

Fonte: Autoria própria

4.3 RELAÇÃO ENTRE NÚMERO DE CANAIS E NÚMERO DE SEMENTES

A Figura 14 mostra a relação entre o número de canais c e o número de sementes s para o método FH. Para obter uma relação entre c e s, é necessário adotar uma taxa de erro para extração de *bits* secretos seguros, ou seja, um valor máximo de probabildade no qual Eve consegue obter a chave secreta após z transmissões. O valor adotado é de 10^{-5}, representando uma chance em cem mil de Eve conseguir obter a chave secreta, probabilidade satisfatória em termos de confidencialidade dos dados transmitidos, para este trabalho. Valores menores que 10^{-5} aumentam a segurança do sistema, porém reduzem a taxa de extração de chaves secretas. Assim, conforme a equação 9, pares de valores (c,s) são obtidos que satisfazem a taxa de erro para extração de *bits* secretos seguros no modelo FH.

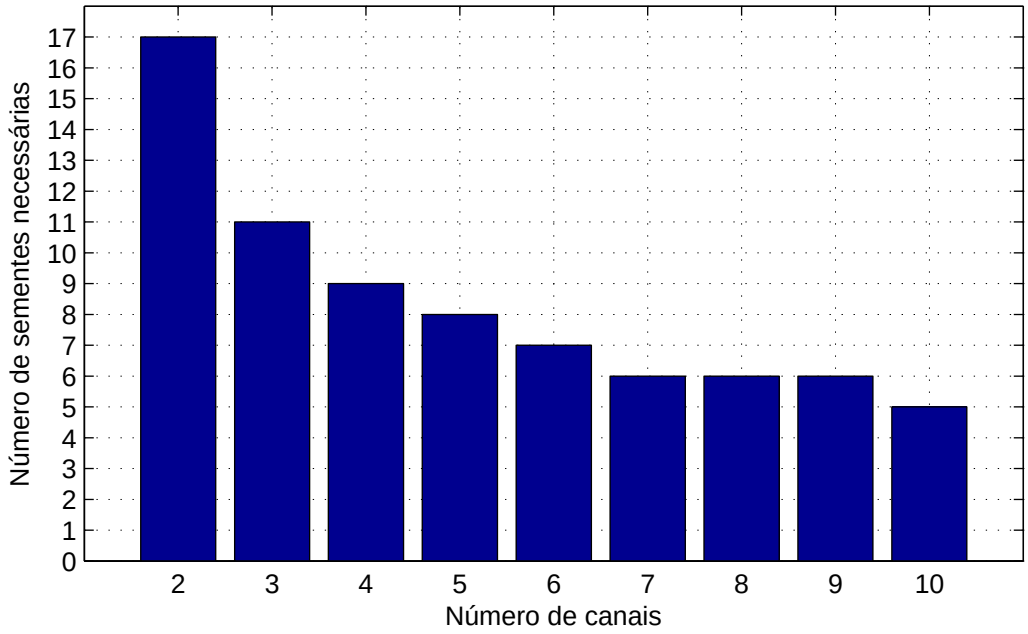

Figura 14: Número de sementes s necessárias para cada número de canais c disponíveis para manter a taxa de erro para extração de *bits* secretos seguros menor que 10^{-5}.

Fonte: Autoria própria

4.4 EXTRAÇÃO DE *BITS* SECRETOS EM FUNÇÃO DO NÚMERO DE ANTENAS NO TRANSMISSOR

A taxa de extração de *bits* secretos seguros entre os métodos MD-RSS e FH é comparado na Figura 15, onde foi estipulado para o FH ter duas transmissões por segundo, e cada semente possui 128 *bits* de comprimento. Para o modelo MD-RSS, foi assumido uma correlação do canal de 19,37% entre Alice e Eve, mantendo o tamanho da chave secreta também como 128 *bits* de comprimento e variando o número de antenas N de uma até dez antenas. Comparando o método D-RSS (que é equivalente ao esquema MD-RSS com $N = 1$ antena) ao método FH, pode-se notar que com o uso de apenas uma antena, a taxa de extração de *bits* é menor que no modelo FH, conforme esperado, pois a taxa de variação do canal é lenta. entretanto, a medida que o número de antenas aumenta, existe um ganho na taxa de extração, mesmo considerando apenas duas antenas. Deve-se notar que tal ganho não é diretamente proporcional ao número de antenas, ou seja, pode-se observar que após um certo número de antenas adicionadas no transmissor, a taxa de extração de *bits* tende a um valor limite finito aproximadamente igual a 24 *bits*/s. Também é possivel notar que a taxa de extração de *bits* para o método FH não é dependente do número de antenas transmissoras, pois o modelo FH não depende da velocidade de desvanecimento do ambiente, mas do número de portadoras disponíveis dentro de uma banda

de frequência. Assim, para duas ou mais antenas, o método MD-RSS possui desempenho maior na taxa de extração de *bits* secretos que o modelo FH.

