Método de biometria ANovel para proteger redes de sensores de área corporal sem fio para telemedicina e saúde

Artigo *dentro* IEEE Communications Magazine · Maio de 2006

DOI: 10.1109 / MCOM.2006.1632652 · Fonte: IEEE Xplore

3 autores , Incluindo:

Carmen CY Poon
Universidade Chinesa de Hong Kong
118 PUBLICAÇÕES **3.930** CITAÇÕES

VER PERFIL

Yuan-Ting Zhang
Universidade Chinesa de Hong Kong
422 PUBLICAÇÕES **10.473** CITAÇÕES

VER PERFIL

Um novo método biométrico para proteger redes de sensores sem fio da área corporal para telemedicina e M-Health

Carmen CY Poon e Yuan-Ting Zhang, Universidade Chinesa de Hong Kong Shu-Di Bao,
Universidade Chinesa de Hong Kong e Universidade do Sudeste

UMA BSTRACT

O desenvolvimento da rede de sensores de área corporal sem fio (BASN) é imperativo para a telemedicina moderna e a saúde móvel, mas a segurança continua sendo um desafio formidável ainda a ser resolvido. Como se espera que os nós do BASN estejam interconectados no corpo humano, o próprio corpo pode formar uma via de comunicação inerentemente segura que não está disponível para todos os outros tipos de redes sem fio. Este artigo explora o uso desse conduíte no mecanismo de segurança do BASN; isto é, por uma abordagem biométrica que usa uma característica intrínseca do corpo humano como a identidade de autenticação ou o meio de garantir a distribuição de uma chave de cifra para proteger as comunicações entre BASN. O método foi testado em 99 indivíduos com 838 segmentos de registros simultâneos de eletrocardiograma e fotopletismograma. Usando o intervalo interpulso (IPI) como característica biométrica, o sistema atingiu uma taxa de erro total mínima de 2,58 por cento quando os IPIs medidos a partir de sinais, que foram amostrados em 1000 Hz, foram codificados em sequências binárias de 128 bits. O estudo abre algumas questões-chave para investigações futuras, incluindo esquemas de compensação para a assincronia de diferentes canais, esquemas de codificação e outras características biométricas adequadas.

Eu NTRODUÇÃO

Quando a telemedicina foi proposta pela primeira vez no início dos anos 1970, sua função era frequentemente limitada, por exemplo, a pacientes que procuravam consulta médica [1]. Hoje em dia, a implicação da palavra telemedicina foi ampliada para o uso de tecnologia de telecomunicações para fornecer informações e serviços médicos para uma infinidade de finalidades, como diagnóstico de doenças, transferência de dados e registros médicos, monitoramento de processos de reabilitação ou tratamento, e até mesmo conduzindo operações cirúrgicas. Mais recentemente, surgiu outra noção que representa a evolução da plataforma de telemedicina tradicional de desktop formulários para simplesmente a prática da medicina para configurações sem fio e móveis para a prestação de serviços médicos e de saúde. Isso é conhecido como saúde móvel ou saúde m [2].

O surgimento do m-health pode ser creditado ao desenvolvimento de dois Ws: dispositivos médicos vestíveis e redes de comunicação sem fio. Dispositivos médicos vestíveis são desenvolvidos com o objetivo de coletar dados médicos de indivíduos de maneira discreta e onipresente, 24 horas por dia, sem interromper suas vidas diárias normais, quando anteriormente apenas dados intermitentes podiam ser coletados durante suas visitas irregulares a clínicas ou hospitais. Por outro lado, os avanços na tecnologia de comunicações sem fio superaram a maioria das barreiras geográficas, temporais e até organizacionais para facilitar uma forma totalmente móvel de transferência de dados e registros médicos [3]. Para utilizar totalmente a tecnologia sem fio em telemedicina e m-health, o verdadeiro desafio está na necessidade de desenvolver outro tipo de rede de área sem fio:

W IRELESS B ODY UMA REA S ENSOR N ETWORKS PARA T ELEMEDICINA E MH EALTH

O desenvolvimento do BASN é derivado do recente desenvolvimento da rede de área corporal (BAN), que é um sistema que interconecta dispositivos ou sensores *usado em* ou *implantado em*
o corpo humano para compartilhar informações e recursos entre os dispositivos. Embora o BASN e o BAN possam parecer muito semelhantes um ao outro, a descrição do BASN é definitivamente preferida quando se refere ao tipo de BAN em telemedicina e m-health onde cada nó compreende um biossensor ou um dispositivo médico com uma unidade de detecção . Resumindo, o BASN também é denominado rede de sensores corporais (BSN).

O BAN foi inicialmente proposto para conectar dispositivos eletrônicos pessoais de consumo para o

0163-6804 / 06 / $ 20,00 © 2006 IEEE

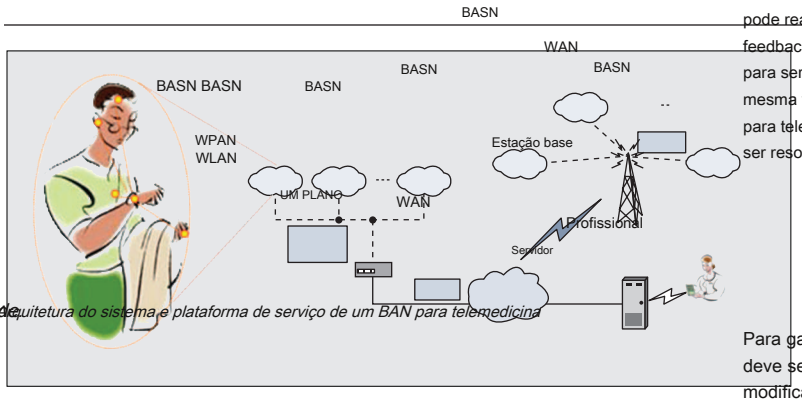

Figura 1. *Arquitetura do sistema e plataforma de serviço de um BAN para telemedicina*

por conveniência para o usuário; no entanto, é considerado praticamente essencial em telemedicina e m-health porque vários sensores colocados em diferentes partes do corpo são frequentemente necessários no caso de muitos pacientes que precisam de coleta contínua e de longo prazo de dados médicos. Isso dá pelo menos duas razões para a criação de um BASN. O primeiro é otimizar o uso de recursos a fim de satisfazer as restrições estritas dos terminais. Por exemplo, dados médicos coletados de diferentes sensores podem ser centralizados antes de serem transmitidos a redes externas para análise, diagnóstico ou tratamento remoto. Em segundo lugar, um BASN aprimora o controle, a programação e a programação de todo o sistema, de modo que seja adaptável à condição corporal e ao ambiente externo. Por exemplo, alguns nós de um BASN podem ter que ser reprogramados de tempos em tempos (por exemplo, um dispositivo para administração de drogas). Em suma, a necessidade de desenvolver o BASN é impulsionada pelo aumento no número de biossensores vestíveis ou implantados a serem colocados nos usuários.

