Sistema de Autenticação de Usuário em Camada Física Empregando Sequências Caóticas

João V. C. Evangelista, Daniel P. B. Chaves e Cecilio Pimentel

***Resumo*— Em um sistema de comunicação típico, os mecanismos de autenticação são dominantemente implementados em níveis acima da camada física; apesar de haver estratégias (*e.g.*, espalhamento espectral) que são implementadas ao custo de recursos do sistema de comunicação, como maior consumo de banda. Alternativamente, a autenticação pode ser realizada na camada física sem impactar nos requisitos do sistema original e apresentando propriedades adicionais, como: transparente para usuários que não possuem a chave secreta, robustez contra interferência e verificação de identidade de usuário confiável. Este trabalho aborda o projeto e os limitantes deste sistema com o emprego de sequências caóticos.**

***Palavras-Chave*— Autenticação de usuário, sequência caótica, segurança incondicional, camada física.**

***Abstract*— In a typical communication system most mechanisms of authentication exist above the physical layer, though some (e.g., spread-spectrum communication) exist at the physical layer often with an additional cost in bandwidth. Alternatively, authentication may be implemented in the physical layer without impact on the original system and still exhibiting additional properties: stealthy to uninformed users, robustness to interference, and trusted user identity verification. This paper addresses the project and limits of this system when chaotic sequences are used for authentication.**

***Keywords*— User authentication, chaotic sequence, unconditional security, physical layer.**

I. Introdução

A autenticação em camada física visa aumentar a segurança do sistema de comunicação com a implementação de serviços de segurança em diversas camadas da rede. Assim, ataques ao sistema precisariam romper a segurança em múltiplas camadas e não só nas camadas superiores. Algumas propostas adotam o envio de uma forma de onda como *tag*, obtida a partir de uma chave secreta compartilhada entre os usuários legítimos. Esse foi o método adotada em [1], [2], onde o sinal de *tag* é gerado a partir de funções de hash, que em seguida é sobreposto à mensagem. A incerteza sobre a chave dada uma observação ruidosa do *tag* é empregada para avaliar a segurança. O sistema resultante apresenta alta incerteza sobre a chave se a relação entre as potências do *tag* e do ruído é baixa, contudo, quando a potência do ruído é reduzida, esta incerteza se aproxima de zero. A avaliação de segurança do sistema proposto não traz uma abordagem analítica para a probabilidade de sucesso de ataques. Em [3], se propõe o emprego das respostas do canal para determinar sinais de *tag*. Essa técnica minimiza os efeitos do *tag* sobre a probabilidade de erro, contudo, falta à proposta análises de segurança. Em geral, as técnicas baseadas em *tag* permitem melhorar a segurança do sistema através de alterações nas propriedades do sinal de *tag*, ao custo do desempenho na detecção de mensagens. Além disso, a segurança do sistema continua atrelada à potência de ruído e falta o desenvolvimento analítico para as diferentes estratégias de ataque.

Outra estratégia procura explorar a diferença de qualidade do canal entre usuários legítimos em relação ao canal entre usuário legítimo e adversário. Em [4] o fato de canais descorrelacionarem rapidamente com a distância é empregado. Particularmente, assumindo que o canal é invariante, o sistema proposto identifica mensagens enviadas pelo adversário quando a qualidade do canal entre usuários legítimos é superior a observada entre usuário legítimo e adversário. Um método similar é proposto em [5], mas com canais variantes no tempo. O problema da identificação do canal entre usuários legítimos é modelado através de um teste de hipótese. Como em [4], persiste a baixa probabilidade em detectar mensagens fraudulentas quando a qualidade do canal entre usuários legítimos é baixa. Em [6], um limiar adaptativo para o teste de hipótese é proposto, o que resultou em uma alta probabilidade em detectar o adversário mesmo com um canal de baixa qualidade entre usuários legítimos. Em [7] é proposto um novo método para obter a resposta do canal, que resulta em alta probabilidade de detectar o adversário quando o canal apresenta baixo espalhamento Doppler. Um método baseado na proposição de desafios para a autenticação do transmissor é proposto em [8], neste caso, o receptor legítimo envia o desafio para o transmissor, que para ser autenticado deve respondê-lo corretamente. Apesar de realizar a análise de sucesso do adversário, só considera ataques passivos. Em todos esses trabalhos a probabilidade de detectar uma mensagem enviado pelo adversário depende da melhor qualidade do canal entre usuários legítimos que a do canal entre o usuário legítimo e o adversário. Além disso, nenhum desses trabalhos derivam a probabilidade de sucesso para ataques ativos.