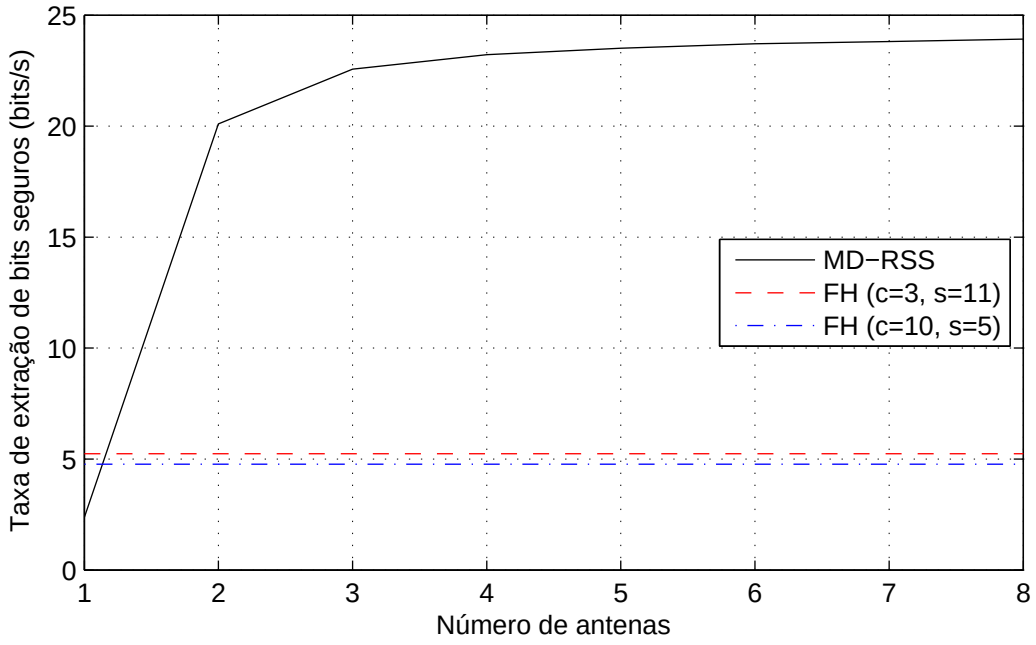

Figura 15: Número de *bits* secretos seguros extraídos por segundo como uma função do número de antenas no transmissor.

Fonte: Autoria própria

4.5 EXTRAÇÃO DE *BITS* SECRETOS EM FUNÇÃO DO NÚMERO DE CANAIS DISPONÍVEIS

Para os próximos resultados, a menos que dito o contrário especificamente, foram adotados para o método MD-RSS os parâmetros de $N = 2$ antenas, o comprimento da chave secreta como 128 *bits* e a correlação do canal entre Alice e Eve como 19,37%. Para o método FH foram adotados os valores para o número de sementes $s = 11$ para o número de canais disponíveis $c = 3$, e o número de sementes $s = 5$ para o número de canais disponíveis $c = 10$. Para valores intermediários do número de canais disponíveis, foram utilizados números de sementes proporcionais para manter a segurança dos *bits* extraídos, conforme já demonstrado anteriormente em (9), com o objetivo de manter a chance de Eve obter a chave secreta menor que 10^{-5}.

Na Figura 16, foi analisada a taxa de extração de *bits* secretos seguros comparada ao número de canais c disponíveis, para ambos os métodos MD-RSS (o qual não depende de c) e FH, considerando o tamanho da semente $s \in \{64, 128, 256\}$ *bits* de comprimento e foram

variados os números de canais c disponíveis de três até dez. Embora o método MD-RSS tenha apresentado pequena mudança na taxa de extração para diferentes tamanhos de sementes, pode-se observar que o mesmo apresenta uma taxa de extração de *bits* secretos seguros maior que o apresentado pelo método FH, indiferente do número de canais disponíveis ou do tamanho das sementes, para todos os valores medidos. No método FH, aumentar o número de canais disponíveis reduz a chance de Eve conseguir obter a semente trocada, porém também prejudica Bob acertar o canal escolhido por Alice para transmitir a semente. Para três ou mais canais disponíveis, a taxa de extração de *bits* seguros no modelo FH mantém-se aproximadamente constante, pois embora diminua a chance de Bob acertar o mesmo canal que Alice, menos sementes são necessárias para formar a chave secreta, conforme pode ser observado. Aumentar o tamanho da semente oferece uma taxa de extração de *bits* secretos maior, pois mais *bits* são transmitidos cada vez que Alice e Bob estão no mesmo canal.

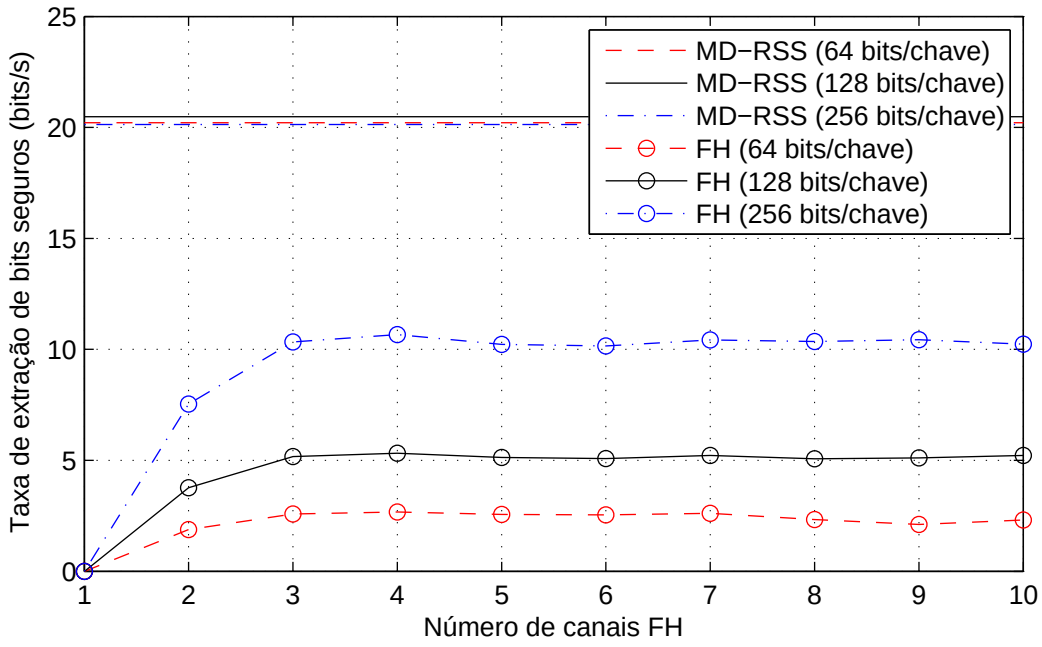

Figura 16: Número de *bits* secretos seguros extraídos por segundo, variando o número de canais c disponíveis.

