PSKA: Esquema de contrato de chave utilizável e seguro para redes de área corporal

Krishna K. Venkatasubramanian, *Membro, IEEE,* Ayan Banerjee,
e Sandeep Kumar S. Gupta, *Membro Sênior, IEEE*

***Resumo* - Uma rede de área corporal (BAN) é uma rede sem fio de sensores de monitoramento de saúde projetados para fornecer assistência médica personalizada. A segurança das comunicações intersensores nos BANs é essencial para preservar não apenas a privacidade dos dados de saúde, mas também para garantir a segurança da assistência médica. Este artigo apresenta *chave de acordo com o sinal fisiológico (PSKA), um esquema para habilitar a comunicação intersensora segura dentro de um BAN em um* utilizável *(plug-n-play, transparente).* O PSKA permite que os nós vizinhos em um BAN concordem com uma chave criptográfica simétrica (compartilhada), de maneira autenticada, usando sinais fisiológicos obtidos do sujeito. Nenhuma inicialização ou pré-implantação é necessária; simplesmente implantar sensores em um BAN é suficiente para fazê-los se comunicar com segurança. Nossa análise, prototipagem e comparação com o protocolo de contrato-chave Dif fi e-Hellman usado com freqüência mostra que o PSKA é um protocolo de contrato-chave viável entre sensores para BANs.**

***Termos do Índice* - Redes de área corporal (BANs), fisiológicas acordo de chave baseado em sinais (PSKA), comunicação segura, segurança utilizável.**

Eu NTRODUÇÃO

As redes de área OBY (BANs) são redes de redes sem fio sensores técnicos, implantados em uma pessoa, para permitir *difundido, individualizado e em tempo real* gestão de saúde. Como os BANs lidam com dados pessoais de saúde, protegê-los, especialmente sua comunicação através do link sem fio, é muito crítico (um dos principais desafios de pesquisa no projeto do BAN [1]). A falta de recursos de segurança adequados pode não apenas levar a uma violação da privacidade do paciente, mas também potencialmente permitir que os adversários comprometam a segurança do paciente, modificando os dados reais, resultando em diagnóstico e tratamento incorretos [2]. De fato, proteger os dados de saúde é um requisito legal, conforme a Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA) (http://www.hhs.gov/ocr/hipaa/), que determina que todas as informações pessoalmente identificáveis em formato eletrônico sejam protegidas .

Artigo recebido em 16 de outubro de 2008; revisado em 20 de março de 2009 e agosto 13, 2009. Publicado pela primeira vez em 11 de dezembro de 2009; versão atual publicada em janeiro 15, 2010. Este trabalho foi apoiado em parte pela National Science Foundation sob Grant CNS-0617671 e Grant CT-0831544. Este artigo foi apresentado em parte na IEEE Military Communications Conference 2008, em San Diego.

KK Venkatasubramanian esteve no IMPACT Laboratory, Arizona State University, Tempe, AZ 85287 EUA. Ele está agora no Departamento de Ciência da Computação e Informação da Universidade da Pensilvânia, Filadélfia, PA 19104 EUA (e-mail: vkris@cis.upenn.edu).

A. Banerjee e SKS Gupta estão no Laboratório IMPACT, Universidade Estadual do Arizona, Tempe, AZ 85287 EUA (e-mail: abanerj3@asu.edu ; sandeep.gupta@asu.edu).

As versões coloridas de uma ou mais figuras deste documento estão disponíveis online em http://ieeexplore.ieee.org.

Identificador de objeto digital 10.1109 / TITB.2009.2037617

Os sensores contam com chaves criptográficas para proteger sua comunicação. As chaves geralmente são disponibilizadas aos sensores por meio de protocolos explícitos de distribuição de chaves. Classes conhecidas de técnicas de distribuição de chaves simétricas [3], [4] requerem alguma forma de pré-implantação. No entanto, dado o tamanho progressivamente crescente dos BANs, essas abordagens podem potencialmente envolver uma latência considerável durante a configuração da rede ou quaisquer ajustes subsequentes, devido à necessidade de pré-implantação. Acreditamos que, para que os BANs sejam úteis, eles devem fornecer segurança utilizável - que seja plug-n-play e amplamente transparente. Por exemplo, deve-se poder adicionar, remover e ajustar os sensores em seu BAN, conforme e quando necessário, sem reconfigurar partes da rede (um requisito muito importante em ambientes de missão crítica) e ainda ter comunicação segura. Em alguns casos, sistemas de criptografia assimétricos como Dif fi e-Hellman (DH) e suas variantes foram usados para evitar a pré-implantação. No entanto, eles são propensos a ataques do tipo intermediário e precisam de mecanismos de autenticação adicionais para serem úteis.

Neste artigo, apresentamos um novo esquema chamado *Acordo-chave com base no sinal fisiológico (PSKA),* que utiliza sinais fisiológicos para permitir que os sensores concordem com uma chave criptográfica simétrica aos pares, de uma maneira autenticada. Não requer *a priori* distribuição de material de chave, basta implantar os sensores em um assunto, facilitando assim a comunicação BAN segura que é *utilizável.* O PSKA está sendo projetado como parte da proteção do sistema de monitoramento de saúde Ayushman [5], desenvolvido no IMPACT Laboratory, Arizona State University. O uso de sinais fisiológicos tem o potencial de eliminar a necessidade de distribuição explícita de chaves, permitindo que os sensores constituintes concordem com as chaves, conforme necessário [6]. A idéia de usar recursos baseados em sinais fisiológicos para concordância chave vem da observação de que o corpo humano é dinâmico e complexo, e o estado fisiológico de um sujeito é bastante singular em um determinado momento [7]. De um modo geral, o PSKA funciona usando recursos de sinal fisiológico e *fuzzy-vault* primitivo criptográfico [8] para ocultar a chave em uma extremidade, transportando-a para a outra e exibindo-a usando os recursos de sinal fisiológico medidos na outra extremidade. O PSKA encontra o *objetivos de design* sugerido em [9] quando sinais fisiológicos são usados como base para o acordo-chave, que são os seguintes.

1) *Comprimento e aleatoriedade:* As chaves acordadas são longas e aleatório para evitar a força bruta.
2) *Baixa latência:* A duração da captura do sinal fisiológico necessário é mínimo.
3) *Distinção:* Conhecendo o recurso derivado dos O valor de aluguel do sinal fisiológico de um sujeito

não fornece uma vantagem significativa em adivinhar as chaves que estão sendo acordadas pelos sensores em outro assunto. Uma característica importante da distinção é que ele autentica os sensores em comunicação, garantindo que apenas os sensores no mesmo BAN possam concordar com uma chave compartilhada.

4) *Variação temporal:* Conhecer os sinais fisiológicos em a qualquer momento não proporcionará vantagem significativa em conhecer as chaves acordadas em futuras execuções do esquema. Esta é uma propriedade importante que *diferencia a técnica proposta das técnicas tradicionais baseadas em biometria,* onde um modelo é criado, ele nunca é alterado [10].

As contribuições deste artigo são três: 1) um esquema para um acordo chave autenticado entre pares entre dois nós nos BANs, ou seja, PSKA (consulte a Seção IV); 2) análise das propriedades de segurança do PSKA (consulte a Seção V); e 3) validação do PSKA, usando dados reais de dois dos sinais fisiológicos mais comumente coletados - fotopletismograma (PPG) e eletrocardiograma (EKG), com base nos objetivos de projeto mencionados anteriormente (consulte a Seção VI).