Este trabalho é baseado na técnica de geração de *tag* sobreposto ao sinal da mensagem, contudo, esta geração emprega sequências caóticas. Há duas contribuições principais neste trabalho: a apresentação de uma técnica de geração de *tag*, empregando sequências caóticas, que possibilita segurança incondicional para a chave; a derivação analítica das probabilidades de sucesso para os ataques de disfarce e de substituição.

A seguir detalhamos na Seção II o ambiente de comunicação utilizado como referência, especificando os agentes envolvidos e suas atribuições no sistema. Os ataques analisados no

João V. C. Evangelista, École de Technologie Superieure, Montreal-QC, Canadá, E-mail: vdecarvalho@lacime.etsmtl.ca; Daniel P. B. Chaves e Cecilio Pimentel, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: daniel.chaves@ufpe.br, cecilio@ufpe.br.

trabalho são explicados na Seção III. O processo de geração do *tag* proposto no trabalho é abordado na Seção IV. Em seguida, as probabilidades de sucesso dos ataques analisados no trabalho são derivadas analiticamente na Seção VI. Um possível diagrama do transmissor para o sistema proposto é discutido na Seção VII. Por fim, a Seção VIII traz as conclusões.

II. O Cenário Considerado

Para os propósitos deste trabalho, consideramos um cenário com três agentes compartilhando um único canal inseguro. Dois deles, designados como usuários legítimos, compartilham uma informação sigilosa, denominada chave secreta. O terceiro é o usuário malicioso que, através de ataques passivos ou ativos, pode comprometer a segurança do sistema de autenticação. A seguir, o papel e a capacidade de cada um desses usuários são detalhados no escopo do sistema considerado. A síntese da relação dos usuários, envolvendo o canal, é apresentada na Fig. 1.

1) Alice: É uma usuária legítima, implicando que emprega o protocolo proposto de autenticação. Ela envia mensagens acompanhadas de códigos de autenticação, *tags*, que dependem da chave compartilhada com o outro usuário legítimo.

2) Bob: Assim como Alice, é um usuário legítimo, e compartilha as mesmas premissas. Ele recupera as mensagens recebidas e decide aceitá-las ou não baseado na identificação de *tags* legítimos.

3) Eve: É uma usuária maliciosa do sistema, para a qual assumimos a hipótese de Kerckhoff [9], portanto, com exceção da chave compartilhada por Alice e Bob, ela conhece todos os detalhes do esquema. Ela é um adversário ativo, cujo o objetivo é inviabilizar a comunicação entre Alice e Bob. Considera-se que ela pode interceptar pacotes enviados por Alice e enviar pacotes maliciosos para Bob.

A. Autenticação em Camada Física

Tipicamente, os protocolos de autenticação são implementados em camadas superiores da rede [10], [11], tendo a segurança associada à dificuldade de solucionar problemas com complexidade superpolinomial, logo, dependente da capacidade computacional do adversário.

Por outro lado, autenticação em camada física é beneficiada pela natureza estocástica do canal sem fio, o que as permite alcançar segurança incondicional, ou seja, independente da capacidade computacional do adversário não há informação suficiente disponível para comprometer a segurança [1]. Neste trabalho propomos um método para geração de *tag* empregando mapas caóticos, que diferencia-se de propostas anteriores por apresenta segurança incondicional independe das características estocásticas do canal.

