Autenticação Contínua e Segura Baseada em Sinais PPG e Comunicação Galvânica

Fernando Nakayama[1], **Paulo Lenz**[1], **Bruno Cremonezi**[1], **Stella Banou**[2]
Denis Rosário[3], **Kaushik Chowdhury**[2], **Michele Nogueira**[1]
Eduardo Cerqueira[3], **Aldri Santos**[1]

[1]NR2 – Universidade Federal do Paraná (UFPR)
[2]ECE – Northeastern University (NU)
[3]GERCOM – Universidade Federal do Pará (UFPA)

{fnqueiroz,pljunior,bmcremonezi,aldri,michele}@inf.ufpr.br,
{sbanou,krc}@ece.neu.edu, {denis,cerqueira}@ufpa.br

Abstract. *Biometric authentication supports different applications and has an essential role for wearable networks due to its power to overcome limitations in the human-machine interfaces of wearable devices. In general, authentication methods rely on one-time events, such as iris and face recognition, what requires validating the user's identity whenever one needs to log in to the system. With the recent advances in biosensors, some signals are continuously collected, allowing then a continuous authentication. However, existing continous authentication methods via ECG and EMG are costly, complex or incovenient to users. Hence, to overcome these issues, this paper presents BEAT, a secure authentication system that employs photoplethysmogram (PPG) as basis for noninvasive, seamless and continuous authentication in wearable networks. In order to achieve security, BEAT transmits data collected by PPG sensors through galvanic coupling communication, that employs the skin as comunication medium. Experimental results show the feasibility and efficiency of the system.*

Resumo. *A autenticação biométrica suporta diferentes aplicações e tem ganho um papel fundamental nas redes vestíveis por suplantar limitações das interação homem-máquina de seus dispositivos. Em geral, os métodos de autenticação dependem de eventos únicos, como reconhecimento de íris ou face, exigindo a validação da identidade do usuário sempre que ele precisa acessar o sistema. Todavia, com a recente inclusão de biosensores em dispositivos vestíveis, biosinais são coletados constantemente, permitindo uma autenticação contínua. Entretanto, os métodos existentes de autenticação contínua via ECG e EMG são custosos, complexos ou inconvenientes para o usuário. Assim, para superar esses problemas, este artigo apresenta o sistema BEAT que emprega os biosinais do fotopletismograma (PPG) como base para uma autenticação não invasiva, transparente e contínua em redes vestíveis. Para alcançar segurança, o sistema BEAT transmite os sinais coletados através de comunicação por acoplamento galvânico, sendo o tecido epitelial o meio de comunicação. Os resultados experimentais demonstram a viabilidade e a eficiência do sistema.*

1. Introdução

Os dispositivos vestíveis têm atraído a atenção da comunidade acadêmica e da indústria, aumentando sua popularidade através das diferentes aplicações. Em Agosto de 2018,

a empresa Gartner publicou as cinco principais tendências tecnológicas para o próximo ciclo de ápice [IDTechEX 2018]. Dentre elas, estão as associadas com os ambientes inteligentes com uma maior integração entre os dispositivos, os usuários e os negócios através de dispositivos vestíveis capazes de coletar e fornecer informações, de modo transparente, sobre os usuários e criar condições a uma maior qualidade de vida. Por dispositivos vestíveis, entendem-se aqueles usados ou acoplados ao corpo humano para monitorar continuamente as atividades de um indivíduo, sem interromper ou limitar seus movimentos [Gao et al. 2016]. Dentre esses dispositivos, os que usam sensores vestíveis do tipo óptico estão em destaque diante ao estimado crescimento de uso até 2022.

A popularização dos dispositivos vestíveis traz grandes desafios e novas possibilidades para a autenticação de usuários. Um dos desafios consiste em como restringir o acesso aos dados e serviços apenas a usuários autorizados, sendo que este controle passa pela autenticação da identidade do usuário [Sandhu and Samarati 1994]. Em geral, a autenticação segue uma abordagem de evento único, pressupondo alguma informação que o usuário saiba (ex. uma senha); algo que ele possua (ex. *tokens*); algo que ele é (ex. o seu cargo); ou alguma característica física ou comportamental única do usuário – biometria (ex. a impressão digital). Apesar das senhas alfanuméricas longas ainda serem consideradas uma das formas mais seguras de autenticação, o custo de manter esse nível de segurança [Li et al. 2014] e a falta de conveniência e praticidade [Mazurek et al. 2013] no contexto de redes vestíveis têm motivado novas soluções de autenticação. Além disso, as soluções de autenticação tradicionais assumem eventos únicos, como a digitação da senha, o uso do *token* e outros, tendo ao longo do tempo o nível de segurança reduzido nas sessões autenticadas e facilitando as ações de malwares.

A biometria é amplamente estudada na literatura e demonstra um grande potencial para a autenticação de usuários no contexto dos dispositivos vestíveis [Wu et al. 2018]. As formas mais comuns de autenticação biométrica passam pelo reconhecimento da impressão digital, da facial ou da íris. Assim como os métodos de autenticação baseados em senha, token e atributo, essas formas de autenticação biométrica tomam como base eventos únicos, sendo também chamada de *one-time authentication*. Desta forma, cada vez que o indivíduo precisa usar o sistema, a autenticação é refeita. Além de ser suscetível a fraudes e ataques, estes métodos não permitem uma autenticação constante [Mosenia et al. 2017]. Dadas as características dos dispositivos vestíveis e as novas formas de interação homem-máquina, o desafio consiste em oferecer soluções que tratem a autenticação como um processo contínuo e não baseada em eventos isolados. O uso do ECG (eletrocardiograma) [Blasco et al. 2016] é um exemplo de biometria explorada na autenticação contínua. Porém, o procedimento de coleta do sinal ECG pode ser inconveniente, visto que o ECG é coletado por eletrodos conectados à pele do usuário e exige ao menos três pontos de contato em lados diferentes do corpo para coletar a frequência cardíaca [Belgacem et al. 2015]. O uso contínuo dos eletrodos traz incômodo ao usuário.

