OPFKA: seguro e eficiente

Chave baseada em características fisiológicas ordenadas

Acordo para Redes Wireless Body Area

Chunqiang Hu * †, Xiuzhen Cheng *, Fan Zhang *, Dengyuan Wu *, Xiaofeng Liao †, Dechang Chen ‡
* Departamento de Ciência da Computação, The George Washington University, Washington DC 20052, EUA
† Faculdade de Ciência da Computação, Universidade de Chongqing, Chongqing 400030, China
‡ Divisão de Epidemiologia e Bioestatística, Uniformed Services University of the Health Sciences, MD 20814, EUA E-mail: {chu, cheng} @ gwu.edu,
{zfwise, andrewwu}@gwmail.gwu.edu, x fl iao@cqu.edu.cn , dechang.chen@usuhs.edu

Resumo —Body Area Networks (BANs) deve jogar um papel importante no monitoramento da saúde do paciente em um futuro próximo. Fornecendo um acordo de chave eficiente com as prosperidades de *plug-n-play* e *transparência* oferecer suporte a comunicações seguras entre sensores é fundamental, especialmente durante os estágios de inicialização e reconfiguração da rede. Neste artigo, apresentamos um novo esquema de acordo-chave denominado *Acordo de chave baseado em características fisiológicas ordenadas (OPFKA),* que permite que dois sensores pertencentes ao mesmo BAN concordem em uma chave criptográfica simétrica gerada a partir das características de sinal fisiológico sobrepostas, evitando assim a pré-distribuição de materiais de codificação entre os sensores embutidos no mesmo corpo humano. Os recursos secretos calculados a partir do mesmo sinal fisiológico em diferentes partes do corpo por diferentes sensores exibem alguma sobreposição, mas não são completamente idênticos. Para superar esse desafio, detalhamos um protocolo computacionalmente eficiente para transferir com segurança os recursos secretos de um sensor para outro, de modo que dois sensores possam identificar facilmente os que se sobrepõem. Este protocolo possui muitos recursos interessantes, como a resistência contra ataques de força bruta. Os resultados experimentais indicam que o OPFKA é seguro, eficiente e viável.

Termos do Índice —Body Area Networks (BANs); inter seguro comunicações de sensores; Inter-intervalo de pulso (IPI); acordo de chave baseado em características fisiológicas.

Eu eu NTRODUÇÃO

A rede da área corporal é uma tecnologia promissora para monitoramento em tempo real de sinais fisiológicos para apoiar várias aplicações médicas [1]. É possibilitado pelo rápido desenvolvimento de redes de sensores sem fio e técnicas de engenharia biomédica [2] - [6]. Uma rede de área corporal (BAN) típica consiste em uma série de sensores vestíveis e implantados para monitorar os parâmetros do corpo humano e os ambientes circundantes, de modo que possa auxiliar o corpo humano fornecendo suporte de vida, feedback visual / áudio, etc. [1]

Ao contrário das redes de sensores convencionais, as BANs lidam com informações médicas com requisitos mais rígidos de segurança e privacidade. A natureza sensível dos dados coletados torna um BAN o alvo para os adversários explorarem; e que os sensores se comunicam sem fio torna a BAN ainda mais vulnerável. A falta de proteções de segurança adequadas pode não só levar a uma violação da privacidade do paciente, mas também dar uma chance para os adversários ameaçarem a segurança do paciente, modificando os dados da BAN, o que pode resultar em diagnósticos e tratamentos errados [7]. Visto que a comunicação sem fio é um dos aspectos mais vulneráveis de uma BAN, a proteção das comunicações entre sensores desempenha um papel crítico na proteção da BAN.

BANs dependem de chaves criptográficas para realizar autenticação e fornecer confidencialidade e integridade de dados. As chaves são normalmente distribuídas aos sensores por protocolos de distribuição de chaves, que normalmente requerem alguma forma de chave de informação pré-implantação [8] - [12]. No entanto, com o aumento do tamanho de um BAN, as abordagens tradicionais envolvem uma latência considerável durante a inicialização da rede ou qualquer processo de ajuste subsequente (por exemplo, implantação de fase), devido às necessidades de pré-implantação de informações. Pretendemos fornecer um esquema de segurança eficiente com as prosperidades de *plug-n-play* e *transparência.*

Ou seja, os usuários podem adicionar, remover e ajustar os sensores de uma BAN sem reconfigurar a rede, mas ainda podem desfrutar dos benefícios das comunicações seguras. Essas características podem ajudar a minimizar a sobrecarga de comunicação durante o processo de inicialização e, assim, revelar menos informações de identificação pessoal do paciente. Alguns esquemas foram propostos para atender a estes

foi apresentado para evitar a chave de informações pré-implantação. No entanto, o nível de segurança dessas técnicas não é alto o suficiente devido à limitação colocada pelo tamanho do recurso e à alta complexidade de computação dos pontos de chaff, conforme analisado posteriormente neste artigo.

Propomos um esquema de segurança denominado *Ordenado-Acordo de chave baseado em características fisiológicas (OPFKA)* nesse papel. OPFKA emprega recursos secretos computados a partir do sinal fisiológico medido em diferentes partes do corpo humano para permitir que os sensores concordem com uma chave criptográfica simétrica de maneira autenticada e plug-n-play para proteger as comunicações entre sensores, ou seja, nenhuma inicialização é necessária . OPFKA não requer nenhuma pré-distribuição de chave. Ele explora a natureza dinâmica e complexa do corpo humano. O OPFKA funciona da seguinte forma: 1) os recursos gerados por cada sensor são ordenados para formar um vetor de recursos e apenas o sensor que coleta os dados conhece a ordem dos recursos; 2) o remetente envia os recursos secretos junto

978-1-4673-5946-7 / 13 / $ 31,00 © 2013 IEEE

com um grande número de dados ruidosos para o receptor; 3) o receptor gera uma chave de acordo com as características comuns, e então retorna os índices das características correspondentes; e
4) o remetente identifica as características comuns em seu próprio vetor de características e calcula a chave de acordo. O OPFKA atende aos objetivos do projeto sugeridos por [14] para que os sinais fisiológicos sejam uma base para a concordância das chaves, ou seja, as chaves são longas e aleatórias para prevenir ataques de força bruta; eles são eficientes em termos de sobrecarga computacional, de comunicação e de armazenamento; e eles possuem as propriedades de variação e distinção no tempo. As principais contribuições do artigo são descritas a seguir.

1) Propomos o OPFKA, um esquema seguro e eficiente para um acordo de chave autenticada entre dois sensores em um BAN. O esquema tem as propriedades de transparência e plug-n-play para suportar facilmente a reconfiguração de rede sem sacrificar a segurança já obtida.
2) Provamos a confiabilidade do OPFKA e analisamos sua eficiência e viabilidade. Em particular, nos concentramos nos seguintes aspectos de segurança: resistência contra ataques de força bruta, segurança de troca de mensagens, aleatoriedade, distinção e variação de tempo. Também discutimos dois métodos para processar sinais fisiológicos.
3) Comparamos OPFKA com PSKA [13] em termos de nível de segurança, resistência contra ataques de força bruta e outros objetivos de projeto mencionados anteriormente, e nossos resultados demonstram a superioridade do OPFKA sobre PSKA.
4) Estimamos o desempenho do OPFKA em termos de sobrecarga computacional, de comunicação e de armazenamento.

O resto do artigo está organizado da seguinte forma. A Seção II apresenta uma visão geral do trabalho relacionado. Apresentamos o modelo do sistema na Seção III e desenvolvemos a ideia principal do OPFKA na Seção IV. A Seção V analisa a segurança do OPFKA, e a Seção VI apresenta a análise de desempenho, seguida da conclusão tirada na Seção VII.

