sensores

Artigo

Projeto de autenticação biométrica segura baseada em ECG em redes de sensores de área corporal

Steffen Peter *, Bhanu Pratap Reddy, Farshad Momtaz e Tony Givargis

Center for Embedded and Cyber-Physical Systems, University of California, Irvine, CA 92697-3455, USA; bpreddy@uci.edu (BPR); fdoktorm@uci.edu (FM); givargis@uci.edu (TG)

* Correspondência: st.peter@uci.edu ; Tel .: + 1-949-824-9023

Editor Acadêmico: Rongxing Lu

Recebido: 7 de janeiro de 2016; Aceito: 13 de abril de 2016; Publicado: 22 de abril de 2016

Abstrato: Redes de sensores de área corporal (BANs) utilizam nós sensores de comunicação sem fio conectados a um corpo humano para aplicações de conveniência, segurança e saúde. As características fisiológicas do corpo, como a frequência cardíaca ou os sinais do eletrocardiograma (ECG), são meios promissores para simplificar o processo de configuração e melhorar a segurança dos BANs. Este documento descreve as etapas de projeto e implementação necessárias para realizar um protocolo de autenticação baseado em ECG para identificar nós sensores anexados ao mesmo corpo humano. Portanto, a primeira parte do artigo aborda o projeto de um sistema de sensor de área corporal, incluindo a configuração do hardware, processamento de sinal analógico e digital e técnicas de detecção de recurso de ECG necessárias. Um fluxo de projeto baseado em modelo é aplicado e os pontos fortes e as limitações de cada etapa do projeto são discutidos. Os dados medidos do mundo real originados do sistema de sensor implementado são então usados para configurar e parametrizar um novo protocolo de autenticação fisiológica para BANs. O protocolo de autenticação utiliza propriedades estatísticas de desvios esperados e detectados para limitar o número de tentativas de autenticação de falso positivo e falso negativo. O resultado do esforço de design holístico descrito é a primeira implementação prática da autenticação biométrica em BANs que reflete as incertezas de tempo e dados nas partes físicas e cibernéticas do sistema. O protocolo de autenticação utiliza propriedades estatísticas de desvios esperados e detectados para limitar o número de tentativas de autenticação de falso positivo e falso negativo. O resultado do esforço de design holístico descrito é a primeira implementação prática da autenticação biométrica em BANs que reflete as incertezas de tempo e dados nas partes físicas e cibernéticas do sistema. O protocolo de autenticação utiliza propriedades estatísticas de desvios esperados e detectados para limitar o número de tentativas de autenticação de falso positivo e falso negativo. O resultado do esforço de design holístico descrito é a primeira implementação prática da autenticação biométrica em BANs que reflete as incertezas de tempo e dados nas partes físicas e cibernéticas do sistema.

Palavras-chave: redes de sensores de área corporal; biométrico; autenticação; Projeto

---

1. Introdução

Redes de sensores de área corporal (BANs) são uma tecnologia promissora para aplicações de conveniência, segurança e saúde [1] Exemplos de BANs incluem rastreadores de condicionamento físico, óculos inteligentes [2], monitoramento vital de equipes de resposta a emergências [3] e dispositivos médicos implantáveis, como marca-passos cardíacos e bombas de insulina. Essas aplicações de rede de área corporal (BAN) relacionadas com a segurança médica e exigem um alto nível de controle de acesso e proteção de dados [4 - 7] No entanto, a meta de boa segurança em BANs é desafiada pelas capacidades de nós sensores de área corporal típicos. Por razões econômicas e práticas, os nós são pequenos e têm recursos limitados, fornecendo apenas memória e poder de computação limitados.

Embora existam protocolos e implementações de segurança para proteger dados em dispositivos severamente restritos [8 , 9], permanece a questão de como os dispositivos que pertencem à mesma área corporal se identificam e confiam uns nos outros. Figura 1 ilustra o problema: os sensores conectados a uma pessoa (Sensor A, B e C) devem se conhecer e confiar uns nos outros, enquanto os sensores conectados a outras pessoas (E) ou dados inteiramente forjados (D) não são confiáveis. Soluções como chaves pré-implantadas [10] ou as configurações manuais são complicadas e sujeitas a erros - especialmente em ambientes com vários BANs interferentes.