Em consonância com o avanço no estado da arte, este trabalho apresenta o sistema BEAT que provê uma autenticação segura, contínua, não intrusiva e sem a necessidade de ações adicionais pelo usuário. O sistema BEAT utiliza sinais vitais relacionados à frequência cardíaca e coletados a partir de sensores PPG (fotopletismograma) para autenticar os usuários. Os sinais vitais são coletados através de um processo em que um transmissor LED no sensor emite luminosidade em alguma parte do corpo humano (ex.

pulso, dedo, lóbulos auriculares) e paralelamente um diodo fotossensível mede a luz absorvida pelos tecidos epiteliais. As medições indicam as mudanças no volume sanguíneo [Liang et al. 2018]. Os dados coletados sobre a dilatação dos vasos sanguíneos são transmitidos pela pele até um dispositivo coordenador da rede vestível (ex. um telefone celular na mão do usuário). A transmissão dos dados está fundamentada na técnica de acoplamento galvânico, do inglês, *Galvanic Coupling* (GC) [Tomlinson et al. 2019], a qual utiliza a pele como um canal de transmissão seguro. O sistema BEAT avança significativamente o estado da arte explorando, em conjunto, os sinais PPG e a comunicação por acoplamento galvânico para a autenticação de usuários em redes vestíveis.

Os resultados experimentais demonstram que o sistema BEAT é viável e eficiente. Nos experimentos, três bases de dados foram utilizadas, sendo duas geradas pela coleta de dados de 30 usuários jovens e saudáveis no laboratório NR2/UFPR dentro do escopo do projeto NSF/RNP de cooperação internacional HealthSense e outra do repositório Physionet contendo 30 usuários em condições críticas de saúde (com problemas diversos, ex. cardíacos e pulmonares). O sistema BEAT obteve uma acurácia de 98,66% e 92,15% quando confrontado com as bases de dados NR2/UFPR e 89,88% com a base do Physionet. O sistema alcançou uma baixa taxa de falsos negativos em qualquer das bases de dados utilizadas; e uma baixa taxa de falsos positivos.

Este trabalho procede como segue. A Seção 2 aborda os trabalhos relacionados. A Seção 3 descreve o o sistema BEAT. A Seção 4 detalha o cenário de avaliação e discute os resultados obtidos. A Seção 5 conclui o artigo e apresenta as direções futuras.

2. Trabalhos Relacionados

Um sistema de reconhecimento biométrico é um sistema de identificação de padrões, que compara as características singulares de um indivíduo com um modelo de referência previamente armazenado. [Jain et al. 1997] identificaram as características biométricas para autenticação, indicando a voz, a impressão digital, o reconhecimento de íris e facial como adequadas para um sistema de autenticação. A partir disto, vários sistemas de autenticação baseados em voz [Kim and Hong 2008], impressão digital [Jain et al. 1997], íris [Huang et al. 2002] e facial [Chen et al. 2000] foram propostos. Entretanto, estes sistemas possuem vulnerabilidades de segurança, ex. a voz pode ser gravada e replicada para autenticação, moldes em látex podem ser falsificados para subjugar os sistemas de impressão digital, a autenticação da íris pode ser forjada através de fotos impressas em alta definição, e a eficiência do reconhecimento facial depende do tipo de modelo de referência e pontos de verificação [Blasco et al. 2016].

Os biosinais possuem características únicas de um indivíduo e com o avanço tecnológico dos sensores vestíveis, eles podem ser continuamente monitorados e armazenados. Vários estudos investigam o uso dos biosinais para a autenticação. A grande maioria deles aborda sinais tradicionais como o EMG (eletromiograma), o EEG (eletroencefalograma) e o ECG. O EMG é um sinal elétrico medido a partir da contração muscular e foi utilizado por [Yamaba et al. 2017] em um modelo de autenticação para *smartphones*. Entretanto, para o correto funcionamento do sistema, o usuário precisava fazer determinados movimentos, envolvendo a contração e o relaxamento musculares. O EEG avalia a atividade elétrica do cérebro. [Miyamoto et al. 2009] e [Marcel and Millán 2007] propuseram modelos de autenticação usando o EEG. A acurácia não foi expressiva em

nenhum dos modelos e o posicionamento dos sensores é um obstáculo. O ECG avalia os impulsos elétricos do coração e serve de base para autenticação em vários trabalhos [Belgacem et al. 2015, Lourenço et al. 2011, Singh and Singh 2012]. Entretanto, a coleta do ECG é inflexível quanto a necessidade de medições paralelas em ambos os lados do corpo. No caso de uso de eletrodos, necessária a aplicação de gel condutor; na aquisição por contato, preciso o toque em dispositivos específicos [Bonissi et al. 2013]. Recentemente, as pesquisas buscam por sistemas para autenticação contínua. Alguns deles consideram características comportamentais ou temporais para a autenticação. Outros seguem estudos práticos utilizando multisensores custosos e requerem constante movimentação do usuário [Wu et al. 2018]. [Lin et al. 2017] utilizaram a variação de batimentos cardíacos para autenticação contínua, obtendo acurácia de 98,61%. Nele os sinais eram coletados por um sensor doppler sem nenhum contato com o usuário. Entretanto, o emprego desses sensores de alto custo inibe a aceitação e o uso das soluções.

O sinal PPG vem sendo explorado na literatura, porém, em geral, para *one-time authentication*. As pesquisas adaptam os métodos tradicionais de autenticação para o uso de sinais PPG. Dentre as abordagens, [Gu et al. 2003] realizaram um estudo com as características da onda PPG e criaram um modelo com quatro características principais, pico, curva superior, curva inferior e intervalo de tempo. [Gu and Zhang 2003] seguiram os mesmos critérios. Em outro trabalho, [Spachos et al. 2011] realizaram uma análise para a extração de duas características das ondas PPG, número de picos e distância entre picos e vales. Os autores seguiram um algoritmo de vizinhos mais próximos como classificador, obtendo precisão de 95% na autenticação. Entretanto, os resultados apontaram uma grande variação na acurácia dependendo da forma de coleta do sinal, sendo os equipamentos e o ambiente, cruciais para coleta de um sinal de qualidade.

Os mecanismos de autenticação baseados em biosinais consideram em sua grande maioria algum tipo de transmissão sem fio. Todavia, as principais tecnologias, como *Bluetooth*, Zigbee e NFC, possuem falhas de segurança identificadas [Alaba et al. 2017]. Assim como em [Tomlinson et al. 2019], neste trabalho seguimos o método *Galvanic Coupling* (GC) para permitir a criação de um canal de comunicação através do corpo humano, tendo a pele e tecidos como condutores. O GC e outras tecnologias que utilizam o corpo humano como meio de comunicação, vêm sendo cada vez mais explorada [Tomlinson et al. 2019, Vasisht et al. 2018]. Além da transmissão através do corpo humano, as abordagens GC atuais são direcionadas à transmissão de dados de forma mais segura, visto que não seria possível a interceptação do sinal. Um outro aspecto consiste no fato dos atuais modelos de autenticação biométrica serem baseados em características estáticas de um indivíduo. Isto valida de forma incompleta a vivacidade de um usuário.