Fonte: Autoria própria

4.6 EXTRAÇÃO DE *BITS* SECRETOS EM FUNÇÃO DO NÚMERO DE SEMENTES PARA COMPOR UMA CHAVE SECRETA

Outra variável que influencia no desempenho é o número de sementes s necessarias para formar a chave secreta. Isto é ilustrado na Figura 17. Pode-se observar que o número de

bits extraídos por segundo é constante para o método MD-RSS, porém a taxa diminui para o método FH a medida que mais sementes são necessárias para compor a chave secreta. Ainda, aumentando o número de canais c reduz a taxa de extração, pois embora diminua a chance e Eve obter a semente em um determinado instante de tempo, a chance de Bob também não estar no mesmo canal que Alice aumenta. Como mostrado nos resultados, o método MD-RSS apresenta uma taxa de extração maior que o modelo FH. Entretanto, para $c = 3$ e $s < 3$, o método FH resulta em uma taxa maior de extração de *bits* secretos, mas grandemente ao custo de segurança, visto que são necessárias pelo menos $s = 11$ sementes para garantir que Eve tenha uma chance menor que 10^{-5} de extrair a chave secreta, conforme demonstado pela equação 9.

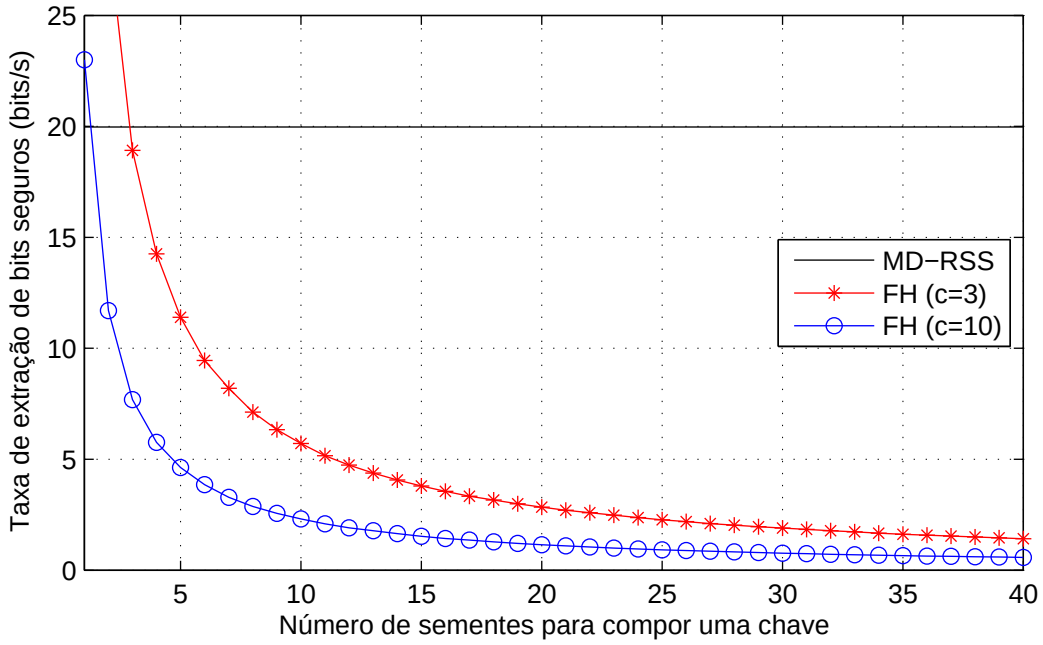

Figura 17: Número de *bits* secretos seguros extraídos por segundo, variando o número de sementes s para compor uma chave secreta.

Fonte: Autoria própria

4.7 EXTRAÇÃO DE *BITS* SECRETOS EM FUNÇÃO DO TAMANHO DA SEMENTE

Finalmente são comparados na Figura 18 os dois métodos através da variação no tamanho da semente, até o limite de 512 *bits* de comprimento. Para o modelo FH, nota-se um aumento na taxa a medida de aumenta-se o tamanho da semente, em *bits*, conforme esperado. Nota-se que, para sementes acima de aproximadamente 494 *bits* de comprimento - utilizando $c = 3$ e $s = 11$, o método FH apresenta uma taxa de extração maior que o modelo MD-RSS. Entretanto, conforme (ZAN; GRUTESER, 2009), quanto maior o tempo de transmissão da se-

mente, maior será a possibilidade da semente ser exposta ao nodo espião.

