Comunicações de Computador 218 (2024) 176–187

Listas de conteúdo disponíveis emCiência Direta

Comunicações de Computador

Página inicial do jornal:www.elsevier.com/locate/comcom

Um esquema de segurança de camada física para redes sem fio 6G usando criptografia pós-quântica

Walid Abdallah*

Universidade de Cartago, Escola Superior de Comunicação de Túnis (SUP' COM), LR11TIC04, Laboratório de Pesquisa em Redes de Comunicação e Segurança. & LR11TIC02, Laboratório de Pesquisa de Sistemas de Comunicação Verdes e Inteligentes, Tunísia
Escola de Aviação Borj El Amri, Tunísia

INFORMAÇÕES DO ARTIGO

Palavras-chave:
Redes 6G
Segurança da camada física
OFDM
Criptografia baseada em rede

ABSTRATO

A sexta geração (6G) de redes móveis está preparada para revolucionar as capacidades de comunicação com o seu alcance infinito. Estas redes apresentarão uma topologia ultradensa, acomodando uma ampla gama de dispositivos, desde macrodispositivos como satélites até nanodispositivos integrados no corpo humano. No entanto, o extenso tráfego de dados processado pelas redes 6G, uma parte significativa do qual é de natureza sensível, apresenta um desafio de segurança. Este artigo apresenta o projeto e implementação de um esquema de criptografia que garante a confidencialidade da transmissão de dados na camada física de redes 6G. A arquitetura de segurança da camada física proposta baseia-se na criptografia de rede, onde cada usuário está associado a um par de bases (uma base pública e uma base privada) e um conjunto de subportadoras ortogonais. O processo de criptografia envolve a projeção do vetor dos símbolos de modulação de amplitude em quadratura (QAM) dos dados transmitidos na base pública do usuário. Um vetor de erro aleatório é então adicionado antes de aplicar a transformada inversa de Fourier da técnica de multiplexação por divisão ortogonal de frequência (OFDM). A segurança deste esquema de criptografia depende da complexidade do problema vetorial mais próximo em uma rede inteira. Para avaliar sua eficácia, analisamos a segurança de nossa criptografia de camada física baseada em rede em relação às propriedades dos pares de bases e vetores de erro. Nossas descobertas indicam que o esquema proposto oferece proteção de segurança satisfatória contra ataques de espionagem, aumentando significativamente a confidencialidade do sinal transmitido. Além disso, avaliamos o desempenho do nosso projeto através de experimentos numéricos, demonstrando sua resiliência contra diversos ataques de segurança.

1. Introdução

A sexta geração de redes móveis sem fio abrangerá uma gama diversificada de nós, abrangendo desde nanodispositivos implantados no corpo humano até macrodispositivos de comunicação integrados em sistemas de plataformas de alta altitude (HAPS) ou satélites. Espera-se que a evolução das redes 5G para 6G aprimore ainda mais o conceito de Internet de Todas as Coisas (IoE), garantindo desempenho consistente em dispositivos e ambientes (aéreo, espacial, terrestre, marítimo) e fornecendo conectividade onipresente [1–4]. O futuro padrão 6G testemunhará uma distribuição intensificada da implantação da rede, refletindo a sua natureza distributiva. O estabelecimento de conectividade autônoma e infinita, facilitada por esta tecnologia emergente, será apoiado por avanços recentes em inteligência artificial, aprendizado de máquina e técnicas modernas de processamento de sinais. Essas técnicas incluem detecção compressiva, teoria de matriz finita aleatória, recozimento simulado, entre outras.

Devido à grande quantidade de dados confidenciais que serão tratados por esta nova geração de redes ultradensas, garantir a privacidade e a segurança será de extrema importância [5,6]. A este respeito, as técnicas de segurança da camada física (PLS) podem desempenhar um papel significativo na segurança das redes 6G, oferecendo uma abordagem ascendente para garantir a confidencialidade nas diferentes camadas da arquitetura de comunicação. O PLS aproveita as características físicas do ambiente de transmissão para obter uma vantagem de segurança contra ataques passivos e ativos que visam comprometer a confidencialidade dos dados. Tem havido um recente aumento de interesse em projetar e desenvolver técnicas eficientes de segurança da camada física para privacidade de transmissão de dados em redes 6G. A implementação de medidas de segurança na camada física pode aumentar as taxas de transmissão e manter a transparência do protocolo e do formato dos dados. No entanto, isto representa uma tarefa desafiadora devido ao paradigma de conectividade disruptivo esperado nas redes 6G, que aumentará as vulnerabilidades e os ataques direcionados à infraestrutura de comunicação. Além disso, a integração prevista de processamento baseado em computação quântica

*Correspondência para: Universidade de Cartago, Escola Superior de Comunicação de Túnis (SUP' COM), LR11TIC04, Laboratório de Pesquisa em Redes de Comunicação e Segurança. & LR11TIC02,Laboratório de Pesquisa de Sistemas de Comunicação Verdes e Inteligentes, Tunísia.
*Endereço de email:*walid.abdallah@supcom.tn.

https://doi.org/10.1016/j.comcom.2024.02.019
Recebido em 19 de julho de 2023; Recebido em formato revisado em 28 de janeiro de 2024; Aceito em 20 de fevereiro de 2024.
Disponível online em 21 de fevereiro de 2024.

e algoritmos de busca [7–9] ampliará ainda mais o número de ameaças. Algoritmos criptográficos clássicos que dependem da dureza do logaritmo discreto e de problemas de fatoração primária, como RSA e Diffie-Hellman, se tornarão obsoletos [10]. Além disso, abordagens de segurança baseadas em criptografia quântica [11] estão atualmente limitados aos procedimentos de distribuição de chaves. A segurança desta abordagem baseia-se no fato de que a observação de um sistema quântico perturba inevitavelmente o seu estado, facilitando a detecção de ataques de espionagem. No entanto, também introduz maior complexidade e custo do sistema.

Neste artigo, propomos um esquema de segurança da camada física que aproveita a criptografia pós-quântica para aumentar a segurança da comunicação em redes 6G. Este esquema é baseado em um sistema criptográfico de chave pública que explora a dureza computacional de problemas de pontos de rede para criptografar fluxos de dados. Ao contrário dos atuais esquemas de criptografia pública, como RSA ou ElGamal, que são baseados na dureza média do caso, os esquemas de criptografia baseados em rede oferecem melhor segurança ao confiar na dureza do pior caso [12]. O esquema de criptografia proposto é particularmente adequado para comunicações da camada física em redes 6G porque pode satisfazer os requisitos de eficiência de processamento de sinal e alta capacidade de transmissão dessas redes. O procedimento de criptografia assume que cada usuário possui uma base privada e uma base pública composta por números inteiros. A comunicação da camada física emprega a técnica de multiplexação por divisão ortogonal de frequência (OFDM). O transmissor inicialmente mapeia o fluxo de bits de dados para um vetor de símbolos modulados em amplitude em quadratura (QAM). Em seguida, ele projeta esse vetor na base pública do receptor, adiciona um ''vetor de erro'' aleatório e aplica a transformada rápida inversa de Fourier do processo OFDM. O receptor recupera os dados transmitidos projetando o fluxo modulado criptografado em sua base privada, encontrando o vetor mais próximo e aplicando o procedimento de desmodulação da técnica OFDM.

Para melhorar o desempenho do criptossistema assimétrico, estudamos os requisitos relacionados ao vetor de erros gerado e adicionado ao fluxo de dados modulados criptografados. Demonstramos que a técnica de criptografia baseada em rede proposta é adequada para as restrições de transmissão da camada física e oferece um nível aceitável de segurança quando parâmetros específicos relativos ao procedimento de criptografia baseado em rede são adequadamente selecionados. Além disso, as diferentes operações realizadas pelos processos de criptografia/descriptografia são quadráticas (baseadas principalmente na multiplicação de matrizes), que podem ser adaptadas às restrições em tempo real da comunicação da camada física em redes 6G.

Além disso, a segurança do esquema baseia-se na complexidade do problema vetorial mais próximo em redes, que se acredita ser resistente à computação quântica quando parâmetros específicos, como a dimensão da rede e o procedimento de geração do vetor de erro, são adequadamente selecionados. . No entanto, vale a pena notar que o esquema proposto pode ser aplicado a qualquer transmissão baseada em múltiplas portadoras, particularmente OFDM, que apresenta maior eficiência espectral e imunidade robusta ao desvanecimento e à interferência intersimbólica. Além disso, até onde sabemos, nosso trabalho é o primeiro a propor o uso de esquemas de criptografia baseados em rede para proteger a transmissão de fluxos de dados na camada física de redes sem fio.

O restante do artigo está estruturado da seguinte forma: Seção2 apresenta uma revisão dos principais trabalhos relacionados às técnicas de segurança da camada física; Seção3apresenta os conceitos matemáticos relacionados à criptografia baseada em rede; Seção4apresenta o esquema de segurança da camada física que utiliza OFDM e a técnica de criptografia baseada em rede; Seção5dedica-se à análise de segurança e avaliação de desempenho do esquema de segurança da camada física proposto usando uma estrutura de simulação; e por fim, Seção6conclui o artigo e discute futuras extensões para este trabalho.

2. Trabalho relacionado

A segurança da camada física (PLS) é reconhecida há décadas como uma defesa de linha de frente que pode fornecer segurança mesmo para dispositivos com recursos limitados [13]. O PLS é considerado um complemento valioso às técnicas de criptografia na proteção de redes sem fio. Enquanto a criptografia depende do poder computacional limitado dos adversários, o PLS aproveita a assimetria na qualidade de recepção entre o receptor legítimo e o invasor, aproveitando os modelos de propagação de canal e as condições ambientais para obter vantagens de segurança.

Vários trabalhos recentes forneceram visões gerais de técnicas de segurança da camada física. Em [14]autores apresentam classificação e aplicação de técnicas de PLS. O papel [15] discute questões de pesquisa abertas e visões futuras para a aplicação de PLS em redes de próxima geração. Em [16] são exploradas técnicas de segurança da camada física e sua implantação na segurança de redes 6G. Além disso, em [17] é investigado o potencial da segurança da camada física no fornecimento de segurança para redes de acesso 6G. Os princípios de segurança da camada física, bem como técnicas para sistemas de comunicação com antena única e multiantena, ambientes multiusuários e implantação de tecnologia de retransmissão, são discutidos em [18]. Os desafios da segurança da comunicação sem fio, especialmente na camada física, são descritos em [19]. Abordagens de autenticação e segurança de transferência para redes heterogêneas 5G (HetNet) usando redes definidas por software (SDN) são descritas em [20]. O papel [21] explora as oportunidades e os desafios da utilização da impressão digital do transceptor do dispositivo para autenticação e privacidade na camada física. Uma visão geral da identificação e autenticação de usuários em redes sem fio usando técnicas não criptográficas de segurança da camada física é apresentada em [22]. Técnicas PLS usando múltiplas entradas múltiplas saídas (MIMO) e técnicas de codificação de erros são detalhadas em [23,24] respectivamente. Além disso, a exploração da incerteza do canal para projetar soluções PLS eficazes é discutida em [25]. Uma revisão abrangente das tecnologias de autenticação e negociação da camada física é alcançada em [26].