Diante dos aspectos levantados, este trabalho apresenta um sistema de autenticação contínua e segura que explora o biosinal proveniente do sensor PPG e a comunicação galvânica. O sistema BEAT é não invasivo e transparente, além de garantir a vivacidade do usuário. Por fim, ele toma como base sensores não custosos e simples que permitem o uso de múltiplas características do sinal PPG, oferecendo maior acurácia.

3. Autenticação Contínua por Sinais PPG e Comunicação Galvânica

Esta seção descreve o sistema de autenticação BEAT que realiza a identificação de um usuário através de sinais biomédicos PPG a partir de dispositivo vestível. O sistema

BEAT emprega comunicação galvânica como um canal de comunicação alternativo seguro e simples. Inicialmente, a seção apresenta uma visão geral do modelo de rede e as premissas. Em seguida, detalha-se cada uma das três etapas do sistema BEAT.

3.1. Modelo da Rede e Premissas

O sistema de autenticação atua no escopo de uma rede vestível. A rede consiste de dispositivos vestíveis organizados em uma topologia em estrela, sendo o coordenador da rede o dispositivo central, em geral, com maior capacidade de recursos em termos de memória e processamento. A fim de alcançar segurança na transmissão dos dados coletados, a comunicação galvânica, i.e., pela pele, serve de canal de comunicação alternativo. Esta comunicação ocorre entre um dispositivo vestível e um dispositivo coordenador da rede. O sistema BEAT segue as etapas: (i) aquisição de dados e pré-processamento do sinal (Figura 1(a)), (ii) transmissão dos dados através da comunicação por acoplamento galvânico (Figura 1(b)) e (iii) o processo de autenticação (Figura 1(c)). Na Figura 1(a), o coordenador da rede vestível é representado pelo telefone celular, entretanto este poderia ser qualquer dispositivo com contato direto com a pele do usuário capaz de servir como *gateway* de comunicação entre a rede vestível e outras redes, tal como uma rede local sem fio (WLAN) ou a Internet. Está fora do escopo deste trabalho atuar sob a comunicação entre o gateway e a Internet; ou entre o gateway e uma WLAN ou outras.

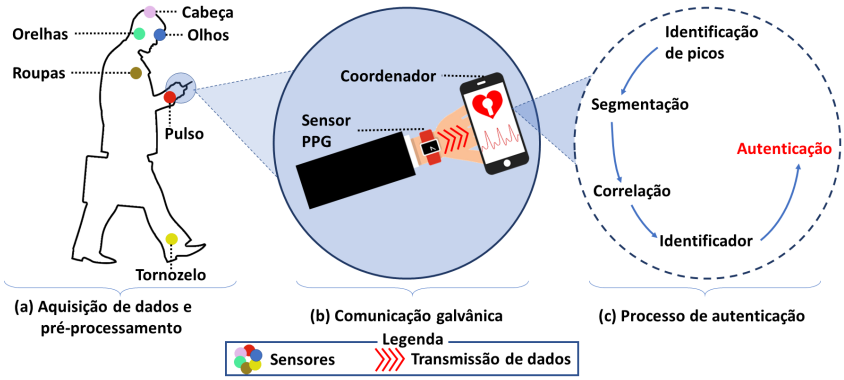


Figura 1. Etapas do Sistema de Autenticação BEAT

A Figura 1(a) ilustra vários dispositivos vestíveis posicionados em diferentes partes do corpo, tal como na cabeça, olhos, orelhas, roupas, pulso e tornozelo. Um dispositivo vestível é definido como um dispositivo autônomo, não invasivo, desempenhando uma função específica relacionada ao corpo, ex. monitorar os sinais vitais de um usuário. Exemplos de dispositivos vestíveis são os *smartglasses*, os relógios inteligentes, os monitores de pulso para atividades físicas, cintas torácicas, tênis inteligentes e outros. A arquitetura genérica de um dispositivo vestível segue os módulos: sensor, computação de baixa potência (processador), e comunicação (Figura 2). Os sinais fisiológicos do corpo são um dos tipos de dados coletados por um sensor em um dispositivo vestível. Após coletados, o dispositivo vestível converte os sinais em dados brutos. Dependendo da tarefa de monitoramento, diferentes tipos de sensores podem ser usados, tais como elétricos, mecânicos, eletroquímico e óptico. Entretanto, cabe ressaltar que neste trabalho focamos em sensores ópticos, tais como aqueles existentes em relógios inteligentes e pulseiras monitoras de atividades físicas, sendo então posicionadas nos pulsos dos usuários. Os sensores ópticos fazem a análise da dilatação dos vasos sanguíneos. Isto ocorre através da emissão de luz contra a pele do usuário e a detecção de sua reflexão (Figura 3).

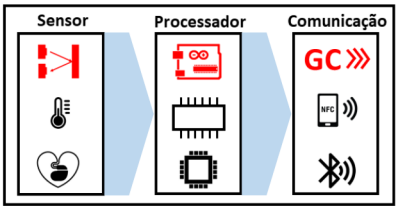


Figura 2. Principais componentes

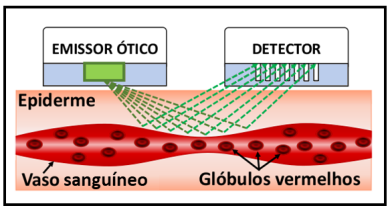


Figura 3. Sensor óptico

3.2. Aquisição dos Dados e Pré-processamento dos Sinais

O processo de aquisição dos dados (Figura 1(b)) é feito com um sensor óptico de fotopletismograma (PPG). Os valores numéricos obtidos a partir do sensor PPG formam uma onda composta de valores de amplitude em uma linha temporal. A onda obtida a partir do sinal PPG permite a extração de diferentes características exclusivas do usuário, as principais estão ilustradas na Figura 4: a quantidade de picos durante um intervalo de tempo, o formato do vale e o formato do pico, a amplitude da onda, e a distância entre o pico e o vale da onda. A fim de tornar a autenticação mais robusta, este trabalho utiliza combinações dessas características para correlacionar toda a linha temporal, usando segmentos de onda. Nota-se que independente do tipo de característica extraída, a identificação dos picos e vales é indispensável.