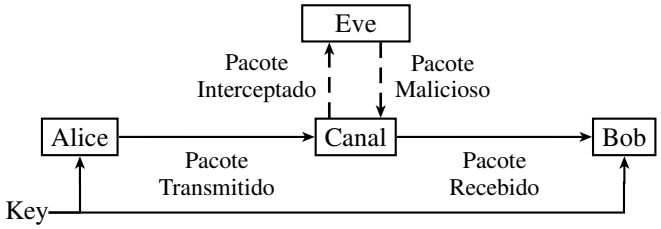

Fig. 1. Cenário de comunicação sobre canal inseguro.

O envio do *tag* para o receptor pode ser feito essencialmente de duas formas: empregando multiplexação por divisão de tempo (TDM) entre o *tag* e a mensagem; ou por incorporação do *tag* na mensagem. Enquanto no primeiro a mensagem e o *tag* são enviados em intervalos de tempo distintos, no segundo são alocadas potências distintas para eles, que são somados e, em seguida, transmitidos como um único pacote.

No TDM é fácil identificar tanto a mensagem como o *tag*, contudo, há uma redução no número de bits de informação por pacote. Já na incorporação do *tag*, como a potência deste é uma fração da que é alocada para a mensagem, a sua identificação é mais difícil. No entanto, essa dificuldade também é vivenciada pelo adversário, além disso, não há a redução do número de bits de informação por pacote. Como uma caraterística mais sutil, a diferença de potência entre a mensagem e o *tag* pode ser empregada como um mecanismo de segurança adicional, como é discutido em [12]. A incorporação do *tag* é o método de autenticação considerado neste trabalho.

B. Função de Autenticação

Uma forma usual de verificar a autenticidade de uma mensagem é empregar uma função $g(\cdot)$ que retorna um *tag* como função da mensagem, $\mathbf{s}$, e da chave secreta, $\mathbf{k}$, compartilhada entre os usuários legítimos. Alice envia o *tag*, $\mathbf{t} = g(\mathbf{s}, \mathbf{k})$, em conjunto com a mensagem para Bob através de um canal com ruído AWGN (*Additive White Gaussian Noise*). Considera-se que a mensagem é recuperada com sucesso tanto por Bob quanto por Eve. Contudo, Bob é o único capaz de gerar o mesmo *tag* $\mathbf{t}$ que Alice, uma vez que só eles detêm a chave secreta. Por outro lado, a informação que Eve possui sobre o *tag* advém da observação deste em presença de ruído. Considera-se que $\mathbf{s}$ e $\mathbf{t}$ são vetores binários de comprimento L, além disso, a chave $\mathbf{k}$ é um vetor binário de comprimento K maior que L.

III. Ataques à Segurança

A seguir são considerados três possíveis ataques à segurança do sistema de autenticação. A abordagem adotada segue [1], [13].

1) Ataque de disfarce: Neste ataque Eve tenta enviar mensagens para Bob passando-se por Alice. Supondo que Eve observa o par $(\mathbf{s}, \tilde{\mathbf{t}})$, onde $\tilde{\mathbf{t}}$ é uma versão ruidosa de $\mathbf{t} = g(\mathbf{s}, \mathbf{k})$. Assim, empregando o conhecimento adquirido com essa observação, Eve estima a chave $\mathbf{k}$ empregada para gerar $\mathbf{t}$ e envia o par fraudulento $(\mathbf{s}', \mathbf{t}')$. A probabilidade de sucesso desse ataque (quando $\mathbf{t}'$ é um tag legítimo para $\mathbf{s}'$) é denotada por P_I, sendo igual à probabilidade de determinar $\mathbf{k}$.

2) Ataque de substituição: Este ataque consiste em Eve interceptar um par $(\mathbf{s}, \tilde{\mathbf{t}})$, $\mathbf{t} = g(\mathbf{s}, \mathbf{k})$, e alterar o conteúdo da mensagem. Eve obtém sucesso se conseguir encontrar uma mensagem $\mathbf{s}'$ diferente de $\mathbf{s}$ que gera o mesmo *tag*, ou seja, $\mathbf{t} = g(\mathbf{s}', \mathbf{k})$. A probabilidade de sucesso deste ataque é denotada por P_S.