Muitos esquemas de segurança da camada física que dependem de técnicas de multiplexação por divisão de frequência ortogonal (OFDM) e múltiplas entradas e múltiplas saídas (MIMO) surgiram nos últimos anos como soluções para fornecer confidencialidade na transmissão de dados na nova geração de redes de comunicação. Estas duas tecnologias podem garantir transmissão de grande capacidade com maior eficiência espectral, alocação flexível de recursos, baixo custo e resiliência contra interferências entre símbolos e fenômenos de desvanecimento.

Em [27] foram propostos dois esquemas de segurança da camada física baseados em OFDM. O primeiro usa pré-codificação no domínio do tempo que emprega intercalação e escalonamento, e o segundo usa um comprimento de prefixo cíclico aleatório para tornar aleatório o período do símbolo OFDM. Ambas as técnicas são realizadas de acordo com uma chave secreta pré-compartilhada entre as partes legítimas.

O trabalho publicado em [28] propuseram um esquema de segurança de camada física baseado em OFDM para redes de rádio cognitivas. O esquema considera a transmissão de retransmissão onde um nó de retransmissão encaminhará o pacote de dados e outro nó de retransmissão gerará ruído aleatório para evitar que um bisbilhoteiro receba corretamente as informações transmitidas. Isto é conseguido otimizando a alocação de energia e subportadoras no nó de origem e no nó de retransmissão.

Um esquema de segurança de camada física baseado em detecção compactada para sistemas de Internet das Coisas (IoT) foi apresentado em [29]. Neste esquema, uma chave secreta é derivada dinamicamente das medições do canal e é usada para codificar o sinal OFDM transmitido. A esteganografia sem fio também foi investigada em [30] para garantir a segurança na camada física das redes IoT, ocultando o sinal OFDM secreto em um sinal de cobertura OFDM pré-codificado por Transformada Discreta de Fourier (DFT). Autores em [31] tentaram melhorar a segurança da comunicação da camada física usando a técnica de encurtamento de canal. O conceito básico é tornar o canal menor ou igual ao prefixo cíclico (CP) nos usuários legítimos, enquanto ele parecerá mais longo que o CP no usuário atacante. O recente trabalho publicado em [32] abordou o projeto de um esquema flexível de segurança da camada física que pode proteger tanto a transmissão de dados quanto a transmissão piloto para evitar a estimativa do canal pelo invasor. Esquemas de segurança da camada física que garantem transmissão segura de baixa latência além do 5G

redes foram descritas em [33]. Os autores neste trabalho demonstram que é possível realizar a privacidade de transmissão bidirecional com latência reduzida usando um protocolo que pode otimizar o uso de recursos de tempo-frequência. A geração artificial de ruído piloto para combater a escuta de sinal e garantir a comunicação OFDM segura foi investigada em [34]. Além disso, o trabalho em [35] explora a técnica de inserção de erro de fase para melhorar a transmissão OFDM. Isto é conseguido girando o mapeamento da constelação dos símbolos modulados M-PSK usando uma chave pré-compartilhada e aproveitando o desvanecimento do canal das subportadoras para introduzir erro de fase no símbolo codificado de acordo com o estado do canal. O projeto de um transceptor embarcado em veículo aéreo não tripulado para permitir comunicação segura full-duplex entre o usuário móvel e a estação base terrestre foi apresentado em [36]. O sistema de comunicação proposto emprega um algoritmo de criptografia auxiliado por transformação de cosseno de mapa logístico entrelaçado (ILM) combinado com ruído artificial que aumenta a segurança da camada física (PLS) para garantir a transmissão segura do sinal OFDM com preenchimento de zero.

Vários outros artigos têm se interessado em usar técnicas de criptografia para fornecer segurança na camada física. O trabalho publicado em [37] se concentra em melhorar a segurança da camada física em redes ópticas passivas (PONs) baseadas em multiplexação por divisão de comprimento de onda (WDM). A proposta prevê um protocolo de troca de chaves Diffie-Hellman baseado em curva elíptica para distribuição segura de chaves entre o terminal de linha óptica (OLT) e a unidade de rede óptica (ONU). O Advanced Encryption Standard (AES) é então empregado para criptografar os dados transmitidos, com criptografia aplicada a dados parciais do canal I/Q para reduzir o tempo de processamento. A transmissão bem-sucedida de um sinal criptografado OFDMA modulado de 16 QAM ao longo de uma distância de 100 km dentro de valores aceitáveis da relação de potência de pico para média é alcançada. Além disso, um esquema de criptografia de camada física usando indução de frequência para sistemas de transmissão baseados em OFDM foi introduzido em [38]. O projeto do transceptor foi implementado em um FPGA Virtex-7 e consiste em um módulo de mudança de frequência baseado em chave secreta e um módulo de criptografia. A operação de descriptografia é realizada por um sincronizador modificado configurado com a mesma chave.

Abordagens de segurança da camada física baseadas no caos foram discutidas em alguns artigos. O trabalho em [39] propuseram o projeto de um sistema de comunicação multientrada e multisaída (MIMO) usando matrizes unitárias variantes no tempo baseadas no caos. A segurança prática da camada física foi alcançada por meio de codificação diferencial sem o uso de estimativa de canal. Autores em [40] abordou o aprimoramento da segurança da camada física em sistemas MIMO OFDM usando uma técnica de criptografia caótica multinível. Isto é realizado primeiro embaralhando o símbolo modulado usando uma matriz de pré-codificação gerada com uma sequência caótica única e, em seguida, um segundo nível de criptografia é alcançado por embaralhamento de fase com base no mapeamento seletivo e em uma sequência caótica. Em outro trabalho recente [41], um esquema de segurança da camada física usando técnica de pré-codificação de reversão de tempo combinada com injeção de ruído artificial foi proposto para sistemas de comunicação baseados em Differential Chaos Shift Keying (OFDM-DCSK) para garantir maior capacidade de transmissão com maior confidencialidade e confiabilidade.

O uso da tecnologia de comunicação por luz visível (VLC) é considerado uma forma de segurança da camada física porque permite o confinamento do sinal transmitido dentro da área coberta pelo ponto de acesso baseado em luz. Um esquema de segurança de camada física para redes VLC baseadas em OFDM usando criptografia caótica foi proposto em [42]. Neste esquema, o texto cifrado foi gerado dinamicamente aproveitando a natureza aleatória das chaves caóticas e dos dados transmitidos. A alocação de subportadoras nos domínios de tempo e frequência é obtida de acordo com uma permutação caótica e reversão de subportadoras. Os autores mostram que seu sistema de comunicação baseado em VLC pode resistir a ataques de criptoanálise de texto simples conhecidos e escolhidos. Em [43] é estudado o projeto de uma solução de backhaul óptico para redes de fidelidade à luz (LiFi). Esta proposta apresenta uma estrutura de ponto de acesso LiFi que implementa técnicas de multiplexação por divisão ortogonal de frequência (OFDM) e codificação óptica. para fornecer acesso multiusuário e permitir processamento e transmissão totalmente ópticos na rede backhaul. Além disso, uma técnica de codificação/decodificação óptica sintonizável baseada no atraso de pulsos ópticos em um vetor de loops de linha de atraso óptico (ODL) é projetada para facilitar o mapeamento eficiente do acesso baseado em OFDM e encaminhamento de dados na rede óptica de backhaul.

Embora os trabalhos acima mencionados constituam contribuições valiosas para o desenho de esquemas de segurança da camada física eficientes e confiáveis, eles, no entanto, apresentam alguns limites. Em primeiro lugar, a maioria dos esquemas propostos baseia-se no conhecimento preciso do modelo de propagação do canal e das posições do remetente, receptor e atacante. Em muitos casos, estes pressupostos não são práticos, especialmente num cenário móvel onde as diferentes partes se movem a velocidades muito elevadas. Além disso, as técnicas de criptografia utilizadas para fornecer confidencialidade nessas abordagens de segurança da camada física são baseadas em algoritmos de criptografia de chave simétrica, que exigem o pré-compartilhamento de chaves de criptografia entre o transmissor e o receptor. Isto é difícil de gerenciar e menos seguro do que quando se usa troca dinâmica e estabelecimento de chaves de criptografia usando algoritmos de criptografia de chave pública. Finalmente, os procedimentos de criptografia existentes empregados nos esquemas PLS descritos não são resistentes ao processamento quântico baseado em computador, e a maioria deles será eliminada do uso quando a próxima era quântica começar.

Consequentemente, muitos trabalhos recentes concentraram-se na implementação de esquemas de criptografia pós-quântica baseados em rede. Em [44] são apresentadas implementações ASIC de dois algoritmos criptográficos pós-quânticos, NTRU e TTS. O principal objetivo é aproveitar a eficiência de processamento de hardware desses algoritmos para proteger sistemas de comunicação máquina a máquina. Além disso, em [45] o uso de criptografia baseada em rede na era da computação quântica é discutido para proteger a Internet das Coisas (IoT). Uma visão geral abrangente dos esquemas de criptografia pós-quântica baseados em rede pode ser encontrada em [46]. Este artigo fornece uma exploração detalhada de algoritmos criptográficos baseados em rede e suas aplicações no contexto da criptografia pós-quântica. Adicionalmente, [47] apresenta uma implementação ultrarrápida baseada em FPGA de operações aritméticas usadas em algoritmos de criptografia pós-quântica. O artigo se concentra na aceleração da computação de operações criptográficas necessárias para esquemas baseados em rede, aproveitando os recursos da tecnologia FPGA para alcançar implementações de alto desempenho. Em nosso trabalho anterior publicado em [48,49], propusemos um esquema de criptografia de chave pública baseado em rede para proteger a transmissão de acesso múltiplo por divisão de código óptico (OCDMA). Demonstramos que este esquema supera as soluções existentes em termos de robustez contra ataques de criptoanálise. Esta abordagem ajuda a reduzir a sobrecarga de processamento normalmente observada nas abordagens clássicas de chave pública e aumenta a eficiência da transmissão do sinal criptografado.

Nosso principal objetivo neste trabalho é desenvolver um esquema de comunicação seguro que ofereça maior confidencialidade para transmissão de dados sem fio na camada física. Para este fim, desenvolvemos um esquema de criptografia que utiliza sistemas criptográficos de chave pública baseados em rede [12, 50–53]. No esquema proposto, o padrão de transmissão modulado OFDM é protegido projetando-o na base pública do receptor e adicionando um vetor pseudo-aleatório semelhante a ruído gerado de acordo com regras específicas. O receptor pode recuperar a mensagem transmitida decifrando o sinal recebido utilizando sua base privada (chave privada) e realizando operações de desmodulação OFDM.

Comparado às abordagens existentes, o esquema PLS proposto não requer nenhum conhecimento sobre as características de propagação do canal ou sobre as posições das entidades evoluídas. Além disso, nenhuma chave secreta deve ser pré-compartilhada entre o transmissor e o receptor para iniciar uma comunicação segura. De fato, neste trabalho, a criptografia de chave pública baseada em rede é executada diretamente no fluxo de dados e não é usada para troca segura de chaves simétricas, como implementado na maioria dos protocolos de segurança (IPsec, SSL/TLS, etc.). Acreditamos também que

O esquema projetado pode permanecer seguro mesmo quando a computação quântica se tornar praticamente disponível, desde que alguns parâmetros, nomeadamente a dimensão da rede e o vetor de ruído de erro, sejam adequadamente selecionados.