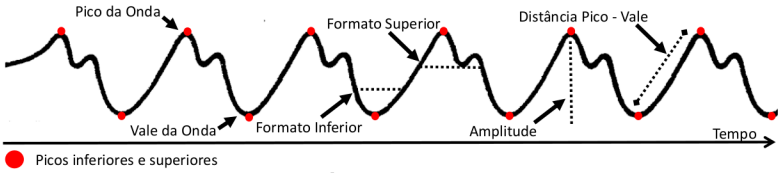


Figura 4. Características da Onda do Sinal PPG

Após a aquisição do sinal PPG, um pré-processamento desse sinal é necessário, pois este é vulnerável a diferentes fontes de ruído, como interferência eletromagnética, excesso de luminosidade e movimentos bruscos do usuário em regiões próximas ao sensor. Em geral, o pré-processamento segue o uso de filtros em (i) hardware ou (ii) software. Os filtros em hardware têm como vantagem serem projetados para extrair dados específicos (ex. dados relacionados à variação cardíaca ou à respiração), sendo mais eficientes e rápidos. Entretanto, os sensores com filtros em hardware são limitados e pouco flexíveis quanto aos dados tratados, restringindo a faixa de frequência que atuam. Por exemplo, um sensor PPG em hardware projetado para atuar na faixa de frequência entre 0 e 125 Hz fornece valores entre 1 e 50 Hz, sendo os valores acima e abaixo do filtro descartados. Caso o sensor não possua filtros em hardware, os dados de todas as faixas de frequência capturadas pelo sensor estarão disponíveis para consulta, no entanto, além de ser um grande volume de dados, muitos dos dados obtidos são desnecessários, principalmente aqueles obtidos em frequências muito altas e muito baixas, sendo ruído.

Os filtros em software limitam a amplitude do sinal coletado de forma similar aos filtros de hardware, porém através de cálculos matemáticos implementados em software. Esses filtros são mais lentos que os filtros em hardware, porém são mais flexíveis quanto a alterações e adições de faixas de frequência a filtrar. Exemplos de técnicas para a filtragem de ondas são a segmentação por faixa de frequência, os filtros de alta frequência (*high-pass*), os baixa frequência (*low-pass*), e os de banda passante (*band-pass*). A escolha do filtro está relacionada à frequência desejada, sendo as principais características relevantes

do sinal PPG obtidas entre 0,5 e 5 Hz. Além disso, outro aspecto a considerar na escolha do filtro consiste na limitação computacional dos dispositivos vestíveis, sendo necessária a escolha de filtros com baixa complexidade computacional. Desta forma, os filtros passa alta, passa baixa e banda passante são preferíveis a filtros que realizam segmentação do sinal em diversas faixas (multidimensionais), pois os primeiros são configuráveis com frequência de corte e número reduzido de operações, aumentando a eficiência energética.

3.3. Transmissão dos Dados por Comunicação Galvânica

O sistema BEAT está fundamentado na comunicação por acoplamento galvânico (GC) a fim de reduzir significativamente a vulnerabilidade a ataques quando comparado ao uso de tecnologias de comunicação convencionais, tais como Bluetooth, Zigbee, e outras. Na comunicação por acoplamento galvânico, os dados são codificados e transmitidos por impulsos elétricos de baixíssima tensão enviados pela pele humana, sendo então imune a ataques, como bisbilhotagem e outros, não havendo até o momento registros de ataques eficientes contra a GC. O acoplamento galvânico atua sobre a comunicação intracorporal e está no escopo do padrão IEEE 802.15.6. No sistema de transmissão intracorporal usando acoplamento galvânico, aplica-se um sinal elétrico diferencial em dois eletrodos de transmissão posicionados na pele. Grande parte dos sinais enviados pelos eletrodos para a pele se dispersa pelo circuito emissor. Entretanto, uma quantidade pequena dos sinais utiliza a pele e tecidos como canal condutor, alcançando os dois eletrodos de contato no equipamento receptor. A principal característica do sinal diferencial no GC consiste do modelo de envio das informações através dos dois eletrodos. Em cada eletrodo, inverte-se proporcionalmente os sinais antes da transmissão pela pele. O dispositivo receptor calcula a diferença entre os dois sinais recebidos, obtendo o sinal original.

O sinal é fortemente influenciado pelas propriedades dielétricas (isolantes) dos tecidos corporais. O canal corporal é utilizado como meio tanto para envio de informações (Tx), quanto para recebimento (Rx), sendo a modulação e a potência do sinal elétrico muito relevantes. A escolha da modulação deve refletir as características do circuito GC, enfatizando-se a robustez e a simplicidade. São dois os principais tipos de modulação utilizados na comunicação galvânica, a modulação por posição do pulso (PPM – *Pulse-Position Modulation*) e a modulação por largura (duração) de pulso (PWM – *Pulse-Width Modulation*). Particularmente, este trabalho segue a modulação PWM por consumir menos energia e se adequar à natureza *On-Off* dos dispositivos digitais. A modulação PWM representa os dados digitais através das variações de amplitude e duração em uma onda portadora. A PWM estima os dados através da presença ou ausência de uma onda portadora e seu percentual de duração em cada estado *On* ou *Off*. A presença de uma onda por um período de tempo específico, tem o valor binário 1, enquanto a ausência da onda portadora por um período de tempo indica valor binário 0.

3.4. Processo de Autenticação

O processo de autenticação do usuário (Figura 1(c)) ocorre no coordenador da rede vestível. Após a aquisição dos dados, pré-processamento do sinal PPG e envio deste para o dispositivo coordenador através da comunicação galvânica, o sinal passa por um tratamento para extrair as características únicas do usuário tendo como entrada a onda do sinal PPG pré-processada. A extração das características é feita em etapas. A primeira etapa consiste em identificar os picos em todo o comprimento do sinal coletado e pré-processado. Esta identificação é fundamental para definir os pontos de referência para

a etapa de segmentação. Para esta etapa, aplicam-se algoritmos que percorrem séries temporais em busca de pontos altos (picos) e baixos (vales). Exemplos de algoritmos são herdados de outras aplicações, como na análise de registro de uso da CPU para encontrar os períodos de maior utilização, ou na localização de agudos em uma onda de áudio. Estes tipos de algoritmos tomam como referência médias móveis ou um conjunto de características (ex. altura mínima e máxima do pico) para o cálculo de limiares.