O trabalho neste artigo aborda o desafio de identificar nós que estão fisicamente ligados ao mesmo corpo humano. Este mecanismo pode ser usado:

- para configuração rápida e conveniente de um BAN, por exemplo para rastreadores de fitness, sensores de tórax e pulseiras inteligentes,

- para a configuração de um ambiente de área corporal confiável e seguro com uma chave compartilhada, e
- como um segundo fator de autenticação em BANs com equipamentos médicos implantados essenciais, para prevenir acesso errôneo acidental ou malicioso aos dispositivos médicos.

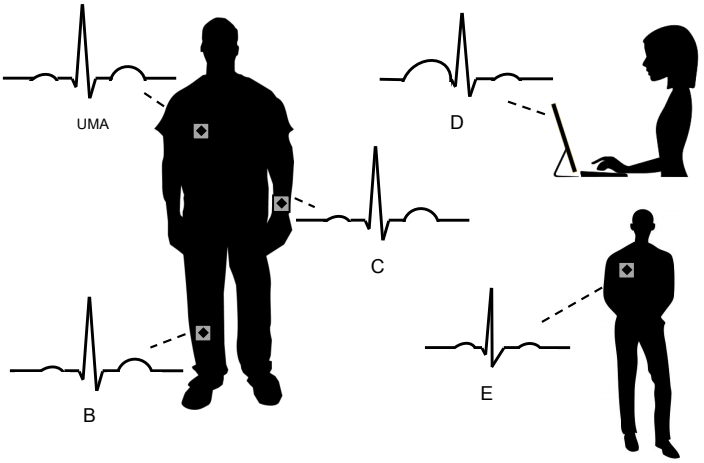

Figura 1. Um BAN compreende sensores conectados a um corpo humano. Os dados de eletrocardiografia (ECG) podem garantir que os sensores, conectados ao mesmo corpo (**ABC)** confiam uns nos outros, mas não confiam nos sensores (**E)** e dispositivos (**D)** que não estão ligados ao mesmo corpo.

Como característica fisiológica neste trabalho, usamos dados de ECG. O ECG registra a atividade elétrica do coração e é característico de uma pessoa em um determinado momento. ECG e dados cardíacos relacionados podem ser obtidos a partir de sensores que estão conectados ao corpo, mesmo localmente, conforme mostrado em [11 - 14] A literatura já discutiu a autenticação baseada em ECG e os protocolos de acordo de chave [15 - 18], no entanto, sem considerar as implicações práticas dos sensores de baixo custo e das plataformas BAN com recursos limitados. Em vez disso, o trabalho existente usou dados clínicos de ECG obtidos de bancos de dados médicos e processou os dados em PCs, ignorando as incertezas originadas de sensores e processamento.

Neste artigo, apresentamos um protocolo de autenticação biométrica que reflete intrinsecamente as propriedades estatísticas das incertezas, para equilibrar sistematicamente o risco de falsas autenticações rejeitadas e falsas tentativas aceitas. Abordamos esses problemas em duas etapas:

1. Projeto e implementação de uma plataforma de sensor (Seção 4), incluindo métodos adequados de processamento de dados e detecção de recursos. Aplicamos um fl uxo de projeto baseado em modelo [19], começando com um modelo analítico em Matlab, teste-o em modelos em tempo real em um PC (Seção 5) e, finalmente, traduzi-lo para o plataforma de sistema embarcado, levando em consideração os recursos limitados de um BAN na Seção 6 . Com base em dados
2. empíricos coletados do nó do sensor implementado, projetamos e parametrizamos um protocolo de estabelecimento de sessão segura na Seção 7 . Mostramos que as propriedades estatísticas das incertezas do sistema podem ser aproveitadas para melhorar a confiança dentro do processo de autenticação.

A contribuição do nosso trabalho é a conexão dos resultados da implementação e a parametrização do protocolo de segurança. Mostramos que a incerteza nas medições pode ser tratada, mas precisa ser refletida no protocolo de segurança para evitar um alto número de rejeições ou autenticações falsas.