Além disso, é digno de nota que o esquema PLS projetado pode ser usado para proteger qualquer comunicação baseada em multiportadoras (OFDM). No entanto, o principal objetivo do nosso trabalho é aumentar a segurança nas redes sem fio 6G porque elas se destinam a permitir altas capacidades de transmissão e integração perfeita de dispositivos muito heterogêneos.

3. Antecedentes da criptografia baseada em rede

Nesta seção, fornecemos a base matemática do esquema de criptografia baseado em rede proposto, usado para fornecer segurança da camada física (PLS) em redes 6G. Começamos apresentando os aspectos teóricos relacionados aos reticulados. As redes são estruturas matemáticas que desempenham um papel crucial no projeto de esquemas de criptografia baseados em redes. A seguir, descrevemos os problemas difíceis que são utilizados no projeto de esquemas de criptografia de chave pública baseados em pontos de rede. Esses problemas constituem a base da segurança da criptografia baseada em rede e envolvem desafios computacionais que se acredita serem difíceis de resolver de forma eficiente. Ao aproveitar estes problemas difíceis, os esquemas de criptografia baseados em rede oferecem uma abordagem promissora para alcançar comunicação segura em redes 6G. É digno de nota que nesta seção lemas e teoremas são apresentados sem provas, a maioria dos quais pode ser encontrada em [54].

3.1. Matemática para rede inteira

Introduzimos aspectos teóricos relativos a objetos matemáticos chamados de redes inteiras. Assim, começamos fornecendo definições e discutindo propriedades interessantes desses objetos.

Uma rede inteira pode ser definida como um conjunto discreto de pontos em um espaço multidimensional, onde cada ponto possui coordenadas inteiras. Pode ser representado como uma estrutura de grade com pontos localizados na interseção de coordenadas inteiras. A rede se estende infinitamente em todas as direções. Formalmente, uma rede é um conjunto de pontos em espaço -dimensional com uma estrutura periódica definida da seguinte forma:

Definição 1(*Malha*)**.**Dado -vetores linearmente independentes, $_1, _2,\ldots, \in \mathbb{R}$, a rede gerada por eles é definida como

$$( ) = \{ = \sum_{=1} , \in \mathbb{Z}\} \quad (1)$$

onde é um × matriz cujas colunas são $_1, _2,\ldots, $. Dizemos que o posto da rede é e sua dimensão é . Se = , a rede é chamada de rede de classificação completa. Em nosso trabalho consideraremos apenas reticulados de classificação completa.

Doravante, o termo ''base'' será usado para se referir tanto à matriz e a coleção de vetores $_1, _2,\ldots, $. Uma peculiaridade de uma rede é que ela possui múltiplas bases. Pode-se observar que uma rede é semelhante a um espaço vetorial, com a distinção de que os vetores em uma rede são obrigados a serem multiplicados por inteiros. Apesar desta restrição aparentemente menor, ela dá origem a numerosos problemas intrigantes e sutis.

Um problema inicial que podemos colocar é como determinar se um determinado conjunto de vetores forma uma base. Portanto, torna-se necessário introduzir alguns conceitos adicionais.

Definição 2(*Período*)**.**A extensão de uma rede ( )é um espaço linear gerado por seus vetores,

$$(( )) = ( ) = \{ , \in \mathbb{R}\} \quad (2)$$

Definição 3(*Paralelepípedo Fundamental*)**.**Para qualquer base de rede definimos o paralelepípedo fundamental como:

$$( ) = \{ , \in \mathbb{R}, \forall : 0 \leq < 1\} \quad (3)$$

Devemos notar que o paralelepípedo fundamental, ( )depende da base . Além disso, um ladrilho de todo o (( ))pode ser obtido colocando uma cópia do ( )em cada ponto da rede ( ). Consequentemente, para verificar se um conjunto de vetores linearmente independentes formam uma base de uma determinada rede, podemos provar que este conjunto deve satisfazer a condição dada pelo seguinte lema.

Lema 1.*Deixar ser uma rede de classificação ,e deixar* $_1, _2,\ldots, \in$ *ser vetores de rede linearmente independentes. O conjunto de vetores* $_1, _2,\ldots,$ *constitui uma base de se e apenas se* $(_1, _2, _3,\ldots,) \cap = \{0\}$*. Onde* $(_1, _2,\ldots,)$*é o paralelepípedo fundamental construído usando vetores* $_1, _2,\ldots,$ *conforme definido anteriormente.*

Outra questão importante relativa às bases da rede é como determinar se duas bases pertencem à mesma rede. Para resolver isso, precisamos introduzir a noção de matriz unimodular.

Definição 4(*Matriz Uni-Modular*)**.**Uma matriz $\in \mathbb{Z}^{\times}$ é chamado unimodular, se seu determinante for verificado, $( ) = \pm 1$

O lema a seguir afirma que uma propriedade importante da matriz unimodular é que sua inversa também é unimodular. Consequentemente, o conjunto de matrizes unimodulares forma um grupo sob multiplicação de matrizes.

Lema 2.*se é uma matriz unimodular então* $^{-1}$ *também é unimodular, em particular* $^{-1} \in \mathbb{Z}^{\times}$

Portanto, podemos provar que duas bases geram a mesma rede se satisfizerem a seguinte condição.

Teorema 1.*Duas bases e são equivalentes se e somente se* $= $ *, onde é uma matriz unimodular.*

Um parâmetro principal que caracteriza uma determinada rede é o seu determinante definido da seguinte forma:

Definição 5(*Determinante da rede*)**.**Deixar ( )ser uma rede de classificação completa . O determinante de , denotado ( )é definido como o volume dimensional de ( ), e nós temos $( ) = |( )|$.

Podemos notar que o determinante da rede independe da escolha da base , já que aplicando o teorema1todas as bases de uma determinada rede têm o mesmo determinante (até o sinal).

Além disso, veremos que nos esquemas de criptografia propostos precisamos criar bases com alto grau de ortogonalidade. A razão de Hadamard é um parâmetro que mede o quanto os vetores de uma base são ortogonais. É definido da seguinte forma:

Definição 6(*Razão Hadamard*)**.**se é um verdadeiro não-singular × matriz. A proporção de Hadamard de é definido como:

$$-( ) = \prod \left[\frac{|( )|}{\| \|} \right]_{1-} \quad (4)$$

onde$\| \|$é a norma euclidiana da i'ésima coluna em .

As colunas de são ortogonais entre si se e somente se $-( ) = 1$;de outra forma$0 < -( ) < 1$.Ao comparar diferentes bases da mesma rede em$\mathbb{R}$, nos preocupamos apenas com o produto do$\| \|$'desde então ( )é o mesmo para todas as bases e serve apenas como fator normalizado.

Podemos notar que a ortogonalidade é uma das maiores preocupações na construção de uma base. Conseqüentemente, uma técnica útil usada na teoria de redes é a ortogonalização de Gram-Schmidt. Este procedimento leva vetores linearmente independentes e cria um conjunto de vetores ortogonais. Realiza uma projeção de cada vetor no espaço ortogonal ao vão dos vetores anteriores. O teorema a seguir fornece uma descrição formal do procedimento de construção

Teorema 2. *Dada uma sequência de vetores linearmente independentes* $_1, _2, \ldots, , $ *podemos construir vetores ortogonais* $??_1, _2, \ldots, $ *pelo seguinte procedimento:*

$$_1 = _1, \quad = 2 \ldots , \quad = - \sum_{=1}^{-1} \tilde{} \quad = \frac{\langle , \rangle}{\| \|^2}$$

É fácil verificar que $(_1, _2, \ldots,) = \prod_{=1} \| \|$ $(_1, _2, \ldots,)$ e $((= _1, _2, \ldots,)) =$

3.2. Problemas difíceis em redes

Os dois problemas computacionais fundamentais associados a uma rede são aqueles de encontrar um vetor diferente de zero mais curto e um vetor na rede que seja o mais próximo de um determinado vetor não-rede. A segurança do algoritmo de chave pública adotado baseia-se na intratabilidade desses dois problemas computacionais em redes.

- O problema do vetor mais curto (SVP): dada uma rede ( ), encontre o menor vetor diferente de zero da rede, ou seja, encontre o vetor diferente de zero $\in$ que minimiza a norma$\| \|$.Minkowski dá uma vantagem limite do comprimento do vetor mais curto que é $\sqrt{}(( ))$ mas ele não nos fornece um algoritmo para encontrar tal vetor.
- O problema do vetor mais próximo (CVP): dada uma base para uma treliça em R e outro vetor $\in$R o problema de encontrar o vetor mais próximo em ( ) é NP-difícil para qualquer norma emR .

Tanto o SVP quanto o CVP são problemas profundos e ambos se tornam computacionalmente difíceis à medida que a dimensão da rede cresce. Está provado que estes dois problemas são NP-difíceis. Existem muitas variantes importantes de SVP e CVP que surgem tanto na teoria quanto na prática. Descrevemos alguns deles que são úteis na construção do criptossistema.

- O menor problema de base (SBP): Dada uma base para uma treliça em R , o objetivo é encontrar a menor base para a mesma treliça. Existem muitas variantes deste problema, dependendo do significado exato da menor. Neste contexto nos preocupamos com bases com alto índice de Hadamard. Assim consideramos a versão na qual procuramos a base de ( )que tem uma proporção de Hadamard muito próxima de1.
- Problema aproximado do vetor mais curto (apprSVP): deixe ( )ser uma função de . Em uma treliça ( )de dimensão , encontre um vetor diferente de zero que não seja maior que ( )vezes mais longo que um vetor diferente de zero mais curto. Em outras palavras, se é um vetor diferente de zero mais curto em , encontre um vetor diferente de zero $\in$ ( )satisfatório$\| \| \leq ( ) \| \|$. Cada escolha de função ( )fornece um apprSVP diferente.
- Problema do vetor mais próximo aproximado (apprCVP): É o mesmo que apprSVP, mas agora estamos procurando um vetor que seja uma solução aproximada para CVP, em vez de uma solução aproximada para SVP.

Esses problemas não possuem algoritmos de tempo polinomial conhecidos e o melhor algoritmo de aproximação de tempo polinomial para o tema é o algoritmo LLL e suas variantes [55]. A descrição desses algoritmos será dada na próxima subseção.

3.3. Algoritmos para resolver problemas de rede

Alguns algoritmos de tempo polinomial são desenvolvidos na literatura para fornecer uma solução aproximada para problemas reticulados difíceis. Os fatores de aproximação desse algoritmo são , onde é uma constante que pode ser muito pequena e é a dimensão da rede. Assim, esses algoritmos são ineficientes quando a dimensão da rede aumenta. Os dois algoritmos que serão apresentados nesta seção são o algoritmo de Babai usado para resolver o apprCVP e o algoritmo LLL usado para resolver o apprSVP e o SBP.

