Criptografia avançada utilizando nanoantenas em comunicações sem fios

Alferes-Aluno Tm TPO Francisco Alves

Resumo - A presente dissertação enquadra-se na procura por soluções de comunicação seguras em escala nanométrica, impulsionada pelo avanço da nanotecnologia e pela integração de dispositivos miniaturizados em sistemas de próxima geração. As nanoantenas, pela sua capacidade de amplificar campos eletromagnéticos além do limite de difração, revelam-se promissoras para transmissões de dados seguras quando associadas a esquemas criptográficos robustos.

Neste trabalho, foram projetadas e simuladas nanoestruturas em COMSOL Multiphysics 6.1, avaliando a sua resposta a impulsos de Dirac, pulsos Gaussianos e sinais de voz sintética. Posteriormente, essa resposta foi integrada em dois modelos de encriptação implementados em MATLAB: o Modelo A, focado na eficiência e baseado em manipulação ao nível do bit e na Transformada de Arnold, e o Modelo B, que combina o protocolo de troca de chaves Elliptic Curve Diffie-Hellman (ECDH) com a cifra simétrica Advanced Encryption Standard em modo Cipher Block Chaining (AES-CBC).

Os resultados demonstram a viabilidade da utilização de nanoantenas para comunicações seguras, confirmando fenómenos de amplificação de campo local e evidenciando um trade-off inevitável entre a integridade do sinal e a confidencialidade dos dados. O Modelo A demonstrou maior capacidade de preservação do sinal, enquanto o Modelo B apresentou uma robustez criptográfica superior, estabelecendo um paradigma de escolha dependente dos requisitos específicos da aplicação.

I. Introdução

Nas últimas décadas, a tecnologia de comunicação sem fios sofreu avanços substanciais, enquanto a nanotecnologia e a nanociência atraíram considerável atenção académica. Estes campos emergiram como áreas cruciais, facilitando o desenvolvimento de soluções inovadoras em setores como a energia, defesa e indústria. Com o surgimento das redes 5G e a concetualização do 6G, a procura por dispositivos que exigem largura de banda substancial e latência reduzida aumentou. As nanoantenas representam um avanço notável, sendo identificadas como estruturas promissoras para transformar a comunicação sem fios devido ao seu tamanho reduzido em relação ao comprimento de onda dos sinais óticos. Simultaneamente, a segurança dos sinais transmitidos tornou-se de importância primordial. Devido à sua operação nos espetros ótico e eletromagnético, as nanoantenas exibem vulnerabilidades inerentes, como interceção de sinal e acesso não autorizado. Para enfrentar estes desafios, a criptografia deve ser empregue como estratégia fundamental.

O objetivo deste trabalho é desenvolver modelos criptográficos que se integrem eficazmente com as características físicas das nanoantenas.

II. Estado da Arte

A. Evolução das comunicações sem fios

A evolução das comunicações sem fios para a banda de Terahertz (THz) representa uma mudança de paradigma, prometendo taxas de transmissão de dados sem precedentes e abrindo caminho para aplicações inovadoras, como a Internet das Nano Coisas (IoNT) [1]. No entanto, a transição para estas frequências ultra-altas introduz desafios significativos que exigem uma reavaliação tanto da camada física como da de segurança. As nanoantenas emergem como componentes cruciais para viabilizar estes sistemas, enquanto a criptografia se torna fundamental para garantir a confidencialidade das informações transmitidas [2]. Este trabalho explora a sinergia entre estas duas áreas, visando o desenvolvimento de sistemas de comunicação que não só sejam eficientes em escala nanométrica, mas que também consigam gerir o compromisso intrínseco entre a fidelidade do sinal e a robustez da segurança.

As comunicações na banda de THz enfrentam dois grandes obstáculos: a elevada perda de propagação no espaço livre e a absorção molecular [3]. A perda de propagação, que aumenta com o quadrado da frequência, é aproximadamente 60 dB superior na banda de THz em comparação com a de micro-ondas, limitando o alcance das comunicações a algumas dezenas de metros [1]. Adicionalmente, moléculas de vapor de água na atmosfera absorvem a energia das ondas THz, atenuando ainda mais o sinal. As nanoantenas, ao explorarem fenómenos de ressonância plasmónica, conseguem confinar e amplificar localmente o campo eletromagnético, o que melhora substancialmente o Rácio Sinal-Ruído (SNR) e mitiga os efeitos da atenuação atmosférica [4].