A segunda etapa consiste na segmentação do sinal coletado. Cada onda é individualizada e, posteriormente, todas as ondas detectadas são sobrepostas e alinhadas utilizando os picos detectados anteriormente como centralizadores. Isto permite correlacionar (terceira etapa) todos os segmentos e calcular a média de correlação. A esta média nos referimos como identificador do usuário (quarta etapa). Este identificador é então comparado aos modelos de referência calculados no processo de registro (explicado a seguir) de cada usuário no sistema. Caso o identificador case com algum modelo de referência existente, o usuário é autenticado. Caso contrário, o acesso ao sistema é rejeitado.

O processo de registro ocorre *offline* e deve acontecer antes do processo de autenticação. O registro ocorre uma única vez e caso o usuário não tenha sido registrado previamente no sistema, ele não será autenticado. As etapas do processo de registro são similares às etapas do processo de autenticação, porém algumas diferenças existem, tais como a captura de uma maior quantidade de dados, a possibilidade de considerar diferentes posições e estados físicos do usuário, e a inexistência de restrição no tempo de resposta. O processo de registro também inicia-se com a aquisição de diferentes amostras do sinal PPG do usuário. Em seguida, ocorre a extração de características, i.e., segmentação do sinal e identificação dos picos. As ondas individualizadas são alinhadas tomando os picos como centralizadores. Isto permite o cálculo da correlação entre todos os segmentos e da sua média. A média de correlação é utilizada para a definição de um limiar de autenticação (modelo de referência do usuário), sendo este o valor mínimo da média para que um usuário seja autenticado no sistema. Cada usuário registrado terá um modelo de referência armazenado no sistema, esse modelo é o produto final obtido no processo de registro descrito. Durante a tentativa de autenticação, o modelo de referência será comparado ao identificador do usuário (calculado *online*) gerado do processo de autenticação.

A Figura 5 resume os processos de registro e de autenticação apresentados. Conforme mencionado, o usuário precisa ter sido previamente registrado para que ele seja autenticado no sistema. O processo de registro ocorre *offline*, ou seja, antes de ser utilizado e pode ocorrer por uma escala de tempo superior à autenticação. O processo de autenticação ocorre *online*, i.e., quando o usuário precisa de acesso ao sistema ou serviço. Todas as etapas deste último processo precisam ser feitas de modo rápido e eficiente.

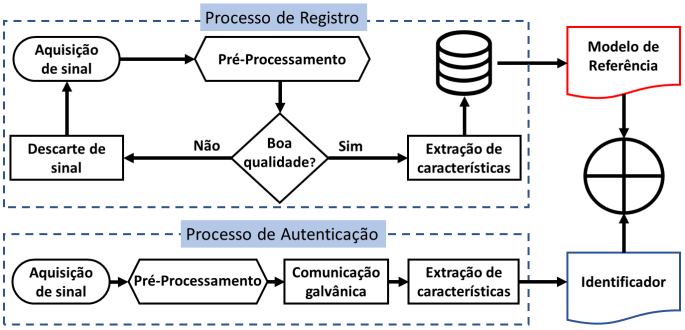


Figura 5. Processos de Registro e de Autenticação do Sistema BEAT

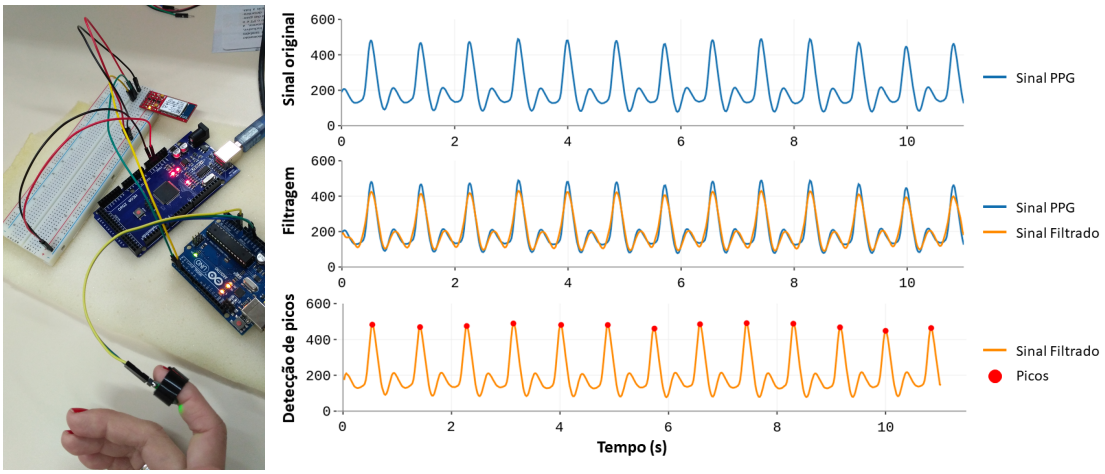
4. Avaliação

Esta seção descreve a metodologia de avaliação do sistema BEAT e os resultados. A avaliação ocorreu seguindo duas abordagens: (i) através de um ambiente experimental criado para os testes dentro do escopo do projeto de cooperação internacional NSF/RNP HealthSense; e (ii) utilizando uma base de dados do repositório Physionet. A intenção em seguir essas duas abordagens foi de comparar seus resultados.

4.1. Ambiente Experimental

O ambiente de testes criado no laboratório NR2/UFPR tomou como base o sensor PPG *Gravity Heart Rate Monitor Sensor* da empresa DfRobot, o qual apresenta pico de resposta espectral de 570 nm. Este sensor foi escolhido após testes com outros tipos/modelos de sensores PPG e pelo baixo custo e alta qualidade nas medições. O sensor PPG foi acoplado a uma plataforma aberta Arduino, versão R3, com microcontrolador ATmega328 de 16 MHz, mesmo microcontrolador utilizado em diversos dispositivos vestíveis. Todos os componentes de hardware seguem as versões padrão dos fabricantes, i.e., não sofreram qualquer alteração física. A Figura 6(a) mostra o testbed utilizado para coleta dos dados no processo de registro dos usuários.