II. Related Work

A maioria dos trabalhos anteriores sobre segurança BAN focou em questões como criptografia [15] [16] [17], gerenciamento de chaves [18] - [21] e controle de acesso [15], [22], [23].

A fim de proteger as comunicações entre sensores, a ideia de empregar sinais fisiológicos foi introduzida pela primeira vez em [1], [24], em que as características derivadas de um sinal fisiológico medido simultaneamente em diferentes partes do corpo são usadas para gerar o chave real compartilhada entre os sensores. Para estabelecer um conjunto comum de recursos, a correção de erros simples pode ser empregada para corrigir as diferenças entre os recursos fisiológicos gerados em diferentes sensores. Com base nessa ideia, [25] propôs o emprego do Inter-Pulse-Interval (IPI) para gerar chaves criptográficas codificando os IPIs em uma chave binária de 128 bits. IPI refere-se ao intervalo de tempo entre a onda R do eletrocardiógrafo (ECG) e a base do pulso do fotopletismograma (PPG). Para que esta abordagem seja aplicável, deve ser notavelmente menor do que o gerado pelo sensor 2 s 275 em diferentes corpos humanos. No entanto, os resultados de um estudo experimental do mundo real [13] indicaram que as distâncias de Hamming de dois IPIs obtidos do mesmo sujeito e de sujeitos diferentes são 60 e 65, respectivamente. Embora [25] tenha sugerido que a correção de erros pode ser usada para melhorar as correspondências das características derivadas do mesmo corpo humano, o esquema ainda não é prático, uma vez que a distância de Hamming dos IPIs para a mesma pessoa após a correção de erros ainda varia de 0 a 40. A principal razão dessa dureza reside no fato de que os erros de translação e rotação podem produzir valores drasticamente diferentes quando os IPIs são codificados ingenuamente em binários.

Para resolver o problema mencionado acima, esquemas baseados em abóbadas fuzzy [7], [13], [26] foram propostos para lidar com o fato de que os sinais fisiológicos têm tendências semelhantes, mas não são completamente idênticos devido à natureza dinâmica do corpo humano. O esquema fuzzy-vault foi aplicado principalmente a autenticação baseada em biometria, como impressões digitais [27] e imagens da íris [28]. Foi argumentado que um adversário tem uma alta probabilidade de adivinhar os pontos legítimos em uma abóbada fuzzy de acordo com a análise em [29]. Como resultado, o adversário tem grande probabilidade de reduzir a complexidade de identificação do polinômio usado pela abóbada. PSKA [13] e Pletismograma [7], que são baseados no mesmo esquema fuzzy vault, mas focam em diferentes sinais fisiológicos para proteger as comunicações inter-sensores, alegaram que eles tinham um alto nível de segurança. No entanto, a força de segurança do PSKA e do pletismograma depende muito do tamanho do cofre, o que significa que a complexidade de quebrar o cofre aumenta se o número de pontos de chaff aumentar. No entanto, o aumento do tamanho da abóbada pode causar colisões entre os recursos gerados por um sensor e o ponto de chaff gerado por outro sensor, o que leva a uma falsa rejeição. Além disso, um trabalho recente [30] propôs um mecanismo de geração de chave secreta que explora as flutuações de intensidade do sinal causadas por movimentos incidentais de dispositivos usados no corpo para construir chaves compartilhadas com um acordo quase perfeito, evitando assim o custo de reconciliação. No entanto, a taxa de geração de bits secretos é muito limitada e o custo é muito alto. Como resultado, o esquema em [30] é inviável para um BAN prático.

Iluminados pelo esquema fuzzy vault, em vez de usar códigos de correção de erros ou reconstruir polinômios, aproveitamos o fato de que os recursos secretos gerados por um sensor são ordenados e apenas o próprio sensor está ciente da ordem dos recursos, e propõe um esquema de contrato de chave eficiente e seguro denominado OPFKA. O OPFKA emprega dados simples com ruído como pontos de chaff para fornecer segurança aprimorada. Nossa análise indica que o OPFKA supera todos os problemas mencionados acima, enquanto atende aos objetivos de projeto sugeridos de acordo de chave baseado em sinal fisiológico [14] para BANs.

III. System Model

Um BAN é uma rede que interconecta fisiológica e sensores de monitoramento ambiental usados ou implantados dentro de um corpo humano. Esses dispositivos de detecção coletam informações fisiológicas e contextuais de um corpo humano em um intervalo regular e as transmitem a um nódulo receptor altamente capaz para

processamento adicional em comunicações sem fio multi-hop. 276 vivenciando o fato de que recursos secretos gerados pelos dois

Assumimos que todos os sensores, usados ou implantados, são capazes de medir os sinais fisiológicos apropriados. Também assumimos que uma entidade que não tem contato físico com um corpo humano não pode coletar nenhum sinal fisiológico e que apenas sensores legítimos estão em contato com o corpo humano. Assim, os invasores são principalmente capazes de monitorar passivamente o tráfego, pois o meio sem fio não é seguro. Além disso, assumimos que entidades maliciosas não podem comprometer os sensores em um BAN sem serem detectados, já que os sensores estão principalmente sob a supervisão do host e / ou do zelador.

As ameaças enfrentadas por um BAN são principalmente de adversários que podem espionar o tráfego do BAN, reproduzir mensagens antigas, injetar mensagens para comprometer a confidencialidade das comunicações do BAN ou falsificar as identidades dos sensores do BAN. Os adversários também podem quebrar o processo de distribuição de chaves usando os dados do sinal fisiológico obtidos de outra pessoa se o esquema não tiver distinção suficiente. Neste artigo, nos concentramos exclusivamente em projetar um esquema seguro e eficiente para garantir a segurança das comunicações entre sensores dentro de uma BAN. As comunicações do coletor em diante podem utilizar esquemas de segurança convencionais, como Secure Socket Layer (SSL), devido aos recursos consideráveis das entidades envolvidas. Observe que não consideramos ataques de negação de serviço (DoS), como bloqueio, interferência eletromagnética,

IV. K EY UMA GREEMENT

O objetivo do OPFKA é promover comunicações inter-sensor seguras, permitindo que dois sensores concordem em uma chave simétrica de par com base no sinal fisiológico comum coletado pelos dois sensores em diferentes partes do corpo. O principal processo de acordo entre dois sensores funciona da seguinte maneira. Primeiro, os dois sensores coletam e processam de forma simultânea e independente um certo sinal fisiológico com base no qual alguns recursos secretos são computados. Esses recursos são organizados em um conjunto ordenado chamado de *vetor de característica* para cada sensor, e a ordem só é conhecida pelo sensor que gera os dados. Mas uma política de pedido comum, que pode vir do mesmo algoritmo de geração de recursos, é adotada por todos os sensores. Então, um dos sensores, digamos o remetente, gera ruídos para ocultar seu vetor de recurso secreto. Em segundo lugar, os recursos secretos e os dados ruidosos são enviados para outro sensor, digamos, o receptor, que pode usar sua própria versão do vetor de recursos para identificar recursos comuns, já que o vetor de recursos do receptor se sobrepõe parcialmente ao do remetente. Assim, o receptor pode gerar uma chave K com base na parte correspondente (sobreposta) do vetor de recurso. Finalmente, o receptor coloca as posições (ou índices) dos recursos correspondentes em um conjunto *EU,* e envia junto com o MAC (Message Authentication Code) da chave K para o remetente, que pode gerar a mesma chave K depois de identificar as características do segredo comum de acordo com *EU.*

Em [13], os autores propuseram o uso do esquema de compartilhamento secreto [31] - [33], para ocultar a chave secreta nos coeficientes de um polinômio. Para este esquema, o custo computacional no processo de reconstrução é alto. Abordamos essa desvantagem por

os sensores são ordenados de acordo com a mesma política e apenas os próprios sensores conhecem os índices (ordem) dos recursos nos vetores de recursos. A Tabela I resume as notações utilizadas e seus significados semânticos, e a Fig. 1 demonstra o protocolo OPFKA, cujos principais procedimentos são detalhados nas subseções a seguir.