3.3.1. Algoritmo de Babai para resolver o apprCVP

Este algoritmo é baseado na observação de que se uma rede $\subset$R tem uma base ortogonal $_1, _2, \ldots, $, é fácil resolver o CVP. É tentador tentar um procedimento semelhante com uma base arbitrária de . Se os vetores na base forem razoavelmente ortogonais entre si, então provavelmente teremos sucesso na resolução do CVP; mas se os vetores de base forem altamente não ortogonais, o algoritmo não funcionará bem. Assim, podemos usar o seguinte teorema para encontrar o ponto da rede mais próximo de qualquer elemento deR .

Teorema 3. *Deixar* $\subset$R *seja uma rede com base* $_1, _2, \ldots,$ *e deixar* $\in$R *seja um vetor arbitrário. Se os vetores na base forem suficientemente ortogonais entre si, então o algoritmo a seguir resolve o CVP.*

Escrever como uma combinação linear de $_1, _2, \ldots, , = _1 _1 + _2 _2 + _3 _3 + \cdots +$ *onde* $_1, _2, \ldots, \in$R

para $=1,2,\ldots, ,$ *definir* $=\lceil \rfloor$ *onde* $\lceil \rfloor$ *é o operador de teto. Vetor de retorno* $= _1 _1 + _2 _2 + \cdots +$

Em geral, se os vetores na base são razoavelmente ortogonais entre si, então o algoritmo resolve alguma versão do apprCVP, mas se os vetores da base são altamente não ortogonais, então o vetor retornado pelo algoritmo geralmente está longe da rede mais próxima. vetor ponto para .

3.3.2. O algoritmo de redução de rede LLL

LLL é um algoritmo usado para encontrar o vetor mais curto em uma rede e para reduzir a base da rede. Suponha que nos seja dada uma base = $\{ _1, _2, \ldots, \}$para uma treliça . O objetivo deste algoritmo é transformar esta base em uma base melhor no sentido de que seus vetores sejam os mais curtos possíveis e mais ortogonais entre si. É óbvio que encontrar tal base e aplicar o algoritmo de Babai dará uma solução melhor para o apprCVP. Este algoritmo é baseado na seguinte definição

Definição 7(*LLL reduzida*)**.**Deixar = $\{ _1, _2, \ldots, \}$ser uma base para um treliça e deixar$??= \{\tilde{} _1, _2, \ldots, \}$ser o Gram-Schmidt associado base ortogonal conforme descrito porTeorema 2. A base é considerado LLL reduzido se satisfizer as duas condições a seguir:

1. Condição de tamanho $| | = \frac{| |}{\| \|^2} \leq _{\frac{1}{2}} \quad 1 < \leq$
2. Condição de Lovasz$\| \|^2 \geq (_{\frac{3}{4}} - _{, -1}^2) \| ??_{-1} \|^2 \quad 1 < \leq$

O resultado fundamental do algoritmo LLL é a seguinte teoria rem

Teorema 4. *Deixar ser uma rede de dimensão .qualquer base reduzida de LLL* $\{ _1, _2, \ldots, \}$ *para tem as seguintes propriedades:*

$\prod_{=1} \| \| \leq 2^{\frac{(-1)}{4}} ( )$

$\| \| \leq 2^{(-1)/2} \| ?? \| \quad$ *para todos* $1 \leq \leq \leq$

Além disso, o primeiro vetor em uma base reduzida LLL satisfaz

$\| _1 \| \leq 2^{\frac{(-1)}{4}} | ( )| \; e \| _1 \| \leq 2^{\frac{1}{2}} (\| \|) \; 0 \in \neq$

Assim, uma base reduzida LLL resolve apprSVB dentro de um fator de $2^{\frac{-1}{2}}$.É claro que este problema se torna intratável quando a dimensão da rede é muito grande.

3.4. Criptosistema baseado em rede

Vários algoritmos de criptografia de chave pública que exploram a dureza de SVP e CVP em uma rede são apresentados. O mais importante deles é o criptossistema Ajtai – Dwork [12], o criptossistema NTRU proposto por Hoffstein, Pipher e silverman [51], e o criptossistema GGH [50] de Goldreich, Goldwasser e Halevi. Em nosso trabalho selecionamos este último criptossistema para garantir a segurança da camada física em redes 6G. Nossa escolha é justificada pela simplicidade e baixo overhead de criptografia do algoritmo GGH. Na verdade, este algoritmo é baseado na observação de que o algoritmo mais conhecido para resolver

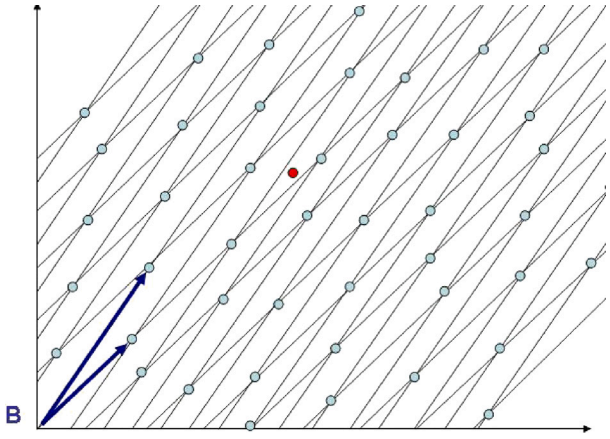

Figura 1. Projeção de ponto em base pública.

apprCVP não poderia ser eficiente se uma base "ruim" fosse selecionada para resolver este problema. Uma base ruim é uma base cujos vetores não são ortogonais e uma base boa é uma base cujos vetores são quase ortogonais e que dá uma boa aproximação do problema CVP. O princípio do processo de criptografia é o seguinte:

Um usuário que deseja receber uma mensagem segura começa escolhendo um conjunto de vetores linearmente independentes

$\{ 1, 2,..., \} \in Z$

que são razoavelmente ortogonais entre si. Este conjunto de vetores é a chave privada do usuário. Deixar é o × matriz cuja coluna são $1, 2...,$ e é a rede gerada por esses vetores.

Em seguida o usuário deve selecionar uma matriz unimodular e então calcula

$$= \quad (5)$$

os vetores coluna de observado $1, 2,..., $ formar uma nova base de e são a chave pública do usuário e são transmitidas a todos os outros usuários que desejam se comunicar com este usuário.

Quando um transmissor deseja enviar uma mensagem confidencial para aquele usuário, ele transforma sua mensagem de texto simples em um vetor . Ele também seleciona um pequeno vetor de erro que atua como uma chave efêmera e então calcula o vetor

$$= (,) = + = \sum_{=1} + \quad (6)$$

é o texto cifrado. Devemos mencionar que não é um ponto de rede de , mas está próximo do ponto da rede porque é muito pequeno.

Um exemplo da construção e da projeção com base (no caso simples onde os pontos estão em um espaço bidimensional) é mostrado emFigura 1. O processo de criptografia transforma um ponto de rede em um ponto não-rede adicionando um pequeno vetor de erro . Considerando que o nosso exemplo mostra uma rede de dimensão 2, pode-se notar que é difícil encontrar o ponto original da rede projetando o ponto não-rede na base pública.

A função de descriptografia é executada usando o algoritmo de arredondamento de Babai com base privada para encontrar um vetor em que está perto . Como foi descrito anteriormente, isso é feito representando como uma combinação linear das colunas de e então arredonde os coeficientes dessa combinação linear para os números inteiros mais próximos para obter um ponto da rede. Desde é uma boa base e o erro é pequeno o ponto da rede é . Assim, multiplicando esses vetores por $^{-1}$recupera o texto simples . Formalmente, se denotarmos $= ^{-1}$, então $= ^{-1}$,e = - , onde⌈⌋o operador de teto.

Figura 2mostra a projeção do ponto não-rede na base privada. É claro que recuperar o ponto original da rede usando o

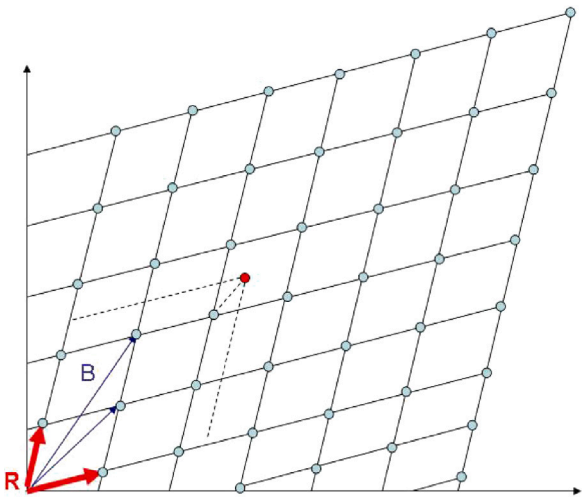

Figura 2. Projeção de ponto em base privada.

a base privada é mais fácil e eficiente do que usar a base pública. Isto se deve ao fato de os vetores da base privada serem mais curtos e mais ortogonais entre si do que os vetores da base pública.

4. Descrição do esquema de segurança da camada física

Nesta seção, descreveremos o esquema de segurança da camada física proposto. Começaremos fornecendo uma visão geral da arquitetura do esquema. Posteriormente, apresentaremos as diversas funções de processamento seguro empregadas para o sinal. Por fim, realizaremos uma análise de segurança do procedimento de criptografia proposto.

4.1. Arquitetura geral

Nesta subseção, descrevemos a arquitetura do sistema de segurança da camada física proposto. Como retratado emFigos. 3e4o sistema é composto por duas partes: o transmissor e o receptor. Forneceremos agora uma explicação detalhada das funções executadas pelo transmissor e pelo receptor.

O transmissor é composto por três blocos de processamento: modulação de dados, criptografia e processamento OFDM. O usuário começa gerando uma sequência de bits que são mapeados em uma sequência de modulação símbolos. Em aplicações práticas, modulação de amplitude em quadratura (QAM-M) é comumente usado para OFDM, onde representa o número de estados da modulação QAM e = $2( )$é o comprimento da sequência de bits representada por cada estado. Conseqüentemente, cada sequência de bits é m√ aplicado a um símbolo complexo = + onde , ∈ {±1,±3,...,± -1}.