B. Nanoantenas

A escolha do material para o design de nanoantenas é determinante para o seu desempenho. Materiais como o grafeno e os nanotubos de carbono oferecem elevada diretividade e sintonização, mas as suas ressonâncias plasmónicas são mais

proeminentes no infravermelho médio [3]. A prata (Ag) exibe a resposta plasmónica mais forte no espectro visível, mas a sua suscetibilidade à oxidação compromete a sua estabilidade a longo prazo [3, 5]. O ouro (Au), por sua vez, oferece um equilíbrio notável entre um forte aumento do campo elétrico e uma excelente estabilidade química, resistindo à degradação ambiental [6]. Conforme demonstrado em estudos comparativos, embora a diretividade da prata possa ser ligeiramente superior (6.739 dBi contra 6.438 dBi do ouro), o ouro proporciona um aumento de campo mais significativo e maior fiabilidade, justificando a sua seleção para o presente estudo [6].

C. Criptografia e segurança das comunicações

No domínio da segurança, os modelos criptográficos tradicionais, como o Data Encryption Standard (DES), tornaram-se vulneráveis ao aumento da capacidade computacional [7]. O Advanced Encryption Standard (AES) e a Criptografia de Curva Elíptica (ECC) surgiram como alternativas mais robustas [8, 9]. A ECC, em particular, oferece um nível de segurança equivalente ao de sistemas de chave pública tradicionais com chaves de menor dimensão, tornando-a ideal para dispositivos com recursos computacionais limitados [10]. Estudos recentes exploraram esquemas híbridos, como a combinação de ECC com AES [9] ou com a Transformada de Arnold [11], para otimizar a segurança e a eficiência.

Contudo, persiste uma lacuna significativa na literatura: a falta de investigação sobre a integração direta de modelos criptográficos robustos com sinais processados e amplificados por nanoantenas na banda THz.

Este trabalho propõe-se a preencher essa lacuna através do design de uma nanoantena de ouro otimizada para a banda THz e da implementação e teste de dois modelos criptográficos distintos aplicados diretamente ao sinal de saída da antena.

III. Modelos Propostos

A metodologia proposta neste trabalho assenta numa abordagem integrada que combina o design eletromagnético de uma nanoantena com a implementação de dois modelos criptográficos distintos. O objetivo estratégico é avaliar o trade-off fundamental entre a integridade do sinal, amplificado pela nanoestrutura, e a robustez da segurança conferida pelos algoritmos de encriptação. Esta análise permite caracterizar o desempenho de um sistema de comunicação completo, desde a camada física até à camada de segurança, quantificando o impacto que diferentes filosofias de segurança têm na fidelidade da informação transmitida.

A. Design da Nanoantena

A nanoantena projetada foi desenhada e simulada no software COMSOL Multiphysics 6.1. A sua arquitetura consiste num filme metálico de ouro (Au) com 100 nm de espessura, depositado sobre um substrato dielétrico (ar), no qual foi gravada uma matriz periódica de 18 aberturas quadradas sub-comprimento de onda, dispostas numa configuração de 3x6. As aberturas, também preenchidas com ar, possuem um lado de 88.89 nm e uma periodicidade de 222.22 nm no eixo x e 266.67 nm no eixo z. Esta geometria foi otimizada para excitar ressonâncias de plasmões de superfície localizadas, que são responsáveis pela amplificação do campo eletromagnético e pelo fenómeno de Transmissão Ótica Extraordinária (EOT) [12]. A escolha do ouro como material metálico foi motivada pelo seu excelente compromisso entre uma forte resposta plasmónica e uma elevada estabilidade química, conforme discutido na secção anterior. Os parâmetros geométricos e de material utilizados no design estão resumidos na Tabela 1. As Figuras 1 e 2 ilustram a estrutura geral, a topologia e um detalhe das aberturas da nanoantena, respetivamente.