II B RECONHECIDO

O uso de sinais fisiológicos para garantir a comunicação intersensor foi apresentado em [11]. Com base nessa idéia inicial, Poon *et al. [* 12] propuseram o uso do intervalo entre pulsos (IPI) para gerar chaves criptográficas. A vantagem de usar o IPI é que ele pode ser derivado de várias fontes, como séries temporais PPG e EKG, medindo a diferença de tempo entre os picos no sinal EKG / PPG. O processo de geração de chaves baseado em IPI funciona da seguinte maneira: 1) os sensores medem primeiro os sinais de EKG e PPG de maneira sincronizada; 2) eles geram uma série de valores IPI a partir de seus respectivos dados; e 3) eles pegam 67 valores IPI contíguos (que levam cerca de 30 s para medir, pois um pico de EKG / PPG gera a cada 300-500 ms) a partir de um ponto inicial específico e os codificam em 128 bits para formar a chave $_{ekg}$ e chave $_{ppg}$ em cada sensor, que pode ser usado para uma comunicação segura entre eles. No entanto, através de nossa própria experimentação com o esquema, descobrimos que, embora as chaves sejam longas e aleatórias (a entropia das chaves geradas está acima de 0,9), a distância média de Hamming entre as chaves $_{ekg}$ e chave $_{ppg}$ para o mesmo assunto é ~ 60 e ~ 65 bits para dois assuntos diferentes. Acreditamos que a principal razão para essa diferença é a *especi fi cidade topográfica* do corpo humano - sinais fisiológicos medidos em diferentes áreas do corpo parecem ter tendências semelhantes (alta correlação), mas não exatamente os mesmos valores. Como resultado, os símbolos de informação nas chaves são reordenados, levando a erros de translação e rotação [8] que produzem valores drasticamente diferentes.

Portanto, adotamos uma abordagem diferente: em vez de tentar gerar chaves a partir de medições de sinais fisiológicos, as usamos para facilitar a concordância das chaves. Isso ocorre porque, dada a natureza dinâmica do corpo humano, as chances de os sinais fisiológicos serem exatamente idênticas são baixas. Além disso, fazemos isso processando sinais fisiológicos no domínio da frequência, em vez do domínio do tempo. O processamento no domínio da frequência tem muitas vantagens: 1) componentes de frequência de sinais fisiológicos, a qualquer momento, têm muitos valores mais comuns, em comparação com os valores no domínio do tempo dos sinais fisiológicos, independentemente de onde são medidos no corpo; 2) a amostra de sinal fisiológico necessária para a concordância das chaves é muito menor; e 3) o nível de sincronização necessário para medir os sinais fisiológicos nos sensores não é muito rigoroso [1] O objetivo deste artigo é mostrar que os sinais fisiológicos podem ser usados para estabelecer chaves simétricas entre sensores no BAN e validar os resultados.

III S YSTEM M ODEL

A ABAN é uma rede de monitoramento fisiológico e ambiental *nós sensores* desgastadas e / ou implantadas em um *sujeito* ou *Individual [* 3] Os nós sensores coletam dados de saúde e contextuais em intervalos regulares e os encaminham por uma rede de várias lojas para uma rede altamente capacitada. *Pia* nó para processamento adicional. Um nó sensor típico (chamado de *sensor),* consiste em um elemento sensor, conversor analógico-digital, pilha de comunicação sem fio, processador e memória. Assumimos que os sensores *comunicar sem fio,* como os fios que passam entre os sensores em um BAN o tornarão intrusivos. O meio sem fio, no entanto, não é confiável. Presume-se que todos os sensores possam medir os sinais fisiológicos apropriados. Qualquer entidade que não esteja em contato com o sujeito não pode medir sinais fisiológicos do sujeito. Assumimos que apenas sensores legítimos estão em contato com o corpo. Além disso, assumimos que entidades mal-intencionadas não podem introduzir nem comprometer sensores dentro do BAN sem serem detectadas, pois qualquer coisa usada está principalmente sob supervisão do host ou do responsável. Portanto, as ameaças enfrentadas por um BAN são principalmente de adversários, que podem espionar todo o tráfego dentro do BAN, injetar mensagens, reproduzir mensagens antigas e falsificar identidades de sensores. Os adversários também podem tentar usar os dados do sinal fisiológico obtidos de outras pessoas para interromper o processo de distribuição principal. Observe que, neste documento, nos concentramos apenas em garantir a comunicação intersensor no BAN. A comunicação do coletor em diante pode utilizar esquemas de segurança convencionais, como o Secure Socket Layer (SSL), dadas as consideráveis capacidades das entidades envolvidas. Finalmente, não consideramos ataques de negação de serviço (DoS), como atolamentos, interferência eletromagnética ou ataques de depleção de bateria neste documento.

IV P HYSIOLOGICAL- S IGNAL- B ASED K EY UMA GREEMENT

O propósito de *PSKA* é *facilitar a comunicação intersensora segura* s entre dois sensores, permitindo que eles concordem com uma chave simétrica em pares, usando recursos baseados em sinais fisiológicos. O processo de concordância com as chaves funciona da seguinte forma (veja a Fig. 1): um dos dois sensores (emissor) gera uma chave simétrica aleatória que depois oculta usando um vetor de característica obtido a partir do sinal fisiológico. Essa chave oculta é enviada para

[1] Nossas experiências mostram uma concordância-chave bem-sucedida, mesmo com uma diferença de 1 s nos horários de início da medição dos sinais fisiológicos usando recursos do domínio da frequência (consulte a SeçãoVI, antes). Soluções proeminentes propostas para sincronização de tempo para redes de sensores [13] atingem a sincronização em microssegundos, o que é mais que suficiente para o PSKA.

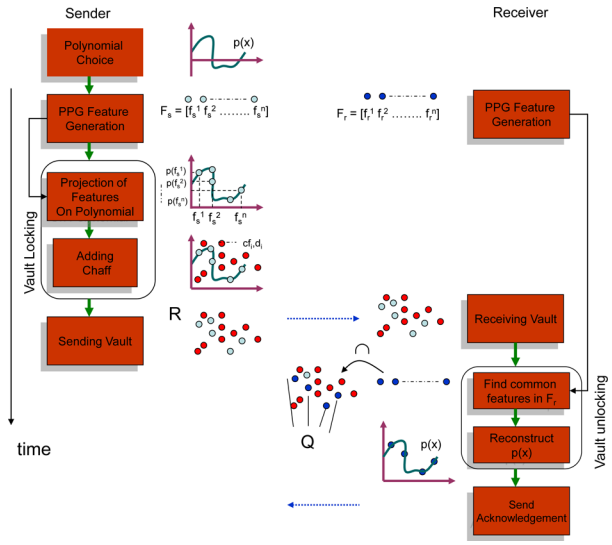

Fig. 1. Protocolo PSKA.

o outro sensor (receptor) que usa sua própria versão do vetor de característica e obtém a chave aleatória depois de compensar as diferenças entre seu vetor de característica e o usado pelo remetente. Em nosso trabalho anterior [11], propusemos o uso de um esquema simples de correção de erros, como a decodificação por maioria [14], como mecanismo compensatório, para chegar a uma chave comum no receptor. A inspiração por trás da ideia foi a observação de que cada medida de um sinal fisiológico era independente de outras; qualquer diferença em seus valores medidos pode ser modelada como erro de comunicação. Um problema inerente ao uso dessa abordagem é que, embora possa corrigir a presença de algumas diferenças nos vetores de recursos, ele não pode lidar com a reordenação ou a presença de recursos adicionais (em um dos sensores) no vetor de recursos [8]. *cofre difuso [*8]