3) Ataque de repasse: Este ataque consiste em Eve armazenar um par legítimo $(\mathbf{s}, \tilde{\mathbf{t}})$ e retransmiti-lo para Bob no futuro. A probabilidade de sucesso deste ataque é denotada por P_R.

IV. Geração de Tag

A função de geração de *tag* proposta neste artigo é baseada em mapas caóticos, o que a difere de outras abordagens, que são baseadas em cifragem e em função de hash. Um mapa caótico unidimensional, o tipo considerado neste artigo, é caracterizado por uma dinâmica decorrente da iteração de uma função não-linear $f : A \to A$ a partir de uma condição inicial $x[0]$, tal que:

$$x[n] = f(x[n-1]),\ n = 1, 2, 3, \ldots$$

Denomina-se $\{x[n]\}_{i=0}^{\infty} = \{x[0], f(x[0]), f^2(x[0]), \ldots\}$ uma órbita de f iniciada em $x[0]$, em que $f^n(x) = f^{n-1}(f(x))$. Neste trabalho, os *tags* são gerados como intervalos finitos de órbitas do mapa caótico, e para fins de autenticação, devem ser descorrelacionados quando associados a mensagens distintas. Devido a sensibilidade às condições iniciais dos mapas caóticos [14], mesmo que as órbitas sejam geradas a partir de pontos infinitesimalmente próximos, em um futuro próximo elas divergem e seguem trajetórias descorrelacionadas. Portanto, os *tags* podem ser gerados associando a mensagens distintas condições iniciais distintas.

O conjunto de possíveis condições iniciais é dado por $\mathcal{X}_0 = \{x^i\}_{i=0}^{2^K-1}$, sendo conhecido por todos os usuários do sistema. De forma similar, o conjunto $\mathcal{X}_n \triangleq \{f^n(x) | \forall\ x \in \mathcal{X}_0\}$ é o resultado de todas as n-ésimas iterações possíveis a partir de $\mathcal{X}_0$. Seja $M(\cdot)$ um mapa injetivo de todos os vetores binários de comprimento K para os elementos de $\mathcal{X}_0$, então uma condição inicial é determinada por

$$x[0] = M\big(\mathbf{k} \oplus (\mathbf{s} || \mathbf{t}_s)\big), \tag{1}$$

onde $\mathbf{t}_s$ é o contador de mensagens, com comprimento $K - L$ e cujo valor é conhecido por todos os usuários, $\oplus$ é a operação XOR, e $||$ é a concatenação de vetores. O contador de mensagens $\mathbf{t}_s$ assume papel importante contra ataque por repasse, uma vez que o *tag* torna-se variante no tempo [1]. Considera-se que $\mathbf{k}$ possui distribuição de probabilidade uniforme, portanto, esse também será o caso do argumento de $M(\cdot)$ em (1); tal que, $P(x[0] = x) = 1/2^K$ para todo $x \in \mathcal{X}_0$.

Ao passo que um mapa caótico evolui por uma órbita, a informação sobre a condição inicial que deu origem a correspondente dinâmica decresce [15], [16]. Esse fenômeno pode ser empregado para limitar a informação máxima sobre a condição inicial, e a partir de (1), sobre a própria chave, que um usuário malicioso pode ter ao observar o *tag*. Essa restrição à informação pode ser alcançada não empregando os L primeiros pontos da órbita como *tag*, ou seja, desprezando um trecho inicial de comprimento σ, $\sigma < K$. Portanto, o *tag* é gerado a partir do valor $x[0]$ definido em (1), como um trecho de órbita de comprimento L após um salto de σ, ou seja:

$$\mathbf{t} = \big[x[\sigma]\ x[\sigma+1]\ \cdots\ x[\sigma+L-1]\big], \tag{2}$$

onde $x[\sigma] \triangleq f^{\sigma}(x[0])$. Como é demonstrado na próxima seção, o parâmetro σ define o grau de proteção da chave.