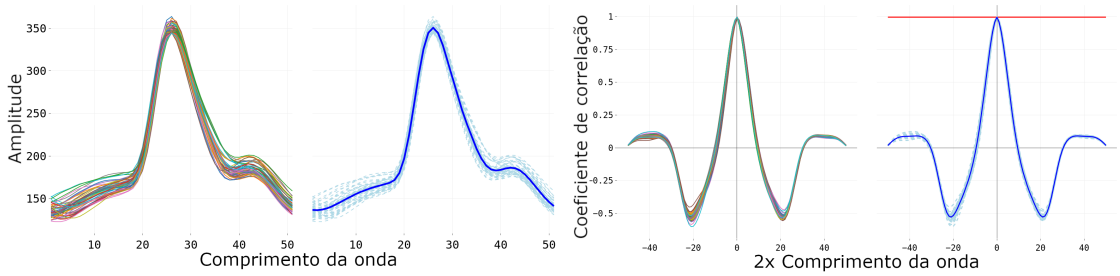
O processo de registro dos usuários (*offline*) ocorreu em um ambiente controlado, restrito de interferências eletromagnéticas e sem incidência direta de luz natural. Os dados relacionados aos sinais PPG dos usuários registrados são tratados e armazenados em um notebook Dell Inspiron 15 com processador de 1,6 GHz e quatro núcleos, em arquivos contendo valores da linha temporal e valores numéricos do sinal PPG para cada indivíduo. A saída do processo de registro foram duas base de dados denominadas NR2/UFPR #1 e NR2/UFPR #2, contendo dados de 30 indivíduos saudáveis entre 23 e 53 anos e sem histórico de problemas cardíacos. Cada indivíduo teve seu o sinal PPG coletado e registrado em dois estados, em pé e sentado. Assim, a base de dados NR2/UFPR #1 possui dados dos indivíduos sentados, já a base de dados NR2/UFPR #2 possui dados dos indivíduos em pé. Os registros dos usuários ocorreram em momentos distintos, como aconteceria em uma situação real. As bases incluem uma amostra de três minutos em cada estado. A Figura 6(b) ilustra para uma amostra as diferenças entre um sinal original (tal como capturado pelo sensor), o sinal filtrado e a indicação dos picos no sinal filtrado.



(a) Sensor PPG (b) Sinais e Pré-Processamento

Figura 6. Processo de Registro dos Usuários

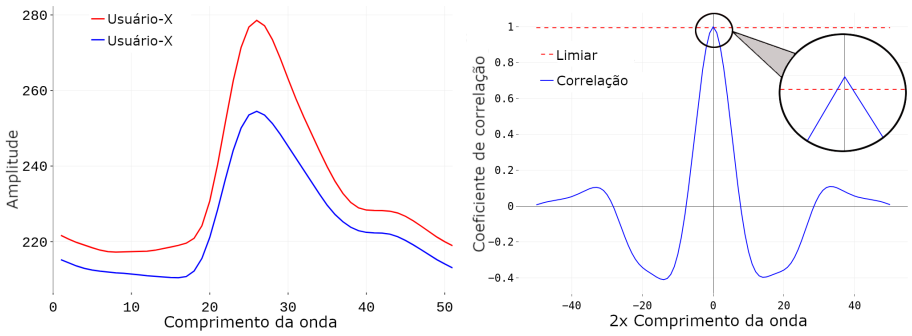
Para obtenção do sinal filtrado, aplicou-se o filtro *low-pass* Chebyshev II de oitava ordem através da ferramenta R. As principais características disponíveis no sinal PPG são obtidas entre 0,5-5 Hz. Assim, a filtragem otimiza o sinal dentro desta faixa. A escolha deste filtro deve-se ao requisito de simplicidade, pois em geral os dispositivos vestíveis são equipados com microcontroladores de baixo poder computacional. Antes da extração de características para a criação do modelo de referência do usuário, é preciso seguir um algoritmo de detecção dos picos, como ilustra a Figura 6(b). A função *findpeaks* da ferramenta R permite a correta identificação dos picos. Após a identificação dos picos e sobreposição das ondas, aplica-se a função de correlação cruzada **ccf** (*cross correlation function*), a fim de obter a média de correlação entre todos os segmentos sobrepostos (Figura 7(a)). Esta função possibilita o cálculo da correlação contemporânea entre duas séries distintas e seus respectivos intervalos de confiança. Baseada na média da correlação cruzada, calcula-se o limiar de autenticação, que servirá como modelo de referência para autenticar um usuário (Figura 7(b)).



(a) Ondas sobrepostas e média (b) Definição de limiar

Figura 7. Correlação entre Ondas de um Mesmo Usuário

Os testes do processo de autenticação coletaram um minuto de dados de cada usuário, nos estados em pé e sentado. Os passos do processo de autenticação foram seguidos como descrito na Seção 3, sendo os casos de sucesso e insucesso contabilizados para o cálculo das métricas apresentadas nos resultados. A Figura 8(a) compara o modelo de referência registrado para um usuário X (curva em vermelho) e o identificador (curva azul) calculado para este mesmo usuário calculado durante o processo de autenticação. Embora as duas curvas não sejam idênticas, elas se encontram dentro do limiar estabelecido, indicando a existência de similaridade suficiente para autenticar o usuário, como observado na Figura 8(b). Ou seja, este é um exemplo de sucesso na autenticação.



(a) Modelo de Referência vs. Identificador (b) Sinal Processado vs. Limiar

Figura 8. Comparação entre Modelo de Referência e Identificador

Entre a coleta do sinal pelo dispositivo vestível (Arduino) e a recepção dos dados pelo dispositivo coordenador, os dados são tratados e enviados pelo tecido corporal, a Figura 9 ilustra o funcionamento do GC implementado neste trabalho. O microcontrolador aciona o sensor PPG no dispositivo vestível e recebe o sinal PPG. Os dados PPG são quantificados e convertidos em binário para interpretação pelo dispositivo microcontrolador. Para preparar a transmissão do sinal, baseados nos dados binários e na duração do bit pré-selecionado, alterna-se a saída de modulação por largura de pulso do microcontrolador, combinada com a lógica interna controlável. Um filtro *low-pass* remove os harmônicos do sinal, preservando a faixa central (FC = 100kHz).