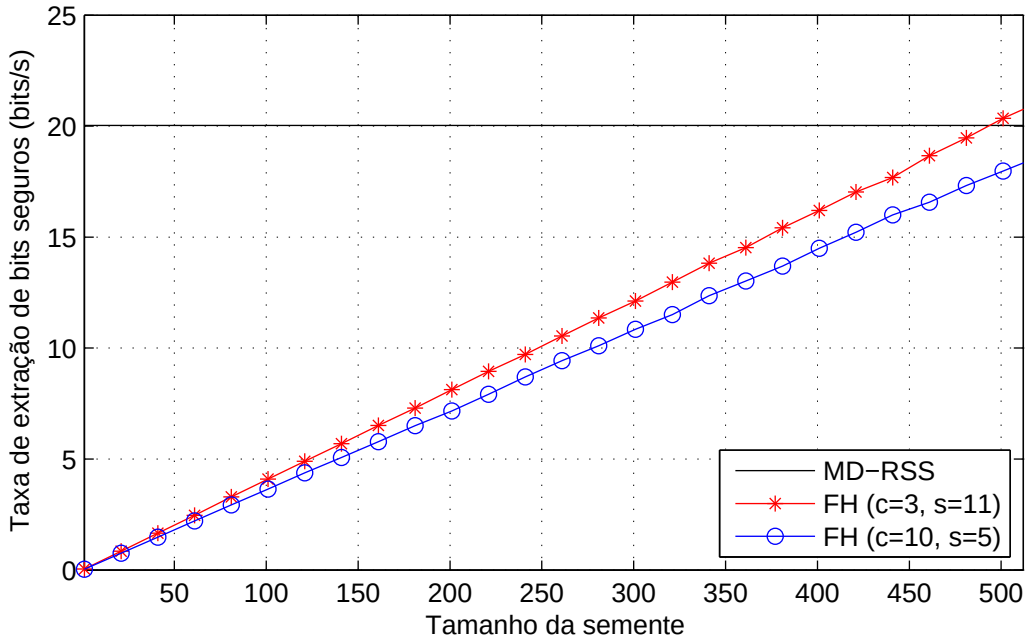

Figura 18: Número de *bits* secretos seguros extraídos por segundo, variando o tamanho da sementes *s* utilizada para compor uma chave secreta.

Fonte: Autoria própria

Conforme ilustrado pelas variadas formas de comparação, o modelo proposto MD-RSS, mesmo com apenas duas antenas transmissoras, é capaz de obter desempenho maior na extração de *bits* secretos que o modelo FH, em um ambiente V2I.

5 CONCLUSÃO

Este trabalho apresenta a utilização de múltiplas antenas *dumb* em uma infraestrutura RSU, dentro de um ambiente de uma rede de comunicação veículo-a-veículo, para aumentar a variação do canal de comunicação artificialmente, tornando um canal de desvanecimento lento em um canal de desvanecimento rápido. Este modelo permite aplicar o algoritimo de concordância de chave baseado na variação do canal (chamado neste trabalho de MD-RSS) ao cenário descrito anteriormente.

Os resultados apresentados neste trabalho mostram que o modelo MD-RSS é capaz de obter um desempenho maior de extração de *bits* secretos seguros que o modelo proposto recentemente de *frequency hopping* (ZAN et al., 2013). Foram analisados diversos parâmetros que influenciam a taxa de extração de *bits* nos modelos MD-RSS e FH e, para cada parâmetro, foram calculados a taxa de extração de *bits* secretos para ambos os métodos, resultando em uma comparação direta entre ambos. Inicialmente determinaram-se parâmetros para o método FH, onde o número de canais c disponíveis determina o número de sementes s necessárias para compor uma chave secreta, obtendo-se assim um par de variáveis correlacionadas, com o objetivo de manter a taxa de erro na extração de *bits* abaixo de um determinado valor (apara ambos os métodos). A seguir, variou-se o número de antenas *dumb* no transmissor e comparou-se a taxa de extração de *bits* entre os dois métodos, obtendo-se uma notável vantagem do método MD-RSS para o caso de duas ou mais antenas utilizadas. Então, variou-se o número de canais c disponíveis no modelo FH e novamente obteve-se um gráfico comparando os dois modelos. O modelo MD-RSS (não influenciado pelo número de canais c disponíveis) novamente apresentou vantagem na taxa de extração de *bits*, indiferente do número de canais. Comparou-se a seguir a taxa de extração ao se variar o número de sementes s, utilizadas para compor uma chave secreta. Novamente, o modelo MD-RSS apresentou resultados melhores quando mantendo a mesma taxa de erro na extração de *bits* secretos. Por último, alterou-se o tamanho da semente transmitida no modelo FH e obteve-se a comparação entre os dois modelos através da taxa de extração de *bits*. Para sementes de tamanho menor que aproximadamente 500 *bits* o modelo MD-RSS apresentou melhor desempenho. Para sementes acima deste comprimento, o modelo

FH torna-se mais rápido, ao risco de expor a chave secreta ao nodo espião.

Em todos os cenários comparados, o modelo proposto MD-RSS apresentou melhor desempenho, considerando diversas variáveis que afetam a taxa de extração de *bits* secretos nos dois modelos comparados.

6 TRABALHOS FUTUROS

Neste trabalho, consideraram-se correlações fixas entre os canais Alice e Bob, e entre Alice e Eve. A correlação desses canais afeta a taxa de extração de *bits* secretos seguros no modelo MD-RSS e trabalhos futuros podem incluir este parâmetro no cálculo da taxa de *bits* extraídos, considerando as distâncias entre cada nodo participante no modelo do sistema (Alice, Bob e Eve).

O modelo FH, utilizado na comparação com o esquema proposto MD-RSS, foi proposto no trabalho de (ZAN et al., 2013) como uma alternativa para concordância de chaves secretas no ambiente V2I. Entretanto, uma possibilidade de continuação deste trabalho seria comparar com o modelo propostos no trabalho (KOSTIC et al., 2001), onde é utilizado o modelo DFH (*Dynamic Frequency Hopping*), onde a estação-base utiliza informações para encontrar a melhor frequência de envio, conforme alguns critérios, resultando em melhor desempenho na taxa de extração de *bits* secretos, em condições ideais, comparado ao modelo FH aleatório.