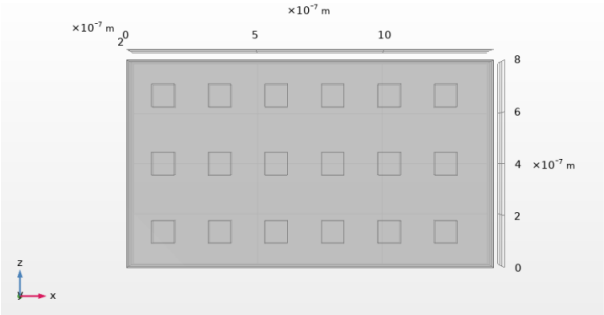

Figura 1: Estrutura do projeto da nanoantena

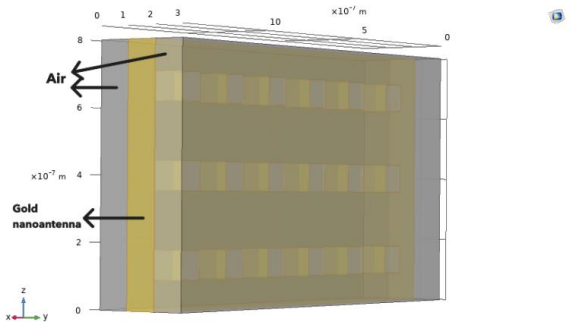

Figura 2: Topologia do modelo de nanoantena projetado.

Tabela 1: Parâmetros geométricos e de material utilizados no design da nanoantena.

Nome	**Valor**	**Unidade**	**Descrição**
Mt	1×10^{-7}	m	Espessura do metal
dt	1×10^{-7}	m	Espessura do dielétrico
λn	8×10^{-7}	m	Comprimento de onda
L	1×10^{-6}	m	Comprimento total da estrutura
Lh	8.8889×10^{-8}	m	Comprimento do lado das aberturas

B. Modelo A: PRNG-XOR + Transformada de Arnold

O Modelo A foi concebido como um sistema de encriptação leve, priorizando a eficiência computacional e a máxima integridade do sinal. A sua arquitetura é composta por cinco blocos sequenciais. O processo inicia-se com a caracterização da resposta da nanoantena, onde o sinal analógico de saída é capturado, normalizado e quantizado em inteiros de 16 bits. Segue-se a codificação para correção de erros. A escolha do código de Hamming (12, 8), um esquema de correção de erros linear e de baixa complexidade, está alinhada com o objetivo do Modelo A de priorizar a eficiência com uma sobrecarga mínima, adicionando 4 bits de paridade a cada bloco de 8 bits de dados para permitir a deteção e correção de erros de um único bit. O terceiro bloco realiza a encriptação bitwise, onde uma chave pseudoaleatória, gerada por um Pseudo-Random Number Generator (PRNG) semeado com uma chave privada, é combinada com o fluxo de bits do sinal através de uma operação XOR. Para aumentar a segurança, o quarto bloco aplica um embaralhamento espacial através da Transformada de Arnold, que reorganiza deterministicamente os bits numa matriz quadrada, dificultando a análise de padrões. Finalmente, o recetor executa o processo inverso para a recuperação do sinal, aplicando a transformada inversa de Arnold e a decriptação XOR com a mesma chave, seguida da descodificação de Hamming para corrigir erros de transmissão.

C. Modelo B: Elliptic Curve Diffie-Hellman + Advanced Encryption Standard

O Modelo B representa uma abordagem criptográfica mais robusta, integrando protocolos modernos para garantir um nível superior de confidencialidade. Este modelo é estruturado em quatro blocos. Tal como no Modelo A, o processo começa com a caracterização e quantização do sinal da nanoantena, mas utiliza uma quantização de 8 bits. O segundo bloco implementa a correção de erros. Para este modelo, foi selecionado o código Reed-Solomon (255, 223), um esquema de correção de erros em bloco significativamente mais poderoso, capaz de corrigir até 16 erros de byte por bloco, o que é crucial para garantir a integridade dos dados antes da aplicação de protocolos criptográficos robustos que são sensíveis a erros de bit. O terceiro bloco é o núcleo do sistema e gere a geração de chaves e a encriptação. Utiliza o protocolo Elliptic Curve Diffie-Hellman (ECDH) sobre a curva secp256r1 para a troca segura de uma chave de sessão partilhada entre o emissor e o recetor. Esta chave de sessão é depois usada para a encriptação simétrica dos dados com o Advanced Encryption Standard em modo Cipher Block Chaining (AES-CBC), que oferece elevada difusão e resistência a ataques criptanalíticos. Por fim, o recetor utiliza a chave de sessão partilhada, que também gerou de forma independente via ECDH, para desencriptar os dados com AES e,

subsequentemente, aplicar o descodificador Reed-Solomon para reconstruir o sinal original. Este modelo privilegia a robustez criptográfica e a confidencialidade, mesmo que à custa de uma maior sobrecarga computacional.