O desenvolvimento do BAN / BASN para telemedicina e m-health está apenas em um estágio inicial. Até o momento, o desenvolvimento tem se concentrado na construção da arquitetura do sistema e da plataforma de serviço, conforme ilustrado na Fig. 1.

Por exemplo, no projeto MobiHealth, Knostantas *et al. [* 4] surgiu com um protótipo BAN inicial integrando tecnologias existentes. O protótipo foi testado em nove ensaios clínicos de diferentes casos de saúde, incluindo monitoramento de pacientes com arritmia cardíaca e insuficiência respiratória. Tecnologias sem fio como Blue tooth e Zigbee foram usadas para comunicações inter-BAN, mas para comunicação com redes externas foram usadas tecnologias como General Packet Radio Service (GPRS) ou Universal Mobile Telecommunations System (UMTS). Os autores concluíram que já haviam definido claramente todos os componentes da arquitetura da plataforma de serviço que propuseram no artigo. No entanto, eles descobriram que se apenas as tecnologias atuais fossem usadas, nem todos os problemas poderiam ser superados. Um exemplo típico é o desafio essencial, mas árduo, relacionado à segurança,

Outro grupo de pesquisadores líderes nesta área [5] relatou recentemente o uso de sensores de movimento sem fio disponíveis no mercado para projetar um protótipo de BAN sem fio para reabilitação física assistida por computador. O protótipo apresentava um rádio compatível com ZigBee padrão e um conjunto comum

de sensores fisiológicos, cinéticos e ambientais. Em seu artigo, eles também introduziram um sistema de telemedicina multicamadas que pode realizar análises em tempo real de dados médicos, fornecer feedback e mensagens de advertência ao usuário e transferir dados para servidores médicos. Coincidentemente, eles compartilhavam a mesma visão de que os problemas de segurança do uso de um BAN para telemedicina continuavam sendo um desafio formidável ainda a ser resolvido.

S ECURIDADE C DESAFIOS E B IOMETRICS

Para garantir a segurança do sistema geral, o BAN / BASN deve ser protegido, por exemplo, contra espionagem, injeção e modificação de pacotes. Questões de segurança em BANs / BASNs para telemedicina e m-health são particularmente importantes porque informações médicas confidenciais devem ser protegidas contra uso não autorizado para vantagem pessoal e atos fraudulentos que podem ser perigosos para a vida de um usuário (por exemplo, alteração das configurações do sistema, dosagens de medicamentos , ou procedimentos de tratamento). Embora as questões de segurança em redes sejam sempre consideradas prioritárias, os estudos realizados nesta área para BANs / BASNs foram poucos. O trabalho muito limitado encontrado nesta área não é aplicável ao BASN em telemedicina e m-health porque os biossensores em um BASN devem operar com restrições extremamente rigorosas, um requisito que era relativamente relaxado em BANs genéricos.

Menos ameaçador do que os problemas de espionagem e adulteração, mas tão importante, é evitar a interferência entre os BASNs de diferentes indivíduos, porque as comunicações dos BASNs podem cruzar-se facilmente quando muitas pessoas tiverem seus próprios BASNs no futuro. Portanto, o problema de anti-interferência também deve ser cuidado no desenvolvimento de um BASN. Mesmo que os dois desafios pareçam não ter relação entre si, os problemas podem convergir para uma pergunta simples: como os sensores ou nós de um BASN podem saber que pertencem ao mesmo indivíduo?

Neste artigo pretendemos apresentar e investigar o desempenho do sistema de uma nova solução biométrica para esta questão. A biometria é uma técnica comumente conhecida como identificação automática ou verificação de um indivíduo por suas características fisiológicas ou comportamentais. Para ser um sistema biométrico prático, postula-se que as características utilizadas devem ser [6]:

- Universal: possuído pela maioria, senão por toda a população
- Distinto: suficientemente diferente em quaisquer dois indivíduos
- Permanente: suficientemente invariável, no que diz respeito ao critério de correspondência, ao longo de um período de tempo razoável
- Coletável: facilmente coletado e medido quantitativamente
- Eficaz: produz um sistema biométrico com bom desempenho; isto é, dados recursos limitados em termos de consumo de energia, complexidade de computação e armazenamento de memória

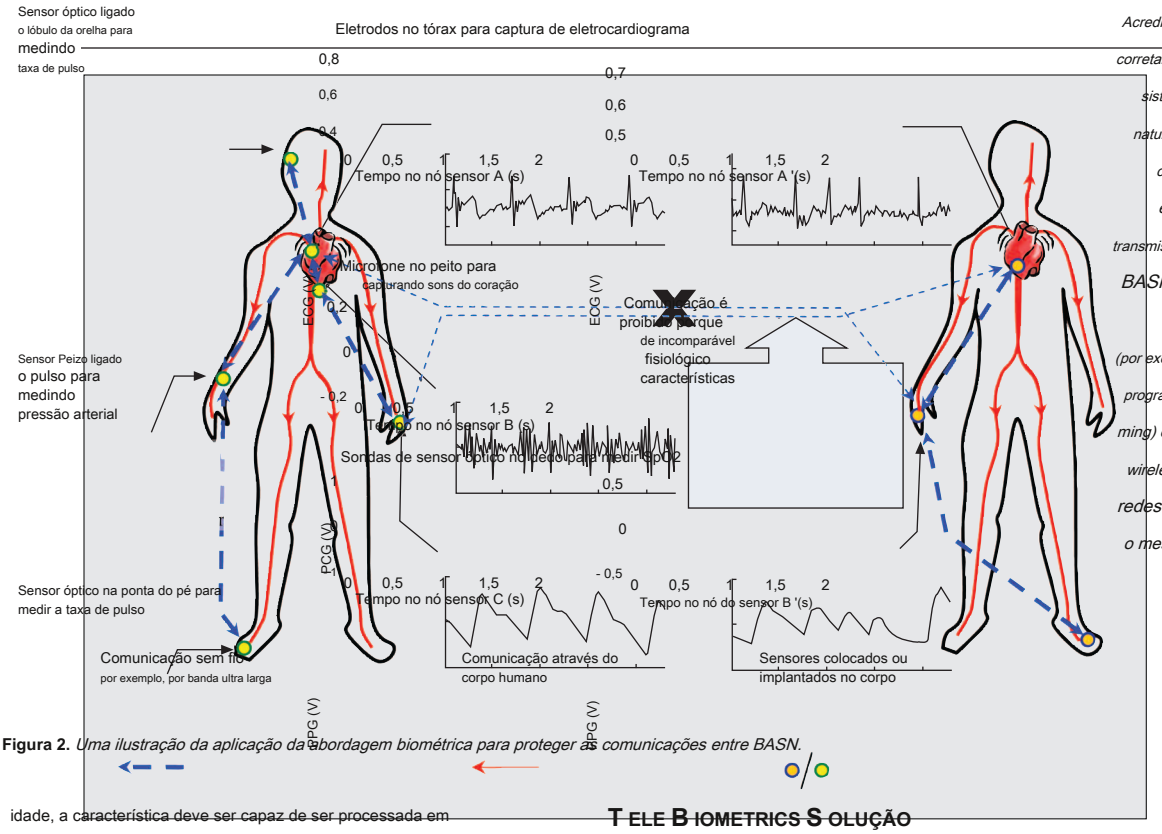

Figura 2. *Uma ilustração da aplicação da abordagem biométrica para proteger as comunicações entre BASN.*

idade, a característica deve ser capaz de ser processada em uma velocidade rápida com precisão reconhecida