A extração de chaves secretas na camada física, analisado neste trabalho, considera Eve como um agente passivo, não interessado em obstruir a geração das chaves secretas. Uma opção para continuidade deste trabalho é estender a análise de geração das chaves secretas considerando um nodo espião ativo, conforme apresentado em (ZENG, 2015). Os ataques ativos podem ser classificados em três categorias: a) um ataque de interferência disruptiva, o qual procura interromper o processo de geração de chaves e reduzir a taxa de geração de chaves dos usuários legítimos; b) um ataque de interferência manipulativa, o qual injeta um sinal para manipular as medições do canal e comprometer uma porção da chave; c) um ataque de manipulação do canal, o qual procura controlar o canal sem fio entre Alice e Bob, permitindo o atacante interferir na chave gerada.

A geração de chaves secretas ocorre entre dois usuários legítimos, Alice e Bob, ao longo da rodovia. Neste processo, a RSU necessita gerar uma chave secreta com cada veículo dentro da sua região. Uma opção para continuidade deste trabalho é extrair uma chave secreta para um grupo de veículos, explorando as medições RSS destes usuários colaborativamente,

modelo proposto no trabalho (LIU et al., 2012) para uma rede móvel sem fio. No modelo apresentado, é definido uma métrica que representa a diferença da RSS em um dispositivo sem fio através de canais diferentes de rádio. Entretanto, ao invés de passar as medidas da RSS diretamente, os valores da nova métrica são passados para outros dispositivos visando facilitar a extração das chaves, impedindo Eve de obter as medidas exatas da RSS entre um par de dispositivos e, consequentemente, não podendo extrair a chave secreta do grupo.

REFERÊNCIAS

AL-SHURMAN, M.; YOO, S.-M. Key pre-distribution using mds codes in mobile ad hoc networks. In: **Proc. 3rd Int. Conf. ITNG**. 2006. p. 566–567.

AONO, T. et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. **Antennas and Propagation, IEEE Transactions on**, v. 53, n. 11, p. 3776–3784, Nov 2005.

ARGYRAKI, K. et al. Creating secrets out of erasures. In: **MobiCom '13 Proceedings of the 19th annual international conference on Mobile computing and networking**. 2013. p. 429–440.

BETTSTETTER, C.; HARTMANN, C.; MOSER, C. How does randomized beamforming improve the connectivity of ad hoc networks? In: **Communications, 2005. ICC 2005. 2005 IEEE International Conference on**. 2005. v. 5, p. 3380–3385 Vol. 5.

BLOM, R. An optimal class of symmetric key generation systems. In: **Proc. EUROCRYPT, New York, NY, USA**. 1985. p. 335–338.

CHAN, A.-F. Distributed symmetric key management for mobile ad hoc networks. In: **INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies**. 2004. v. 4, p. 2414–2424 vol.4.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. **Information Theory, IEEE Transactions on**, v. 22, n. 6, p. 644–654, Nov 1976.

DORLE, S. et al. Design of base station's vehicular communication network for intelligent traffic control. In: **Vehicle Power and Propulsion Conference, 2009. VPPC '09. IEEE**. 2009. p. 1118–1121.

EDMAN, M.; KIAYIAS, A.; YENER, B. On passive interference attacks against physical-layer key extraction. In: **Proc. 4th Euro. Wksp. System Security**. 2011. p. 8:1–8:6.

ESCHENAUER, L.; GLIGOR, V. D. A key-management scheme for distributed sensor networks. In: **Proc. ACM Conf. CCS**. 2002. p. 41–47.

HERSHEY, J.; HASSAN, A.; YARLAGADDA, R. Unconventional cryptographic keying variable management. **Communications, IEEE Transactions on**, v. 43, n. 1, p. 3–6, Jan 1995.

KENNEY, J. Dedicated short-range communications (dsrc) standards in the united states. **Proceedings of the IEEE**, v. 99, n. 7, p. 1162–1182, July 2011.

KIM, A.; KNISS, V.; SLOAN, S. **An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policyand Institucional Issues**. 2011. Disponível em: <http://ntl.bts.gov/lib/43000/43500/43513/FHWA-JPO-11-130_FINAL_Comm_Security_Approach_11_07_11.pdf>.

KITAURA, A. et al. A scheme of private key agreement based on delay profiles in uwb systems. In: **Sarnoff Symposium, 2006 IEEE**. 2006. p. 1–6.

KOBLITZ, N. An elliptic curve implementation of the finite field digital signature algorithm. In: **18th Annu. Int. CRYPTO, London, U.K.** 1998. p. 327–337.

KOSTIC, Z.; MARIC, I.; WANG, X. Fundamentals of dynamic frequency hopping in cellular systems. **Selected Areas in Communications, IEEE Journal on**, v. 19, n. 11, p. 2254–2266, 2001.

LI, X.; RATAZZI, E. Mimo transmissions with information-theoretic secrecy for secret-key agreement in wireless networks. In: **Military Communications Conference, 2005. MILCOM 2005. IEEE**. 2005. p. 1353–1359 Vol. 3.

LIU, H. et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In: **INFOCOM, 2012 Proceedings IEEE**. 2012. p. 927–935.

LIU, H. et al. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. **Mobile Computing, IEEE Transactions on**, v. 13, n. 12, p. 2820–2835, 2014.

LIU, Y.; DRAPER, S.; SAYEED, A. Exploiting channel diversity in secret key generation from multipath fading randomness. **Information Forensics and Security, IEEE Transactions on**, v. 7, n. 5, p. 1484–1497, Oct 2012.

MATHUR, S. et al. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In: **Proc. ACM MobiCom**. 2008. p. 128–139.

MAURER, U. Secret key agreement by public discussion from common information. **Information Theory, IEEE Transactions on**, v. 39, n. 3, p. 733–742, May 1993.

NAFI, N.; KHAN, J. A vanet based intelligent road traffic signalling system. In: **Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian**. 2012. p. 1–6.