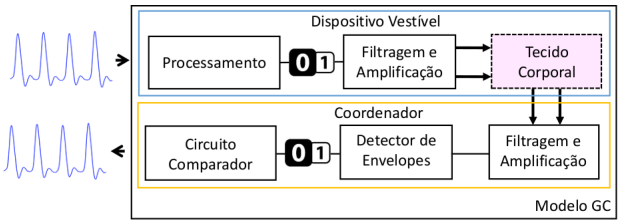


Figura 9. Modelo Implementado do GC

Após a filtragem e preparação, os dados são enviados através do canal de comunicação dentro da carga útil (*payload*) de um quadro, que consiste em um preâmbulo (código Barker de 13 bits) para sincronização, campo de comprimento de dados, carga útil (64 bits) e um CRC de 8 bits. Assim que o sinal se propaga pelo corpo humano, o hardware do receptor analógico utiliza um filtro *high-pass* para remover qualquer ruído de baixa frequência associado à interferência da linha de alimentação. Um amplificador (MAX4488 da Maxim Integrated TM) neutraliza a atenuação do canal e do filtro de alta frequência, enquanto eleva o nível do sinal para atender aos requisitos de voltagem de ativação do diodo tipo schottky. Um circuito detector de envelopes é implementado para converter os sinais ao estado original e remover qualquer oscilação de onda portadora antes de entregar o sinal para o circuito comparador. Os limiares de potência são controlados por um potenciômetro e é construído para reproduzir a sequência binária original recebida do transmissor. O receptor decodifica os dados, obtendo o sinal PPG original e dando sequência ao processo de extração e verificação do identificador.

Além dos testes realizados no ambiente experimental descrito, avaliou-se o sistema BEAT tomando como entrada a base de dados do *Beth Israel Deaconess Medical Centre*, presente no repositório Physionet [Goldberger et al. 2000]. Esta base contém sinais PPG coletados de 30 indivíduos na frequência de 125 Hz pelo centro israelense. Os indivíduos desta base sofriam de alguma condição de saúde crítica (ex. problemas cardíacos, respiratórios, outros) e estavam em repouso no leito hospitalar. As anotações dos registros divulgados na base de dados foram feitas manualmente. O uso da base de dados do Physionet tem como objetivo comparar os resultados do processo de autenticação com os resultados obtidos com as bases NR2/UFPR. Entretanto, cabe ressaltar que como a base do Physionet foi gerada e divulgada pelo centro israelita, nós não tivemos controle em sua criação, ex. qualidade do ambiente em que foram coletados os dados ou a qualidade do sensor PPG. Cada sinal da base PPG foi segmentado, utilizando-se três minutos de informação para criação do modelo de usuário e um minuto para o identificador. Observa-se também que após a construção dos modelos de referência para cada usuário, apenas o processo de autenticação (Figura 1(c)) foi avaliado para a base de dados do Physionet.

4.2. Resultados

A referência principal de avaliação empregada foi a taxa de sucesso na autenticação dos usuários e suas variações. Neste contexto, um erro é calculado pela taxa de falsos positivos

ou taxa de falsos negativos. Na Tabela 1, observam-se as indicações das três bases de dados e seus resultados para as métricas verdadeiro positivo e negativo, falso positivo e negativo, acurácia e total de inferências, sendo o total de inferências a comparação de todas as identidades com todos os modelos de usuários.

	Verdadeiro Postivo (VP)	Falso Positivo (FP)	Verdadeiro Negativo (VN)	Falso Negativo (FN)	Total de inferências (TI)	Acurácia
Base NR2/UFPR #1	30	12	858	0	900	**98,66%**
Base NR2/UFPR #2	23	50	600	3	676	**92,15%**
Physionet	30	91	779	0	900	**89.88%**

Tabela 1. Bases de dados NR2/UFPR e Physionet

O sistema de autenticação, quando confrontado com as bases de dados disponíveis, obteve os seguintes resultados: para a base NR2/UFPR #1 o sistema obteve os melhores resultados, tendo uma acurácia de 98,66%, 12 falsos positivos e nenhum falso negativo. Para a base da Physionet, o sistema obteve uma acurácia de 89,88% e nenhum falso negativo, porém alcançou 91 falsos positivos em 900 inferências. A base NR2/UFPR #2 apresentou inconsistência nos dados de alguns usuários, não sendo possível encontrar uma sequência de picos satisfatória e de maneira sequencial, sendo assim, esta base contou com apenas 26 usuários válidos dos 30 e 676 inferências. Para a base NR2/UFPR #2, considerando os usuários válidos, o sistema obteve acurácia de 92,15%, 3 FNs e 50 FPs.

Mesmo com a aplicação de filtros para suavização e diminuição de ruídos, alguns fatores não puderam ser contornados, como a movimentação excessiva durante a coleta, a interferência eletromagnética, e outros fatores ambientais. O sistema se mostrou mais eficiente com a base NR2/UFPR #1, pois foi a base em que os dados foram coletados de forma mais controlada. A posição sentada do usuário permitiu o descanso do braço onde o sensor está posicionado, o que gera menos movimentação e uma onda mais estável. Observam-se na Figura 10 os resultados de todas os identificadores confrontados, nota-se que para a base NR2/UFPR #1, os falsos positivos estão dispersos no mapa de autenticação, indicando que os dados de coleta são estáveis, possibilitando extrair diversas características da onda. Mesmo com o sinal obtido de usuários em estado de saúde debilitado, o sistema obteve uma acurácia próximo de 90% para a base Physionet. Estimamos que alto número de falsos positivos pode estar relacionado ao sinal PPG de baixa qualidade presente na base, uma vez que 60,4% de todos os falsos positivos são atribuídos a apenas 4 usuários. Avaliando os dois mapas de autenticação, observa-se que nenhum deles obteve falsos negativos, indicando que em todos os casos em que um usuário legítimo tentou se autenticar, o sistema obteve sucesso.