A. Cofre Difuso

O esquema de cofre difuso proposto em [8] é projetado para bloquear (ocultar) um segredo (*S)* em uma construção chamada de *cofre* usando um conjunto de valores *UMA*. Uma vez bloqueado, o cofre só pode ser desbloqueado com outro conjunto de valores *B* que tem um *signi fi cativo* número de valores em comum com o conjunto *UMA*. Conforme ilustrado na Fig. 1, a construção e o travamento do cofre são realizados por: 1) gerar um *v* polinômio de ordem th *p* sobre a variável *x* que codifica o segredo *S;* 2) calcular o valor do polinômio em diferentes valores de *x* do conjunto *UMA* e criando um conjunto $R = \{a_{Eu}, p(a_{Eu})\}$,

Onde $1 \le Eu \le |A|$; e 3) adicionar um conjunto de pontos gerado aleatoriamente chamado *palha* para *R,* que não se encontra no polinômio. Depois que o cofre é construído, desbloqueá-lo com base no conjunto *B*

é feito através da construção de um conjunto $Q = \{(u, v) \mid (u, v) \in R, você \in B\}$.

O processo de desbloqueio é possível apenas se *Q* tem um número significativo de pontos legítimos (sem palha) que estão no polinômio [8]. Podemos mapear esse esquema no PSKA, definindo os recursos obtidos no remetente para definir *UMA,* os obtidos no receptor para definir *B,* e gerar um polinômio, cujos coeficientes formam a chave secreta a ser acordada.

Considere o exemplo a seguir que ilustra a operação do cofre difuso. Seja o polinômio $p(x) = x + 1$ conjunto $A = \{1, 2, 3\}$, e $B = \{1, 3, 4\}$ então o cofre *R* criado calculando o valor do polinômio em cada ponto do *UMA* é $R = \{(1, 2), (2, 3), (3, 4), (4, 7), (6, 9), (7, 12), (8, 5)\}$. Os últimos quatro pontos são os pontos de palha que não caem no polinômio. Para desbloquear o cofre, o conjunto *Q* é construído, onde $Q = \{(1, 2), (3, 4), (4, 7)\}$. Como o conjunto *Q* possui dois pontos no polinômio, podemos usá-lo para reconstruir facilmente o polinômio de primeira ordem e, assim, desvendar o segredo.

B. Bloqueio e desbloqueio do cofre no PSKA

O uso de polinômios garante que os conjuntos *UMA* e *B* não precisa ter nenhuma ordem para eles, desde que tenham um número significativo de valores comuns. A presença dos pontos de palha acrescenta segurança ao cofre e oculta pontos legítimos e o polinômio real. A menos que o adversário conheça um grande número de pontos no polinômio, ele não poderá reconstruí-lo. Nesta seção, mostramos como o esquema de cofre difuso para um acordo-chave com o PSKA. Nós usamos o termo *remetente* para o sensor que cria o cofre e o bloqueia, e o *receptor* para o sensor que desbloqueia o cofre para acessar a chave secreta. O contrato principal ocorre da seguinte maneira.

1) Geração de Recursos: Primeiro, o remetente e o receptor obtêm recursos baseados em sinais fisiológicos. Este é um processo de quatro etapas: a) Os dois sensores coletam o sinal fisiológico de maneira vagamente sincronizada, a uma taxa de amostragem específica por um período fixo; b) As amostras são divididas em janelas e uma transformada rápida de Fourier (FFT) é executada em cada uma dessas partes; c) Os coeficientes de FFT de cada uma das janelas sobrepostas (um número pré-definido de pontos contíguos de séries temporais de sinais) são passados através de uma função de detecção de pico (um simples detector de máximos locais) que retorna uma tupla da forma $\langle k_{Eu}$ $_x, k_{Eu}{}_y \rangle$ Onde k_{Eu} $_x$ é o ponto FFT no qual o pico é observado (é a localização de pico na *x*- eixo, também chamado *índice de pico),* k_{Eu} $_y$ são seus valores coeficientes de FFT correspondentes (magnitude do pico ou *valor de pico),* e *Eu* é o índice dos picos. O número de picos observados por um sensor varia de acordo com a situação; d) Cada um desses índices de pico (k_x) e valor de pico (k_y) pares são quantizados e convertidos em uma sequência binária e concatenados ([k_x k_y]) para formar um *característica.* Recursos individuais obtidos a partir de uma única medição são agrupados para formar um vetor de recursos $F_D = \{f_1{}_D, f_2{}_D, \ldots f_N{}_D\}$, Onde f_{eu} $_D = [k_{eu}$ $_x k_{eu}{}_y]$ *D* é também o remetente (*s)* ou receptor (*r)* nó e *N* é o tamanho do vetor de característica, ou seja, número de índices em que os picos foram observados. Os valores dos diferentes parâmetros usados para a geração de recursos dependem do sinal fisiológico usado e precisam ser ajustados durante a implantação. Escolhemos os picos de FFT como características por dois motivos: 1) são simples de detectar e 2) caracterizam muito bem a fisiologia do sujeito. Eles são ideais para distinguir entre sensores que estão no mesmo BAN ou em BANs diferentes, fornecendo um mecanismo de autenticação eficiente e uma base para o acordo principal (consulte a Seção VI, para mais detalhes). No final do processo de geração de recursos, o remetente e o destinatário possuem vetores de recursos no formato $F_s = \{f_1{}_s, f_2{}_s \ldots f_N{}_s\}$ e $F_r = \{f_1{}_r, f_2{}_r, \ldots f_N{}_r\}$, respectivamente.

2) Escolha polinomial: Depois que os recursos são gerados, o remetente gera um v polinômio de ordem th do formulário $p(x) = c_v x_v + c_{v-1} x_{v-1} + \ldots + c_0$, onde o valor dos coeficientes (c_{Eu} s) são selecionados aleatoriamente (usando um gerador de números pseudo-aleatórios, por exemplo). A ordem do polinômio (v) usado no BAN não é um segredo e é conhecido por todos os sensores na rede. Os coeficientes, concatenados juntos, formam a chave secreta que o remetente deseja comunicar ao destinatário (Key = $c_v c_{v-1} | \ldots | c_0$) Definimos o comprimento dessa chave em 128 bits (chaves mais longas podem ser usadas com facilidade) e, dependendo da ordem do polinômio usado, os coeficientes são obtidos dividindo a chave de acordo.

3) Criação do Vault: Com o vetor polinomial e de recurso disponível, o remetente agora cria o cofre difuso, computando o conjunto $P = \{f_{Eu}$ $_s\ p(f_{Eus})\}$, Onde f_{Eu} $_s \in F_s$ e $1 \le Eu \le N$. Isso também calcula um conjunto muito maior de M pontos aleatórios do formulário $C = \{cf_j\ d_j\}$ Onde cf_j $\in F_s\ d_j = p(cf_j)$ e $1 \le j \le M$. Cada ponto de palha cf_{Eu} está dentro do mesmo intervalo (0– 2^{13}) como o dos recursos. Portanto, 2^{13} é o limite para o número total de pontos no cofre ($|R|$), que é igual a $|M + N|$. Nós nos referimos a $|R|$ Enquanto o *tamanho do cofre.*

4) Bloqueio de cofre: O remetente então permite aleatoriamente os valores no cofre R = RandPermute ($P \cup C$) garantir que os pontos de palha e os pontos legítimos sejam indistinguíveis. A cardinalidade do conjunto C pode variar em relação ao nível de segurança necessário. Quanto maior o conjunto C, o mais difícil é quebrar o cofre. A seção V discute a relação entre o tamanho do cofre e sua segurança com mais detalhes.

