Análise do algoritmo *single-bit* de geração de chaves criptográficas usando informação do canal

Yan Podkorytoff Ike Chícharo, Pedro Ivo da Cruz e Murilo Bellezoni Loiola

***Resumo*— Este trabalho tem como objetivo o estudo de um algoritmo de quantização para a geração de chaves de criptografia a partir da informação do canal, avaliando-o em relação a sua capacidade de acordo de chave, número de bits gerados e sua aleatoriedade.**

***Palavras-Chave*— segurança da informação na camada física, geração de chave, comunicações sem fio.**

***Abstract*— This work studies a quantization algorithm for encription key generation from wireless channel features. The algorithm is evaluated in terms of key disagreement rate, number of generated bits and randomness.**

***Keywords*— physical-layer security, key generation, wireless communications.**

I. Introdução

Os mecanismos de criptografias convencionais se baseiam na dificuldade de se gerar as chaves criptográficas [1]. Esta dificuldade pode não ser mais verdade com os avanços no desenvolvimento de hardwares com alto poder de processamento e da computação quântica [2]. Além do mais, com o surgimento do conceito de Internet das Coisas, (IoT, do inglês *Internet of Things*), a utilização de redes descentralizadas, com dispositivos de baixo consumo energético e com poder computacional restrito inviabiliza a utilização dos mecanismos tradicionais [3].

A geração de chaves criptográficas a partir da informação do canal sem fio (CSI, do inglês *channel state information*), proposta inicialmente em [4], vem sendo estudada extensivamente como forma de resolver estes problemas [5]. Como a CSI é considerada aleatória, uma sequência de bits gerada a partir dela também será aleatória. Como observado na Fig. 1, Alice e Bob observam o mesmo canal h, o que permite que uma mesma chave seja gerada em ambos, enquanto Eve, um nó espião, observa um canal diferente g devido à descorrelação espacial e, portanto, não será capaz de gerar a mesma chave [5]. A variação temporal do canal permite que diferentes medidas da CSI possam ser feitas em instantes de tempo diferentes, possibilitando a geração de uma chave criptográfica grande o suficiente para ser utilizada nos algoritmos de quantização [5].

Uma das etapas de geração da chave consiste na quantização da CSI, gerando uma sequência de bits que será utilizada como chave de criptografia. Este trabalho avalia algumas dessas técnicas de quantização no que se refere ao tamanho das chaves geradas, à taxa de desacordo de chave (KDR, do inglês *key disagreement rate*), à taxa de geração de chave (KGR, do inglês *key generation rate*) e a sua aleatoriedade, avaliada de acordo com o teste de frequência de bit proposto pelo *National Institute of Standards and Technology* [6].

Yan P. I. Chícharo, Pedro I. da Cruz e Murilo B. Loiola estão com o Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Universidade Federal do ABC, Santo André, SP, Brasil, E-mails: yan.ike@aluno.ufabc.edu.br, pedro.cruz@aluno.ufabc.edu.br, murilo.loiola@ufabc.edu.br.

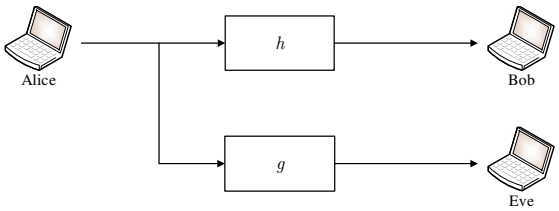

Fig. 1. Modelo para geração de chaves criptográficas a partir da CSI.

II. Geração da Chave Criptográfica

Neste trabalho, o modelo de desvanecimento por bloco foi utilizado [7], sendo que a resposta ao impulso do canal é considerada constante durante a transmissão de um bloco de informação e varia aleatoriamente de um bloco para o outro. Desta forma, Alice e Bob observarão o mesmo canal, porém suas estimativas da CSI sofrerão efeito de diferentes fontes de ruído, que implicará em erros no acordo de chave.

O algoritmo de quantização utilizado foi apresentado em [8] e foi utilizado em diversos trabalhos. Neste algoritmo, dois limiares são calculados, q_+ e q_- de acordo com

$$q_\pm = \mu_X \pm \alpha \cdot \sigma_X, \tag{1}$$

onde μ_X, σ_X representam, respectivamente, a média e a variância de X_u, $u = \{a, b\}$, que por sua vez representa um vetor contendo todas as medidas de CSI realizadas em Alice (a) e Bob (b) e α é uma constante maior que zero que controla a distância entre os limiares e a média. Em seguida, as amostras da CSI são então convertidas em bits de acordo com o seguinte critério:

$$Q(X_u) = \begin{cases} 1, & \text{caso } x_u(n) > q_+ \\ 0, & \text{caso } x_u(n) < q_-. \end{cases} \tag{2}$$

Amostras entre os limiares são descartadas pelo algoritmo de quantização. Alice e Bob armazenam e enviam um ao outro os índices das amostras descartadas para que ambos desprezem essas amostras em suas chaves. Neste trabalho, variável X_u contém a resposta em frequência do canal obtida através do cálculo de transformada discreta de Fourier de 256 pontos da CSI estimada nos usuários.