- Aceitável: disposição do público em geral para usar como um identificador
- Invulnerável: relativamente difícil de reproduzir, de modo que o sistema biométrico não seria facilmente contornado por atos fraudulentos

Em vez de aplicar a biometria geralmente na autenticação do usuário de criptossistemas comuns, pretendemos desenvolver uma técnica que autenticaria os nós sensores e / ou protegeria a transmissão da chave de criptografia entre eles no BASN. Conforme ilustrado na Fig. 2, uma vez que o corpo humano é fisiológica e biologicamente bem conhecido por consistir em seus próprios sistemas de transmissão ou transporte (por exemplo, o sistema de circulação sanguínea), gostaríamos de investigar como fazer uso de essas vias de comunicação protegidas estão disponíveis especificamente no BASN, mas não em outras redes sem fio. Acredita-se que, se usados corretamente, esses sistemas podem ser conduítes naturalmente protegidos para transmissão de informações dentro de um BASN, onde outras técnicas (por exemplo, programação de hardware ou software) devem ser usadas em redes sem fio genéricas para atingir o mesmo propósito.

A ideia é particularmente prática em proteger o BASN com uma aplicação de telemedicina ou m-Health, pois os nós desses BASN já incluiriam biossensores para coletar dados médicos, que poderiam ser características fisiológicas que representam exclusivamente um indivíduo. Se essas características intrínsecas podem ser usadas para verificar se dois sensores pertencem ao mesmo indivíduo, os múltiplos usos dos sinais fisiológicos registrados irão certamente economizar recursos enquanto medidas de segurança adequadas são empregadas.

T ELE B IOMETRICS S OLUÇÃO

A técnica é desenvolvida com base em um criptosistema simétrico, que assume que um esquema de distribuição de chaves robusto e seguro está disponível. A este respeito, Cherukuri *et al. [*7] proposto usando um grupo de números aleatórios semelhantes gerados a partir das propriedades do corpo humano em locais diferentes (ou seja, uma característica biométrica) para criptografar e descriptografar a chave simétrica para distribuição segura dela. Uma vez que a característica biométrica capturada em diferentes locais do corpo deve ter pequenas variações, eles empregaram um esquema de comprometimento fuzzy [8] para garantir que os erros em uma chave de criptografia recuperada possam ser toleráveis até certo grau. No terminal de transmissão, o traço biométrico (*b)* estava acostumado a

comprometa a chave (*k),* diga, usando $f_{comprometer}(k, b) =$ (*hash (k) || b* $\oplus$ *k),* Onde $\oplus$ é o XOR bit a bit operação e || significa concatenação. No terminal receptor, o outro biossensor capturaria sua própria cópia da característica, uma versão variante *b (b '*), e use-o para descomprimir a chave *k.* Se a característica selecionada for única o suficiente para representar um indivíduo, a chave de criptografia só deve ser recuperada pela característica obtida do mesmo indivíduo. Por outro lado, como a característica biométrica é usada para criptografar a chave simétrica, uma grande preocupação seria se seu grau de aleatoriedade é suficiente para fins criptográficos. A aleatoriedade insuficiente abriria a possibilidade para os invasores adivinharem a característica codificada e, assim, obter a chave de criptografia para descriptografar os dados médicos confidenciais. Cherukuri *et al. [*7] sugeriu o uso de parâmetros fisiológicos com níveis mais altos de entropia (por exemplo, glicose no sangue, pressão arterial e temperatura). Segundo eles, a frequência cardíaca não é uma boa escolha porque

Acredita-se que, se usados corretamente, esses sistemas podem ser naturalmente seguro conduítes para em formação transmissão dentro de um BASN, onde outro técnicas (por exemplo, por hardware ou programa de software ming) deve ser usado em wireless genérico redes para alcançar o mesmo propósito.

Se estes forem intrínsecos características podem ser usado para verificar se dois sensores pertencem ao mesmo indivíduo, o múltiplos usos de o gravado sinais fisiológicos certamente salvará recursos enquanto segurança adequada medidas são empregado.

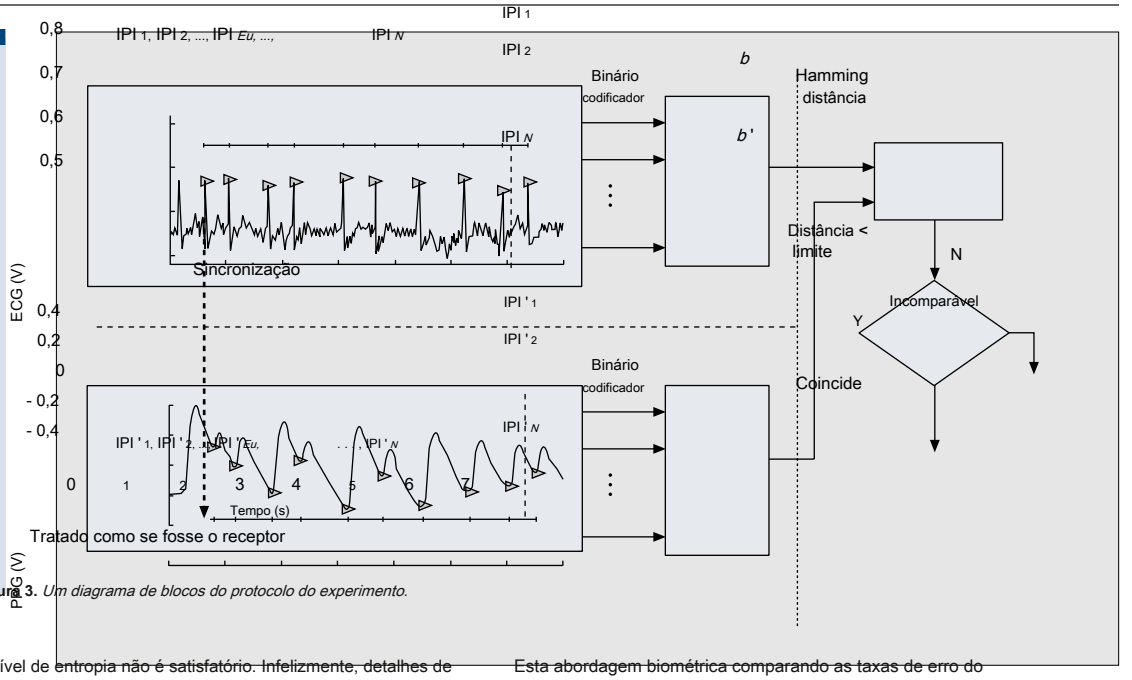

Figura 3. *Um diagrama de blocos do protocolo do experimento.*

seu nível de entropia não é satisfatório. Infelizmente, detalhes de seu trabalho não foram encontrados.