A seguir, serão apresentados e discutidos os resultados experimentais obtidos para a resposta da nanoantena e para o desempenho comparativo de ambos os modelos criptográficos.

IV. Resultados e Discussão

Esta secção apresenta a avaliação de desempenho do sistema proposto, com o objetivo de quantificar o trade-off entre a fidelidade do sinal e a segurança. Primeiramente, analisa-se a resposta eletromagnética da nanoantena projetada, caracterizando o seu comportamento face a diferentes sinais de excitação. Subsequentemente, avalia-se a performance dos dois modelos criptográficos (Modelo A e Modelo B) quando aplicados aos sinais amplificados pela nanoantena, comparando a sua eficácia em termos de integridade do sinal e robustez de segurança.

A. Resposta da Nanoantena

A análise da resposta eletromagnética da nanoantena foi realizada através de uma simulação em varrimento de frequência (0.1 a 3 THz) no COMSOL. O primeiro passo consistiu em identificar o ponto espacial de máxima intensidade de campo elétrico, que corresponde à região de maior confinamento de energia e, portanto, à resposta mais significativa da estrutura. O ponto de máxima intensidade de campo elétrico, que corresponde à região de maior confinamento de energia, foi identificado nas arestas de uma das aberturas centrais da matriz (Figura 3). A função de transferência complexa da nanoantena, H(f), foi então calculada nesse local específico, capturando a transformação em amplitude e fase que um sinal incidente sofre ao interagir com a estrutura.

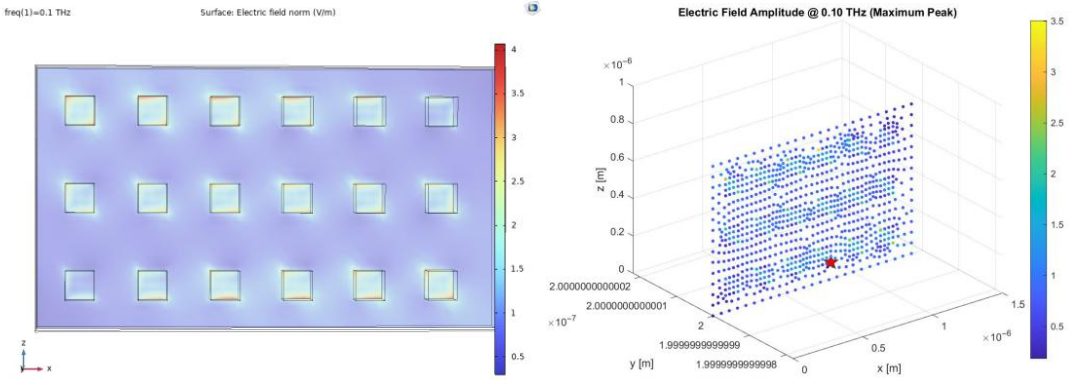

Figura 3: Distribuição espacial da norma do campo elétrico e ponto de maior intensidade na superfície da nanoantena na frequência de ressonância.

Para avaliar o comportamento temporal, a nanoantena foi excitada com três sinais distintos: um impulso de Dirac, um pulso Gaussiano e um sinal de voz sintético. A resposta a um impulso de Dirac revela a resposta impulsiva intrínseca do sistema, mostrando como a nanoantena "ressoa" após uma excitação de banda larga. A resposta a um pulso Gaussiano (Figura 4) demonstra como a estrutura filtra e distorce um sinal de banda limitada, realçando o seu comportamento de filtragem. Finalmente, a resposta ao sinal de voz sintético (Figura 5) simula um cenário de comunicação mais realista, mostrando a amplificação do sinal modulado, o que confirma a sua viabilidade para aplicações práticas.