Antes da modulação, uma conversão serial para paralelo é aplicada para formar um vetor de sequências de pedaços. representa a classificação da rede usada para criptografia e também corresponde ao número de subportadoras usado no processo OFDM. Assim, a entrada para o processo de criptografia é um vetor de símbolos complexos, $[0, 1,..., \quad ^{-1}]$ onde representa o símbolo QAM representa uma sequência de bits transmitida e corresponde a um ponto específico da constelação. A criptografia baseada em rede O processo é então aplicado a esse vetor, gerando um complexo criptografado vetor, $[0, 1,..., ^{-1}]$. Mais detalhes deste processo de criptografia serão explicados em uma subseção futura. Na próxima etapa, o processo OFDM é executado para gerar um sinal discreto no domínio do tempo $= [0, 1,..., ^{-1}]$ usando a transformada discreta inversa de Fourier, conforme indicado pela seguinte fórmula:

$$= \sqrt{} \frac{1}{} \sum_{=0}^{1} \exp(2), 0 \leq \leq -1 \quad (7)$$

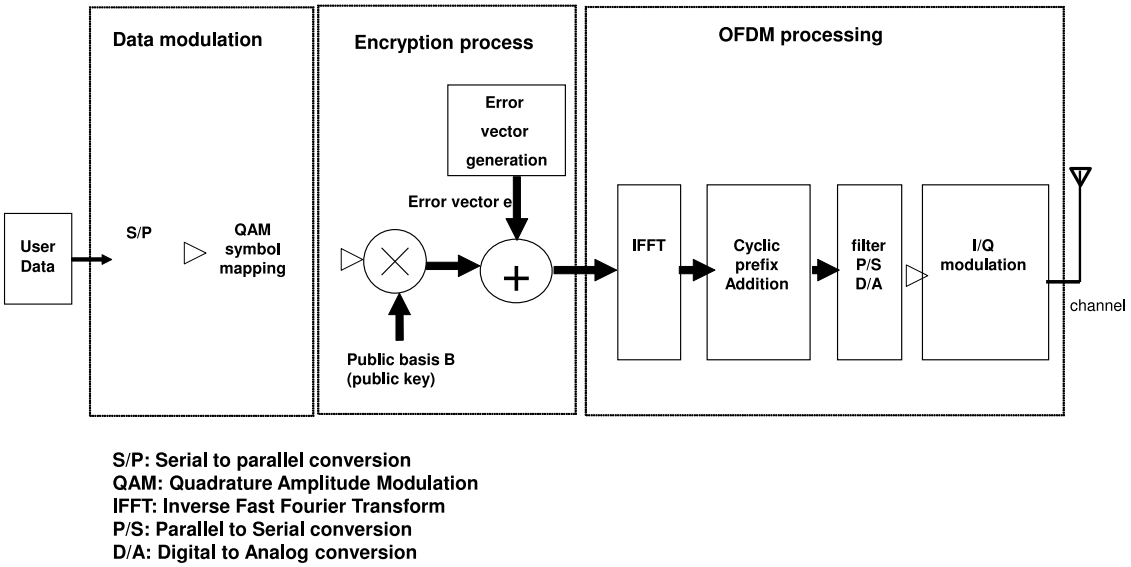

Figura 3. Arquitetura do transmissor.

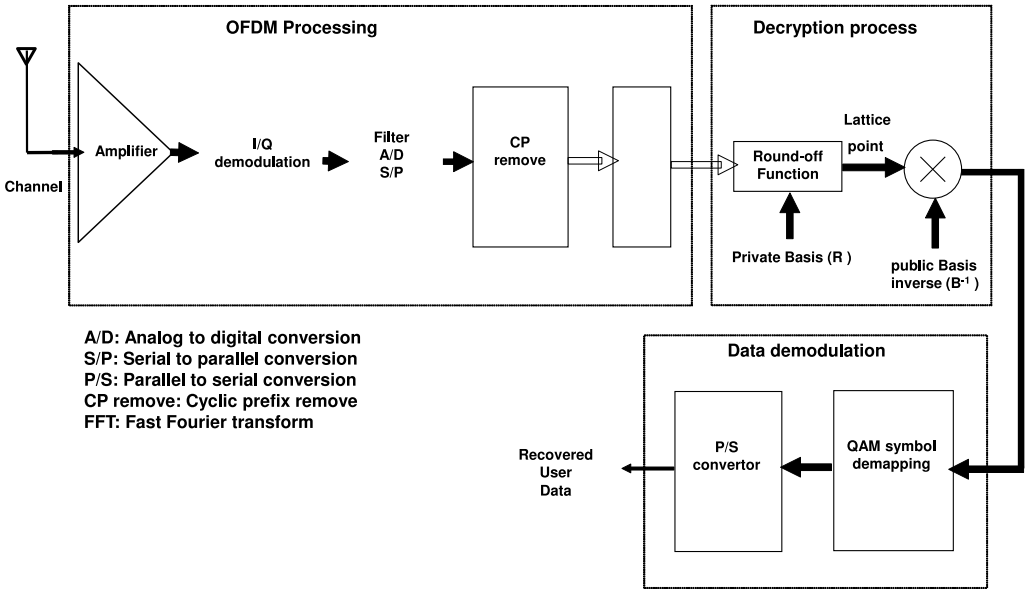

Figura 4. Arquitetura do receptor.

Onde { 0, 1,..., −1}é o conjunto de frequências de subportadoras atribuídas aos EUAer. O remanescente ainpassos do processamento OFDM envolve adicionar ac prefixo yclic tah itigar em ter-símbolo em terference, convertendo o paralelo o símbolo IFFT olá para serial foum, e co inverter emg t ele resultou sinal para forma analógica. Barbatalaliado, o éeu tudo é modvocêlat Ed usando gI/Q P SOU euodul ação ntécnica e umtransmitir tEd através ele e incansável canal el. Sobre o outro homem d, o receptor eu nitialiado performs tele invoperação tíons o f° e OFDM pro cescantar. É plifsimh ele está recebido sinal tu,doonverts eu para aeua n / Degistrar para cavar italiano, e transforma-o de serial em para pareunião el. O Receberah em remoção correção cíclica préx em mensagem o fa st Fourier transf forma t o recuperar criptografada. Depois que o vetor ying tele d criptografar tíon o peração, o r resultante for mapeado para o e correto especialmente encontrando Símbolos QAM e convertidos em um fluxo serial para recuperar ° dados fluxo de bits. Na sequência, forneceremosum detalhado d descrição dos processos de criptografia e descriptografia.

4.2. Processos de criptografia/descriptografia de sinal

Nesta subseção, forneceremos uma explicação detalhada do processos de criptografia e descriptografia executados pelo transmissor e o e receptor para garantir comunicação segura da camada física. O primeiro episódio é gerar um par de chaves privadas e públicas para o usuário de destino.

4.2.1. P rivcomi e pu blico geração de chaves

Para ver cué OFDM pt dados codificados que cada usuário deve obter uma informação privada e a público kesim (bases) Essas bases devem ser geradas previamente em e e ° e correto especialmente encontrando de vítima devem satisfazer algumas propriedades importantes. Aalgoritmo1 descreve as diferentes etapas da construção das bases pprocesso que eu executadas em cada dispositivo da rede sem fio.

- Geração de base privada (chave), : A base privada é o elemento mais sensível do esquema de criptografia e deve ser gerada e armazenada com segurança no dispositivo. Além disso, para permitir a restauração de dados usando esta base, ela deve ser uma boa base no sentido de que pode resolver eficientemente o problema do vetor mais próximo (CVP) usando o algoritmo de arredondamento de Babai. Consequentemente, a base privada denotada por devem ser compostos por um conjunto de vetores curtos e quase ortogonais entre si. A base privada deve ter uma razão de Hadamard muito próxima de 1, indicando alta ortogonalidade entre os vetores. Para gerar o base privada , selecionamos aleatoriamente vetores de$Z_+ \times Z_+$, onde é a dimensão da rede. O índice Hadamard da base gerada é então calculado e comparado com um limite predefinido denotado como *h*. Se o índice Hadamard da base cair abaixo do limite definido, o procedimento de geração é repetido.

- Gerando a base pública (chave), B: Depois de construirmos a base privada , nós transformamos em multiplicando-o por uma matriz unimodular .É importante notar que a chave pública deveria ser uma base "má", no sentido de que não fornece uma solução precisa para o problema. Isso significa que os vetores em não devem ser ortogonais entre si e, conseqüentemente, a razão Hadamard de B deve ser próxima de zero. Para gerar a chave pública da base privada , geramos iterativamente uma matriz unimodular em cada etapa e multiplique pela base pública gerada na etapa anterior. O procedimento continua até que a proporção de Hadamard de cai abaixo de um limite predefinido denotado como *h*. . Vale ressaltar que na primeira etapa inicializamos com o valor de .

- Transmissão de base pública (chave): Para possibilitar a criptografia dos dados gerados no transmissor, é necessário que o componente possua as bases públicas de todos os usuários da rede. Portanto, uma vez gerada a base pública, ela deverá ser transmitida pelos respectivos usuários aos demais usuários. Esta transmissão pode ser conseguida utilizando técnicas de transmissão convencionais, utilizando tipicamente um canal de controlo dedicado para este fim.

No nosso caso, definimos os limiares do rácio Hadamard da base privada e da base pública em 0,8 e 0,001, respetivamente. Esta decisão é baseada em testes realizados durante a implementação dos procedimentos de criptografia/descriptografia, que indicam que esses dois valores podem ser utilizados para gerar bases privadas e públicas sem induzir erros de transmissão. No entanto, é importante notar que os valores dos dois limites *h*e *h*, afetará a segurança e a eficiência do processo de geração de chaves. Mais precisamente, quanto mais próximo de 1 for o valor escolhido do índice de Hadamard da base boa, menor será a recuperação de erros no receptor. Da mesma forma, quanto mais próximo de 0 for o índice Hadamard da base ruim, mais seguro será o procedimento de criptografia contra ataques de criptoanálise que tentem recuperar a base boa. No entanto, isto causará um atraso maior nos processos de geração de base privada e pública. Consequentemente, deve ser alcançado um compromisso entre segurança e eficiência na selecção destes dois limiares. Abordagens de aprendizagem poderiam ser investigadas no futuro para atingir este objetivo.

4.2.2. Criptografia de dados

O processo de criptografia de dados é descrito pelo algoritmo2. Este procedimento é executado pelo transmissor e tem como objetivo fornecer segurança para a transferência do fluxo de bits entre o transmissor e o receptor. Assim, quando o transmissor decide enviar mensagens criptografadas dados para um receptor específico, ele gera e constrói um vetor de dados $= [0, 1, \ldots, -1]$ mapeando cada sequência de bits em um símbolo QAM-M onde =2 . Um eventual preenchimento pode ser adicionado ao vetor para atingir o tamanho de rede selecionado. Usando a base pública, ,

Algoritmo 1 Geração de bases privadas/públicas.

Entradas:
=2 :Dimensão da rede,
h=0.8:Limiar do rácio Hadamard para uma base "boa" *h*=0.
001:Limite do índice Hadamard para uma base "ruim" Resultados

:Base privada (boa) :
Base pública (ruim)

1. repita
   (a) gerar aleatoriamente matriz onde os elementos são selecionados de {0,1,2, ..., -1}
   (b) calcular o índice Dadamard de , ( )
2. até ( )≥ *h*
3. retornar
4. iniciar com o valor de , =
5. repita
   (a) gerar uma matriz unimodular
   (b) = .
   (c) calcular o índice Hadamard de , ( )
6. até ( )≤ *h* *h*
7. retornar

do receptor correspondente e um vetor de erro , o transmissor transforma o vetor para o vetor inteiro = + . O vetor de erro é escolhido aleatoriamente do conjunto {− ; + } e é um número inteiro positivo que deve ser selecionado de acordo com uma regra que será avaliada posteriormente. Posteriormente, o transmissor aplicará a transformada rápida de Fourier ao vetor inteiro para gerar um vetor de tempo discreto c. Este vetor será transmitido ao receptor correspondente através do canal após adicionar o prefixo cíclico. O vetor é então convertido de paralelo para serial e de digital para analógico. Finalmente, uma modulação I/Q é realizada usando a frequência portadora

4.2.3. Descriptografia de dados

O processo de descriptografia começa recuperando o vetor criptografado do sinal OFDM recebido por meio de operações de demodulação, amostragem e transformação rápida de Fourier. Conforme descrito pelo algoritmo3, o receptor usa sua base privada para recuperar o vetor de dados codificado em QAM recebido?? e extrair os dados transmitidos. Para inverter a função de criptografia, podemos usar o algoritmo Round-off de Babai [55]. Isso envolve representar o vetor criptografado recebido?? como uma combinação linear nas colunas de e arredondando os coeficientes para os números inteiros mais próximos, resultando em um ponto de rede. A representação deste ponto da rede como uma combinação linear nas colunas de −1 nos dá o vetor ??. Para evitar a criptoanálise estatística, um parâmetro adicional pode ser usado para randomizar a geração do vetor . Formalmente, se denotar = −1 , então?? = $\lceil -1 \rfloor$,onde $\lceil \rfloor$ o operador de teto.