5) Troca de cofre: O remetente comunica o cofre R ao receptor usando a seguinte mensagem: Remetente → Receiver: ID s EU IRIA r, R, *não,* MAC (chave, R / *Não* / EU IRIA s) Aqui, ID s e ID r são os IDs do remetente e do destinatário, respectivamente, *Não* é um nonce (número aleatório exclusivo) para atualização de transação, MAC é um código de autenticação de mensagens [por exemplo, Código de autenticação de mensagens Hash - algoritmo de hash seguro 1 (HMAC-SHA1)] e a chave (Chave) usada é aquela que é trancado no cofre.

6) Desbloqueio do cofre: O receptor ao receber o cofre R, primeiro calcula o conjunto Q, Onde $Q = \{(b, c) | (b, c) \in R, b \in F_s\}$. Em seguida, tenta reconstruir o polinômio p com base nos pontos em Q usando a interpolação lagrangiana (como sugerido em [10]), segundo a qual, o conhecimento de $v + 1$ 1 pontos $\{(x_0, y_0), (x_1, y_1), \ldots, (x_v, y_v)\}$ em um polinômio permite a reconstrução de um polinômio de ordem th executando a seguinte combinação linear: $p'(x) = \sum_{j=0}^{v} y_j d_j(x)$,

Onde $d_j(x) = \prod_{i=v}$ $_{i=j, i=0} (x - x_{Eu})/(x_j - x_{Eu})$. Para o receptor ser capaz de desbloquear com êxito o cofre, a condição $|Q > v$ deve segurar. Leva então $v + 1$ 1 pontos (de Q) de cada vez e tenta desbloquear o cofre. Os coeficientes do polinômio resultante são então usados para verificar o MAC. Isso não apenas confirma a exatidão do processo de desbloqueio, mas também autentica o remetente no destinatário (confirma que o remetente está no mesmo BAN que o destinatário). Isso se deve à propriedade de distinção e variação temporal dos recursos do sinal fisiológico que garante: 1) os recursos gerados a partir de sinais fisiológicos para o PSKA são drasticamente diferentes para duas pessoas diferentes e 2) os cofres antigos não podem ser reproduzidos, pois os recursos teria mudado a essa altura e não pode ser desbloqueado (consulte a Seção VI, para mais detalhes).

7) Confirmação do Vault: Se o desbloqueio foi bem-sucedido, o destinatário envia uma resposta de volta ao remetente para informá-lo sobre o desbloqueio correto do cofre usando a seguinte mensagem: Receptor → Remetente: MAC (chave, *Não* EU IRIA s EU IRIA r) Os símbolos têm o mesmo significado descrito anteriormente. A verificação bem-sucedida da confirmação autentica o destinatário no remetente. Isso ocorre porque apenas um nó no BAN (receptor), que mediu o mesmo sinal fisiológico ao mesmo tempo que ele próprio, poderia ter desbloqueado o cofre, dadas as propriedades de distinção e variação temporal dos recursos baseados em sinais fisiológicos.

A Fig. 1 mostra o processo de geração de recursos. Nos referimos à execução dessas sete etapas como um *iteração* do PSKA. A chave aleatória (Chave) gerada na primeira etapa é usada para permitir a comunicação confidencial, autenticada e protegida pela integridade entre os sensores em um *plug-n-playmanner tornando BANs mais utilizáveis.* Nenhum dos esquemas tradicionais de distribuição de chaves [4], [15] nem as abordagens baseadas em sinais fisiológicos [12] consideram essa propriedade. Além disso, com o PSKA, nenhuma chave aleatória ou recursos fisiológicos são reutilizados. Isso garante que qualquer conhecimento de chaves passadas ou características fisiológicas (devido à propriedade de variação temporal, conforme visto na Seção VI) de um sujeito não possa ser usado para subverter o cofre.

V. Segurança de PSKA

Os problemas de segurança no PSKA surgem principalmente devido aos seus requisitos de troca de cofre e respondem a ele para se autenticar e ingressar no BAN. Um bisbilhoteiro pode gravar o cofre e tentar construir o polinômio oculto (chave) dele. Nesta seção, discutiremos as implicações de segurança dos dois principais aspectos do PSKA: o cofre e sua troca.

A. Segurança do Vault

O uso da construção de cofre difuso no PSKA garante que, embora os dois sensores possam não ter todos os recursos em comum, eles ainda possam concordar com uma chave comum de maneira segura. A segurança do esquema PSKA é baseada na dificuldade da reconstrução polinomial. A ocultação da característica legítima aponta para um número muito maior de pontos falsos, cujos valores estão na mesma faixa, dificulta muito a tarefa de identificar os pontos legítimos. Um adversário, que não conhece nenhum ponto legítimo (como não pode medir os sinais fisiológicos relevantes do corpo do hospedeiro), deve tentar cada um dos $v + 1$ 1 pontos em conjunto R para poder chegar ao polinômio correto. Da mesma forma, quanto mais o número de recursos que uma entidade está ciente, mais fácil é reconstruir o polinômio oculto, um fato explorado pelo receptor para abrir o cofre. A Fig. 2 mostra a força do cofre para diferentes valores de ordem polinomial usados para diferentes números de pontos de palha. A força do cofre é determinada pelo número de combinações que um adversário deve tentar para encontrar $v + 1$ 1 pontos legítimos no cofre. Para facilitar a compreensão, representamos esse requisito de computação em termos de sua equivalência em forçar brutalmente uma chave de um determinado comprimento (bits). Como esperado, aumentar o número de pontos de palha, aumenta a segurança

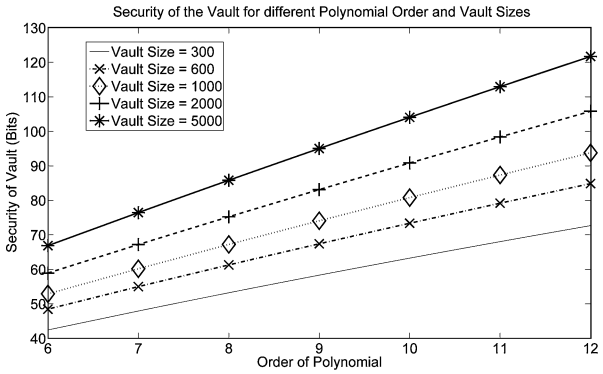

Fig. 2. Ordens polinomiais erradas da força do cofre para diferentes tamanhos de cofre.

fornecido pelo cofre. Quanto maior a ordem do polinômio, os recursos mais comuns que precisamos encontrar e, portanto, maior a segurança. Observe que o PSKA garante o desbloqueio bem-sucedido do cofre, desde que o número de recursos comuns no Q são maiores que v. Escolhendo a ordem do polinômio para um valor $|F_s \cap F_r| < v < |F_s \cap F_r|$, onde $|F_s \cap F_r|$ são as número de características comuns entre vetores de características de dois indivíduos diferentes e $|F_s \cap F_r|$ Como é o número de recursos comuns entre vetores de recursos para o mesmo indivíduo, podemos garantir o êxito do desbloqueio do cofre para o receptor, mas não para o adversário.

B. Segurança do Exchange

As fases de troca e reconhecimento de cofre tornam muito difícil para os adversários saberem a chave que está sendo acordada, pelas seguintes razões.