TABELA I
T CAPAZ DE NOTAÇÕES.

Notação	Definição
H	Uma função hash criptográfica padrão, por exemplo, SHA-1 A posição de um
Índice	recurso secreto correspondente
IDs, IDr	Os ids do remetente e do receptor O conjunto de
Q	características comuns
FFT	Transformação rápida de Fourier
IPI	Sinal de intervalo de pulso
N	O número de recursos
M	O número dos pontos de chaff (ruídos) Código de
MAC	autenticação da mensagem

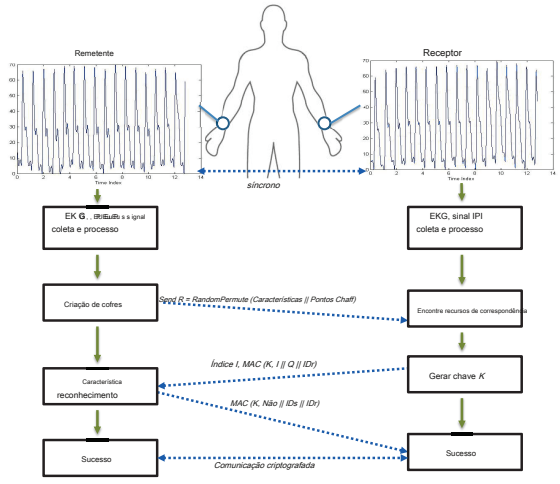

Fig. 1. O protocolo OPFKA.

A. Ocultando os Recursos

OPFKA é projetado para esconder o conjunto *UMA* de recursos secretos gerados pelo remetente em uma construção chamada de *Cofre,* denotado por R. Uma vez que o conjunto *UMA* foi escondido no cofre, ninguém pode distinguir as características secretas dos pontos de joio. Conforme ilustrado na Fig. 1, o remetente constrói o Coffer por i) gerando um conjunto de pontos de debulha aleatórios *C;* ii) adicionar *UMA* e *C*

para o cofre R; e iii) realizar uma permutação aleatória em

R. Assim que o receptor obtém o Cofre R, ele pode utilizar seu próprio conjunto de recursos secretos B para encontrar os que se sobrepõem. Denotamos o conjunto de características comuns por Q, ie, $Q = \{u \mid u \in R \cap B\}$.

Em seguida, o receptor gera uma chave K usando o conjunto Q, por exemplo,

$K = H(Q)$, e então envia de volta o MAC de Q junto com o conjunto de índices *Eu* dos recursos sobrepostos. Depois que o remetente recebe o conjunto de índices *EU,* ele pode descobrir o conjunto de recursos comuns correspondente Q. If $|Q|$ é maior do que um limite, o remetente gera uma chave K' e então verifica o MAC de Q. Se for sucesso, o que implica que $K' = K$, o remetente envia de volta um

confirmação para o receptor. Este procedimento garante que se ambos os sensores estiverem cientes do conjunto de características comuns, eles podem gerar a mesma chave secreta *K.*

B. Embalagem e desembalagem do caixão em OPFKA

O OPFKA exige que os recursos secretos nos conjuntos A e B se sobreponham até certo ponto. A presença dos pontos de joio adiciona segurança ao Cofre e oculta as características secretas originais. Uma vez que ninguém pode distinguir os pontos de joio e as características, um atacante tem que realizar um ataque de força bruta para descobrir as características comuns. Nesta subseção, demonstramos como empregar o esquema proposto para acordo de chave em um BAN.

1) Geração de recursos: A geração dos recursos tem grande influência na eficácia do OPFKA. Uma vez que os sinais fisiológicos coletados em ambos os lados não são exatamente os mesmos, métodos podem ser usados para ajudar a melhorar a taxa de sucesso da concordância da chave e reduzir as taxas de falsa aceitação e falsa rejeição [25]. Abaixo, propomos dois métodos para geração de recursos.

O método FFT aprimorado: PSKA [13] propôs o seguindo o esquema simples de geração de recursos. Dois sensores que pretendem estabelecer uma chave compartilhada amostram um sinal de EKG ou PPG em uma determinada frequência simultaneamente por um curto período de tempo: 12,8 segundos para PPG na frequência de 60 Hz e 4 segundos para EKG na frequência de 125 Hz. Em seguida, as amostras são particionadas em janelas de tamanho 256 e uma Transformação Rápida de Fourier (FFT) de 256 pontos é executada em cada janela. Em seguida, os coeficientes FFT de cada janela são passados através de uma função de detecção de pico que retorna tuplas da forma

$\bullet k_{Eu,x}, k_{Eu,y} \bullet$. Aqui $k_{Eu}{}_{x}$ e $k_{Eu}{}_{y}$ são o índice e o correspondente valor do *Eu* o pico na sequência do coeficiente FFT e são denominados como *índice de pico* e *valor de pico,* respectivamente. De 13 bits característica ($[k_{Eu,1}, k_{Eu,2}]$ é gerado pela primeira quantização de um $k_{Eu}{}_{x}$ para um 8-bit binário e o correspondente $k_{Eu}{}_{y}$ para um binário de 5 bits e então concatená-los. Para um sinal PPG, cerca de 30 recursos podem ser gerados e o número de recursos comuns para dois sensores no mesmo BAN é cerca de 12. Em contraste, o número de recursos comuns para dois sensores monitorando corpos humanos diferentes é cerca de 2. PSKA cria um abóbada com um tamanho que varia de 1000 a 5000 e incorpora os recursos à abóbada. Nossa análise (Seção V) indica que as características secretas do receptor podem combinar com alguns pontos de debulha. Teoricamente, o tamanho máximo de um cofre é 2^{13}, que é cerca de 8000. Se o tamanho real da abóbada for 3000, a probabilidade de que o receptor tenha características que combinem com os pontos de joio é bastante alta.

Não há chance de o receptor observar que ele possui recursos correspondentes aos pontos de chaff, portanto, a recuperação da chave de sessão pode ser interrompida. Para reduzir a chance de colisões, damos um passo adiante, expandindo o 13- recursos de bits para os de 20 bits por meio de uma função unilateral (por exemplo, empregando uma função hash salgada e obtendo os primeiros 20 bits de sua saída). Por meio da expansão de recursos, a chance de colisão é reduzida significativamente - todos os recursos comuns no receptor devem ser gerados pelo remetente. Além disso, registramos o ordem dos recursos gerados neste método FFT aprimorado 2.277

A geração dos recursos por nosso método FFT aprimorado leva apenas alguns segundos para um sinal PPG em nosso estudo; mas o FFT a detecção de transformadas e de pico consomem alta computação poder. A seguir, apresentamos nosso método de geração de segundo recurso, que leva mais tempo (1-1,5 minutos), mas consome menos energia computacional.