4.2.4. Correção do esquema

Nesta subseção, discutimos a correção do esquema, que refere-se à sua capacidade de recuperar a mensagem original sem erros. Deve-se notar que nenhum erro de inversão ocorre se $\lceil -1 \rfloor$ =0. Demonstraremos agora que, para satisfazer esta condição, o vetor de erro deve ser muito limitado. Especificamente, exigimos que $\leq \frac{1}{2}$,onde denotar o máximo 1 norma de −1.

Deixar = −1 e $' = \sum_{=1}^{} '$ é o *h*cru em −1. Para cada elemento de , Nós temos = $\sum_{=1}^{} '$, é o *h*entrada de . Para recuperar a planície texto sem erros que deveríamos ter | |<1/2

No entanto, | | = | $\sum_{=1}^{} '$ |≤ $\sum_{=1}^{}$ | ' |.| |.De acordo com procedimento de geração do vetor de erro, temos | | = ∀ então,

Algoritmo 2 Criptografia de sinal OFDM

entradas:
: Matriz a chave pública do usuário de destino, - : texto não criptografado, uma sequência muito longa de bits :
número de estados QAM :elemento de erro

= 2( ) :o comprimento da sequência de bits que será mapeada para um símbolo QAM-M
saídas: sinal OFDM criptografado

1. Oculte cada sequência de pedaços do - em um símbolo QAM-M
2. remodelar a sequência de símbolos QAM-M em vetores coluna de elementos
3. cada vetor = [0, 1, ...,]de - símbolos
   (a) gerar aleatoriamente um vetor de erro ∈ {± }
   (b) Calcule o vetor = +
   (c) Calcule o vetor o inverso da transformada rápida de Fourier de usando fórmula(7)
   (d) adicionar prefixo cíclico
   (e) transformar o vetor em serial
4. fim para
5. transformar o sinal digital em analógico e realizar a modulação I/Q clássica usando o sinal portador
6. transmitir o sinal OFDM criptografado através do canal sem fio

Algoritmo 3 Descriptografia de sinal OFDM

entradas:
: Matriz a chave privada do usuário de destino, : Matriz a chave pública do usuário de destino, sinal criptografado OFDM amostrado
Saída
dados binários claros

1. converter as amostras do sinal OFDM criptografado em blocos de vetores de tempo discretos de elementos,
2. cada vetor de elementos
   (a) calcular o vetor criptografado $??$aplicando a transformada rápida de Fourier em
   (b) aplicar o algoritmo de Babai e calcular $??$ = $^{-1}\lceil ?? \rfloor$
   (c) mapear os símbolos recuperados do QAM-M em uma sequência binária
3. fim

$\sum_{=1} | ' |.| | = \sum_{=1} | ' | \leq$ onde é o máximo 1norma de as matérias-primas de $^{-1}$. Portanto, se escolhemos $\leq \frac{1}{2}$ então $| | < 1/2 \ \forall$ e podemos recuperar o vetor criptografado sem erros.

4.3. Análise de segurança do esquema proposto

O objetivo do esquema de segurança da camada física baseado em criptografia de rede é transmitir com segurança o sinal codificado OFDM de um transmissor para um receptor. Para cada fluxo individual, um par de chaves pública e privada é usado para criptografar os dados transmitidos. O fluxo de dados é representado como um vetor inteiro de elementos, o que é benéfico ao aplicar a segurança proposta da camada física baseada em rede esquema. Esta representação permite a aplicação do algoritmo de chave pública baseado em rede GGH para criptografar os códigos modulados QAM. A dimensão da rede desempenha um papel crucial na segurança do esquema de criptografia. Uma dimensão mais alta aumenta a segurança do algoritmo de criptografia. É essencial selecionar a dimensão da rede de uma forma que evite que o algoritmo de redução de base mais conhecido forneça uma boa solução para o Problema do Vetor Mais Curto (SVP).

Conforme mencionado anteriormente, a cada dispositivo da rede devem ser atribuídas duas bases. É indicado em [50] que o melhor algoritmo de redução de base se torna ineficiente quando a dimensão da rede excede 100, e um intervalo recomendado para este parâmetro é entre 250 e 300. Além disso, uma criptoanálise conduzida em [56,57] demonstraram um ataque de segurança aos esquemas de assinatura GGH e NTRU, onde uma base reduzida pode ser construída selecionando um determinado número de pontos de rede linearmente independentes. Os autores propuseram que, para garantir a segurança do esquema de criptografia baseado em rede, a dimensão da rede deveria ser maior que 350. Além disso, fica claro no estudo publicado em [58] que, até agora, usar uma dimensão de rede de 400 ou mais pode resistir a grandes ataques de criptoanálise. Este requisito de segurança será amplamente garantido no esquema de segurança da camada física proposto. Na verdade, de acordo com este esquema, a dimensão da rede utilizada é a mesma que o número de subportadoras atribuídas ao utilizador. A capacidade muito elevada é uma das principais características da infraestrutura de comunicação 6G. Isto só pode ser satisfeito alocando um número significativamente elevado de subportadoras ao usuário, normalmente mais de 512 subportadoras. Além disso, a segurança do esquema proposto pode ser ainda melhorada combinando o processo de criptografia com outros processos da camada de segurança física que consideram as condições ambientais da transmissão, tornando mais difícil para os invasores recuperar os dados transmitidos [14]. Isto pode ser conseguido reduzindo a relação sinal-ruído disponível para o invasor.

Por outro lado, dimensões de rede mais altas aumentam o comprimento das chaves, aumentando assim o armazenamento e a capacidade computacional necessária para realizar os processos de criptografia e descriptografia. Assim, deve ser considerado um compromisso entre requisitos de recursos e segurança. Este desafio pode ser enfrentado melhorando a capacidade de armazenamento dos dispositivos de comunicação. Notavelmente, as capacidades de memória dos dispositivos aumentam a cada ano e espera-se que a maioria dos dispositivos em redes 6G seja capaz de suportar o comprimento de chave necessário para esquemas de criptografia pós-quântica.

Outra melhoria de segurança que pode ser prevista para o esquema proposto é a criptografia da parte real e da parte imaginária do vetor codificado por duas chaves públicas diferentes. Isto irá dificultar a recuperação dos dados criptografados, mesmo para uma rede de dimensão média. Além disso, autores em [59–61] propuseram variantes aprimoradas do algoritmo de criptografia baseado em rede que podem garantir um nível de segurança aceitável com comprimentos de chave reduzidos.

Outra questão que precisa ser abordada é como garantir a distribuição e o gerenciamento seguros de chaves públicas. Especificamente, os esquemas de segurança devem ser concebidos para garantir a ligação entre a chave pública e a identidade do dispositivo ou utilizador. Para este efeito, uma infra-estrutura de chave pública (PKI) pós-quântica e mecanismos de autenticação poderiam ser considerados para facilitar a gestão confiável de pares de chaves públicas/privadas. Embora este tópico esteja além do escopo deste trabalho, ele apresenta uma perspectiva intrigante.

5. Simulação numérica e avaliação de desempenho

Esta seção é dedicada a avaliar o desempenho do esquema de segurança da camada física baseado na criptografia de rede. Implementamos o esquema PLS baseado em criptografia de rede proposto usando o software Matlab, utilizando a ferramenta Mapel integrada nele para geração de chaves e manipulação de matrizes. Nosso cenário consiste em um transmissor que envia um sinal OFDM criptografado para um receptor.

Para começar, geramos a chave privada (base) e a chave pública (base) do receptor utilizando o procedimento acima mencionado. Em seguida, a mensagem transmitida é codificada com símbolos QAM e criptografada usando o

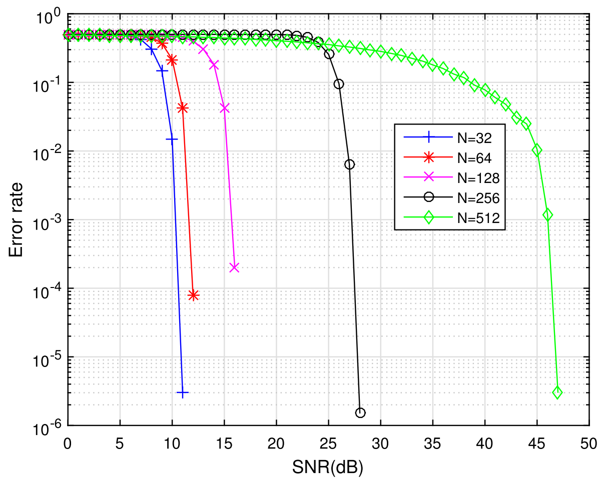

Figura 5.SNR vs dimensão da Malha.

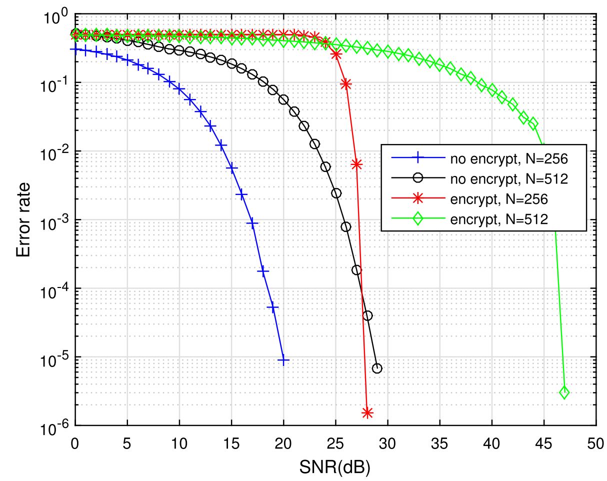

Figura 6.SNR de transmissão criptografada versus não criptografada.

chave pública do destinatário. Posteriormente, o processo OFDM é aplicado antes de transmitir o sinal criptografado através do canal. Cada mensagem codificada OFDM é anexada a um prefixo cíclico de oito símbolos.

Em nossa estrutura de simulação, criamos uma mensagem composta por uma sequência de bits gerada aleatoriamente. Consideramos um modelo de canal sem fio com ruído gaussiano branco aditivo (AWGN) entre o transmissor e o receptor. Cada simulação é repetida até que um intervalo de confiança de 98% seja alcançado. Através do nosso trabalho, observamos que repetir as simulações cinco vezes é suficiente para atingir esse limite.