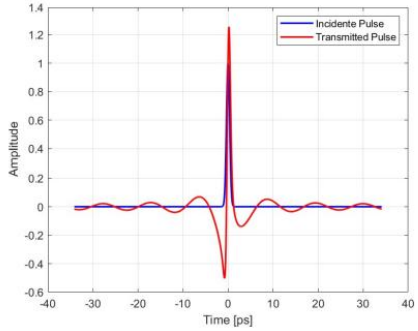

Figura 4: Resposta temporal da nanoantena a um pulso de Dirac.

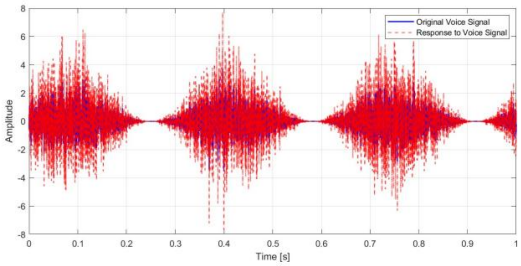

Figura 5: Resposta temporal da nanoantena a um sinal de voz.

B. Análise de Desempenho do Modelo A

O desempenho do Modelo A foi avaliado em múltiplos cenários para quantificar a sua capacidade de preservação do sinal e a sua sensibilidade à chave de encriptação. A Tabela 2 resume as métricas de Coeficiente de Correlação, Erro Quadrático Médio (RMSE) e Rácio Pico de Sinal-Ruído (PSNR) para os sinais de Dirac e Gaussiano. Em condições ideais (sem ruído e com a chave correta), o modelo alcançou uma recuperação quase perfeita, com um coeficiente de correlação de 1.00 e um PSNR superior a 100 dB, indicando uma degradação de sinal insignificante. Quando submetido a um ambiente ruidoso, o desempenho degradou-se, mas manteve uma correlação razoável (0.65-0.75). Crucialmente, na ausência da chave correta, a correlação caiu para valores próximos de zero (≈0.01) e o PSNR para cerca de 6 dB, demonstrando que o sinal não pode ser recuperado sem a chave correta, o que confirma a eficácia da encriptação. A Figura 6 ilustra a excelente qualidade da recuperação em ambiente ideal.

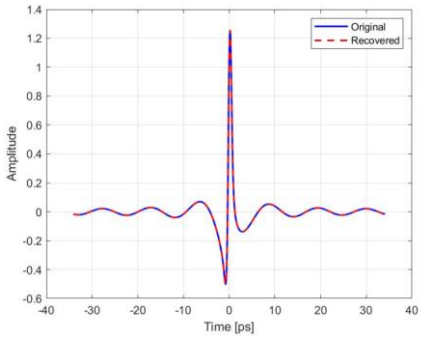

Figura 6: Sinal original vs sinal recuperado em ambiente ideal.

Tabela 2: Resumo dos resultados do Modelo A para os sinais de Dirac e Gaussiano.

Sinal	Cenário	Coeficiente de Correlação	RMSE	PSNR (dB)
Dirac	Ideal	1.00	1.2147×10^{-5}	103.76
	Ruidoso (0.2 V/m)	0.6513	0.11506	24.23
	Chave Errada	0.0126	0.94768	5.91
Gaussiano	Ideal	1.00	7.6890×10^{-6}	104.27
	Ruidoso (0.2 V/m)	0.7507	0.11595	20.70
	Chave Errada	0.0118	0.64662	5.78

A resiliência do modelo foi também testada com o sinal de voz sintético sob diversas condições de degradação. Em cenários de ruído aditivo gaussiano branco (AWGN) e quantização, a recuperação do sinal foi excelente, com correlações superiores a 0.99. No entanto, em cenários de propagação multipercurso e eco, a performance foi mais modesta, com correlações de 0.25 e 0.85, respetivamente, destacando a sensibilidade do modelo a distorções temporais complexas.

C. Análise de Desempenho do Modelo B

O Modelo B foi avaliado com foco tanto na qualidade da reconstrução do sinal como nas suas propriedades criptográficas. A Tabela 3 sumariza as principais métricas para os três tipos de sinal. Os resultados mostram uma boa qualidade de reconstrução, com valores de PSNR entre 24 e 28 dB e coeficientes de correlação entre 0.75 e 0.90. Embora estes valores de fidelidade sejam inferiores aos do Modelo A em condições ideais, indicam que o sinal é recuperado com uma distorção aceitável para muitas aplicações de comunicação digital. A Figura 7 ilustra a qualidade da reconstrução para o sinal de voz sintético.