OTMANI, A.; TILLICH, J.-P.; ANDRIYANOVA, I. On the minimum distance of generalized ldpc codes. In: **Information Theory, 2007. ISIT 2007. IEEE International Symposium on**. 2007. p. 751–755.

OTWAY, D.; REES, O. Efficient and timely mutual authentication. In: **ACM SIGOPS Oper. Syst. Rev.** 1987. v. 21, n. 1, p. 8–10.

PATWARI, N. et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. **Mobile Computing, IEEE Transactions on**, v. 9, n. 1, p. 17–30, 2010.

PERRIG, A. et al. Spins: Security protocols for sensor networks. **Wireless Networks**, v. 8, n. 5, p. 521–534, Sep 2002.

PREMNATH, S. et al. Secret key extraction using bluetooth wireless signal strength measurements. In: **Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference on**. 2014. p. 293–301.

PREMNATH, S. N. et al. Secret key extraction from wireless signal strength in real environments. **Mobile Computing, IEEE Transactions on**, v. 12, n. 5, p. 917–930, May 2013. ISSN 1536-1233.

STEINER, J.; SCHILLER, J. I. Kerberos: An authentication service for open network systems. In: **USENIX Conference**. 1988. p. 191–202.

VISWANATH, P.; TSE, D. N. C.; LAROIA, R. Opportunistic beamforming using dumb antenas. **IEEE Transactions on Information Theory**, v. 48, n. 6, p. 1277 – 1294, June 2002.

WANG, H.-M.; ZHENG, T.; XIA, X.-G. Secure miso wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. **Wireless Communications, IEEE Transactions on**, v. 14, n. 1, p. 94–106, Jan 2015.

WEI, Y.; ZENG, K.; MOHAPATRA, P. Adaptive wireless channel probing for shared key generation based on pid controller. **Mobile Computing, IEEE Transactions on**, v. 12, n. 9, p. 1842–1852, 2013.

WEIXIN, L. et al. The differential detection ofdm cooperative diversity system in vehicle-to-vehicle communications. In: **ITS Telecommunications Proceedings, 2006 6th International Conference on**. 2006. p. 1118–1121.

YE, C. et al. Information-theoretically secret key generation for fading wireless channels. **Information Forensics and Security, IEEE Transactions on**, v. 5, n. 2, p. 240–254, June 2010.

ZAN, B.; GRUTESER, M. Random channel hopping schemes for key agreement in wireless networks. In: **Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on**. 2009. p. 2886–2890.

ZAN, B.; GRUTESER, M.; HU, F. Improving robustness of key extraction from wireless channels with differential techniques. In: **Computing, Networking and Communications (ICNC), 2012 International Conference on**. 2012. p. 980–984.

ZAN, B.; GRUTESER, M.; HU, F. Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems. **Vehicular Technology, IEEE Transactions on**, v. 62, n. 8, p. 4020–4027, 2013.

ZENG, K. Physical layer key generation in wireless networks: challenges and opportunities. **Communications Magazine, IEEE**, v. 53, n. 6, p. 33–39, 2015.

ZENG, K. et al. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: **INFOCOM, 2010 Proceedings IEEE**. 2010. p. 1–9.

ZHANG, C. et al. Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks. In: **Communications, 2008. ICC '08. IEEE International Conference on**. 2008. p. 1451–1457.

ZIV, J.; LEMPEL, A. Compression of individual sequences via variable-rate coding. **Information Theory, IEEE Transactions on**, v. 24, n. 5, 1978.

APÊNDICE A – EXTRAÇÃO DE CHAVES SECRETAS

O uso de dispositivos sem fio tornou-se uma parte importante do nosso dia-a-dia (*smartphones* e *laptops*, por exemplo), permitindo o compartilhamento de informações e diversas transações de dados de maneiras que antes não eram possiveis. Para garantir a implementação e utilização desta tecnologia, a comunicação segura é essencial para possibilitar a confidencialidade dos dados transmitidos, a integridade dos dados e a autenticidade dos dispositivos entre diversos aparelhos sem fio. Por exemplo, a comunicação entre veículos e infraestruturas em uma rodovia permite a troca de informações sobre a posição, velocidade e movimento de cada veículo, possibilitando o controle do tráfego e redução de congestionamentos e acidentes de trânsito.

De acordo com Liu et al. (2012), embora existam pesquisas sobre aplicações de métodos baseados em criptografias tradicionais, como a PKI (*Public Key Infrastructure*) em redes sem fio, esses métodos não são sempre aplicáveis, por causa de recursos limitados nos dispositivos sem fio - bateria limitada e poder computacional - e a ausência de infraestruturas fixas de gerenciamento de chaves, devido a grande dinâmica do ambiente sem fio móvel, no ambiente V2V. No ambiente V2I, embora podemos assumir que a infraestrutura está conectada a um servidor central de confiança, o meio de transmissão sem fio aberto torna o procedimento de distribuição da chave vulnerável à escuta indevida - indivíduos dentro do alcance da comunicação dos usuários legítimos podem monitorar quaisquer trocas de informações da geração da chave secreta.