Em nossos estudos, no entanto, demonstramos que usar as informações de tempo dos batimentos cardíacos pode, de fato, ser uma excelente característica biométrica para proteger o BASN. Conforme demonstrado pelo teste Qui-quadrado e medição da entropia, verifica-se que um traço biométrico gerado a partir de uma sequência de intervalo interpulso (IPI) possui um alto nível de aleatoriedade. Este achado também é apoiado pela natureza caótica da variabilidade da frequência cardíaca relatada na literatura [9]. Com base no esquema de compromisso difuso [8] e no esquema de transmissão de chave segura em [7], alguns de nós, Bao *et al.*

[10], surgiu com um criptosistema simétrico específico para BASN, que também considerou a geração da chave de criptografia *k* de sinais fisiológicos e avaliação de aleatoriedade de *k.*

Para este fim, a ligação do traço biométrico com a chave de criptografia pode ser alcançada por alguns algoritmos existentes de integração biométrica em criptosistemas [6]. Esta solução biométrica é adequada para proteger BASN em telemedicina e m-Health porque um nível de segurança mais alto pode ser alcançado com menos computação e requerimento de memória quando comparado com os criptossistemas genéricos.

Além de proteger a transmissão da chave de criptografia dentro dos nós de um BASN, o traço biométrico também pode ser usado como uma identidade para autenticação de entidade (ou seja, autenticação nó a nó) em um BASN, conforme proposto por Bao *et al.* em [11]. Nesse artigo, um possível protocolo de comunicação de duas sessões foi discutido em que o servidor iniciava enviando *b* junto com um nonce para o cliente para comparação, e se *b* coincide *b ′*, o cliente respondeu enviando de volta o nonce junto com *b ′*. Um caminho de comunicação só seria estabelecido se o servidor e o cliente descobrissem que a cópia recebida (*b ′* / *b)* corresponde à cópia que tem em mãos (*b* / *b ′*).

Neste estudo, avaliamos ainda mais o desempenho Esta abordagem biométrica comparando as taxas de erro do sistema operacional biométrico sob diferentes condições (ou seja, quando diferentes comprimentos de bit foram usados ou os sinais foram amostrados em taxas diferentes).

E XPERIMENTAL T ESTING E R ESULTS

Utilizamos dados coletados previamente em dois experimentos, cujo objetivo original era capturar simultaneamente dados de eletrocardiograma (ECG) e fotopletismograma (PPG) para a estimativa da pressão arterial. Os circuitos internos foram projetados para capturar ECG e PPG por meio de eletrodos de aço inoxidável e sensores ópticos infravermelhos. Em um experimento, 14 indivíduos saudáveis foram recrutados e dois PPGs capturados dos dedos indicadores das duas mãos de cada indivíduo, e um ECG capturado de três dedos dos indivíduos foram registrados simultaneamente por 2-3 min. Em outro experimento [12], 85 indivíduos foram recrutados e, em um período de 2 meses, ECG e PPG foram capturados por 2-3 minutos em 3/4 dias. ECG e PPG foram amostrados em 1000 Hz. Um algoritmo foi desenvolvido para marcar o pico da onda R do ECG e a base do pulso do PPG.

Dividimos os pares de ECG e PPG em segmentos de forma que o segmento de ECG correspondente contivesse exatamente 68 ondas R (resultando em 67 IPIs). Um total de 838 segmentos de dados foi obtido dos 99 indivíduos. Conforme mostrado na Fig.
3, IPIs foram obtidos independente dos diferentes sinais fisiológicos, e a sequência de IPIs em um segmento foi codificada em uma sequência binária *b* de 128 bits. Uma vez que a distância de Hamming foi usada para avaliar a dissimilaridade entre duas sequências binárias *b* e *b ′*, o método de codificação foi cuidadosamente selecionado de modo que a distância de Hamming dos códigos binários correspondentes a quaisquer dois IPIs semelhantes seriam

pequeno. Duas sequências binárias só seriam consideradas "combinadas" se a distância de Hamming fosse menor que um limite. Idealmente, b e b' deve corresponder apenas se eles foram registrados pela mesma pessoa durante o mesmo período de tempo.

Semelhante aos sistemas de verificação biométrica genéricos, avaliamos o desempenho da abordagem biométrica proposta por dois tipos de erros:

- Taxa de rejeição falsa (FRR), cuja taxa b e b' medidos pela mesma pessoa durante o mesmo período de tempo eram incomparáveis (ou seja, correspondendo a um nó no mesmo BASN sendo rejeitado pelo nó de julgamento)

- Taxa de aceitação falsa (FAR), cuja taxa b coincide b' medido de uma pessoa diferente ou em um momento diferente (ou seja, correspondendo a um nó de outro BASN ou um impostor sendo aceito como um nó legal)

Além das condições estabelecidas acima, investigamos o desempenho do sistema operacional quando o número de IPIs usados para cada b foi reduzido de 67 IPIs para 34 IPIs para que b teria 64 bits em vez de 128 bits. Também estudamos o cenário quando o ECG e o PPG foram reduzidos de 1000 Hz para 200 Hz. Os painéis esquerdo e direito da Fig. 4 mostram, respectivamente, a metade da taxa de erro total (HTER = 1/2 (FAR + FRR)) em relação à distância, e a taxa de aceitação genuína em relação à taxa de falsa aceitação para o diferentes condições de teste. As condições de teste e o HTER mínimo correspondente estão resumidos na Tabela 1.

D ISCUSSION

Neste estudo, o conjunto de ECG e PPG foi dividido em segmentos de forma que o segmento de ECG correspondente contivesse um número exato de ondas R. Fazendo isso, assumimos que existe um processo de sincronização de tempo entre os diferentes nós. A sincronização de tempo de nós em uma rede sem fio é muito importante, e as soluções de sincronização de última geração para redes de sensores sem fio já alcançaram uma precisão de cerca de 100 μ s. Embora a sincronização instantânea com precisão de 1 ms seja suficiente para o esquema proposto, o esquema requer que o circuito de sincronização interaja com o circuito de detecção de sinal fisiológico para registrar o carimbo de data / hora na chegada do sinal de sincronização. Devido à fisiologia do sistema circulatório humano, a geração do complexo QRS em um ciclo cardíaco deve preceder a detecção de um pulso na periferia. Portanto, se o sinal de sincronização, que indica o início da geração do traço biométrico, for emitido por um nó mestre que captura o ECG, é garantido que os IPIs capturados por outros nós corresponderão ao capturado pelo nó mestre. Não obstante, a situação não é direta se o sinal de sincronização for emitido por um nodo que não possui informações sobre o início de um ciclo cardíaco. Uma possível solução é examinar o uso de um esquema de decisão que permite um desalinhamento de IPI em duas sequências binárias.