V. Segurança Incondicional

A entropia condicional da chave dada uma observação sem ruído da mensagem e do *tag*, $H(\mathbf{k}|\mathbf{s}, \mathbf{t})$, é empregada para quantificar a segurança incondicional do sistema de autenticação proposto [1], [17]. Inicialmente escreveremos $H(\mathbf{k}|\mathbf{s}, \mathbf{t})$ em termos da órbita empregada para gerar o *tag*. Considere $H(x[0], \mathbf{k}|\mathbf{s}, \mathbf{t})$, que pode ser escrita como:

$$H(x[0], \mathbf{k}|\mathbf{s}, \mathbf{t}) = H(x[0]|\mathbf{k}, \mathbf{s}, \mathbf{t}) + H(\mathbf{k}|\mathbf{s}, \mathbf{t}) \tag{3}$$

$$= H(\mathbf{k}|x[0], \mathbf{s}, \mathbf{t}) + H(x[0]|\mathbf{s}, \mathbf{t}). \tag{4}$$

De (1) temos que $H(x[0]|\mathbf{k}, \mathbf{s}, \mathbf{t}) = 0$, além disso, como $M(\cdot)$ em (1) é injetivo, então $H(\mathbf{k}|x[0], \mathbf{s}, \mathbf{t}) = 0$, logo

$$H(\mathbf{k}|\mathbf{s}, \mathbf{t}) = H(x[0]|\mathbf{s}, \mathbf{t}). \tag{5}$$

Além disso,

$$H(x[0], \mathbf{s}|\mathbf{t}) = H(x[0]|\mathbf{s}, \mathbf{t}) + H(\mathbf{s}|\mathbf{t}) \tag{6}$$

$$= H(\mathbf{s}|x[0], \mathbf{t}) + H(x[0]|\mathbf{t}), \tag{7}$$

como $\mathbf{s}$ é independente de $\mathbf{t}$ e $x[0]$, então $H(\mathbf{s}|\mathbf{t}) = H(\mathbf{s})$ e $H(\mathbf{s}|x[0], \mathbf{t}) = H(\mathbf{s})$. Portanto, $H(x[0]|\mathbf{s}, \mathbf{t}) = H(x[0]|\mathbf{t})$, que associado a (5) implica na seguinte igualdade

$$H(\mathbf{k}|\mathbf{s}, \mathbf{t}) = H(x[0]|\mathbf{t}). \tag{8}$$

Supondo que $x[\sigma]$ é conhecido, saber o valor de $x[i]$, $i > \sigma$, não fornece informação adicional sobre a condição inicial. Assim, podemos reescrever (8) como

$$H(\mathbf{k}|\mathbf{s}, \mathbf{t}) = H(x[0]|x[\sigma]). \tag{9}$$

O *tag* é gerado por uma função $f : A \to A$ não inversível, tal que, $f^{-1}(\cdot)$ associa um ponto a múltiplos pontos. Portanto, como os σ pontos iniciais da órbita não são transmitidos, o conjunto de possíveis condições iniciais que geram $x[\sigma]$ cresce exponencialmente com σ. Para formalizar essa ideia, define-se o conjunto das i-ésimas pré-imagens de y sobre $f(\cdot)$ por:

$$\mathcal{S}_i(y) = \{x | f^i(x) = y\}. \tag{10}$$

Como uma suposição não restritiva, a análise a seguir considera *mapas de pré-imagem binária constante*, ou seja, com $|\mathcal{S}_i(y)| = 2^i$, $i \geq 0$, para todo y pertencente à imagem de $f(\cdot)$, a não ser por um conjunto finito de pontos. Vários mapas de interesse satisfazem essa propriedade, *e.g.*, mapa da tenda [14], mapa tanh [18], mapa logístico [14], entre outros.