O resultado é o primeiro protocolo de autenticação biométrica que funciona em nós BAN reais. O sistema apresentado mostra 100% de autenticações corretas com uma probabilidade de um ataque bem-sucedido de menos de 0,1%. Apresentamos o design do hardware, o algoritmo e a implementação do software, e discutimos os parâmetros do protocolo de segurança selecionados.

2. Preliminares e Metodologia

Esta seção apresenta brevemente os fundamentos e a terminologia do ECG e, a seguir, discute a metodologia de projeto que usamos ao longo deste artigo.

2.1. ECG Básico

Eletrocardiografia (ECG) é definida como o processo de registro da atividade elétrica do coração durante um período de tempo usando eletrodos colocados no corpo de uma pessoa. Esses eletrodos detectam as minúsculas mudanças elétricas na pele que surgem da despolarização do músculo cardíaco durante cada batimento cardíaco [1]

Um traço esquemático de dois batimentos cardíacos é mostrado na Figura 2 . Características dominantes do sinal são os cinco picos, chamados P, Q, R, S e T, enquanto o pico mais significativo é o R pico. Todas as informações fornecidas pelo ECG existem principalmente entre 0,05 Hz a 100 Hz, uma vez que o comprimento de um complexo QRS é normalmente entre 0,06 e 0,1 s [20] Embora características como o tempo Q-to-R ou R-to-S possam ser aplicadas para fins de autenticação, neste artigo, nos concentramos nos intervalos entre pulsos (IPI). Como mostrado na figura 2 , o IPI pode ser medido entre dois picos Q adjacentes (Q-IPI), picos R (R-IPI) ou picos S (S-IPI). Uma vez que a frequência cardíaca (HR) típica de um ser humano varia entre 30 e 240 batimentos por minuto (bpm) [20], o IPI varia entre 250 ms e 2000 ms (IPI = 60 s / HR).

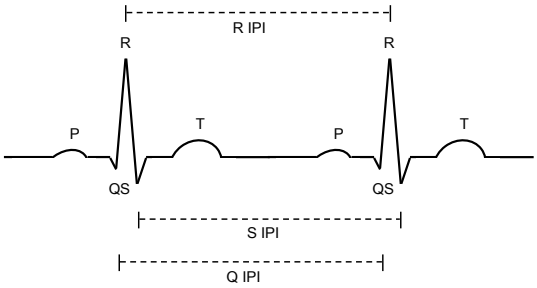

Figura 2. Características do sinal cardíaco e intervalos interpulso (IPI) entre os picos.

Embora a ocorrência de batimentos cardíacos não seja simultânea em cada local do corpo, os IPIs de uma pessoa são aproximadamente equivalentes, independentemente do local medido. Portanto, o IPI é adequado para uma aplicação em BANs. O IPI é particularmente interessante, pois pode ser medido não apenas por sensores de ECG, mas por [12], acústico [13] ou pressão do tecido [14] sensores e outros dispositivos BAN.

2.2. Declaração do problema, metodologia e esboço

A ideia geral do protocolo de autenticação biométrica que apresentamos na Seção 7 é medir os IPIs por um determinado tempo em nós diferentes. Os nós são considerados no mesmo corpo se os IPIs medidos forem equivalentes ou muito semelhantes. Os principais desafios neste processo são:

- incerteza do fenômeno físico (biológico) subjacente,
- incerteza de tempo e jitter nas partes cibernéticas (sensores, interfaces, processamento) e
- parametrização do protocolo de autenticação, para omitir a rejeição de emparelhamentos de sensores válidos, mas reduzir a probabilidade de tentativas de emparelhamento inválido serem bem-sucedidas devido a uma alta tolerância de desvio.