Selecionamos a distância de Hamming como a métrica para o traço biométrico proposto porque funciona bem com a operação XOR bit a bit, que é uma das operações mais comuns usadas em criptosistemas. Ao usar essa métrica de distância, podemos ter certeza de que o desempenho mostrado neste estudo reflete a situação em que a característica biométrica é realmente usada na proteção do BASN (por exemplo, usando alguns dos protocolos de comunicação discutidos anteriormente para autenticação de entidade ou distribuição de chave de cifra).

A partir do experimento, o HTER mínimo foi encontrado em 2,58 por cento para 99 indivíduos (FRR = 3,99 por cento). Para os 14 indivíduos saudáveis, o HTER mínimo é quase 0 por cento. Verifica-se que o aumento nas taxas de erro não se deve simplesmente ao maior tamanho da amostra. Na verdade, quando o exame foi limitado a apenas 85 indivíduos, dois terços dos quais tinham 50 anos ou mais e sofriam de uma ou mais doenças crônicas no momento do experimento, o HTER mínimo é ainda maior (4,26 por cento). Descobrimos que a principal razão para o aumento da taxa de erro nos 85 indivíduos é devido à assincronia dos IPIs obtidos no ECG e no PPG. Percebe-se que os sinais captados dos 85 indivíduos são mais ruidosos do que os obtidos dos 14 indivíduos saudáveis, e o algoritmo de detecção automatizado não foi capaz de identificar o mesmo número de ondas R no ECG e pulsos no PPG para alguns dos segmentos de dados. Isso pode ser devido a artefatos de movimento ou às suas condições de saúde (por exemplo, uma onda R no ECG não resulta em um pulso correspondente no PPG). A falta de um ponto característico no ECG ou no PPG resultará em uma incompatibilidade na série de IPIs obtidos posteriormente. Como nosso esquema de codificação não cuidou dessa situação, a distância de Hamming obtida entre duas séries assíncronas de IPIs é grande. Isso pode justificar porque FARs, que contribuíram principalmente para a parte direita das curvas HTER na Fig. 4a, não mostram diferenças significativas para os diferentes grupos de sujeitos, mas os FRRs (parte esquerda das curvas HTER) sim. A falta de um ponto característico no ECG ou no PPG resultará em uma incompatibilidade na série de IPIs obtidos posteriormente. Como nosso esquema de codificação não cuidou dessa situação, a distância de Hamming obtida entre duas séries assíncronas de IPIs é grande. Isso pode justificar porque FARs, que contribuíram principalmente para a parte direita das curvas HTER na Fig. 4a, não mostram diferenças significativas para os diferentes grupos de sujeitos, mas os FRRs (parte esquerda das curvas HTER) sim. A falta de um ponto característico no ECG ou no PPG resultará em uma incompatibilidade na série de IPIs obtidos posteriormente. Como nosso esquema de codificação não cuidou dessa situação, a distância de Hamming obtida entre duas séries assíncronas de IPIs é grande. Isso pode justificar porque FARs, que contribuíram principalmente para a parte direita das curvas HT

Por outro lado, o comprimento de bit de cada sequência afeta principalmente o FAR (Fig. 4c). O HTER mínimo é aumentado de 4,26% para 6,98% quando o número de IPIs usados para codificação é reduzido de 67 para 34. Descobrimos que o esquema de codificação atual pode não ser ideal para obter um sistema de alto desempenho. Para uma pessoa com uma freqüência cardíaca média de 60 batimentos por minuto, o sistema exigiria mais de 1 minuto para adquirir informações suficientes para 1 sequência binária. No futuro, é importante investigar outros esquemas de codificação, por exemplo, usar vários IPIs em vez de IPI individuais, a fim de maximizar o desempenho com um número mínimo de batimentos cardíacos necessários.

Por último, descobriu-se que a redução da taxa de amostragem de 1000 Hz para 200 Hz não tem um efeito significativo no desempenho do sistema. Operar com uma taxa de amostragem mais baixa economiza recursos e, portanto, é desejável. No entanto, prevê-se que reduzir ainda mais a taxa de amostragem pode degradar o desempenho, pois os espectros de ECG e PPG seriam distorcidos se a taxa de amostragem fosse abaixo de 100 Hz.

A razão pela qual o IPI pode possivelmente ser usado para proteger BASNs pode ser entendida a partir dos requisitos de segurança comuns estabelecidos para sistemas biométricos genéricos. Na verdade, o IPI atende à maior parte dos

A situação não será simples se a sincronização sinal é emitido por um nodo que não possui informação sobre o início de um ciclo cardíaco. Uma possível solução será examinar usando uma decisão esquema que permite um desalinhamento de IPI em dois binários sequências.

Como mencionado antes, um importante limitação do BASN é que deve ser operado com extremamente restrições estritas. Para usar o abordagem proposta, o aumento em complexidade de sensores individuais seria mínimo se um biométrico comum característica, por exemplo, IPI está prontamente disponível em todos os sensores.

# do assuntos	# De dados segmentos	Amostragem taxa (Hz)	# de IPIs usados / seqüência binária	Codificação bits	Mínimo HTER (%)	FRR (%)	LONGE (%)
14	49	1000	67	128	0,01	0,00	0,03
85	789	1000	67	128	4,26	6,46	2.06
99	838	1000	67	128	2,58	3,99	1,18
85	1599	1000	34	64	6,98	9,51	4,46
85	789	200	67	128	4,65	6,95	2,35

Tabela 1. *Condições de teste, o HTER mínimo resultante e o FAR e FRR correspondentes.*

requisitos universalmente aceitos de uma boa característica apresentada por Jain *et al. [*6]. Não é difícil descobrir que o IPI é uma característica universal, colecionável, eficaz e aceitável. O IPI é um sinal vital que pode ser coletado de qualquer ser humano. Mais importante, pode ser obtido com diferentes tipos de sensores e de vários tipos de sinais fisiológicos relacionados ao sistema cardiovascular (por exemplo, ECG, PPG e sons cardíacos). Esses sinais fisiológicos, que normalmente são sinais unidimensionais de baixa frequência, podem ser coletados por equipamentos médicos a um custo razoavelmente baixo. Como suas dimensões são poucas e sua resolução é baixa, processá-los e obter a característica deles provavelmente será computacionalmente barato. Portanto, essa característica é eficaz e pode render um bom desempenho. Além do que, além do mais, esses sinais fisiológicos são frequentemente os sinais fisiológicos básicos que serão coletados em uma aplicação de telemedicina ou m-health para fins clínicos. Isso garante que sua aceitabilidade não seja um problema e que o cálculo do IPI deles para garantir a transmissão de dados dificilmente aumentará os recursos exigidos dos terminais. Esta última característica é importante para a aplicação de BASNs em telemedicina e m-health, que deve operar em um ambiente com restrições extremamente rigorosas.