A partir de (9), o nível de segurança incondicional depende da incerteza sobre a condição inicial $x[0]$ a partir do conhecimento de $x[\sigma]$. Portanto, um número exponencial de condições iniciais deve conduzir a cada possível $x[\sigma]$, a partir das quais é gerado o mesmo *tag*. Os possíveis $x[\sigma]$ para cada *tag* formam um conjunto $\mathcal{X}_\sigma$ com cardinalidade $2^{K-\sigma}$, no qual os valores ocorrem com mesma probabilidade, dado que o conjunto de condições iniciais possui distribuição uniforme como consequência da aleatoriedade da chave. Segue que há 2^σ condições inicias distintas que podem gerar cada possível *tag*, portanto, a probabilidade condicional de $x[0]$ dado $x[\sigma]$ é

$$P(x[0] = x | x[\sigma] = y) = \begin{cases} \frac{1}{2^\sigma}, & \text{if } x \in \mathcal{S}_\sigma(y) \\ 0, & \text{caso contrário.} \end{cases} \tag{11}$$

A entropia condicional em (9) é determinada a partir de (11) como segue:

$$\begin{aligned} &H(\mathbf{k}|\mathbf{s},\mathbf{t}) = H(x[0]|x[\sigma]) = \\ &= -\sum_{j=0}^{2^{K-\sigma}-1} P(x[\sigma]=X_\sigma^j)\times \\ &\sum_{i=0}^{2^K-1} P(x[0]=X_0^i|x[\sigma]=X_\sigma^j)\log_2 P(x[0]=X_0^i|x[\sigma]=X_\sigma^j) \\ &= \sigma. \end{aligned} \tag{12}$$

Conclui-se que os *tags* gerados a partir de mapas caóticos, através do método proposto, propiciam um nível de segurança incondicional igual ao salto σ.

VI. Mecanismos de Segurança

Nesta seção são determinadas as probabilidades de sucesso dos ataques elencados na Seção III. Considera-se a seguir que Eve não possui restrições computacionais e nem de acesso ao canal.

A. Mecanismo de Segurança Contra Ataque de Disfarce

O sucesso deste ataque depende de quanto Eve sabe sobre a chave secreta empregada, uma informação que é adquirida com a troca de mensagens e respectivos *tags* entre os usuários legítimos. Considerando que Eve recuperou corretamente a mensagem, a segurança do sistema depende da dificuldade que ela terá em estimar a condição inicial. Dois mecanismos interferem nesta estimativa, o primeiro provém da observação ruidosa do *tag*, dada por $\tilde{\mathbf{t}} = \mathbf{t} + \mathbf{w}$, em que $\mathbf{w} = [\omega_0,\ldots,\omega_{L-1}]$ é um vetor AWGN. O usuário legítimo pode empregar esse mecanismo para aumentar a robustez do sistema contra ataque de disfarce, para isso, basta diminuir a potência do $\mathbf{t}$, dificultando sua identificação.

O segundo mecanismo foi discutido na Seção V. Ao transmitir um trecho de órbita como *tag*, após a σ-ésima iteração do mapa caótico, o que Eve observa é

$$\tilde{\mathbf{t}} = \big[x[\sigma]+\omega_0,\cdots,x[\sigma+L-1]+\omega_{L-1}\big]. \tag{13}$$

Portanto, a probabilidade de sucesso do ataque, P_I, é calculada a partir da quantidade de informação sobre a condição inicial obtida por Eve através da observação de $\tilde{\mathbf{t}}$ em (13). Essa informação é dada por $H(x[0]|\tilde{x}_\sigma^{\sigma+L-1})$, em que $\tilde{x}_\sigma^{\sigma+L-1}$ denota a sequência de observações ruidosas $\tilde{x}[\sigma]$, $\tilde{x}[\sigma+1],\ldots,\tilde{x}[\sigma+L-1]$, tal que, $\tilde{x}[i]=x[i]+\omega_{\sigma-i}$. Para o cálculo dessa incerteza, considere:

$$\begin{aligned} &H(x[0],x[\sigma]|\widetilde{x}_\sigma^{\sigma+L-1}) \\ &\quad = H(x[\sigma]|x[0],\widetilde{x}_\sigma^{\sigma+L-1}) + H(x[0]|\widetilde{x}_\sigma^{\sigma+L-1}) \\ &\quad = H(x[0]|x[\sigma],\widetilde{x}_\sigma^{\sigma+L-1}) + H(x[\sigma]|\widetilde{x}_\sigma^{\sigma+L-1}), \end{aligned}$$