O Método IPI: Foi demonstrado em [25] que os IPIs têm um alto nível de aleatoriedade e podem ser obtidos com diferentes tipos de sensores de diferentes sinais fisiológicos (por exemplo, o ECG, PPG ou pressão arterial) em diferentes partes do corpo (por exemplo, tórax, pontas dos dedos ou membros). A coleta de IPIs é relativamente fácil. O estudo experimental relatado em [22] indica que os últimos 4 dígitos da representação binária de um IPI são quase completamente aleatórios, o que significa que podemos extrair 4 bits de cada IPI.

O remetente e o receptor coletam IPIs simultaneamente por cerca de 1 a 1,5 minutos para obter 90 IPIs (a coleta de um IPI leva cerca de 850 ms em média). Cada IPI é quantificado primeiro em uma representação binária de 4 bits e três IPIs adjacentes são concatenados para formar um recurso secreto de 12 bits, que é então expandido e oculto em um Coffer. Um estudo experimental relatado em [22] afirmou que cerca de 75% dos pares de IPI coletados em dois sensores coincidem, o que indica que a probabilidade dos recursos secretos do remetente e do receptor coincidirem é de cerca de 42%. Isso significa que existem cerca de 12 recursos correspondentes calculados a partir dos 90 IPIs. Para reduzir a chance de colisão, expandimos os recursos de 12 bits para 20 bits e registramos a ordem dos recursos.

Observe que o método IPI precisa apenas coletar IPIs e quantificá-los. Não são necessárias operações complexas, como transformação FFT e detecção de pico. Assim, o método IPI consome menos energia computacional ao custo de um tempo de amostragem mais longo em comparação com o método FFT aprimorado. Portanto, o método IPI pode ser usado para gerar uma chave de sessão de hora em hora, já que o padrão IEEE 802.15 emergente [34] para redes corporais sugere que a chave precisa ser renovada uma vez toda hora. Denotamos os vetores de característica de comprimento *N* por $F_s = \{f_{1,s}, f_{2,s}, ..., f_{N,s}\}$ e $F_r = \{f_{1,r}, f_{2,r}, ..., f_{N,r}\}$ para o remetente e o receptor, respectivamente. O algoritmo 1 detalha o procedimento de geração de recursos para o método IPI e o método FFT aprimorado.

2) Criação de cofres: Depois que os vetores de características são calculados, o remetente pode criar um Coffer, que contém o conjunto $F_s = \{f_{1,s}, f_{2,s}, ..., f_{N,s}\}$ e um conjunto maior de *M* palha aleatória pontos do formulário $F'_s = \{f'_{j,s}\}$, com $f'_{j,s} \in F_s, 1 \le j \le M.$ Cada ponto de joio $f'_{j,s}$ está dentro do mesmo intervalo dos recursos dentro F_s. Uma permutação aleatória nos valores no Coffer é então realizada, ou seja, R = RandPermute ($F_s \cup F'_{s}$), para garantir que os pontos de joio e os pontos de característica legítimos são indistinguível. A cardinalidade do conjunto F'_s pode variar com respeito ao nível do requisito de segurança. Quanto maior o conjunto F_s, o mais difícil de quebrar o Coffer. O tamanho do Coffer R é igual a $|N| + |M|$. O Algoritmo 2 detalha o processo de criação do Coffer. A Seção V discute a relação entre o tamanho do Coffer e sua força de segurança com mais detalhes.

Algoritmo 1 Geração de recursos.

1: O emissor e o receptor coletam o sinal fisiológico;
2: E se empregando FFT para quantificar o sinal então
3: Particionar amostras em janelas;
4: para cada janela de amostras Faz
5: Execute FFT e detecção de pico; Retorna
6: tuplas do formulário $\bullet k_{Eu_x}, k_{Eu_y} \bullet$;
7: Quantize k_{Eu_x} e k_{Eu_y} para um número binário de 5 bits e um número binário de 8 bits, respectivamente;
8: Concatenar k_{Eu_x} e k_{Eu_y} para formar um recurso de 13 bits ($[k_{Eu_x} | k_{Eu_y}]$);
9: Calcular H ($[k_{Eu_x} | k_{Eu_y}]$) e pegue os primeiros 20 bits de a saída.
10: fim para
11: outro
12: Colete IPIs;
13: Quantifique cada IPI;
14: para cada um dos três IPIs adjacentes Faz
15: Concatene seus últimos 4 dígitos binários para formar um Recurso de 12 bits;
16: Calcular H ($[k_{Eu_x} | k_{Eu_y}]$) e pegue os primeiros 20 bits de a saída.
17: fim para
18: fim se
19: Produza os vetores de recursos: $F_s = \{f_{1_s}, f_{2_s}, ..., f_{N_s}\}$ (para o remetente) ou $F_r = \{f_{1_r}, f_{2_r}, ..., f_{N_r}\}$ (para o receptor).

Algoritmo 2 Criação de cofres.

1: Calcular M pontos de joio aleatórios: $F'_s = \{f'_{j_s}\}$, Onde f'_{j_s} / F_s;
2: Permute aleatoriamente os pontos para obter $R =$ mais detalhes.). Algoritmo 4 ilustra o procedimento de recurso RandPermute ($F_s \cup F'_s$);
3: Produza o Coffer R.

3) Troca de recursos: Existem duas etapas neste processo: a) O remetente comunica o Coffer R para o destinatário usando a seguinte mensagem: Remetente → Destinatário:
$\{IDs, IDr, R, No\}$. Aqui, IDs e IDr são os ids do remetente e do receptor, respectivamente, e $Não$ é um nonce (número aleatório único) para atualização da transação. b) Após o recebedor obter o Cofre R, compara R com seus próprios recursos para encontrar os correspondentes do Coffer e registra os índices / posições desses recursos correspondentes (o conjunto Q) em seu próprio vetor de recursos. Denote as posições dos recursos correspondentes pelo conjunto de índices $I = \{i\}$, Onde

$Eu \in N$, e então gerar a chave secreta $K = H(Q)$
usando os recursos correspondentes. O destinatário responde ao remetente usando a seguinte mensagem: Destinatário → Remetente:
$\{IDs, IDr, I, MAC(K, I | Q | IDr)\}$. O Algoritmo 3 ilustra o gerado no Algoritmo 3 e o Algoritmo 4 é usado para habilitar o processo de troca de características.

4) Reconhecimento do recurso: Ao receber os cátions de mensagem entre dois sensores de maneira plug-n-play, que
$\{IDs, IDr, I, MAC(K, I | Q | IDr)\}$, o remetente primeiro identifica 2 s 278

Algoritmo 3 Troca de recursos.

1: O remetente envia a mensagem $\{IDs, IDr, R, No\}$ ao receptor;
2: O receptor identifica os recursos correspondentes $Q = R \cap B$.
3: O receptor identifica as posições dos recursos correspondentes em seu conjunto de recursos B, que são denotados por $I = \{i | i \in N\}$;
4: O receptor gera uma chave secreta K usando a correspondência recursos Q: $K = H(Q)$;
5: O receptor retorna a mensagem ao remetente: $\{IDs, IDr, I, MAC(K, I | Q | IDr)\}$.

as características comuns de acordo com o conjunto EU, que contém as posições dos recursos correspondentes. If $|Q|$ é maior do que um limite, o remetente gera uma chave $K' = H(Q)$ da mesma forma que o receptor. Se o remetente gerar a chave com sucesso K' e con fi rma o MAC, o que implica que K' é igual a K, ele envia de volta uma confirmação ao receptor usando a seguinte mensagem: Remetente → Destinatário:

$MAC(K, No | IDs | IDr)$. Para o remetente gerar K com sucesso, os recursos indexados devem ser exatamente os mesmos do receptor. Este processo não apenas confirma a exatidão da chave gerada K, mas também autentica o remetente para o destinatário. Isso ocorre porque a distintividade e a propriedade de variância temporal das características do sinal fisiológico garantem que i) as características geradas a partir de um sinal fisiológico para OPFKA são drasticamente diferentes para duas pessoas diferentes e ii) Cofres antigos não podem ser reproduzidos porque as características teriam mudado por esse tempo, de forma que o remetente não possa verificar o MAC com sucesso (ver Seção VI para

Algoritmo 4 Reconhecimento do recurso.