Talvez a característica mais distintiva do uso dessa biometria em BASNs em comparação com seu uso em sistemas biométricos convencionais é que a característica a ser usada em BASNs deve ser de natureza aleatória. Isso é contrário ao requisito de um traço para um sistema biométrico convencional, onde os modelos do traço são armazenados no sistema como uma referência para comparação com uma cópia do traço capturada em tempo real para fins de identificação ou autenticação. Devido à forma como o sistema convencional opera, a característica deve ser invariável no tempo; caso contrário, é inútil comparar características recém-capturadas com aquelas disponíveis no banco de dados. Ao contrário dos sistemas biométricos convencionais, o traço biométrico em um BASN é capturado independentemente, mas simultaneamente. Portanto, não há necessidade de que o traço seja permanente. De fato , o nível de segurança é aumentado quando o traço muda com o tempo e possui uma natureza caótica, pois isso tornaria muito difícil para um invasor adivinhar o traço, que pode ser a identidade de autenticação ou o meio de proteger a chave de cifra. Além disso, se o sinal muda com o tempo, o sistema pode até mesmo reatribuir uma nova chave uma vez que enquanto, e assim aumentar ainda mais o nível de segurança. Portanto, os critérios para exigir que o traço seja distinto, permanente e invulnerável devem ser modificados no caso de aplicá-lo em BASNs como segue:

- Distintivo: a característica deve ser suficientemente diferente em quaisquer dois indivíduos quando cópias dela forem capturadas simultaneamente, mesmo se as cópias forem capturadas por diferentes tipos de biossensores e em diferentes locais do corpo.

- Variante no tempo, mas invulnerável: a característica deve mudar com o tempo e ter um alto nível de aleatoriedade para que as características biométricas capturadas em momentos diferentes não coincidam, mesmo que sejam obtidas do mesmo indivíduo. Isso garante um nível de segurança muito mais alto.

Com esses princípios estabelecidos, o uso da biometria em BASNs para telemedicina e saúde móvel pode ser estendido para o uso de outros sinais ou parâmetros fisiológicos como traços, desde que satisfaçam os critérios discutidos acima. No entanto, o IPI é selecionado para pesquisa devido às suas características únicas. O IPI pode ser obtido com diferentes tipos de sensores e de diferentes sinais fisiológicos (por exemplo, ECG, PPG, sons cardíacos, onda de pressão sanguínea e fluxo sanguíneo) de modo que esteja disponível para uma infinidade de biossensores que servem a diferentes funções em BASNs. O IPI também tem a vantagem de que a variação é geralmente aceitável, mesmo se medida em diferentes partes do corpo (por exemplo, no tórax, pontas dos dedos ou um membro inferior). Ao contrário da temperatura corporal, que varia se os sensores forem implantados no corpo ou colocados na superfície corporal,

Como mencionado antes, uma limitação importante de um BASN é que ele deve operar sob restrições extremamente rigorosas. Para usar a abordagem proposta, o aumento na complexidade de sensores individuais seria mínimo se uma característica biométrica comum (por exemplo, IPI) estivesse prontamente disponível em todos os sensores. Ilustramos um exemplo (Fig. 2) com uma lista de biossensores práticos que capturam sinais fisiológicos que incorporam informações IPI. Para sinais que incorporam a característica biométrica, o aumento na complexidade dos sensores, em termos de computação e requisitos de memória, seria mínimo.

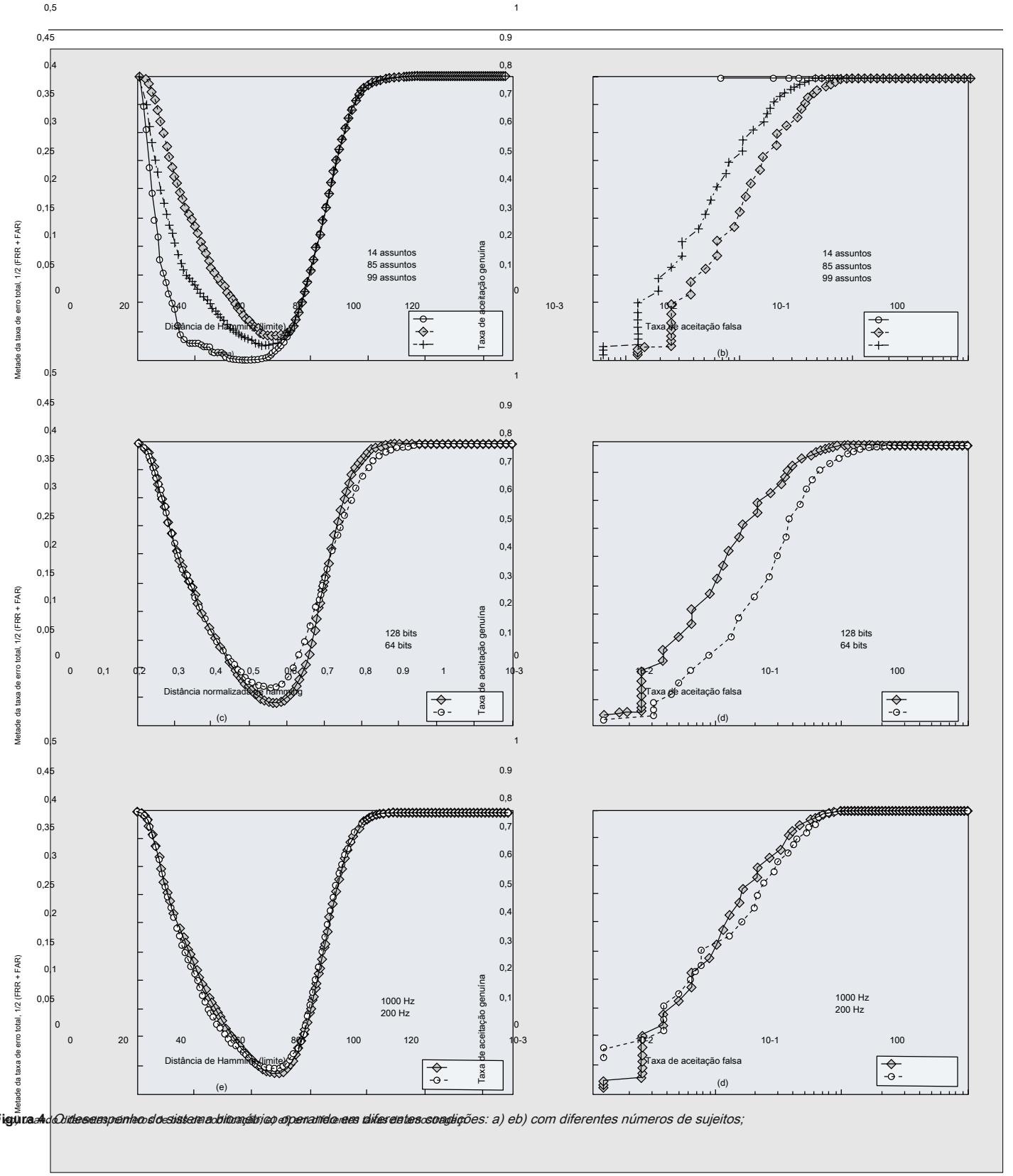

Figura 4. *Os desempenhos do sistema biométrico operando em diferentes condições: a) eb) com diferentes números de sujeitos; c) e d) com diferentes números de bits de características; e) e d) com diferentes frequências de amostragem.*