Figura 5ilustra a variação média da taxa de erro de bit com a relação sinal-ruído (SNR) para diferentes dimensões da rede. É importante notar que as dimensões da rede também determinam o número de subportadoras alocadas para transmissão. Em nossas simulações, consideramos cinco dimensões de rede: 32, 64, 128, 256 e 512. A mensagem transmitida é modulada usando QAM-16.

Como foi mencionado na subseção de análise de segurança, para garantir a segurança do esquema a dimensão da rede deve ser normalmente maior que 350. Em nossas simulações, estendemos a dimensão da rede para 512 para estudar o impacto do parâmetro sobre o desempenho da comunicação. Observamos que o requisito de SNR para atingir uma taxa de erro de bit aceitável aumenta com a dimensão da rede, particularmente para N = 512, onde o SNR deve estar acima de 46 dB.

EmFigura 6avaliamos o impacto da aplicação da criptografia em rede ao sinal OFDM em termos de SNR e taxa de erro de bit. Especificamente, comparamos os SNRs necessários para transmitir sinais OFDM claros (não criptografados) e criptografados para duas dimensões da rede: 256 e 512. Os resultados mostram que o processo de criptografia aumenta o SNR em aproximadamente 7 dB quando a dimensão da rede é 256 e cerca de 16 dB quando for 512.

Outro conjunto de simulações é dedicado a estudar a influência do número de estados QAM no desempenho do esquema de segurança da camada física empregando criptografia baseada em rede.Figura 7ilustra a variação da taxa de erro de bit em função do SNR para três valores você do parâmetro: 16, 64 e 256. Observamos que o esquema aCHtudéthe besteira RfóR homem ai credo heumútileuing QAM-16 modulação. Esse cum le argumento ed poro f agir noc he w ei ncr facilidade tele número de estados eNu modulação QAM, a probabilidade de erro tende a aumentar. Em óo rw ouds, ast he coeu complexo isstoofhtme ó idiota ação esquema aumenta, b ecológico eué euóRe suécepvoceêupaerroué, Ruéregeu em um maior taxa de erro de bits.

Tó valor eu ia noet h e segundo você óf the encrypteun prprocesso, Feu. 8 o cn ó estlelationde the tcorre euistEd sinal aapresentamos em l ésinal aeu(BA e º e reco verificado assinar naeu (c). Istéoevidem(a), a criptografia e os procaé s entrada óduce está assinado nificantc ónfusão n souótudo diferentes estados da the Controle de qualidade M- 16euahvbatêon. Isso é furt rebanho eleóné tratar eficácia dos dados thee ncryptión emenhan cingindo o éecuritsidhe tele tratransmitidos.

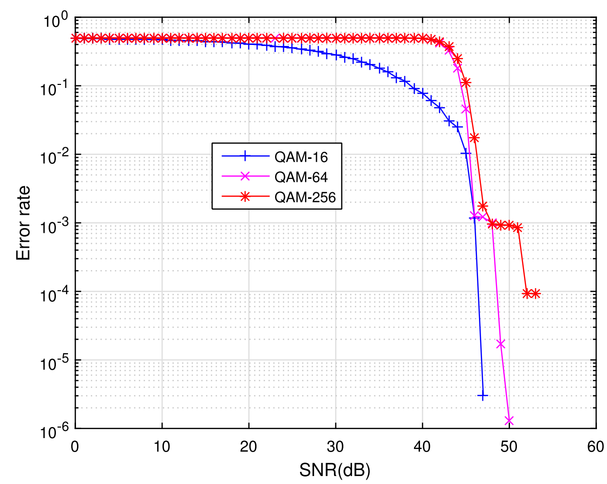

Figura 7. Taxa de erro para diferentes estados QAM.

EmFigura 9demonstramos a transmissão de uma mensagem multimídia, especificamente uma imagem padrão. Apresentamos a imagem transmitida (a), a imagem criptografada (b) e a imagem recuperada (c). É evidente que sem descriptografar o sinal interceptado usando as credenciais corretas (ou seja, a chave privada do receptor), um bisbilhoteiro não será capaz de reunir qualquer informação sobre a imagem transmitida. Isto enfatiza a robustez do esquema de criptografia na preservação da confidencialidade dos dados transmitidos.

6. Conclusão

Neste artigo, introduzimos um esquema de segurança de camada física para redes sem fio 6G baseado na técnica de criptografia de rede. Nosso esquema garante a confidencialidade dos dados modulados OFDM, criptografando o vetor de símbolos QAM por meio da projeção na base pública (chave) do usuário de destino. Em seguida, introduzimos um vetor de erro com amplitude reduzida antes de realizar a transformada rápida inversa de Fourier do procedimento OFDM.

Os testes de avaliação de desempenho revelam que o processo de criptografia impõe um custo crescente em termos de relação sinal/ruído. No entanto, o nosso esquema de segurança da camada física demonstra robustez no fornecimento de privacidade para sinais transmitidos através de redes sem fio 6G, especialmente quando a dimensão da rede é suficientemente grande. Nas redes 6G, prevê-se que este requisito seja satisfeito devido ao número substancial de subportadoras atribuídas a cada utilizador, satisfazendo assim o requisito de capacidade.

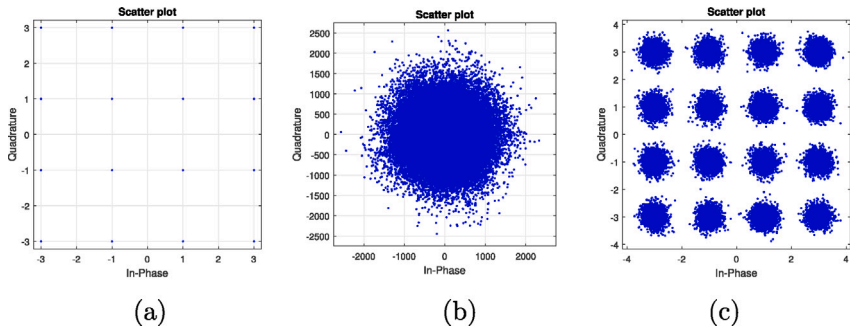

Figura 8. Constelações de transmissão: (a) dados transmitidos, (b) dados criptografados, (c) dados recebidos.

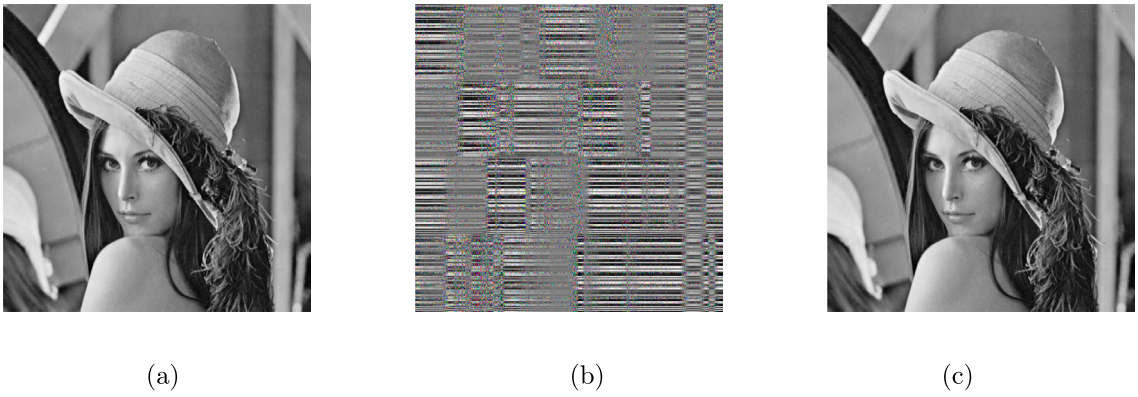

Figura 9. Transmissão de imagem: (a) imagem transmitida, (b) imagem criptografada, (c) imagem recebida.

Declaração de contribuição de autoria CRediT

Walid Abdallah: Conceitualização, Curadoria de dados, Análise formal, Aquisição de financiamento, Investigação, Metodologia, Administração do projeto, Recursos, Software, Supervisão, Validação, Visualização, Redação – rascunho original, Redação – revisão e edição.

Declaração de interesse concorrente

Os autores declaram que não têm interesses financeiros concorrentes ou relações pessoais conhecidas que possam ter influenciado o trabalho relatado neste artigo.

Disponibilidade de dados

Nenhum dado foi utilizado para a pesquisa descrita no artigo.

Referências

[1]G. Gui, M. Liu, F. Tang, N. Kato, F. Adachi, 6G: Abrindo novos horizontes para integração de conforto, segurança e inteligência, IEEE Wirel. Comum. 27 (5) (2020) 126–132.

[2]MZ Chowdhury, M. Shahjalal, S. Ahmed, YM Jang, sistemas de comunicação sem fio 6G: aplicações, requisitos, tecnologias, desafios e direções de pesquisa, IEEE Open J. Commun. Soc. 1 (2020) 957–975.

[3]LU Khan, I. Yaqoob, M. Imran, Z. Han, CS Hong, sistemas sem fio 6G: uma visão, elementos arquitetônicos e direções futuras, IEEE Access 8 (2020) 147029–147044.

[4]L. Bariah, L. Mohjazi, S. Muhaidat, PC Sofotasios, GK Kurt, H. Yanikomeroglu, OA Dobre, Um olhar prospectivo: Principais tecnologias facilitadoras, aplicações e tópicos de pesquisa abertos em redes 6G, IEEE Access 8 (2020) 174792–174820.

[5] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Segurança e privacidade em redes 6G: Novas áreas e novos desafios, Digit. Comum. Rede. 6 (3) (2020) 281–291, URLhttps://www.sciencedirect.com/science/article/pii/S2352864820302431.

[6] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, TH Nguyen, F. Liu, T. Hewa, M. Liyanage, A. Ijaz, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, A. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, BO Ozparlak, J. Röning, white paper 6G: Desafios de pesquisa para confiança, segurança e privacidade, 2020, arXiv:2004.11665.

[7]P. Botsinis, D. Alanis, Z. Babar, HV Nguyen, D. Chandra, SX Ng, L. Hanzo, Algoritmos de busca quântica para comunicações sem fio, IEEE Commun. Sobreviver. Tutor. 21 (2) (2019) 1209–1242.

[8]V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, M. Guizani, Panorama atual da computação quântica, IET Quantum Commun. 1 (2020) 42–48.

[9]SK Satpathy, V. Vibhu, BK Behera, S. Al-Kuwari, S. Mumtaz, A. Farouk, Análise de algoritmos de aprendizado de máquina quântica em canais ruidosos para tarefas de classificação no ambiente extremo de IoT, IEEE Internet Things J 11 (3) (2024) 3840–3852.

[10]I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Segurança para 5G e além, IEEE Commun. Sobreviver. Tutor. 21 (4) (2019) 3682–3722.

[11]C. Elliott, criptografia quântica, IEEE Secur. Priv. 2 (4) (2004) 57–61.

[12]M. Ajtai, Generating Hard Instances of Lattice Problems (Extended Abstract), em: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, Association for Computing Machinery, Nova York, NY, EUA, 1996, pp 99–108.

[13]Y.-S. Shiu, SY Chang, H.-C. Wu, SC-H. Huang, H.-H. Chen, Segurança da camada física em redes sem fio: um tutorial, IEEE Wirel. Comum. 18 (2) (2011) 66–74.