1: o remetente recebe a mensagem: $\{IDs, IDr, I, MAC(K, I | Q | IDr)\}$;
2: Identifica as características comuns (colocadas no conjunto Q) de acordo com a posição definida EU;
3: se $|Q| \geq Limite$ então
4: Gera a chave K' usando os recursos comuns; Veri fi ca o MAC;
5:
6: E se $MAC(K', I | Q | IDr) = MAC(K, I | Q | IDr)$ então
7: Retorna $MAC(K, No | IDs | IDr)$ para o receptor;
8: fim se
9: outro
10: O remetente envia $Nenhum$ para o receptor.
11: fim se

A Fig. 1 ilustra o protocolo OPFKA. A chave secreta K

comunicação confidencial, autenticada e protegida por integridade

não é considerado nos esquemas tradicionais de distribuição de chaves [9]

[16] e as abordagens baseadas em sinais fisiológicos [25]. Além disso, com OPFKA, nenhuma chave e nenhum recurso fisiológico é reutilizado. Isso garante que qualquer conhecimento das chaves passadas ou características fisiológicas passadas de um sujeito não possa ser reutilizado para subverter o Coffer, devido à propriedade de variância temporal, conforme visto na Seção VI.

V. Segurança de OPFKA

Nesta seção, discutimos as implicações de segurança dos dois aspectos principais do OPFKA: o Coffer e a troca de mensagens.

A. Coffer Security

O uso do OPFKA garante que, embora os dois sensores possam não ter todos os recursos em comum, eles ainda podem concordar sobre uma chave comum de maneira segura. A segurança do OPFKA pode ser entendida como uma função de alçapão unidirecional. A ocultação dos pontos de característica legítimos entre um número muito maior de pontos falsos de joio, cujos valores estão na mesma faixa, torna a identificação dos pontos legítimos muito

difícil. Um adversário que não conhece nenhuma legitimação 2 e do corpo do hospedeiro), tem que experimentar cada uma das características 279 3) Se um adversário obtiver o pontos (uma vez que não pode coletar os sinais fisiológicos relevantes

conjunto de características legítimas de no set *A* a fim de gerar a chave secreta *K*. A Fig. 2 demonstra a resistência do Coffer para diferentes tamanhos de Coffer. A força do Cofre é determinada pelo número de combinações que um adversário tenta examinar a fim de descobrir os pontos legítimos e seus índices no Cofre. Para facilitar o entendimento, representamos esse requisito computacional em termos de sua equivalência à força bruta de uma chave de um determinado comprimento (bits). Como esperado, aumentar o tamanho do Coffer aumenta automaticamente a segurança fornecida pelo Coffer. Observe que OPFKA garante uma troca de recursos bem-sucedida, desde que o número de recursos comuns | *Q* | é maior do que um limite.

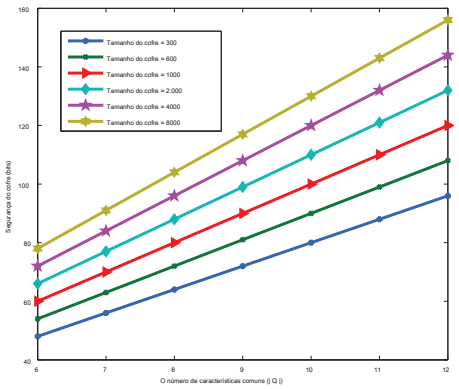

Fig. 2. Resistência do caixão.

Também comparamos a segurança do OPFKA com a do PSKA [13] e descobrimos que a força de segurança do OPFKA é maior do que a do PSKA em todos os níveis de segurança. Observe que PSKA [13] e Pletismograma [7] empregam o mesmo esquema de abóbada difusa, mas o Pletismograma [7] se concentra no sinal PPG enquanto PSKA [13] considera PPG e ECG. Portanto, neste estudo não comparamos o OPFKA com o pletismograma [7], pois o último emprega a mesma abordagem técnica do PSKA [13]. A Tabela II relata a força de segurança de nosso esquema e do PSKA. De acordo com nosso estudo experimental, um cofre de 4000 pontos é melhor do que um cofre de 5000 pontos em termos de resistência de segurança.

B. Troca de mensagens e confirmação

As fases de troca e reconhecimento de recursos tornam muito difícil para os adversários detectar a chave que está sendo combinada devido aos seguintes motivos.

1) No processo de troca de recursos, a presença de *IDr* na mensagem do remetente para o receptor informa aos sensores nas proximidades do remetente quem é o destinatário pretendido. O nonce *Não* é usado para manter a atualização do protocolo, ou seja, para garantir que a confirmação recebida é uma resposta à sua última transmissão.

2) Se uma entidade maliciosa enviar uma mensagem de troca de recurso (reproduzindo trocas anteriores ou criando seu próprio Coffer usando recursos fisiológicos antigos), ela será descartada por qualquer receptor, pois o MAC não corresponderia devido à variação temporal do características fisiológicas.

o Coffer, ainda é difícil para o adversário gerar a chave *K* porque os recursos estão fora de ordem devido à permutação aleatória na etapa de criação do cofre, mas a chave *K* é gerado pelos recursos ordenados.

VI. Avaliação de OPFKA

Nesta seção, fornecemos uma avaliação do OPFKA por realizando uma série de experimentos em nosso esquema. Avaliaremos a chave gerada de acordo com os algoritmos propostos na Seção IV. Os sinais de EKG são obtidos do banco de dados PhysioBank (http://www.physionet.org/physiobank). Abordaremos as seguintes características importantes de uma chave:
1) chaves longas e aleatórias; 2) armazenamento de memória; 3) sobrecarga de comunicação; 4) consumo de energia nas comunicações; 5) distinção; e 6) variância temporal.

1) Chaves longas e aleatórias: As chaves a serem acordadas são geradas pelo remetente e pelo receptor de acordo com os recursos de correspondência solicitados usando uma função hash. O comprimento e a aleatoriedade das chaves acordadas podem, portanto, ser garantidos.

2) Armazenamento de memória: Em nosso esquema proposto, *IDs* e *IDr* leva 16 bytes cada, os recursos e os pontos de chaff são de 20 bits (2,5 Bytes) cada, o índice é de no máximo 1 byte, o nonce *Não* tem 16 bytes e o MAC tem 16 bytes. Assim, o custo de memória estimado é

$$2\ (|\ IDs\ |\ +\ |\ IDr\ |)\ +\ 2{,}5\ |\ R\ |\ +\ |\ I\ |\ +\ |\ Não\ |\ +\ 2\ |\ MAC\ |\ (1)$$

A Fig. 3 ilustra a relação entre o armazenamento da memória e o tamanho do Coffer. Podemos ver que a maior parte da memória é levada pelo Coffer. Um ponto de joio no Coffer leva 20 bits. Um ponto de chaff na abóbada de PSKA leva 36 bits [13] em comparação. Portanto, concluímos que nosso esquema tem uma vantagem sobre o PSKA no armazenamento de memória.