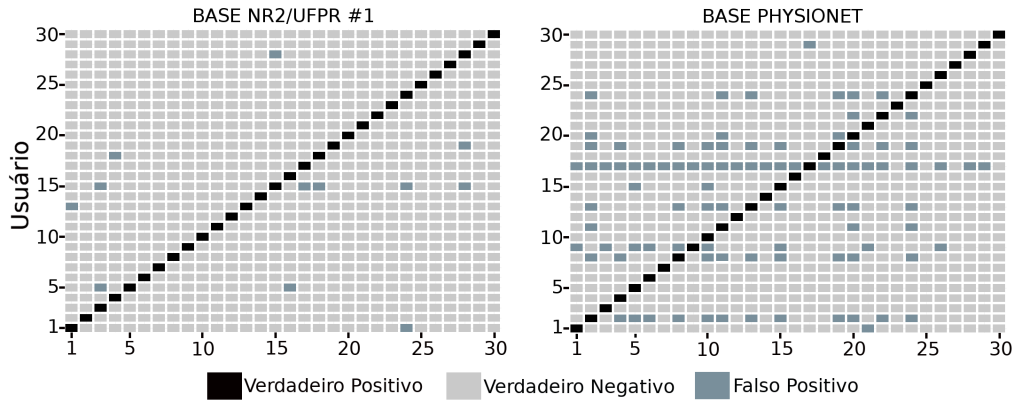


Figura 10. Mapa de Autenticação

5. Conclusões

Este trabalho apresentou BEAT, um sistema de autenticação que utiliza as características de um biosinal PPG e a pele como canal de comunicação para autenticar usuários em uma rede vestível. O sinal PPG é obtido de maneira constante e não intrusiva, e transmitido de forma segura através de comunicação galvânica, mantendo o usuário conectado continuamente. O sistema BEAT foi testado através de experimentação. Três bases de dados distintas serviram de referência para o cálculo da acurácia, falsos positivos e negativos, e verdadeiros positivos e negativos. Os resultados indicam acurácias acima de 90% para as bases de dados geradas considerando um ambiente controlado e acurácia próxima de 90% para a base de dados do repositório Physionet. Obteve-se um alto índice de verdadeiros positivos e baixo nível de falsos negativos, a incidência de falsos positivos no sistema BEAT está relacionada diretamente à qualidade do sinal PPG. Os resultados dos experimentos com o sistema indicam a viabilidade do sinal PPG como autenticador biométrico tomando a comunicação galvânica como meio de transmissão de dados. Em trabalhos futuros, pretende-se explorar dispositivos com uma maior imunidade aos problemas inerentes à obtenção do sinal e aperfeiçoar a extração de suas características.

Agradecimentos

Os autores agradecem o apoio da UFPR, CAPES, CNPQ, RNP e *National Science Foundation* (NSF). Este trabalho contou com auxílio financeiro do projeto de cooperação EUA-Brasil HealthSense, sob o termo de cooperação #99/2017 RNP/FUNPAR/UFPR.

Referências

Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28.

Belgacem, N., Fournier, R., Nait-Ali, A., and Bereksi-Reguig, F. (2015). A novel biometric authentication approach using ECG and EMG signals. *J. of Medical Engr. & Tech.*, 39(4):226–238.

Blasco, J., Chen, T. M., Tapiador, J., and Peris-Lopez, P. (2016). A survey of wearable biometric recognition systems. *ACM Computing Surveys (CSUR)*, 49(3):1–35.

Bonissi, A., Labati, R. D., Perico, L., Sassi, R., Scotti, F., and Sparagino, L. (2013). A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *IEEE BIOMS*, pages 28–33. IEEE.

Chen, L.-F., Liao, H.-Y. M., Ko, M.-T., Lin, J.-C., and Yu, G.-J. (2000). A new lda-based face recognition system which can solve the small sample size problem. *Pattern recognition*, 33(10):1713–1726.

Gao, W., Emaminejad, S., Nyein, H. Y. Y., Challa, S., Chen, K., Peck, A., Fahad, H. M., Ota, H., Shiraki, H., Kiriya, D., et al. (2016). Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis. *Nature*, 529(7587):509–527.

Goldberger, A. L., Amaral, L. A. N., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., and Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation*, 101(23):215–220.

Gu, Y. and Zhang, Y. (2003). Photoplethysmographic authentication through fuzzy logic. In *IEEE EMBS*, pages 136–137. IEEE.

Gu, Y., Zhang, Y., and Zhang, Y. (2003). A novel biometric approach in human verification by photoplethysmographic signals. In *IEEE EMBS*, pages 13–14. IEEE.

Huang, Y.-P., Luo, S.-W., and Chen, E.-Y. (2002). An efficient iris recognition system. In *In Proceedings of International Conference on Machine Learning and Cybernetics*, volume 1, pages 450–454. IEEE.

IDTechEX (2018). Wearable technology market by 2028. `https://goo.gl/7E1pKb`. Accessed: 2018-12-05.

Jain, A. K., Hong, L., Pankanti, S., and Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9):1365–1388.

Kim, D.-S. and Hong, K.-S. (2008). Multimodal biometric authentication using teeth image and voice in mobile environment. *IEEE Transactions on Consumer Electronics*, 54(4):1790–1797.

Li, Z., Han, W., and Xu, W. (2014). A large-scale empirical analysis of chinese web passwords. In *USENIX Security Symposium*, pages 559–574.

Liang, Y., Elgendi, M., Chen, Z., and Ward, R. (2018). An optimal filter for short photoplethysmogram signals. *Scientific data*, 5:180076.

Lin, F., Song, C., Zhuang, Y., Xu, W., Li, C., and Ren, K. (2017). Cardiac scan: A non-contact and continuous heart-based user authentication system. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 315–328. ACM.

Lourenço, A., Silva, H., and Fred, A. (2011). Unveiling the biometric potential of finger-based ecg signals. *Computational intelligence and neuroscience*, 2011:1–8.

Marcel, S. and Millán, J. d. R. (2007). Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):743–752.

Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Kelley, P. G., Shay, R., and Ur, B. (2013). Measuring password guessability for an entire university. In *Proceedings of the ACM SIGSAC*, pages 173–186. ACM.

Miyamoto, C., Baba, S., and Nakanishi, I. (2009). Biometric person authentication using new spectral features of electroencephalogram (EEG). In *IEEE ISPACS*, pages 1–4. IEEE.

Mosenia, A., Sur-Kolay, S., Raghunathan, A., and Jha, N. K. (2017). Caba: Continuous authentication based on bioaura. *IEEE Transactions on Computers*, 66(5):759–772.

Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48.

Singh, Y. N. and Singh, S. K. (2012). Evaluation of electrocardiogram for biometric authentication. *J. Information Security*, 3(1):39–48.

Spachos, P., Gao, J., and Hatzinakos, D. (2011). Feasibility study of photoplethysmographic signals for biometric identification. In *IEEE DSP*, pages 1–5. IEEE.

Tomlinson, W., Banou, S., Yu, C., Nogueira, M., and Chowdhury, K. (2019). Secure on-skin biometric signal transmission using galvanic coupling (to appear). In *IEEE INFOCOM*. IEEE.

Vasisht, D., Zhang, G., Abari, O., Lu, H.-M., Flanz, J., and Katabi, D. (2018). In-body backscatter communication and localization. In *ACM SIGCOMM*.

Wu, G., Wang, J., Zhang, Y., and Jiang, S. (2018). A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors*, 18(1):179.

Yamaba, H., Kurogi, A., Kubota, S.-I., Katayama, T., Park, M., and Okazaki, N. (2017). Evaluation of feature values of surface electromyograms for user authentication on mobile devices. *Artificial Life and Robotics*, 22(1):108–112.