1) A presença de ID r na mensagem de troca do cofre informa os 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 o reconhecimento recebido seja em resposta à sua transmissão mais recente.
2) Se uma entidade mal-intencionada enviar uma mensagem de troca de cofre (repetindo trocas anteriores ou criando seu próprio cofre usando recursos fisiológicos antigos), ela será descartada por qualquer receptor, pois o MAC não corresponderá devido à diferença na Chave usada, dada a variação temporal das características fisiológicas.
3) O cofre possui muitas ordens de grandeza e número de pontos de palha comparados aos pontos legítimos (por exemplo, 1000 pontos de palha a 30 pontos de característica legítimos), o que dificulta aos adversários saber quais pontos são legítimos e quais não são (Como discutido anteriormente). Uma entidade mal-intencionada que não pode desbloquear o cofre não pode enviar uma confirmação válida, pois precisaria gerar um MAC válido sem a Chave.
4) Uma entidade maliciosa que tenta montar um ataque do tipo intermediário deve estar ciente dos recursos fisiológicos do sinal que estão sendo usados. Sem eles, qualquer modificação do cofre durante a troca seria capturada, pois nenhum dos ($|Q$ $v+1$) As teclas desbloqueadas pelo receptor verificarão o MAC.

QUADRO I
PSKA F EATURE- G ENERATION P ARAMETERS

Signal	Parameters	Values
PPG	Sampling	60 Hz
	Sampling Duration	12.8 secs
	FFT	256 points, 5 windows[a]
EKG	Sampling	125 Hz
	Sampling Duration	4 secs
	FFT	256 points, 2 windows[b]
PPG/EKG	Peak Value Quantization	5 bits
	Peak Index Quantization	8 bits
	Feature Length	13 bits

[a] First 32 points per window were concatenated together for peak-based feature generation.
[b] First 128 points per window were concatenated together for peak-based feature generation.

VI P ERFORMANCE DE PSKA

Validamos a abordagem do PSKA usando dois dos sinais fisiológicos mais comuns que podem ser coletados de uma pessoaPPG e ECG. O primeiro é o prazer da mudança volumétrica na distensão das artérias, devido à perfusão do sangue através delas durante um ciclo cardíaco, enquanto o segundo é a representação do ciclo cardíaco de um sujeito gerado pela atividade elétrica do coração. A base para a validação foi o cumprimento dos objetivos de projeto estabelecidos na Seção I. Começamos discutindo o procedimento de coleta de dados para nossos experimentos, seguido pela análise do desempenho dos dois sinais fisiológicos quando usados com PSKA.

A. Coleta de dados e extração de recursos

Os dados de PPG utilizados para nossa análise foram coletados de dez voluntários no Laboratório IMPACT. Usamos as placas de oxímetro de pulso da Smith Medical (http: //www.smithsoem. Com / applications / oxiboards.htm) para coletar os dados dos voluntários. Solicitou-se aos voluntários que se sentassem de pé, com as mãos firmemente colocadas em uma mesa; um sensor de oxímetro foi colocado no dedo indicador de cada mão. Assumimos, para os propósitos de nosso experimento, que os dois sensores de comunicação utilizam sinais medidos em cada dedo. Os dados foram coletados por 5 minutos de cada sujeito a uma taxa de amostragem de 60 Hz. Os dados do eletrocardiograma (para dez sujeitos, de duas derivações de cada pessoa), por outro lado, foram obtidos no banco de dados do PhysioBank (http://www.physionet.org/physiobank). Assumimos que os dois sensores de comunicação utilizam sinais de cada derivação para um acordo-chave. Cerca de 15 min de dados foram baixados para nossa análise, com os sinais amostrados em 125 Hz. A implementação e análise do PSKA foram feitas no MATLAB. A tabela I mostra os parâmetros de geração de recursos.

B. Resultados

Nesta seção, discutiremos os resultados obtidos para o PSKA quando usado com sinais PPG e EKG como o sinal fisiológico de escolha. Nosso objetivo é demonstrar que os resultados seguem as metas de design estabelecidas anteriormente.

1) Teclas longas e aleatórias: As chaves a serem acordadas são geradas pelo remetente na forma de coeficientes polinomiais usando um gerador de números pseudo-aleatórios. O comprimento e a aleatoriedade das chaves acordadas podem, portanto, ser garantidos.

TABELA II ESTATÍSTICAS DE RECURSOS DO PPG / ECG

Signal	Parameters	Values
PPG	Number of Iterations (1.6 s apart)	113
	Avg. Feature Vector Length	∼30
	Avg. # Common Features (Same Subject)	12
	Mode # of Features (Same Subject)	14.8
	Avg. # Common Features (Different Subjects)	2
	Mode # of Features (Different Subjects)	0.8
EKG	Number of Iterations (4 s apart)	180
	Avg. Feature Vector Length	∼87
	Avg. # Common Features (Same Subject)	24.7
	Mode # of Features (Same Subject)	25.2
	Avg. # Common Features (Different Subjects)	9.5
	Mode # of Features (Different Subjects)	8.1

2) Baixa latência: A duração da amostragem necessária para a concordância da chave segura depende do sinal fisiológico utilizado. Com o PPG (amostrado a 60 Hz), nossos melhores resultados foram obtidos com 12,8 s de dados. Enquanto no ECG (amostrado em 125 Hz), esse número caiu para 4 s de dados. Em geral, observamos que, quanto mais detalhados os dados disponíveis, menor a latência. Ambos os sinais superam o IPI, o que requer cerca de 30 s de dados.

3) Distinção: Um requisito importante do PSKA é que os sinais fisiológicos possam distinguir as pessoas. Isso garante que o cofre criado por um sensor em um BAN não possa ser desbloqueado por outro sensor localizado em outro assunto (acidental ou maliciosamente), com base nos recursos gerados a partir de suas medições. Portanto, o número de recursos comuns para sensores no mesmo assunto deve ser "signi fi cativamente" mais do que o número de recursos comuns para sensores no assunto diferente. Nossa definição de significante depende da ordem polinomial *v* usava. A Tabela II mostra as estatísticas observadas para os recursos quando o PSKA foi executado com base nos sinais PPG e EKG. A diferença entre o número de recursos comuns entre dois sensores no mesmo assunto e dois sensores em dois assuntos diferentes é significativa. Portanto, dada a estatística das diferenças no número de características comuns, agora podemos decidir os possíveis valores para *v*. A ordem polinomial deve ser tal que minimizemos tanto a *falso-positivo,* ou seja, o número de vezes que os recursos comuns entre duas pessoas o excedem e os *falsos negativos,* ou seja, o número de vezes que os recursos comuns para o mesmo assunto estão abaixo dele. A Fig. 3 mostra a porcentagem de falsos positivos e falsos negativos quando PPG e EKG são usados com PSKA para diferentes ordens de polinômios. Para PPG, as taxas de falso positivo e falso negativo são minimizadas quando a ordem do polinômio usado é 6 enquanto para o ECG, é 14) Esses resultados mostram que o uso de recursos derivados dos sinais PPG e EKG para gerar um cofre não oferece nenhuma vantagem significativa a um adversário, que usa recursos derivados de outro assunto, desde que uma ordem polinomial apropriada seja escolhida.

4) Variação Temporal: As Figs. 4 e 5 mostram a variação temporal dos recursos de sinal PPG e EKG, respectivamente. o *x*- eixo do gráfico é a diferença de tempo entre os tempos de início da medição PPG e ECG de duas iterações do PSKA, o *y*- eixo é a ordem polinomial usada, enquanto o *z*- eixo mostra o *violações médias,* que é a porcentagem de vezes que o número de características comuns entre a primeira e a segunda iterações do PSKA é maior que a ordem do polinômio usado.