TABELA II
T ELE S ECURIDADE S TRENGTH OF OPFKA E PSKA.

Esquema	OPFKA (bits)	PSKA (bits)		OPFKA (bits)	PSKA (bits)
Tamanho do cofre = 300, | *Q* | = 6	48	42	Tamanho do cofre = 1000, | *Q* | = 10	100	80
Tamanho do cofre = 300, | *Q* | = 7	56	47	Tamanho do cofre = 1000, | *Q* | = 11	110	87
Tamanho do cofre = 300, | *Q* | = 8	64	52	Tamanho do cofre = 1000, | *Q* | = 12	120	94
Tamanho do cofre = 300, | *Q* | = 9	72	57	Tamanho do caixão = 2000, | *Q* | = 6	66	59
Tamanho do cofre = 300, | *Q* | = 10	80	62	Tamanho do caixão = 2000, | *Q* | = 7	77	67
Tamanho do cofre = 300, | *Q* | = 11	88	67	Tamanho do caixão = 2000, | *Q* | = 8	88	75
Tamanho do cofre = 300, | *Q* | = 12	96	72	Tamanho do caixão = 2000, | *Q* | = 9	99	83
Tamanho do cofre = 600, | *Q* | = 6	54	48	Tamanho do caixão = 2000, | *Q* | = 10	110	91
Tamanho do cofre = 600, | *Q* | = 7	63	54	Tamanho do caixão = 2000, | *Q* | = 11	121	99
Tamanho do cofre = 600, | *Q* | = 8	72	60	Tamanho do caixão = 2000, | *Q* | = 12	132	107
Tamanho do cofre = 600, | *Q* | = 9	81	66	Tamanho do cofre = 5000, | *Q* | = 6	74	67
Tamanho do cofre = 600, | *Q* | = 10	90	72	Tamanho do cofre = 5000, | *Q* | = 7	86	76
Tamanho do cofre = 600, | *Q* | = 11	99	78	Tamanho do cofre = 5000, | *Q* | = 8	98	85
Tamanho do cofre = 600, | *Q* | = 12	108	84	Tamanho do cofre = 5000, | *Q* | = 9	110	94
Tamanho do cofre = 1000, | *Q* | = 6	60	52	Tamanho do cofre = 5000, | *Q* | = 10	122	103
Tamanho do cofre = 1000, | *Q* | = 7	70	59	Tamanho do cofre = 5000, | *Q* | = 11	134	112
Tamanho do cofre = 1000, | *Q* | = 8	80	66	Tamanho do cofre = 5000, | *Q* | = 12	146	121
Tamanho do cofre = 1000, | *Q* | = 9	90	73			

TABELA III
T ELE C SUPERFÍCIE DE OMUNICAÇÃO DE OPFKA E PSKA.

	Coffer Exchange	Recurso Ack	Total
OPFKA	4 *ID* | + 2,5 | *R* | + | / | + | *Não* | + | *MAC* |	| *MAC* |	4 *ID* | + 2,5 | *R* | + | / | + | *Não* | + 2 | *MAC* |
PSKA	4 *ID* | + 4,5 | *R* | + | *Não* | + | *MAC* |	| *MAC* |	4 *ID* | + 4,5 | *R* | + | *Não* | + 2 | *MAC* |

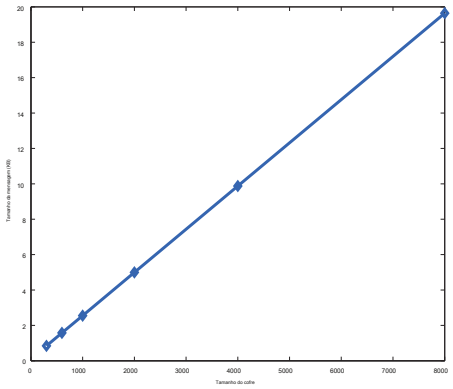

Fig. 3. A relação entre o armazenamento da memória e o tamanho do Coffer.

113 bytes; portanto, o consumo de energia ao transmitir e receber as mensagens é igual a (2,5 ∗ \| *R* \| + 113) ∗ (28,6 + 59,2) *µJ* = (0,2195 \| *R* \| + 9,9214) *mJ.* Para PSKA, o total o tamanho da mensagem é 4,5 \| *R* \| + 112 bytes; assim, a energia total consumida pela transmissão e recebimento das mensagens é igual para (4,5 \| *R* \| + 112) ∗ (28,6 + 59,2) *µJ* = (0,3951 \| *R* \| + 9,8336) *mJ.* Resumimos os resultados do consumo de energia para OPFKA e PSKA na Tabela IV. Fig.5 ilustra o

TABELA IV
E NERGY C ONSUMPTION D UE TO M ESSAGE E XCHANGE

Os esquemas	Consumo de energia (*mJ)*
OPFKA	0,2195 | *R* | + 9,9214
PSKA	0,3951 | *R* | + 9,8336

3) Sobrecarga de comunicação: Os processos de troca de recursos e reconhecimento de recursos são os que mais contribuem para a sobrecarga de comunicação, que está principalmente associada com o tamanho da mensagem no Algoritmo 3 e Algoritmo 4. 280 A Tabela III relata o overhead de comunicação de OPFKA e PSKA [13]. A Fig. 4 ilustra a relação entre o overhead de comunicação e o tamanho do Coffer. Observamos que a sobrecarga de comunicação aumenta com o tamanho do Coffer.

4) Consumo de energia devido às comunicações: Nesta subseção, utilizamos o método proposto em [35] para avaliar o consumo de energia resultante da troca de mensagens. Conforme apresentado em [36], um rádio Chipcon CC1000 usado em ciscos Crossbow MICA2DOT consome 28,6 *µJ* e 59,2 *µJ* para receber e transmitir um byte, respectivamente.

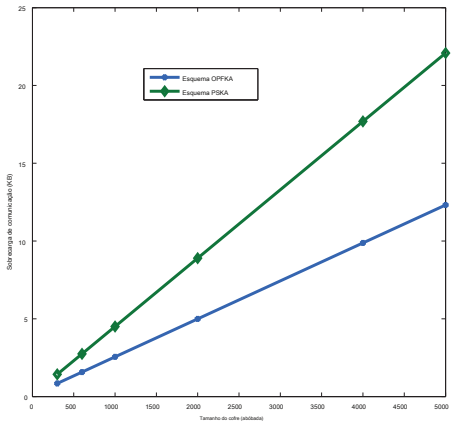

Fig. 4. Comparação entre OPFKA e PSKA em termos de sobrecarga de comunicação.

Para o nosso esquema OPFKA, o tamanho total da mensagem é 2,5 ∗ \| *R* \| +

consumo de energia devido às comunicações em função de 281 e a aleatoriedade é suficientemente alta, o que indica que o tamanho do cofre | *R* /. Obviamente, OPFKA oferece um menor consumo de energia em comparação com PSKA.

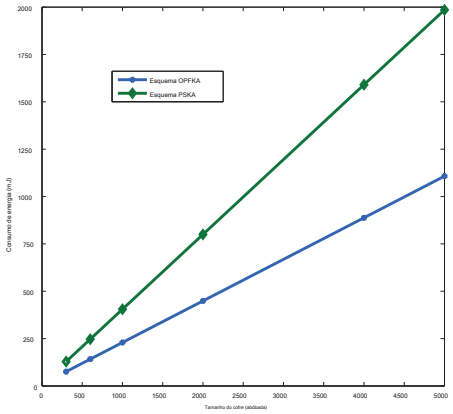

Fig. 5. Consumo de energia *vs.* o tamanho do Cofre (abóbada).