III. Resultados e Discussão

Foi simulado um sistema de comunicação, onde o canal foi estimado através de um estimador de mínimos quadrados [7]. Foram coletadas 10^4 diferentes respostas em frequência de 256 pontos em Alice e Bob, usadas para gerar a chave.

A variação da KDR de acordo com a SNR (do inglês *Signal-to-Noise Ratio*) e o parâmetro α é apresentada na Fig. 2. Como pode ser observado, o aumento do parâmetro α proporciona ao algoritmo uma redução na KDR. Três características do canal foram analisadas: a parte real da resposta ao impulso obtida; a magnitude da resposta ao impulso obtida; e o *fine-grained CSI* [5]. Os resultados apresentados na Fig. 2 foram obtidos utilizando a parte real da resposta ao impulso para a geração das chaves criptográficas. Resultados equivalentes foram obtidos com a utilização das outras características. Como pode ser observado, o aumento do valor do parâmetro alfa permite uma redução na KDR.

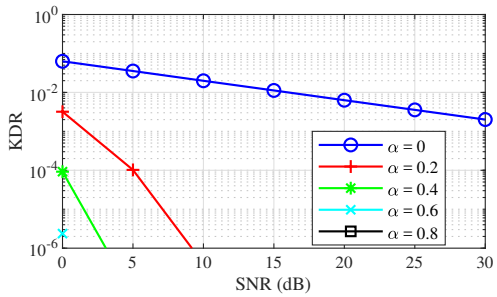

Fig. 2. Taxa de desacordo de chaves com a variação do parâmetro α a partir resposta do canal.

No entanto, esse aumento prejudica a KGR, como mostra a Fig. 3. A medida que se aumenta o valor de α, a KGR diminui devido a quantidade de amostras de X_u descartadas pelo algoritmo de quantização.

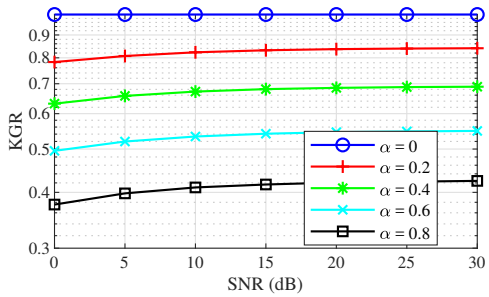

Fig. 3. Taxa de geração de chaves com a variação do parâmetro α a partir resposta do canal.

Para a análise da aleatoriedade das chaves, o canal foi submetido a uma SNR fixada em 30 dB. Foi utilizado o teste de frequência de bit, estabelecida pelo NIST (do inglês *National Institute of Standards & Technology*) [6], que avalia a sequência de bits a partir da variável *p-value* (P_v), descrita em [6]. Esta sequência é considerada aleatória se $P_v \geq 0.01$.

A tabela I apresenta os resultados obtidos utilizando a fine-grained CSI, a parte real e a magnitude da resposta ao impulso do canal em relação ao tamanho de bloco utilizado para calcular os limites de quantização, com $\alpha = 0.4$ e SNR $= 30$ dB. Nesta etapa, X_u é dividida em blocos de tamanho N, que são quantizados independentemente. Devido ao fato de o fine-grained CSI gerar o dobro do número de bits para a chave, foi realizado o teste para tamanho de bloco de até 512000 bits.

TABELA I

P_V OBTIDOS NO TESTE DE FREQUÊNCIA.

		Channel State Information		
		Fine-grained CSI	Real	Magnitude
N	16	0.9620	0.9621	0.0882
	128000	0.4938	0.5346	0.1003
	256000	0.4331	0.5767	0.3416
	384000	0.4399		
	512000	0.5218		

De acordo com os resultados, a magnitude apresentou os menores valores de P_V. Isto se deve ao fato de a curva dos coeficientes apresentarem uma proporção muito diferente de 0's e 1's na cadeia binária. Em contraposição, pode-se observar bons resultados para o uso da parte real da resposta ao impulso do canal e do *fine-grained CSI* com blocos de 16 bits. Essas diferenças entre os resultados de diferentes características do canal deve-se ao fato destas possuírem diferentes distribuições de probabilidade, o que impacta o nível de aleatoriedade da chave. Em tempo, a magnitude possui uma distribuição *Rayleigh*, enquanto o *fine-grained CSI* e a parte real possuem distribuições Gaussianas.

Outro ponto a ser notado é que a diminuição de N proporciona uma maior extração da aleatoriedade do sistema, impedindo a criação de longas sequências de 0's e 1's.

IV. Conclusões

A partir dos resultados apresentados neste trabalho, pode-se observar que o aumento no parâmetro α produziu significativas reduções na KDR em detrimento da redução na KGR.

Também foi observado o impacto de diferentes características do canal e do tamanho de bloco na aleatoriedade da chave.

Referências

[1] W. Stallings, *Cryptography and Network Security (4th Edition)*. Prentice-Hall, Inc., 2005.

[2] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[3] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the internet of things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, pp. 1–16, 2017.

[4] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, 1995.

[5] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, 2016.

[6] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, *SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute of Standards & Technology, 2010.

[7] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications with MATLAB*. Wiley Publishing, 2010.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy," in *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*. New York, New York, USA: ACM Press, 2008, p. 128.