Para enfrentar esses desafios, neste artigo, buscamos um fl uxo de projeto baseado em modelo que gravita em torno de dados de sensores reais, em vez de uma biblioteca de dados ideal. A metodologia e o esboço do nosso trabalho são mostrados na Figura 3 . Como primeiro passo, selecionamos o hardware, incluindo os sensores e suas interfaces. O acesso ao sensor inclui o projeto de uma placa do sensor para filtragem analógica e pré-processamento de sinal. Em seguida, selecionamos e implementamos as etapas de processamento de sinal digital e o algoritmo de detecção de IPI que funciona com os dados coletados. Para o primeiro teste prático, usamos a placa do sensor da implementação Matlab das etapas de processamento de sinal, rodando em um PC, conforme discutido na Seção 5 . Para a implementação de BAN real, aplicamos a geração automática do código do sistema a partir do ambiente Matlab / Simulink e comparamos o desempenho a uma implementação manual em C. O benefício da abordagem Simulink é o fluxo de design baseado em modelo contínuo, enquanto o O principal benefício da implementação C é seu desempenho superior. Por fim, aplicamos os dados do sensor, reunidos em

nosso protótipo, para parametrizar um protocolo de autenticação BAN biométrico seguro. O resultado é um protocolo que utiliza as propriedades dos dados do sensor medido para melhorar a con fi ança na autenticação.

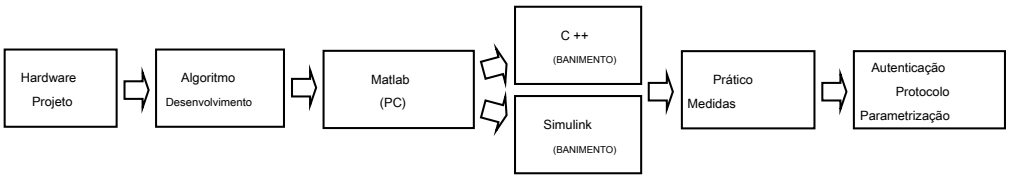

Figura 3. Fluxo de desenvolvimento.

3. Trabalho Relacionado

Segurança geral e privacidade em redes corporais é um tópico complexo que foi abordado em uma série de artigos de visão geral [4 - 6 , 21] Um subdomínio deste campo é a aplicação de propriedades biométricas e fisiológicas do corpo como meio para estabelecer autenticação ou para gerar chaves em tais BANs. Em particular, a autenticação baseada em ECG e IPI recebeu atenção significativa da pesquisa [15 - 17 , 22 , 23]

Por exemplo, protocolo de estabelecimento de chave de sinal baseado em ECG (ESKE) [16] é um esquema de geração de chave tolerante a ruído que funciona sem pré-implantação do material chave. ESKE aplica filtragem wavelet e requer um tamanho de amostra de mais de 30 s para uma única autenticação, o que é inadequado para a maioria dos cenários de BAN. Outro esquema de acordo chave [15] é baseado no Esquema Fuzzy Vault [24] O método permite que um receptor reconstrua uma mensagem se a maioria dos coeficientes do polinômio de criptografia for conhecida. Uma abordagem semelhante é buscada no esquema de acordo de chave baseado em sinal fisiológico (PSKA) [17], que cria uma chave de sessão a partir das informações de frequência dos dados de ECG. No entanto, o PSKA ainda precisa que o receptor e o remetente compartilhem um conjunto de valores-chave equivalentes exatos, o que não pode ser garantido na maioria dos BANs. Esses trabalhos são todos executados em um PC e em estruturas como o Matlab. Além disso, os métodos requerem longos períodos de amostragem para evitar adivinhação of fl ine da chave. Em vez disso, nosso trabalho separa acordo de chave e autenticação. Dessa forma, aplicamos métodos tradicionais de acordo de chave bem estabelecidos, como Dif fi e-Hellman como base, e usamos a autenticação fisiológica como uma etapa adicional.

O protocolo de acordo de chave baseado em características fisiológicas ordenadas (OPFKA) [22] foi implementado em uma plataforma BAN. No entanto, OPFKA também só foi testado com bancos de dados médicos, como o banco de dados de arritmia do MIT-BIH [25], como uma fonte para os sinais de ECG de referência. Esses trabalhos não discutem o impacto de erros de detecção, medição e tempo. Nosso trabalho mostra claramente a importância de lidar e controlar as incertezas da medição. Na verdade, nenhum dos esquemas apresentados funcionou com os dados reais que coletamos de nosso nó sensor implementado.