como $x[0]$ determina completamente $x[\sigma]$, então $H(x[\sigma]|x[0],\widetilde{x}_\sigma^{\sigma+L-1})=0$. Além disso, com o conhecimento de $x[\sigma]$, $\tilde{x}_\sigma^{\sigma+L-1}$ não fornece informação adicional sobre $x[0]$, portanto, $H(x[0]|x[\sigma],\widetilde{x}_\sigma^{\sigma+L-1}) = H(x[0]|x[\sigma])$. Desses resultados e de (12) segue a expressão

$$\begin{aligned} H(x[0]|\widetilde{x}_\sigma^{\sigma+L-1}) &= H(x[0]|x[\sigma]) + H(x[\sigma]|\widetilde{x}_\sigma^{\sigma+L-1}) \\ &= \sigma + H(x[\sigma]|\widetilde{x}^{\sigma+L-1}). \end{aligned} \tag{14}$$

A incerteza sobre $x[\sigma]$ quantificada por $H(x[\sigma]|\widetilde{x}_\sigma^{\sigma+L-1})$ decorre da observação ruidosa do *tag*, como descrito em (13). A partir de (14) obtém-se a desigualdade

$$\sigma \le H(x[0]|\widetilde{x}_\sigma^{\sigma+L-1}). \tag{15}$$

Portanto, nesta proposta, o ruído fornece um nível extra de segurança, quantificado pelo termo $H(x[\sigma]|\widetilde{x}_\sigma^{\sigma+L-1})$ em (14). Quaisquer das 2^σ condições podem gerar $x[\sigma]$ com distribuição uniforme, do que segue, a partir de (14), a probabilidade de sucesso do ataque de disfarce

$$P_I \le 2^{-\sigma}. \tag{16}$$

A desigualdade (16) é observada com igual quando o valor $x[\sigma]$ é completamente conhecido.

B. Mecanismo de Segurança Contra Ataque de Substituição

O sucesso deste ataque depende da capacidade que Eve possui de enviar um par $(\mathbf{s}',\tilde{\mathbf{t}})$, a partir de um par interceptado $(\mathbf{s},\tilde{\mathbf{t}})$, com $\mathbf{s}'\neq\mathbf{s}$. Para se contrapor a este ataque, a função de geração de *tag* deve ser resistente a pré-imagem [11].

A partir de (1), uma mensagem $\mathbf{s}$ pode ser mapeada em qualquer das 2^K possíveis condições iniciais, dado que a chave possui distribuição de probabilidade uniforme. Além disso, segue do desenvolvimento empregado para derivar (11) que cada possível *tag* pode ser gerado por 2^σ condições iniciais. Portanto a probabilidade de uma mensagem $\mathbf{s}$ escolhida aleatoriamente gerar um *tag* específico é igual a

$$P_S = 2^{\sigma-K}.$$

Os parâmetros σ (salto) é K (comprimento da chave) devem ser adequadamente escolhidos para garantir que $P_S \approx 0$ e, consequentemente, a robustez contra ataque de substituição.

VII. Diagrama do Transmissor

A Fig. 2 ilustra o diagrama em bloco de um transmissor que emprega a técnica de autenticação com sequências caóticas. A mensagem, a chave e o conteúdo do contador são combinados por (1) e definem a condição inicial do mapa dentre um elemento do conjunto $\mathcal{X}_0$. A saída do circuito caótico é um sinal analógico que é escalonado pelo fator $\rho_{\mathbf{t}}$ e sofre conversão ascendente igual a do sinal da mensagem, que passa por um processo similar. Os sinais resultantes são somados e, em seguida, amplificados e transmitidos.