5) Distintividade: A distinção é um dos critérios mais importantes para nosso esquema, uma vez que nosso objetivo principal é distinguir os sensores em um BAN daqueles em outro BAN. Uma taxa de rejeição falsa (FRR) se refere à probabilidade de que dois sensores no mesmo BAN falhem em estabelecer uma chave de sessão. Uma taxa de aceitação falsa (FAR) representa a probabilidade de que dois sensores em diferentes BANs estabeleçam com sucesso uma chave comum ou dois sensores no mesmo BAN de forma assíncrona estabeleçam uma chave de sessão. Uma vez que nosso método FFT aprimorado é semelhante ao processo de geração de recursos em PSKA [13], a distinção, eficiência e variação temporal da chave gerada por OPFKA com base no método FFT aprimorado não serão discutidos aqui, pois a análise é semelhante ao realizado em [13]. Portanto, nos concentramos na distinção de nosso método IPI aqui. Os dados foram coletados de 11 sujeitos (obtidos do banco de dados PhysioBank (http://physionet.org/physiobank/database)). Algoritmos baseados em wavelet mencionados em [37] [38] [22] são executados no sinal de ECG para detectar um ciclo de batimento cardíaco. IPI é o intervalo de tempo entre ondas R adjacentes. Após a quantização, concatenação e expansão, obtemos os recursos secretos. A curva vermelha na Fig. 6 mostra o FAR para dois sensores síncronos em diferentes BANs. Podemos ver que o FAR reduz quase a zero quando o limite é maior que 5, o que indica que nosso esquema pode distinguir com sucesso dois BANs. Normalmente, o limite deve ser maior que 10 se o tamanho do Coffer for em torno de 2.000. A curva azul na Fig. 6 representa o FRR para dois sensores síncronos em diferentes BANs. Discutimos o caso de dois sensores assíncronos no mesmo BAN na próxima subseção: variância temporal. Podemos ver que o FRR é quase zero se o limite for inferior a 12.

6) Variância Temporal: Uma variação temporal mais alta implica que o sinal tem uma melhor aleatoriedade, o que pode reduzir a habilidade do adversário em ataques de repetição. Experimentamos principalmente a variação temporal de nosso método IPI aqui. Como mencionado em [22], podemos extrair com segurança 4 bits de um IPI IPIs assíncronos não devem corresponder uns aos outros. Mas, na realidade, a probabilidade de que os recursos assíncronos correspondam entre si não é zero. Se dois sensores estabelecerem uma chave com recursos IPI assíncronos, ocorre uma falsa aceitação. A Fig. 7 ilustra o FAR entre dois sensores assíncronos no mesmo BAN. o *x*-
eixo é a diferença de tempo. Por exemplo, o valor 20 significa que dois sensores têm uma diferença de tempo de 20 IPIs. Podemos ver que a FAR é reduzida a quase zero se a diferença de tempo for maior que 125 IPIs, que é cerca de 2 minutos. Teoricamente, se houver alguma diferença de tempo, o FAR deve ser próximo de zero para IPIs verdadeiramente aleatórios. Como usamos um nível de quantização fixo, para um ser humano com batimento cardíaco relativamente plácido, um certo nível de precisão pode ser perdido. Observe que os resultados de nossos experimentos são consistentes com aqueles em [22]. A distribuição das distâncias de Hamming entre as feições síncronas corresponde perfeitamente à distribuição binomial teórica. Mas eles não são completamente iguais. Se os sensores podem ajustar dinamicamente seus níveis de quantização de acordo com IPIs históricos ou o estado de saúde do paciente, o resultado deve ser melhorado. Deixamos isso para nossas pesquisas futuras.

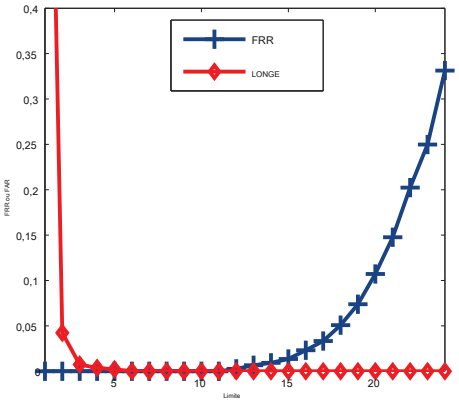

Fig. 6. FAR e FRR entre dois sensores síncronos em diferentes BAN

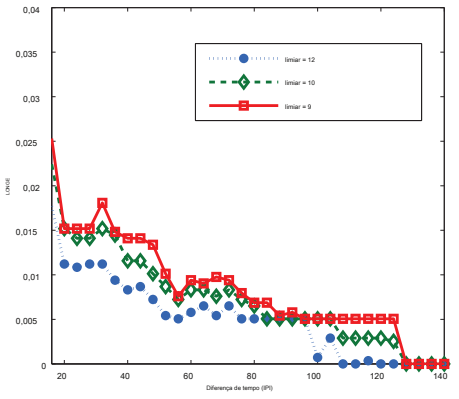

Fig. 7. Variância de tempo.

VII. Conclusão

Neste artigo, apresentamos uma chave segura e eficiente a-esquema de greement, ou seja, o Ordered-Physiological-Feature-

Acordo de chave baseado (OPFKA), para permitir comunicações inter-sensor seguras em uma BAN. O OPFKA permite que dois sensores em um BAN concordem com uma chave criptográfica simétrica gerada a partir de seus recursos comuns de maneira autenticada e transparente, sem qualquer pré-distribuição ou inicialização de material de codificação. A análise de segurança do OPFKA mostra que o OPFKA atende aos objetivos de design do acordo de chave. Analisamos o desempenho, armazenamento de memória e custo de comunicação do OPFKA e demonstramos que o esquema tem baixo custo computacional, baixo armazenamento de memória e baixo overhead de comunicação, o que indica que OPFKA é uma abordagem viável e eficiente para proteger inter- comunicações do sensor dentro de uma BAN.

UMA RECONHECIMENTO

Este projeto foi apoiado em parte pelos subsídios da National Science Foundation dos EUA CNS-1017662 e CNS-0963957, e em parte pela National Natural Science Foundation of China sob os subsídios 60973114 e 61170249.

R EFERÊNCIAS

[1] K. Venkatasubramanian e S. Gupta, "Security for pervasive health monitoring sensor applications," in *a Quarta Conferência Internacional sobre Sensoriamento Inteligente e Processamento de Informação,* 2006, pp. 197–202.

[2] L. Schwiebert, S. Gupta e J. Weinmann, "Desafios de pesquisa em redes sem fio de sensores biomédicos", em *Anais da 7ª Conferência Internacional Anual sobre Computação Móvel e Redes,* 2001, pp. 151–165.

[3] R. Schmidt, T. Norgall, J. Mörsdorf, J. Bernhard e T. von der Grün, "Rede de área corporal (BAN) - um elemento chave de infraestrutura para aplicações médicas centradas no paciente", *Biomedizinische Technik / Biomedical En- gineering,* vol. 47, nº s1a, pp. 365-368, 2002.

[4] J. Penders, J. vande Molengraft, L. Brown, B. Grundlehner, B. Gyselinckx e CV Hoof, "Potencial e desafios das redes da área do corpo para a saúde pessoal", em *Sociedade de Engenharia em Medicina e Biologia,* 2009, pp. 6569–6572.

[5] K. Venkatasubramanian, S. Gupta, R. Jetley e P. Jones, "Interoperable medical devices," *IEEE Pulse,* vol. 1, não. 2, pp. 16–27, 2010.