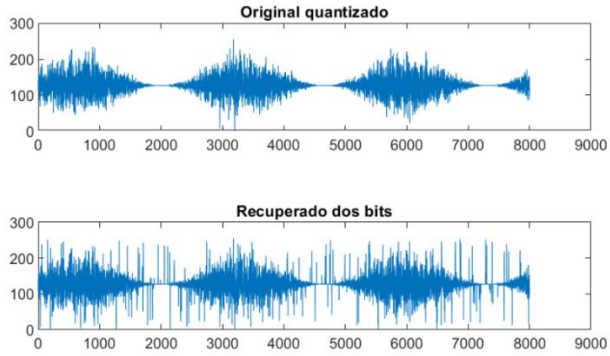

Figura 7: Sinal de voz original vs sinal recuperado.

Tabela 3: Resumo dos resultados de desempenho do Modelo B.

Métrica	**Pulso de Dirac**	**Pulso Gaussiano**	**Sinal de Voz**
RMSE	10.1257	11.4235	15.1256
PSNR (dB)	28.02	26.97	24.54
Coef. Correlação	0.7580	0.9087	0.8062
Entropia (Original)	1.8278	2.4746	4.5371
Entropia (Recup.)	1.5987	2.5292	3.9869
Efeito Avalanche	0.5005	0.5052	0.4992

O ponto forte do Modelo B reside nas suas propriedades de segurança. O efeito avalanche, que mede a alteração no texto cifrado quando um único bit da chave é modificado, situou-se consistentemente em torno de 0.5. Este valor é considerado ideal e indica uma excelente difusão, significando que pequenas alterações na chave produzem alterações drásticas e imprevisíveis na saída, o que torna o sistema resistente a ataques de criptanálise diferencial. A análise de entropia também confirmou que a estrutura estatística do sinal original foi razoavelmente preservada após a desencriptação, validando a robustez criptográfica do modelo.

D. Discussão Comparativa

A análise comparativa dos dois modelos revela um trade-off fundamental entre a integridade do sinal e a confidencialidade criptográfica. A Tabela 4 apresenta uma avaliação qualitativa que sintetiza as forças e fraquezas de cada abordagem.

Tabela 4: Comparação qualitativa entre o Modelo A e o Modelo B.

Critério	**Modelo A**	**Modelo B**
Integridade do Sinal	★★★★★	★★★☆☆
Robustez ao Ruído	★★★★☆	★★★☆☆
Confidencialidade	★★☆☆☆	★★★★★
Segurança da Gestão de Chaves	★☆☆☆☆	★★★★★
Eficiência Computacional	★★★★★	★★★☆☆
Robustez Criptográfica	★★☆☆☆	★★★★★
Avaliação Geral	★★★☆☆	★★★★☆

O Modelo A distingue-se pela elevada eficiência computacional e pela capacidade de preservar a fidelidade do sinal, sendo adequado a aplicações em que a integridade da forma de onda é prioritária e os recursos são limitados. Contudo, a sua segurança assenta num PRNG com chave estática e na Transformada de Arnold para embaralhamento espacial, o que o torna vulnerável a ataques mais sofisticados, nomeadamente ataques de texto conhecido.

Em contrapartida, o Modelo B oferece uma segurança muito superior. A utilização de ECDH para a troca de chaves e de AES-CBC para a encriptação alinha-o com os padrões criptográficos modernos. O seu forte efeito avalanche e a elevada difusão garantem uma confidencialidade robusta. Esta segurança acrescida tem, no entanto, um custo: uma maior complexidade computacional e uma degradação mais acentuada do sinal recuperado.

A conclusão central desta análise é que não existe uma solução única. A escolha entre o Modelo A e o Modelo B dependerá intrinsecamente dos requisitos da aplicação. Sistemas de baixo risco e com fortes restrições de processamento beneficiarão da simplicidade e fidelidade do Modelo A, enquanto sistemas de segurança crítica, onde a confidencialidade é inegociável, exigirão a robustez do Modelo B. Esta dualidade define o panorama atual das comunicações seguras em nano-redes e orienta as conclusões deste trabalho.