VIII. Conclusões

A autenticação em camada física empregando sequências caóticas demonstrou ser competitiva em relação as propostas clássicas, que dependem de quanto o canal é severo para o usuário malicioso. A proposta admite considerável controle dos níveis de segurança para diferentes ataques, bastando a escolha adequada dos parâmetros σ (salto) e $\mathbf{k}$ (chave secreta).

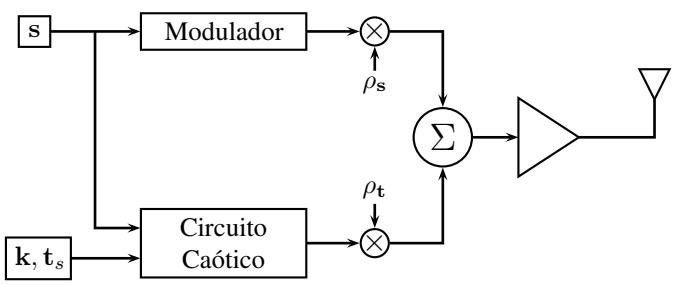

Fig. 2. Diagrama de bloco de um transmissor de RF empregando o sistema de autenticação em camada física com sequências caóticas.

Como aspecto singular, deve-se frisar a segurança incondicional da chave como consequência do ganho de entropia com o fluxo caótico. Até onde é de conhecimento dos autores, esta é a única proposta que apresenta tal característica.

AGRADECIMENTOS

Este trabalho foi parcialmente financiado pelo CNPq e FACEPE.

REFERÊNCIAS

[1] P. Yu, J. Baras, and B. Sadler, "Physical-Layer Authentication," *IEEE Trans. Inf. Forens. Security*, vol. 3, pp. 38–51, Mar 2008.

[2] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag*, vol. 53, pp. 48–53, Jun 2015.

[3] N. Goergen, W. Lin, K. Liu, and T. Clancy, "Extrinsic Channel-Like Fingerprinting Overlays Using Subspace Embedding," *IEEE Trans. Inf. Forens. Security*, vol. 6, pp. 1355–1369, Dec 2011.

[4] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements," in *Proc. of the 5th ACM Workshop on Wireless Security (WiSe'2006)*, (New York, NY, USA), pp. 33–42, ACM, 2006.

[5] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul 2008.

[6] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Military Commun. Conf. (MILCOM'2011)*, pp. 538–542, Nov 2011.

[7] S. V. Vaerenbergh, Ó. González, J. Via, and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," in *Proc. of IEEE Int. Conf. on Acoust., Speech, and Signal Process. (ICASSP '14), 2014*, pp. 2410–2414, May 2014.

[8] X. Wu and Z. Yang, "Physical-Layer Authentication for Multi-Carrier Transmission," *IEEE Commun. Lett.*, vol. 19, pp. 74–77, Jan 2015.

[9] J. L. Massey, *Lecture Notes on Applied Digital Information Technology II*.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY: Pearson Education, third ed., 2002.

[11] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. New York, NY: Springer, first ed., 2009.

[12] P. L. Yu and B. M. Sadler, "MIMO Authentication via Deliberate Fingerprinting at the Physical Layer," *IEEE Trans. Inf. Forens. Security*, vol. 6, pp. 606–615, Sep 2011.

[13] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, Jul 2000.

[14] S. H. Strogatz, *Nonlinear dynamics and chaos : with applications to physics, biology, chemistry, and engineering*. Cambridge, MA: Westview Press, second ed., 2014.

[15] R. Metzler, Y. Bar-Yam, and M. Kardar, "Information flow through a chaotic channel: Prediction and postdiction at finite resolution," *Phys, Rev. E*, vol. 70, Aug. 2004.

[16] J. V. C. Evangelista, "Physical-layer authentication using chaotic maps," Master's thesis, PPGEE-UFPE, Agosto 2016.

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY: Wiley, second ed., 2006.

[18] D. P. B. Chaves, C. E. C. Souza, and C. Pimentel, "A smooth chaotic map with parameterized shape and symmetry," *EURASIP Journal on Advances in Signal Processing*, vol. 48, pp. 1537–1538, Nov 2016.