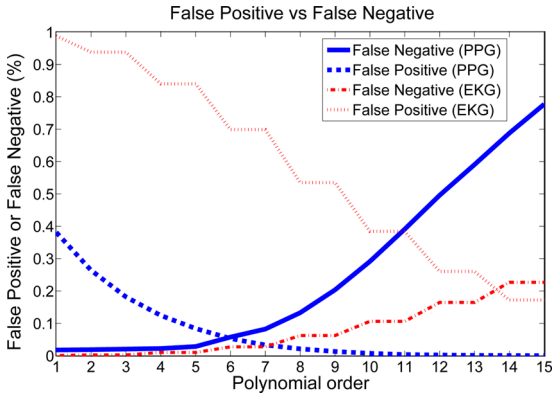

Fig. 3. Taxas de falso-positivo versus falso-negativo para ECG e PPG.

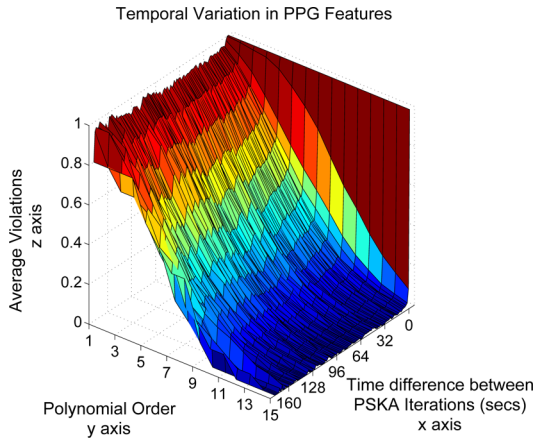

Fig. 4. Variação temporal nos recursos de PPG.

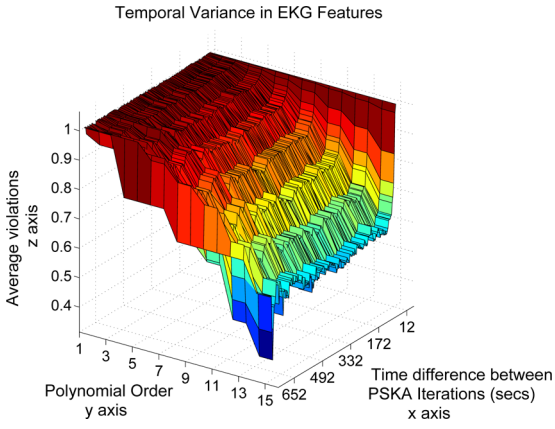

Fig. 5. Variação temporal nos recursos de eletrocardiograma.

(Consideramos mais de 100 horários aleatórios de início para o PPG e o ECG, em todos os dez indivíduos para calcular a violação média.) Como esperado, quando a diferença de tempo entre as duas iterações do PSKA para o PPG e o ECG é muito próxima, as violações são muito graves. Alto; já que os valores dos recursos nas duas iterações são muito semelhantes. No entanto, à medida que a diferença horária aumenta, as violações caem drasticamente para o PPG, chegando quase a zero nos primeiros segundos para polinômios de ordem 9 e acima. Para o eletrocardiograma, com seu maior número de picos comuns entre duas pessoas diferentes, a queda nas violações é mais gradual e

TABELA III
PSKA C C OST OMPUTACIONAL (EM C CLÍNICAS DE FECHAMENTO VGERAGE C), E IMPRESSÃO EM IMPRESSÃO

Signal	Entity	Key Gen	FFT	Feature Gen	Key Hide	Key Un-Hide	Total Cycles	Memory Footprint
PPG	Sender	9	1280	5112.2	31.95	-	6,433.15	47.35KB
	Recvr.	-	1280	5045.42	-	5454.38	11,779.80	45.3KB
EKG	Sender	12	512	22424.46	87.59	-	23,036.05	48.41KB
	Recvr.	-	512	22221.64	-	9789.28	32,522.92	46.31KB

não caia significativamente antes 14 polinômios de ordem th e diferença de tempo de cerca de 600 s entre duas iterações do PSKA. Por fim, como esperado para EKG e PPG, quanto maior a ordem do polinômio, maior o número de recursos comuns necessários e, portanto, menor a chance de violações. Assim, podemos ver que o PSKA atende a todos os nossos objetivos de design. O PSKA baseado em PPG requer uma ordem polinomial menor e mostra mais variação de tempo em comparação com o PSKA baseado em EKG. Curiosamente, os gráficos de variação temporal para ECG e PPG também ilustram o nível de sincronização necessário entre os sensores quando um deles é usado como sinal fisiológico de escolha. Vemos que, tanto para ECG quanto para PPG, as violações são mais altas quando a diferença de tempo entre as iterações é de cerca de 1 s, independentemente da ordem polinomial usada. Isso significa que os recursos medidos com 1 s de distância não foram alterados consideravelmente, permitindo assim o desbloqueio bem-sucedido do cofre. Podemos, portanto, dizer que, mesmo que os sensores de comunicação medam seus sinais fisiológicos para o PSKA com um segundo de diferença (ainda mais para o ECG), eles conseguirão concordar com uma chave comum.

VII P ROTOTYPE Eu MPLEMENTAÇÃO

Para estimar o custo e o desempenho do PSKA em hardware, o prototipamos usando uma linguagem de descrição de hardware de circuito integrado (VHDL) de velocidade muito alta. A ferramenta de software Altera Quartus foi usada emulando uma plataforma Stratix II (http://www.altera.com). Os detalhes da implementação não foram apresentados aqui por razões de espaço e podem ser encontrados em nosso artigo [16]. As métricas usadas para a avaliação são:

1) ciclos de clock da CPU e 2) área de cobertura da memória. A Tabela III mostra o custo computacional médio associado à nossa implementação do PSKA usando PPG e EKG. O custo é expresso em termos de ciclos de clock necessários para executar as várias tarefas do PSKA: 1) geração de coeficiente polinomial; 2) computação FFT; 3) geração de recursos; 4) ocultação de chaves (avaliação polinomial e geração de pontos de palha para o remetente); e 5) exibição de chave (interpolação lagrangiana). Os resultados foram calculados com a execução do PSKA em mais de 100 iterações, em horários aleatórios de início para cada um dos dez sujeitos, nos casos de ECG e PPG. Os ciclos de relógio necessários para a geração de recursos são ligeiramente diferentes para remetentes e receptores, devido à diferença no número de recursos observados em cada extremidade. $v + 1$ (v é a ordem polinomial) pontos de cada vez a partir do número total de recursos observados (Q) Além disso, o estágio de ocultação de chaves é mais barato, embora exija geração de chaff point e projeção polinomial de recursos, porque é executado em paralelo com a geração de recursos. Se feito sequencialmente, exigiria cerca de 3000 ciclos extras. Outra conseqüência desses resultados é que a execução do PSKA não afeta os requisitos de latência do objetivo do projeto. Se assumirmos um relógio de 8MHz [como a plataformaMote desenvolvida pela Crossbow, Inc., (http://www.xbow.com)]], o tempo necessário para executar uma iteração do PSKA seria de apenas alguns milissegundos. A Tabela III também mostra a pegada de memória da implementação do PSKA baseada em PPG e EKG. O componente principal desses valores de pegada são os pontos de palha (3000, 13 bits x- valores e 23 bits y- valores), características fisiológicas (valores de 13 bits, cerca de 30 para PPG e cerca de 85 para ECG) e suas projeções polinomiais (valores de 23 bits). A pegada de memória do PSKA baseado em EKG é maior que a do PSKA baseado em PPG, devido ao seu maior número de recursos.