A principal vantagem da geração de chave secreta utilizando informações da camada física de um canal de rádio é que ela permite dois dispositivos sem fio quaisquer, dentro do alcance de comunicação de ambos, extrair uma chave criptográfica simétrica sem a necessidade de uma infraestrutura fixa ou um canal seguro de comunicação. Baseado no princípio da reciprocidade do canal - onde dois nodos situados nos extremos de um canal observam as mesmas características deste canal, dois dispositivos sem fio podem extrair *bits* secretos idênticos independentemente usando uma sequência de amostras coletadas do canal de rádio entre eles, dentro do tempo de coerência do canal (LIU et al., 2014). Conforme (MATHUR et al., 2008),

ao contrário de algorítimos de geração de chaves existentes, como por exemplo Diffie-Hellman (DIFFIE; HELLMAN, 1976), o qual baseia-se em operações computacionais pesadas de problemas, a geração de chaves secretas usando a aleatoriedade do canal devido as variações espaço-temporais, pode alcançar o *information-theoretical secrecy* (onde a segurança deriva puramente da teoria da informação, ou seja, não pode ser quebrada mesmo quando um adversário possui poder computacional ilimitado), no sentido que o segredo das chaves geradas não é dependente da dificuldade de um problema computacional, mas sim depende das leis da física dos canais de desvanecimento sem fio.

Comparando as várias informações da camada física do canal de rádio, como por exemplo a fase do canal, realizar a amostragem do RSS (*Received Signal Strength*) é um método atrativo para gerar chaves secretas, conforme (LIU et al., 2014), pois as leituras do RSS estão prontamente disponíveis nas infraestruturas sem fio existentes, proporcinando uma grande economia de custos. Este mecanismo é chamando *geração de chave na camada física*, no qual os dispositivos sem fio medem características do canal sem fio altamente correlacionadas - força do sinal recebido ou resposta ao impulso do canal, por exemplo - e as usam como fontes aleatórias compartilhadas para gerar a chave secreta, conforme (ZENG, 2015). Na teoria, em um ambiente rico em desvanecimento de múltiplos caminhos, um espião passivo que está a mais de meio comprimento de onda distante dos usuários legítimos irá obter medidas descorrelacionadas do canal e assim não pode obter muita informação sobre a chave gerada.

Embora estudos teóricos proporcionem guias sobre como desenvolver um protocolo de concordância de chaves na camada física, ainda existem desafios significativos em conseguir um método de geração de chaves eficiente e comprovadamente seguro na prática. Alguns desafios estão na dificuldade de medir a informação vazada ao espião, a medição das correlações do canal, reduzir o *overhead* da reconciliação e decidir a taxa de compressão no estágio da amplificação de privacidade (ZENG, 2015).

A.1 GERAÇÃO DE CHAVES NA CAMADA FÍSICA

No processo de geração de chaves, consideramos um cenário onde dois usuários legítimos, Alice e Bob desejam gerar uma chave secreta compartilhada usando medições do canal. Existe um espião passivo, Eve, que pode escutar as transmissões entre Alice e Bob.

Alice e Bob utilizam geralmente os cinco passos para gerar a chave: análise do canal, extração aleatória, quantização, reconciliação e amplificação de privacidade.

A.1.1 ANÁLISE DO CANAL

Este procedimento é utilizado para coletar medidas do canal por Alice e Bob. As medidas do canal podem ser CSI (*Channel State information*), RSS (*Received Signal Strength*) ou fase. neste passo, Alice e Bob trocam sinais de exploração do canal entre si. Uma exploração do canal contém um par de explorações do canal bi-direcionais com um pequeno atraso de tempo, considerando um rádio *half-duplex*. Os sinais recebidos são normalmente modelados como os ganhos do canal no tempo do sinal (no domínio da frequência) transmitido, adicionado o ruído. Alice e Bob observam sinais recebidos altamente correlacionados devido a reciprocidade do canal (ZENG, 2015).

A.1.2 EXTRAÇÃO ALEATÓRIA

Os sinais recebidos em Alice e Bob podem conter partes determinísticas que podem ser determinadas ou inferidas pelo espião. Por exemplo, os sinais recebidos em Alice e Bob têm o mesmo padrão de flutuação em larga escala. Esta flutuação é determinada pela distância entre Alice e Bob. Se Eve está perto de um dos dois, elta irá observar esta mudança em larga escala. Assim, Alice e Bob não devem utilizar este componente em larga escala para gerar chaves compartilhadas, ou esta chave será facilmente determinada pelo espião. Alice e Bob necessitam extrair a aleatoriedade causada pelo desvanecimento do canal para gerar chaves compartilhadas através da remoção do componente em larga escala (ZENG, 2015). Por exemplo, um método de janela móvel de médias pode ser utilizado para extrair aleatoriedade em pequena escala (ZENG et al., 2010).

A.1.3 QUANTIZAÇÃO

Este passo é utilizado para quantificar as medições aletatórias extraídas em *bits*.

A.1.4 RECONCILIAÇÃO

Esta é uma forma de correção de erro ocorrida entre Alice e Bob para garantir que as chaves geradas separadamente em ambos os lados seja idêntica. Devido a imperfeição na reciprocidade, os *bits* extraídos nos lados de Alice e Bob após quantização não são normalmente idênticos, embora eles sejam altamente similares. Esta imperfeição vem principalmente do fato que Alice e Bob não podem medir o canal ao mesmo tempo devido a propriedade *half-duplex* do radio. Assim, os ruídos nos lados de Alice e Bob são geralmente independentes. Durante a fase de reconciliação dos dados, informações sobre a paridade de *bits* podem ser trocadas para

corrigir erros e uma certa quantia de informações dos *bits* pode ser revelada para Eve (ZENG, 2015).

A.1.5 AMPLIFICAÇÃO DE PRIVACIDADE

Este é um método para eliminar a informação parcial sobre a chave que Eve possui e a correlação entre os *bits*. Esta informação parcial de Eve vem da escuta durante ambas as fases de exploração e reconciliação (ZENG, 2015).

Embora existam extensivos estudos sobre geração de chaves na camada física sobre ataques passivos, restam desafios significativos e problemas não solucionados em projetar em método de geração de chaves eficiente e comprovadamente seguro na prática.