No entanto, o IPI tem suas próprias limitações e, obviamente, não importa o quão comumente ele possa ser encontrado em sinais fisiológicos, nem todo biossensor captura sinais com informações de IPI. Exemplos típicos são sensores de movimento colocados nos joelhos ou em sapatos. Para esses nós, um sensor extra podem ser necessários para implementar a abordagem proposta. Foi apontado que ter um biossensor apenas para garantir a comunicação entre BASN pode resultar em sensores mais volumosos e, conseqüentemente, limitar sua aceitação. Apesar disso, o aumento da complexidade é

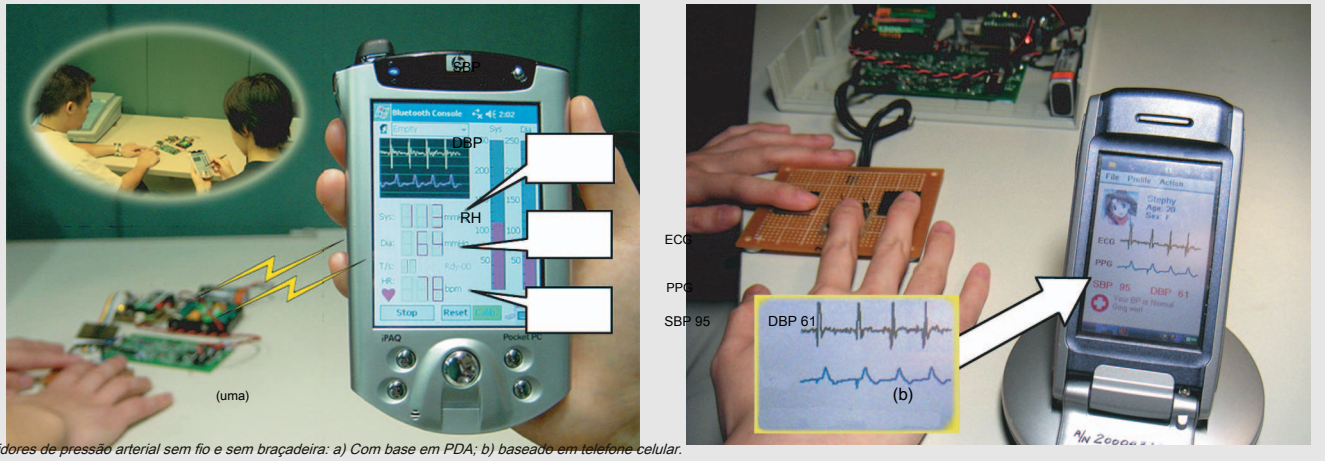

Figura 5. *Medidores de pressão arterial sem fio e sem braçadeira: a) Com base em PDA; b) baseado em telefone celular.*

vale a pena em vista da segurança aumentada que pode trazer, especialmente quando comparada com a exigida pela tecnologia existente para atingir um nível de segurança semelhante. O aumento da complexidade pode ser minimizado pela seleção cuidadosa do tipo de sensores. Também é importante explorar outros usos do sensor extra (por exemplo, investigando métodos de fusão de dados para explorar totalmente as novas informações). Com relação aos sensores colocados em partes do corpo onde a captura de informações de IPI é difícil, a situação será mais difícil e pode exigir que um nó com menos restrição de recursos atue como uma ponte para distribuir a chave cifrada para os sensores por outros métodos.

Por último, também foi apontado que uma tecnologia em desenvolvimento (banda ultra larga, UWB, radar [13]) para captura remota da freqüência cardíaca poderia colocar ameaças de segurança na tecnologia proposta. Embora a tecnologia de radar UWB atual possa não estar madura o suficiente para realizar esse ato fraudulento, ela de fato abre essa possibilidade futura. Nesse sentido, mais estudos devem ser realizados para investigar como aprimorar a tecnologia proposta para prevenir esse tipo de ataque.

C INCLUINDO R EMARKS AND UMA PPLICATION S CENÁRIO

Este artigo apresenta uma nova abordagem biométrica para proteger BASNs sem fio para telemedicina e m-health e ilustra o conceito usando o IPI como exemplo. Avaliando o método em 838 conjuntos de dados coletados de 99 sujeitos, verifica-se que o HTER mínimo é 2,58 por cento (FAR = 1,18 por cento e FRR = 3,99 por cento) quando os sinais são amostrados em 1000 Hz e o traço é codificado em uma sequência binária de 128 bits. O estudo abriu algumas questões-chave para investigação futura, incluindo esquemas de compensação para a assincronia de diferentes canais (devido a doenças, fenômenos fisiológicos, artefatos de movimento, erros de dicção, etc.), esquemas de codificação e outros biométodos adequados traços ricos.

Os resultados deste estudo complementam o principal trabalho de pesquisa de nosso centro de pesquisa no desenvolvimento de sensores e sistemas inteligentes vestíveis (WISS) para aplicações de telemedicina e saúde móvel [3, 12]. WISS podem ser nós de BASNs; exemplos incluem um dispositivo de medição de pressão arterial sem fio e sem braçadeira que é desenvolvido com base em um PDA e telefone celular [12]. A Figura 5 ilustra os protótipos deste dispositivo, onde um módulo de detecção é usado para coletar sinais fisiológicos do usuário, e uma estação base pessoal (um PDA ou telefone celular) é usada para receber os parâmetros fisiológicos, como frequência cardíaca, sangue pressão e suas variabilidades. Atualmente, os sinais são transmitidos via transmissão Bluetooth. Em um futuro previsível, estaremos ativamente procurando integrar um biossensor a este tipo de estação base pessoal para transformá-lo em um nó mestre de um BASN para que todos os outros módulos de detecção usados ou implantados no corpo possam ser conectados a ele. O sistema biométrico discutido neste artigo pode ser empregado para garantir a autenticidade, confidencialidade e integridade da transmissão de dados entre o nó mestre e todos os outros nós sensoriais. Assim como o desenvolvimento dos dois Ws ampliou o escopo da telemedicina e trouxe a noção de m-Health, o uso da biometria para proteger BASNs sem fio pode ser a chave para abrir uma nova era para telemedicina e m-health.