V. Conclusões

Este trabalho teve como objetivo central investigar a viabilidade e as implicações práticas da integração de nanoantenas com modelos criptográficos para o desenvolvimento de sistemas de comunicação sem fios seguros em escala nanométrica. As contribuições deste estudo reafirmam o potencial desta sinergia e, simultaneamente, expõem os desafios e os compromissos inerentes a esta nova fronteira tecnológica.

As principais conclusões extraídas confirmam a viabilidade técnica da abordagem proposta. A simulação da nanoantena em COMSOL demonstrou a sua capacidade de gerar fenómenos de amplificação de campo local, essenciais para compensar as perdas de propagação na banda de THz. A implementação e teste dos dois modelos criptográficos sobre os sinais amplificados permitiram validar a sua funcionalidade e quantificar o trade-off central do estudo. O Modelo A, mais leve, provou ser excecional na preservação da integridade do sinal, sendo adequado para sistemas com recursos computacionais limitados onde a fidelidade da forma de onda é crítica. Em contraste, o Modelo B, baseado em ECC e AES, garantiu um nível de segurança robusto, alinhado com os padrões criptográficos modernos, embora à custa de uma maior degradação do sinal e de uma maior sobrecarga computacional. A principal ilação deste trabalho é a confirmação de um trade-off fundamental entre a fidelidade do sinal e a robustez da segurança. A escolha do modelo criptográfico ideal não é universal, dependendo diretamente dos requisitos específicos da aplicação: sistemas que priorizam a eficiência e a qualidade do sinal tenderão para soluções como o Modelo A, enquanto aplicações de segurança crítica exigirão a confidencialidade garantida pelo Modelo B.

Bibliografia

[1] J. M. Jornet and I. F. Akyildiz, “Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band,” IEEE Transactions on Wireless Communications, vol. 10, no. 10, pp. 3211–3221, 2011.

[2] B. S. Rawat, A. Bhat, and J. Pištora, “Thz band nanoantennas for future mobile communication,” in 2013 International Conference on Signal Processing and Communication (ICSC). IEEE, 2013, pp. 48–52.

[3] S. Dash, C. Liaskos, I. F. Akyildiz, and A. Pitsillides, “Nanoantennas design for thz communication: material selection and performance enhancement,” in Proceedings of the 7th ACM international conference on nanoscale computing and communication, 2020, pp. 1–6.

[4] B. Rawat, A. Bhat, and J. Pistora, “Thz band nanoantennas for future mobile communication,” pp. 48–52, 12 2013.

[5] J. A. Dionne and H. A. Atwater, “Plasmonics: Metal-worthy methods and materials in nanophotonics,” Mrs Bulletin, vol. 37, no. 8, pp. 717–724, 2012.

[6] S. Kavitha, K. Sairam, and A. Singh, “Silver and gold nano antennas for thz optical communication,” in 2021 international Conference on innovative computing, intelligent communication and smart electrical systems (ICSES). IEEE, 2021, pp. 1–6.

[7] J. Li, “5g wireless communication network security system encryption based on des algorithm,” in 2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI). IEEE, 2022, pp. 1045–1049.

[8] A. Tidrea, A. Korodi, and I. Silea, “Elliptic curve cryptography considerations for securing automation and scada systems,” Sensors, vol. 23, no. 5, p. 2686, 2023.

[9] D. Dayana, R. Pandian, A. R. Babu, S. Nirmalraj, S. S. Jebaseelan et al., “Elevating security in wireless sensor networks using ecc and aes cryptographic techniques,” in 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). IEEE, 2023, pp. 1–6.

[10] S. Kumar and D. Sharma, “A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm,” Artificial Intelligence Review, vol. 57, no. 4, p. 87, 2024.

[11] R. Shelke and M. Nemade, “Audio encryption algorithm using modified elliptical curve cryptography and arnold transform for audio watermarking,” in 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018, pp. 1–4.

[12] T. Ebbesen, H. Lezec, H. Ghaemi, T. Thio, and P. Wolff, “Extraordinary optical transmission through sub-wavelength hole arrays,” Nature, vol. 391, pp. 667–669, 02 1998.