Para colocar o desempenho do PSKA em perspectiva, o comparamos com a implementação dos protocolos de contratos principais DH e ECDH (DH) e curva elíptica na mesma plataforma usando VHDL. Para DH, usamos módulo de 1024 bits e expoente de 160 bits, o que equivale a 80 bits de segurança na criptografia simétrica, enquanto que para ECDH, usamos uma chave pública de 163 bits, como em [15]. O custo computacional e a pegada de memória são idênticos para remetentes e receptores no DH e no ECDH. Encontramos DH que realiza 327.680 ciclos, cerca de dez vezes o número de ciclos de clock que o PSKA, principalmente porque requer exponenciação de grandes números. O protocolo ECDH leva apenas 135 456 ciclos de clock, o que é muito mais barato que o DH, mas ainda utiliza mais ciclos computacionais que o PSKA, devido às suas multiplicações e adições de curvas elípticas. A área de cobertura da memória para os protocolos DH (7 KB) e ECDH (2,5 KB) é muito menor que a dos PSKAb, porque eles não exigem o armazenamento de nenhum recurso ou ponto de palha. Note-se que ambos os protocolos DH não fornecem nenhuma forma de autenticação [17]. Um determinado sensor pode, portanto, concordar potencialmente com uma chave com qualquer entidade (maliciosa ou não). Portanto, qualquer execução dos protocolos DH deve ser precedida por um protocolo de autenticação, o que aumentará ainda mais sua sobrecarga. Com o PSKA, a autenticação é incorporada, devido à propriedade distintiva do esquema. Portanto, afirmamos que é viável implementar o PSKA para permitir segurança utilizável nos BANs. Note-se que ambos os protocolos DH não fornecem nenhuma forma de autenticação [17]. Um determinado sensor pode, portanto, concordar potencialmente com uma chave com qualquer entidade (maliciosa ou não). Portanto, qualquer execução dos protocolos DH deve ser precedida por um protocolo de autenticação, o que aumentará ainda mais sua sobrecarga. Com o PSKA, a autenticação é incorporada, devido à propriedade distintiva do esquema. Portanto, afirmamos que é viável implementar o PSKA para permitir segurança utilizável nos BANs. Note-se que ambos os protocolos DH não fornecem nenhuma forma de autenticação [17]. Um determinado sensor pode, portanto, concordar potencialmente com uma chave com qualquer entidade (maliciosa ou não). Portanto, qualquer execução dos protocolos DH deve ser precedida por um protocolo de autenticação, o que aumentará ainda mai

VIII R EXALTADO W ORK

Em nosso trabalho preliminar [2], apresentamos o PSKA baseado em PPG para um acordo-chave. No entanto, o trabalho teve escopo limitado e não incluiu a execução do PSKA usando EKG, análise comparativa entre implementações baseadas em EKG e PPG do PSKA e um estudo do custo de implementação do PSKA. O uso do eletrocardiograma diretamente para a geração de chaves foi estudado por nós em [9]. No entanto, mais tarde descobriu-se que a maneira como os recursos foram extraídos durante o processo tendia a distorcer o sinal original

consideravelmente e, portanto, não era um caminho sólido para a geração de chaves. Bui e Hatzinakos [18] apresentam uma abordagem para comunicações seguras em BANs, que usa sinais IPI e códigos de correção de erros para chegar à chave comum. No entanto, a escolha de recursos no domínio do tempo os torna suscetíveis a problemas de sincronização e reordenação / introdução de recursos.

Até agora, o esquema de cofre difuso foi aplicado principalmente à autenticação baseada em biometria, como impressões digitais [10] e imagens de íris [19]. No entanto, o gabarito biométrico não variante abre o cofre nebuloso para ataques que envolvem modificação do gabarito [20]. Da mesma forma, Kholmatov e Yanikoglu [21] apresentam um ataque em que o atacante intercepta dois cofres gerados a partir dos mesmos dados biométricos (impressão digital) com diferentes pontos de entulho e os correlaciona para revelar os recursos biométricos ocultos. Ambos os ataques são bem-sucedidos porque os recursos de impressão digital nos cofres não são alterados. Esses ataques não são possíveis com o PSKA, porque os valores dos recursos nos cofres fuzzy gerados em duas iterações do PSKA são drasticamente diferentes devido à propriedade de variação temporal dos sinais fisiológicos utilizados.

v para 8 *v* registro 2 *v* (| *R* | / | *N* |) *v*. A conseqüência desse resultado é que, com uma probabilidade próxima a 1, a complexidade de identificar o polinômio usado pelo cofre diminui. Usando nossos parâmetros para PPG, o PSKA agora é tão seguro quanto forçar brutalmente uma chave de 75 bits em vez da chave original de 95 bits, que ainda é bastante forte. O sinal do eletrocardiograma fornece de maneira semelhante uma segurança de cerca de 80 bits. Nos dois casos, se aumentarmos o número de pontos de palha, podemos aumentar novamente a complexidade de quebrar o cofre.

IX C ONCLUSÃO

Neste artigo, apresentamos um esquema de contrato-chave utilizável e seguro para os BANs chamado PPSKA. Ele permite que dois sensores concordem com uma chave compartilhada, de maneira autenticada, sem qualquer forma de inicialização ou configuração. A implantação simples dos sensores é suficiente para permitir que eles concordem com uma chave comum, de maneira transparente. A análise de segurança do protocolo PSKA mostrou que os sinais fisiológicos atendem aos objetivos do projeto para os principais acordos, a saber: *comprimento e aleatoriedade, baixa latência,* e *distinção.* Analisamos o desempenho e o custo do uso do protocolo PSKA ao prototipá-lo em VHDL e concluímos que o PSKA é uma abordagem viável para garantir um acordo-chave nos BANs. Uma descoberta recente sobre a sustentabilidade das técnicas de eliminação de energia do PSKAvia do corpo humano [23] também apóia sua viabilidade. Trabalhos futuros incluem um estudo de campo expandido do PSKA para entender melhor as propriedades de distinção e variação temporal do esquema. A discussão detalhada de muitas das questões deste artigo pode ser encontrada na versão estendida deste artigo em http://impact.asu.edu/pub.html.

UMA AGRADECIMENTO

Os autores gostariam de agradecer ao editor da área Dr. W. Wu e aos revisores anônimos por suas sugestões úteis.

R EFERÊNCIAS

[1] L. Schwiebert, SK Gupta e J. Weinmann, “Desafios da pesquisa em redes sem fio de sensores biomédicos ", em *Proc. 7th Int. Conf. Computação móvel. Netw. (MobiCom 2001),* Roma, Itália, pp. 151-165. [2] K. Venkatasubramanian, A. Banerjee e SKS Gupta, "Comunicação segura entre sensores baseada em pletismograma em redes de área corporal", em *Proc. IEEE Military Commun. Conf.,* Novembro de 2008, pp. 1-7. [3] F. Adelstein, SKS Gupta, GG Richard e L. Schwiebert, *Fundamentes da Computação Móvel e Pervasiva.* Nova York: McGraw-Hill, 2005.