O sistema biométrico discutido neste artigo pode ser empregado para garantir a autenticidade, confidencialidade e integridade da transmissão de dados entre o nó mestre e todos os outros nós sensoriais. Assim como o desenvolvimento dos dois Ws ampliou o escopo da telemedicina e trouxe a noção de m-Health, o uso da biometria para proteger BASNs sem fio pode ser a chave para abrir uma nova era para telemedicina e m-health. O sistema biométrico discutido neste artigo pode ser empregado para garantir a autenticidade, confidencialidade e integridade da transmissão de dados entre o nó mestre e todos os outros nós sensoriais. Assim como o desenvolvimento dos dois Ws ampliou o escopo da telemedicina e trouxe a noção de m-Health, o uso da biometria para proteger BASNs sem fio pode ser a chave para abrir uma nova era para telemedicina e m-health.

UMA RECONHECIMENTO

Este trabalho foi financiado em parte pelo Fundo de Inovação e Tecnologia de Hong Kong. Somos gratos à Standard Telecommunication Ltd., IDT Technology Ltd., Jetfly Technology Ltd., Golden Meditech Company Ltd. e Bird International Ltd. pelo apoio dado aos projetos da ITF. Agradecemos também aos revisores por seus valiosos comentários e sugestões.

R EFERÊNCIAS

[1] RL Bashshur, TG Reardon e GW Shannon, "Telemedicine: a New Health Care Delivery System," *Ann. Rev. Saúde Pública,* vol. 21, 2000, pp. 613–17.

[2] KSH Istepanian, E. Jovanov e YT Zhang, "Convidado Introdução editorial à seção especial sobre M-Health: Beyond Seamless Mobility e Global Wireless Health-Care Connectivity, " *IEEE Trans. Info. Tech. Biomed.,* vol. 8, não. 4, 2004, pp. 405–14.

[3] K. Hung e YT Zhang, "Implementation of a WAP- Sistema de telemedicina baseado para monitoramento de pacientes ", *IEEE Trans. Info. Tech. Biomed.,* vol. 7, não. 2 de junho 2003, pp. 101–07.

[4] D. Konstantas *et al.,* "Monitoramento móvel do paciente: o MobiHealth System, " *Proc. Int'l. Cong. Med. e Care Compunetics,* Haia, Holanda, 2–4 de junho de 2004. [5] E. Jovanov *et al.,* "A Wireless Body Area Network of Sensores de movimento inteligentes para reabilitação física assistida por computador, " *J. NeuroEng. e Rehab.,* vol. 2, não. 11, março de 2005, p. 6

[6] U. Uludag *et al.,* "Biometric Cryptosystems: Issues and Chal- desafios, " *Proc. IEEE,* vol. 92, no. 6, junho de 2004, pp. 948–60. [7] S. Cherukuri, KK Venkatasubramanian e SKS Gupta, "BioSec: A Biometric based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body", *Proc. IEEE Int'l. Conf. Wksp. De processamento paralelo,* 6–9 de outubro de 2003, pp. 432–39. [8] A. Juels e M. Wattenberg, "A Fuzzy Commitment Esquema, " *Proc. 6th ACM Conf. Comp. e Commun. Sec.,* G. Tsudik, Ed., 1999, pp. 28-36.

[9] I. Radojicic, D. Mandic e D. Vulic, "On the Presence do Caos Determinístico em Sinais de VFC, " *Proc. Comp. em cardiologia,* Setembro de 2001, pp. 465–68.

[10] SD Bao, YT Zhang e LF Shen, "A New Sym- métrico Cryptosystem of Body Area Sensor Networks for Telemedicine, " *Proc. 6th Asian-Pacific Conf. Med. e Bio. Eng.,* Japão, abril de 2005.

[11] SD Bao, YT Zhang e LF Shen, "Physiological Signal Based Entity Authentication for Body Area Sen- sor Networks and Mobile Healthcare Systems, " *Proc. 27º IEEE Int'l. Conf. Eng. Med. e Bio. Soc.,* Shanghai, China, setembro de 2005.

[12] CCY Poon e YT Zhang, "Cuffless and Noninva- sive Measurements of Arterial Blood Pressure by Pulse Transit Time ", *Proc. 27º IEEE Int'l. Conf. Eng. Med. e Bio. Soc.,* Xangai, China, setembro de 2005.

[13] EM Staderini, "UWB Radars in Medicine ", *IEEE AESS Sys.,* Janeiro de 2002, pp. 13–18.

BIOGRAFIAS

CARMEN CY POON (cpoon@ee.cuhk.edu.hk) a recebeu BASc. em ciência da engenharia (opção biomédica) e ela MASc. Doutor em engenharia biomédica pela University of Toronto, Canadá. Ela é atualmente um Ph.D. estudante da Universidade Chinesa de Hong Kong (CUHK). Seus interesses de pesquisa incluem processamento de biossinais e modelagem de biossistemas, e desenvolvimento de dispositivos médicos vestíveis para telemedicina e m-health. Ela recebeu o primeiro prêmio, o Prêmio IFMBE de Melhor Estudante Chinês, na 27ª Conferência Internacional Anual da Sociedade de Engenharia em Medicina e Biologia do IEEE em 2005.

YUAN- TING ZAGUENTAR (ytzhang@ee.cuhk.edu.hk) recebeu seu Ph.D. da Universidade de New Brunswick, Canadá, em 1990. Ele ingressou na CUHK como palestrante em 1994, tornou-se professor associado em 1996 e professor em 2002. Atualmente, ele atua como diretor do Joint Research Centre for Biomedical Engineering, Head da Division of Biomedical Engineering na CUHK, e chairman (adjunto) do Departamento de Engenharia Biomédica da Sun Yat-sen University, China. Ele foi o vice-presidente da IEEE Engineer- ing in Medicine and Biology Society (EMBS) em 2000 e 2001. Sua pesquisa concentra-se em dispositivos médicos vestíveis, redes de sensores corporais e processamento de sinal baseado em biomodelo para telemedicina e saúde móvel.

SHU- DEu BAO recebeu seu diploma de bacharelado pela Universidade de Ningbo, China, em 1999, e seu diploma de mestrado pela Universidade do Sudeste, Nanjing, China, em 2003. Atualmente é Ph.D. candidato em engenharia eletrônica pela Southeast University e assistente de pesquisa na CUHK. Ela ganhou o Young Investigator Award (YIA) e o YIA Best Presentation Award na 6ª Conferência Asiático-Pacífico sobre Engenharia Médica e Biológica realizada no Japão em 2005. Seus interesses de pesquisa atuais incluem recuperação de informações, segurança e tolerância a falhas e comunicações eficientes para redes de sensores corporais e sistemas de telemedicina.

Assim como o desenvolvimento do dois Ws tem ampliou o escopo da telemedicina e trouxe sobre o noção de m-Health, o uso de biometria para proteção sem fio BASN pode ser a chave na abertura de uma nova era para a telemedicina e m-Health.