A.1.6 DIFICULDADE EM ESTIMAR INFORMAÇÕES VAZADAS NA PRÁTICA

A *secret key capacity* é definida como a informação mútua condicional entre Alice e Bob dado a observação de Eve (MAURER, 1993). Na teoria, pode-se calcular vários limites de *key capacity* assumindo o conhecimento do CSI do espião. Na prática, porém, é muito difícil estimar quanta informação foi vazada para um espião passivo. Em (EDMAN et al., 2011), foi demonstrado, através de um trabalho experimental, que existe uma forte correlação nas medidas observadas por um espião passivo, mesmo estando localizado a uma distância significativamente maior que meio comprimento de onda dos dispositivos legítimos. Este resultado pode ocorrer devido um ambiente pobre de dispersão com múltiplos caminhos, ou interferência. Logo, não existe claramente uma distância segura para garantir o segredo da chave gerada. Ainda, é difícil conhecer as localizações ou número de espiões passivos na prática, o que incrementa a dificuldade em estimar a informação vazada (ZENG, 2015).

Embora seja um problema crítico ainda não resolvido no projeto de um método comprovadamente seguro de geração de chaves na camada física, uma solução possível pode ser adicionar ruído em um dos canais para causar interferência, criando canais de cancelamento do ambiente para o espião (ARGYRAKI et al., 2013).

A.1.7 SOBRECARGA NA RECONCILIAÇÃO

O processo de reconciliação é essencialmente um processo de correção de erros com troca de informações entre Alice e Bob. A causa da discordância de *bits* vem da imperfeição da reciprocidade das características do canal medido, o qual é causado principalmente pelo atraso de tempo entre medições do canal bi-direcional durante a fase de exploração do canal.

A sobrecarga na reconciliação é a razão entre o número total de *bits* enviados (*bits* extraídos e informações para correção de erros) pelo número de *bits* extraídos, menos 1, e pode ser significante se a taxa de concordância de *bits* for baixa antes da reconciliação. Alguns dos métodos utilizados incluem o algorítimo Cascade e o LDPC (*Low Density Parity Check*). Entretanto, foi demonstado que se o método Cascade for utilizado para reconciliar dois segmentos de *bits* com discordância de 10 por cento, o número de *bits* expostos chega a ser aproximadamente 60 por cento (ZENG, 2015). Em códigos LDPC, a distância mínima do código é um parâmetro importante, pois determina o limite de decodificação do código. Para códigos grandes, encontrar esse limite não é direto e pode não ser solucionável dentro de um tempo polinomial (OTMANI et al., 2007).

Para minimizar a sobrecarga de reconciliação, é importante conseguir uma taxa alta de concordância de *bit* antes da reconciliação. Um método simples para conseguir esta taxa alta de reconciliação é reduzir o tempo de atraso entre explorações do canal bi-direcional. porém, este atraso de tempo é restrito pelo tempo de comutação entre transmissao e recepção da antena e o protocolo de controle de acesso ao meio. Uma segunda maneira para reduzir a discordância de *bits* é utilizar uma quantização de baixo nível ao custo de uma chave de tamanho reduzido. (ZENG et al., 2010) mostrou que uma quantização de baixo nível é mais robusta ao ruído, porém o comprimento da chave é reduzido significativamente. Uma terceira maneira para reduzir o custo da reconciliação é pré-processar os dados medidos. Um filtro pode ser aplicado para processar os traços medidos pelo indicador RSS (RSSI) e reduzir a frequência máxima de mudanças na potência do sinal recebido surgidas do movimento em ambientes de desvanecimento em pequena escala (PATWARI et al., 2010).

A.1.8 CORRELAÇÃO ESPACIAL E TEMPORAL

Na prática, sempre existe correlação espacial e temporal entre as medições do canal, o qual induz *bits* correlacionados na geração da chave, necessitando, antes da quantização, descorrelacionar as medições do canal. Algumas soluções incluem aplicar a transformada discreta de Karhunen-Loève (KTL) para converter os vetores de canal medido em componentes descorrelacionadas (não necessariamente independentes) (PATWARI et al., 2010). O KTL garante co-variação zero entre elementos transformados, porém não momentos de alta ordem (acima de terceira ordem). Um nodo espião sofisticado pode utilizar momentos de alta ordem para prever *bits* parciais em uma chave (ZENG, 2015).

A.1.9 AMPLIFICAÇÃO DE PRIVACIDADE

Na fase de amplificação de privacidade, Alice e Bob comprimem as sequências de *bits* obtidas após a reconciliação para sua entropia real. Por exemplo, uma função *hash* (algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo) pode ser aplicada. Entretando, na prática, não é trivial decidir a taxa de compressão, pois é muito difícil estimar com precisão quanta informação é vazada ao espião durante a fase de exploração do canal. Sem conhecer a informação vazada, é difícil decidir a taxa de compressão. Além disso, devido a correlação espacial e temporal das medidas do canal, os *bits* gerados podem ter correlações inerentes, que reduzem a entropia da chave gerada, Para poder estimar a entropia de uma sequência de *bits*, é necessário normalmente um largo número de *bits*, os quais podem não ser possivel de se obter na prática. Por exemplo, considerando que quando gerando uma chave de 128 *bits*, existem 2^{128} permutações possíveis de *bits*. Um verdadeiro gerador de *bits* aleatórios deverá gerar cada uma das 2^{128} permutações com igual probabilidade (ZENG, 2015). Assim, conforme (WEI et al., 2013), para estimar a entropia de uma sequência curta de *bits* finitos, pode-se aplicar o conceito de entropia aproximada e usar a medição de complexidade Lempel-Ziv (medida de imprevisibilidade e complexidade de uma série) (ZIV; LEMPEL, 1978).