[4] S. Zhu, S. Setia e S. Jajodia, “LEAP +: mecanismos de segurança eficientes para redes de sensores distribuídos em larga escala " *ACM Trans. Sens. Netw. (TOSN),* vol. 2, n. 4, pp. 500-528, novembro de 2006. [5] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai e SKS Gupta, “Ayushman: uma infraestrutura de monitoramento de saúde sem fio baseada em rede e banco de testes", em *Proc. IEEE Int. Conf. Distrib. Comput. Sens. Syst.,* Jun. 2005, pp. 406-407. [6] K. Venkatasubramanian e SKS Gupta, “Valor fisiológico baseado soluções de segurança úteis e eficazes para redes de sensores corporais ” *ACMTrans. Sens. Netw. (TOSN),* a ser publicado. [7] BJ West, "Estudos de fenômenos não lineares nas ciências da vida", em *Onde A medicina deu errado: redescobrindo o caminho para a complexidade 11.* Pecadogapore: World Scienti fi c, 2006. [8] A. Juels e M. Sudan, “Um esquema de cofre difuso”, em *Proc. IEEE Int. Symp. Inf. Teoria,* 2002, p. 408

[9] K. Venkatasubramanian, A. Banerjee e SKS Gupta, “EKG-based acordo chave nas redes de sensores corporais " *Proc. 2º Workshop Mission Crit. Rede,* Abril de 2008, pp. 1-6.

[10] U. Uludag, S. Pankanti e AK Jain, "Cofre difuso para impressões digitais", no *Proc. Autenticação biométrica de pessoa baseada em áudio e vídeo,* Jul. 2005, pp. 310–319.

[11] S. Cherukuri, K. Venkatasubramanian e SKS Gupta, “BioSec: Uma abordagem biométrica para garantir a comunicação em redes sem fio de biossensores implantados no corpo humano ”, em *Proc. Workshop sobre privacidade de segurança sem fio,* Outubro de 2003, pp. 432–439

[12] CCY Poon, Y.-T. Zhang e S.-D. Bao, “Uma nova biometria método para proteger redes de sensores de área corporal sem fio para telemedicina e saúde M ", *IEEE Commun. Mag.,* vol. 44, n. 4, pp. 73–81, abr. 2006.

[13] J. Elson, L. Girod e D. Estrin, “Sincronização de tempo de rede de granulação fina usando difusões de referência ", em *Proc. 5th Symp. Oper. Syst. Des. Implementação,* 2002, pp. 147-163.

[14] A. Juels e M. Wattenberg, "Um esquema de compromisso nebuloso", em *Proc. 9ª Conf. ACM Comput. Comum. Segurança,* Nov. 1999, pp. 28–36. [15] DJ Malan, M. Welsh e MD Smith, “Uma infraestrutura de chave pública distribuição de chaves no TinyOS com base na criptografia de curva elíptica ” *Proc. IEEE 2ª Int. Conf. Sens. Ad Hoc Commun. Rede,* Outubro de 2004, pp. 71–80.

[16] A. Banerjee, K. Venkatasubramanian e SKS Gupta, “Desafios da implementação de soluções de segurança ciber-física em redes de área corporal ”, apresentado no 4º Int. Conf. Body Area Netw., Los Angeles, Califórnia, abr. 2009.

[17] AJ Menezes, PC van Oorschot e SA Vanstone, *Manual de Criptografia Aplicada.* Boca Raton, FL: CRC Press, outubro de 1996. [18] FM Bui e D. Hatzinakos, “Métodos biométricos para comunicação segura em redes de sensores corporais: gerenciamento de chaves com eficiência de recursos e embaralhamento de dados no nível do sinal ” *Proc. EURASIP J. Adv. Processo de sinal.,* 2008, pp. 1-16.

[19] ES Reddy e IR Babu, “Autenticação usando vault fuzzy baseado em íris texturas " *Proc. 2nd Asia Int. Conf. Modelo. Simul.,* 2008, pp. 361–368.

[20] WJ Scheirer e TE Boult, “Quebrando cofres difusos e biométricos criptografia " *Proc. Biometrics Symp.,* Setembro de 2007, pp. 1-6. [21] A. Kholmatov e B. Yanikoglu, “Realização do ataque de correlação contra o esquema do cofre difuso " *SPIE Segurança, Forense, Esteganografia e Marca D'água de Conteúdo Multimídia X,* vol. 6819, pp. 1-7, janeiro de 2008.

[22] P. Mihailescu. (Agosto de 2007). O cofre nebuloso para impressões digitais é vulnerável ataque de força bruta. O repositório de pesquisa em computação. [Conectados]. Disponível: http://www.citebase.org/abstract?id=oai:arXiv.org/0708.2974 [23] K. Venkatasubramanian, A. Banerjee e SKS Gupta, “Green and soluções ciber-físicas sustentáveis para redes de área corporal ”, em *Proc. 6ª Int. Sensível ao corpo implantável na oficina Sens. Netw. (BSN 2009),* Washington, DC, pp. 240-245.

Krishna K. Venkatasubramanian (S'06 – M'10) recebeu o bacharelado em ciência da computação da Webster University, St. Louis, MO, e os mestres e doutores. graduado em ciência da computação pela Arizona State University, Tempe.

Atualmente, é pesquisador de pós-doutorado no Departamento de Ciência da Computação e Informação da Universidade da Pensilvânia, Filadélfia. Seus interesses de pesquisa incluem sistemas ciber-físicos seguros, redes de área corporal, gerenciamento de confiança e segurança de dispositivos médicos. Sua lista de publicações está disponível

disponível em http://www.seas.upenn.edu/ ~ vkris /

Dr. Venkatasubramanian é membro da Association for Computing Machinery.

Ayan Banerjee recebeu o diploma de BE em engenharia eletrônica e de telecomunicações da Universidade de Jadavpur, Kolkata, Índia. Atualmente, ele trabalha para o doutorado. formado pela Escola de Computação, Informática e Engenharia de Sistemas de Decisão, Arizona State University, Tempe.

Desde o outono de 2007, ele trabalha no Laboratório de Tecnologias Inteligentes para Aplicações Móveis e Pervasivas e Tecnologias de Computação da Universidade Estadual do Arizona. Seus interesses atuais de pesquisa incluem segurança e proteção de sistemas ciber-físicos.

Sandeep Kumar S. Gupta (S'93 – M'95 – SM'00) recebeu o diploma de B.Tech em ciência da computação e engenharia (CSE) do Instituto de Tecnologia da Universidade Hindu de Banaras, Varanasi, Índia,
M.Tech. Bacharel em CSE pelo Indian Institute of Technology, Kanpur, Índia, e MS e Ph.D. Licenciatura em Ciência da Computação e Informação pela Universidade Estadual de Ohio, Columbus.

Atualmente, é professor da Escola de Engenharia de Computação, Informática e Sistemas de Decisão da Universidade Estadual do Arizona, Tempe, onde chefia o Laboratório IMPACT. Seus interesses atuais de pesquisa incluem sistemas distribuídos adaptáveis, confiáveis e com consciência da crítica, com ênfase em redes de sensores sem fio, computação e comunicação com consciência térmica e de energia e assistência médica abrangente. Ele co-autor do livro *Fundamentos da Computação Móvel e Pervasiva (* McGraw Hill). Ele é membro do conselho editorial das Cartas de Comunicação do IEEE, das Transferências do IEEE SOBRE SISTEMAS DE P ARALLEL E D ISTRIBUÍDOS e *Redes sem fio da Springer.*

Dr. Gupta é membro da Association for Computing Machinery.