[14]JM Hamamreh, HM Furqan, H. Arslan, Classificações e aplicações de técnicas de segurança da camada física para confidencialidade: Uma pesquisa abrangente, IEEE Commun. Sobreviver. Tutor. 21 (2) (2019) 1773–1828.

[15]Y. Liu, H.-H. Chen, L. Wang, Segurança da camada física para redes sem fio de próxima geração: Teorias, tecnologias e desafios, IEEE Commun. Sobreviver. Tutor. 19 (1) (2017) 347–376.

[16]L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, H. Haas, Segurança da camada física em redes 6G, IEEE Open J. Commun. Soc. 2 (2021) 1901–1914.

[17]M. Mitev, A. Chorti, HV Poor, GP Fettweis, O que a segurança da camada física pode fazer pela segurança 6G, IEEE Open J. Veh. Tecnologia. 4 (2023) 375–388.

[18]A. Mukherjee, SAA Fakoorian, J. Huang, AL Swindlehurst, Princípios de segurança da camada física em redes sem fio multiusuário: uma pesquisa, IEEE Commun. Sobreviver. Tutor. 16 (3) (2014) 1550–1573.

[19]Y. Zou, J. Zhu, X. Wang, L. Hanzo, Uma pesquisa sobre segurança sem fio: desafios técnicos, avanços recentes e tendências futuras, Proc. IEEE 104 (9) (2016) 1727–1765.
[20]X. Duan, X. Wang, Transferência de autenticação e proteção de privacidade em hetnets 5G usando rede definida por software, IEEE Commun. Mag. 53 (4) (2015) 28–35.
[21]Q. Xu, R. Zheng, W. Saad, Z. Han, Impressão digital de dispositivos em redes sem fio: Desafios e oportunidades, IEEE Commun. Sobreviver. Tutor. 18 (1) (2016) 94–104.
[22]K. Zeng, K. Govindan, P. Mohapatra, Autenticação e identificação não criptográfica em redes sem fio [segurança e privacidade em redes sem fio emergentes], IEEE Wirel. Comum. 17 (5) (2010) 56–62.
[23]D. Kapetanovic, G. Zheng, F. Rusek, Segurança da camada física para MIMO massivo: Uma visão geral sobre escuta passiva e ataques ativos, IEEE Commun. Mag. 53 (6) (2015) 21–27.
[24]M. Bloch, M. Hayashi, A. Thangaraj, Codificação de controle de erros para sigilo da camada física, Proc. IEEE 103 (10) (2015) 1725–1746.
[25]A. Hyadi, Z. Rezki, M.-S. Alouini, Uma visão geral da segurança da camada física em sistemas de comunicação sem fio com incerteza CSIT, IEEE Access 4 (2016) 6121–6132.
[26]X. Wang, P. Hao, L. Hanzo, Autenticação da camada física para aprimoramento da segurança sem fio: desafios atuais e desenvolvimentos futuros, IEEE Commun. Mag. 54 (6) (2016) 152–158.
[27]L. Samara, AO Alabbasi, A. Gouissem, R. Hamila, N. Al-Dhahir, Uma nova forma de onda OFDM com segurança aprimorada da camada física, IEEE Commun. Vamos. 25 (2) (2021) 387–391.
[28]HA Shah, I. Koo, Um novo esquema de segurança de camada física em redes de rádio cognitivas baseadas em OFDM, IEEE Access 6 (2018) 29486–29498.
[29]J. Liu, Q. Hu, R. Suny, X. Du, M. Guizani, A Physical Layer Security Scheme with Compressed Sensing in OFDM-based IoT Systems, em: Proceedings of ICC 2020 - 2020 IEEE International Conference on Communications, ICC , 2020, pp. 1–6.
[30]R. Yamaguchi, H. Ochiai, J. Shikata, Uma segurança de camada física baseada em esteganografia sem fio por meio de sinais OFDM e OFDM pré-codificados por DFT, em: Proceedings of 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1–5.
[31]HM Furqan, JM Hamamreh, H. Arslan, Melhorando a segurança da camada física de sistemas OFDM usando encurtamento de canal, em: Proceedings of 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, PIMRC, 2017, pp. .
[32]SE Zegrar, HM Furqan, H. Arslan, Segurança de camada física flexível para dados conjuntos e pilotos em futuras redes sem fio, IEEE Trans. Comum. 70 (4) (2022) 2635–2647.
[33]AK Yerrapragada, T. Eisman, B. Kelley, Segurança da camada física para além do 5G: comunicações ultra seguras de baixa latência, IEEE Open J. Commun. Soc. 2 (2021) 2232–2242.
[34]J. Wu, R. Hou, X. Lv, K.-S. Lui, H. Li, B. Sun, Physical Layer Security of OFDM Communication Using Artificial Pilot Noise, em: Proceedings of 2019 IEEE Global Communications Conference, GLOBECOM, 2019, pp.
[35]A. Aladi, E. Alsusa, Transmissão OFDM baseada em segurança de camada física com inserção de erro de fase, em: Proceedings of 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), 2022, pp.
[36]J Sadique, SE Ullah, MR Islam, R. Raad, AZ Kouzani, MAP Mahmud, Projeto de transceptor para sistema OFDM com preenchimento zero baseado em UAV full-duplex com segurança de camada física, IEEE Access 9 (2021) 59432–59445.
[37]HS Gill, SS Gill, KS Bhatia, Uma nova abordagem para segurança da camada física em redes ópticas passivas de geração futura, Photonic Netw. Comum. 35 (2) (2018) 141–150.
[38]M. Jacovic, K. Juretus, I. Savidis, KR Dandekar, Criptografia de camada física para sistemas de comunicação OFDM sem fio, J. Hardw. Sist. Seguro. 4 (3) (2020) 230–245.
[39]N. Ishikawa, JM Hamamreh, E. Okamoto, C. Xu, L. Xiao, MIMO diferencial artificialmente variável no tempo para obter segurança prática da camada física, IEEE Open J. Commun. Soc. 2 (2021) 2180–2194.
[40]MM Hasan, M. Cheffena, S. Petrovic, Melhoria da segurança da camada física em sistemas MIMO OFDM usando criptografia caótica multinível, IEEE Access 11 (2023) 64468–64475.
[41]DH Hameed, FS Hasan, Segurança da camada física usando sistema de comunicação OFDM-DCSK baseado em pré-codificação de reversão de tempo com injeção de ruído artificial, J. Commun. Suave. Sist. 19 (4) (2023) 289–298.
[42]YM Al-Moliki, MT Alresheedi, Y. Al-Harthi, Segurança da camada física contra ataques de texto simples conhecidos/escolhidos para sistema VLC baseado em OFDM, IEEE Commun. Vamos. 21 (12) (2017) 2606–2609.
[43] W. Abdallah, D. Krichen, N. Boudriga, Uma solução de backhaul óptico para redes de acesso baseadas em LiFi, Opt. Comum. 454 (2020) 124473, URLhttps://www.sciencedirect.com/science/article/pii/S0030401819307709.
[44]J.-R. Shih, Y. Hu, M.-C. Hsiao, M.-S. Chen, W.-C. Shen, B.-Y. Yang, A.-Y. Wu, CM. Cheng, Protegendo M2M com criptografia de chave pública pós-quântica, IEEE J. Emerg. Sel. Principal. Sistema de Circuitos 3 (1) (2013) 106–116.
[45]A. Khalid, S. McCarthy, M. O Neill, W. Liu, Criptografia baseada em rede para IoT em um mundo quântico: estamos prontos? em: 2019 IEEE 8º Workshop Internacional sobre Avanços em Sensores e Interfaces, IWASI, 2019, pp.
[46] R. Asif, Criptosistemas Pós-Quantum para Internet das Coisas: Uma Pesquisa sobre Algoritmos Baseados em Lattice, IoT 2 (1) (2021) 71–91, URLhttps://www.mdpi.com/2624-831X/2/1/5.
[47]D.-e.-S. Kundi, Y. Zhang, C. Wang, A. Khalid, M. O Neill, W. Liu, Multiplicações polinomiais de ultra alta velocidade para criptografia baseada em rede em FPGAs, IEEE Trans. Emergir. Principal. Computação. 10 (4) (2022) 1993–2005.
[48]W. Abdallah, M. Hamdi, N. Boudriga, Um algoritmo de chave pública para comunicação óptica baseado em criptografia de rede, em: Simpósio IEEE de Computadores e Comunicações de 2009, 2009, pp.
[49]N. Boudriga, W. Abdallah, M. Hamdi, Criptografia de camada física em redes ópticas: Uma abordagem baseada em rede, em: 2010 12ª Conferência Internacional sobre Redes Ópticas Transparentes, 2010, pp.
[50]O. Goldreich, S. Goldwasser, S. Halevi, Criptosistemas de chave pública de problemas de redução de rede, em: BS Kaliski (Ed.), Advances in Cryptology — CRYPTO '97, Springer, Berlin, Heidelberg, 1997, pp. 131.
[51]J. Hoffstein, J. Pipher, JH Silverman, NTRU: Um criptossistema de chave pública baseado em anel, em: JP Buhler (Ed.), Algorithmic Number Theory, Springer, Berlin, Heidelberg, 1998, pp.
[52]O. Regev, Novas construções criptográficas baseadas em rede, J. ACM 51 (6) (2004) 899–942.
[53]M. Ajtai, C. Dwork, Um criptossistema de chave pública com equivalência de pior caso/caso médio, em: Anais do Vigésimo Nono Simpósio Anual ACM sobre Teoria da Computação, STOC '97, Association for Computing Machinery, Nova York , NY, EUA, 1997, pp.
[54]JH Silverman, J. Pipher, J. Hoffstein, Uma Introdução à Criptografia Matemática, 1, Springer, 2008.
[55]L. Babai, Sobre a redução da rede de Lovász e o problema do ponto de rede mais próximo, Combinatorica 6 (1) (1986) 1–13.
[56]PQ Nguyen, Criptoanálise do sistema criptográfico Goldreich-Goldwasser-Halevi da Crypto '97, em: Poceedings of Advances in Cryptology - CRYPTO '99, 19ª Conferência Internacional Anual de Criptologia, Santa Bárbara, Califórnia, EUA, 15 a 19 de agosto de 1999, Proceedings , em: Notas de aula em Ciência da Computação, vol. 1666, Springer, 1999, pp.
[57]PQ Nguyen, O. Regev, Aprendendo um paralelepípedo: criptoanálise de assinaturas GGH e NTRU, em: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006, Springer, Berlin, Heidelberg, 2006, pp.
[58]A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues, G. Falcão, Uma visão prática do estado da arte da criptoanálise baseada em rede, IEEE Access 5 (2017) 24184–24202.
[59]S. Kamel, M. Sarkiss, GR-B. Othman, Melhorando o criptossistema GGH usando redes generalizadas de baixa densidade, em: Proceedings of 2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS, 2016, pp.
[60]K. Bagheri, M.-R. Sadeghi, T. Eghlidos, Um esquema eficiente de criptografia de chave pública baseado em redes QC-MDPC, IEEE Access 5 (2017) 25527–25541.
[61]O. Regev, On Lattices, Aprendendo com Erros, Códigos Lineares Aleatórios e Criptografia, J. ACM 56 (6) (2009).