[6] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao e V. Leung, "Body area networks: a survey," *Redes e aplicativos móveis,* vol. 16, não. 2, pp. 171–193, 2011.

[7] K. Venkatasubramanian, A. Banerjee, e S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," em *Conferência de Comunicações Militares,* 2008, pp. 1-7.

[8] L. Eschenauer e V. Gligor, "Um esquema de gerenciamento de chaves para redes de sensores distribuídas", em *ACM CCS,* 2002, pp. 41–47.

[9] S. Zhu, S. Setia e S. Jajodia, "LEAP +: Eficientes mecanismos de segurança para redes de sensores distribuídos em grande escala," *Transações ACM em Redes de Sensores (TOSN),* vol. 2, não. 4, pp. 500–528, 2006.

[10] F. Liu, X. Cheng, L. Ma e K. Xing, "SBK: A self-con fi guring frame- work for bootstrapping keys in sensor networks", *Transações IEEE em computação móvel,* vol. 7, não. 7, pp. 858–868, 2008.

[11] F. Liu e X. Cheng, "LKE: A self-con fi guring scheme for location-aware key establishment in wireless sensor networks", *Transação IEEE em comunicações sem fio,* vol. 7, não. 1, pp. 224–232, janeiro de 2008.

[12] L. Ma, X. Cheng, F. Liu, F. An e M. Rivera, "iPAK: An in-situ pairwise key bootstrapping scheme for wireless sensor networks", *Transações IEEE em sistemas paralelos e distribuídos,* vol. 18, não. 8, pp. 1174–1184, agosto de 2007.

[13] K. Venkatasubramanian, A. Banerjee e S. Gupta, "PSKA: Esquema de acordo de chave utilizável e seguro para redes de área corporal", *IEEE Transactions on Information Technology in Biomedicine,* vol. 14, não. 1, pp. 60–68, 2010.

[14] K. Venkatasubramanian, A. Banerjee e S. Gupta, "acordo chave baseado em EKG em redes de sensores corporais," em *Em Atas do 2º Workshop sobre redes de missão crítica,* 2008, pp. 1-6.

[15] C. Tan, H. Wang, S. Zhong e Q. Li, "Body sensor network security: an abordagem de criptografia baseada em identidade ", em *ACM Wisec,* 2008, pp. 148-153

[16] D. Malan, M. Welsh e M. Smith, "Uma infraestrutura de chave pública para distribuição de chaves em tinyos com base na criptografia de curva elíptica", em *IEEE SECON,* 2004, pp. 71–80.

[17] C. Tan, H. Wang, S. Zhong e Q. Li, "IBE-Lite: a lightweight identity-based cryptography for body sensor networks", *IEEE Transactions on Information Technology in Biomedicine ,,* vol. 13, não. 6, pp. 926-932, 2009.

[18] S. Keoh, E. Lupu e M. Sloman, "Protegendo redes de sensores corporais: associação de sensores e gerenciamento de chaves", em *IEEE PerCom,* 2009, pp. 1-6.

[19] M. Li, S. Yu, W. Lou e K. Ren, "Associação de sensor de segurança baseada em pareamento de dispositivo de grupo e gerenciamento de chave para redes de área corporal", em *IEEE INFOCOM,* 2010, pp. 1–9.

[20] Y. Law, G. Moniava, Z. Gong, P. Hartel e M. Palaniswami, "Kalwen: Um novo esquema de gerenciamento de chave prático e interoperável para redes de sensores corporais", *Redes de segurança e comunicação,* vol. 4, não. 11, pp. 1309–1329, 2011.

[21] M. Li, S. Yu, J. Guttman, W. Lou e K. Ren, "Secure ad-hoc trust initialization and key management in wireless body area networks," *Transações ACM em redes de sensores (TOSN), (para aparecer),* 2012

[22] F. Xu, Z. Qin, C. Tan, B. Wang e Q. Li, "IMDGuard: Protegendo dispositivos médicos implantáveis com o guardião vestível externo", em *IEEE INFOCOM,* 2011, pp. 1862–1870.

[23] C. Hu, N. Zhang, H. Li, X. Cheng e X. Liao, "Body area network: A fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications (edição especial sobre tecnologias emergentes em comunicações),* 2012

[24] S. Cherukuri, K. Venkatasubramanian, e S. Gupta, "Biosec: uma abordagem biométrica para garantir a comunicação em redes sem fio de biossensores implantados no corpo humano", em *Conferência Internacional sobre Workshops de Processamento Paralelo,* 2003, pp. 432-439.

[25] C. Poon, Y. Zhang e S. Bao, "Um novo método biométrico para proteger redes de sensores de área corporal sem fio para telemedicina e m-health", *IEEE Communications Magazine,* vol. 44, não. 4, pp. 73–81, 2006.

[26] A. Juels e M. Sudan, "A fuzzy vault scheme," *Projetos, códigos e criptografia,* vol. 38, nº 2, pp. 237-257, 2006.

[27] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fi ngerprints," em *Autenticação biométrica de pessoa baseada em áudio e vídeo,* 2005, pp. 55–71

[28] E. Reddy e I. Babu, "Authentication using fuzzy vault based on iris textures," in *Procedimentos da 2ª Conferência Internacional da Ásia sobre Modelagem e Simulação (AMS),* 2008, pp. 361–368.

[29] W. Maisel, M. Moynahan, B. Zuckerman, T. Gross, O. Tovar, D. Tillman e D. Schultz, "Pacemaker and icd generator malfunctions," *JAMA: o jornal da American Medical Association,* vol. 295, no. 16, pág. 1901, 2006.

[30] S. Ali, V. Sivaraman e D. Ostry, "Geração de chave secreta de reconciliação zero para dispositivos de monitoramento de saúde usados no corpo", em *ACM Wisec,* 2012, pp. 39–50.

[31] A. Shamir, "Como compartilhar um segredo", *Comunicações do ACM,* vol. 22, não. 11, pp. 612-613, 1979.

[32] G. BLAKLEY, "Proteção de chaves criptográficas", em *AFIPS Conference Proceedings,* vol. 48. AFIPS Press, 1979, pp. 313–317.

[33] C. Hu, X. Liao e X. Cheng, "Veri fi capaz multi-secret sharing based on LFSR sequence," *Ciência da Computação Teórica,* vol. 445, pp. 52–62, agosto de 2012.

[34] D. Davenport, N. Seidl, J. Moss, M. Patel, A. Batra, JM Ho, S. Hosur, JC Roh, T. Schmidl, O. Omeni e A. Wong, "Medwin Mac and Security Proposal - Documentation," IEEE 802.15 WPAN Task Group 6., setembro de 2009.

[35] K. Ren, W. Lou, K. Zeng e P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications,* vol. 6, não. 11, pp. 4136-4144, 2007.

[36] A. Wander, N. Gura, H. Eberle, V. Gupta e S. Shantz, "Análise de energia de criptografia de chave pública para redes de sensores sem fio", em *IEEE PerCom,* 2005, pp. 324-328.

[37] C. Li, C. Zheng e C. Tai, "Detecção de pontos característicos de ecg usando transformações wavelet", *IEEE Transactions on Biomedical Engineering,* vol. 42, nº 1, pp. 21-28, 1995.

[38] J. Mart´ınez, R. Almeida, S. Olmos, A. Rocha, e P. Laguna, "A wavelet-based ecg delineator: Evaluation on standard database", *IEEE Transactions on Biomedical Engineering,* vol. 51, nº 4, pp. 570-581, 2004.