A viabilidade da autenticação baseada em IPI para BSNs foi mostrada em [18] e [26] Poon [18] demonstrou a aplicabilidade da autenticação baseada em IPI mesmo para diferentes tipos de sensores. Seus experimentos mostraram a interoperabilidade entre os sensores de ECG e oxímetro de pulso (PPG). O trabalho também demonstrou a adequação da autenticação IPI para pessoas mais velhas e menos saudáveis. Ao contrário do nosso trabalho, [18 , 26] aplicam códigos binários que requerem um grande número de valores IPI (> 30) para uma autenticação. Eles também não consideram o impacto das decisões de projeto no processamento de sinais e no projeto de sistemas embarcados.

A aplicação de características fisiológicas também foi discutida para autenticação permanente do usuário, por exemplo, para armazenamento persistente na nuvem [27] A ideia é utilizar chaves de criptografia baseadas em características permanentes da fisiologia humana. Embora nosso trabalho não tenha como objetivo direto a autenticação permanente, a implementação e o fl uxo de design que descrevemos podem ser aplicados para apoiar a identificação permanente em nós BAN no futuro.

Uma gama de abordagens alternativas foi apresentada para configurar BANs seguros e fornecer proteção de acesso e privacidade [28] Como um exemplo, [29] aplica-se à comunicação de campo próximo para garantir a proximidade dos nós de BAN em aplicações médicas. Outras abordagens incluem a troca de chave autenticada por senha e acordo [10], pulseiras, sensores de proximidade ou usando o corpo como um

meio de comunicação [30] Consideramos essas abordagens como possíveis segundos fatores em um processo de autenticação seguro para BANs.

4. Interface de hardware do sensor

Uma vez que o objetivo deste trabalho é usar dados reais do sensor para a autenticação, como uma primeira etapa, temos que selecionar sensores adequados e fazer a interface dos sensores com os nós de computação. Um critério neste ponto era não escolher sensores clínicos e sistemas de filtro, que de fato estão disponíveis [31], mas devido ao custo e tamanho, não são aplicáveis aos BANs. Em vez disso, usamos sensores de baixo custo e projetamos uma placa de processamento de sensores, que então pode ser conectada aos nós BAN.

4.1. Sensores

Como sensores, usamos eletrodos de pano úmido convencionais com hidrogel adesivo condutor reposicionável para medir a atividade elétrica da superfície da pele [32] Um dos principais desafios desses sensores é sua tensão DC offset relativamente baixa, com amplitude de sinal bruto abaixo de 0,5 mV. O ruído adicional se origina internamente no dispositivo, mas também no ambiente. Como resultado, os experimentos iniciais com uma conversão simples de analógico para digital falharam devido ao nível de baixa tensão, um sinal de desvanecimento rápido e alto ruído.

4.2. Placa Sensor

Para extrair, estabilizar e limpar o sinal, projetamos uma placa de sensor que amplifica e filtra os sinais. Aplicamos uma abordagem de amplificador de diferença padrão [31] O amplificador de diferença é uma solução adequada, uma vez que os dados básicos do ECG são obtidos como uma saída da diferença de duas derivações colocadas no corpo. O diagrama de blocos de nossa placa do sensor é mostrado na Figura 4 . O circuito consiste em três partes: o amplificador diferencial, um filtro e um pós-amplificador. Como amplificador diferencial, usamos um amplificador de instrumentação INA121, devido à sua alta precisão e alta rejeição de ruído e sua sensibilidade à faixa de entrada de ECG. O capacitor (C1) na saída do amplificador de instrumentação estabiliza o sinal removendo o deslocamento DC. A saída do amplificador de instrumentação ainda é ruidosa e contém muitos componentes de frequência indesejados. Portanto, aplicamos um amplificador operacional (LM358) para filtrar as frequências características do ECG. Após o estágio de filtro, a pós-amplificação do sinal é realizada para corresponder aos requisitos de entrada do dispositivo de processamento. Em outras palavras, a faixa do sinal de saída é determinada pelo próximo dispositivo que vai usar e processar o sinal de saída. Por exemplo, 6 requer níveis de entrada na faixa de 1 mV a 10 mV. Com base neste requisito, usamos um amplificador de inversão simples em que R4 e R5 são escolhidos apropriadamente para o ganho necessário, dado como G = - R5 / R4. Os parâmetros podem ser adaptados para refletir os requisitos de entrada da plataforma de processamento.

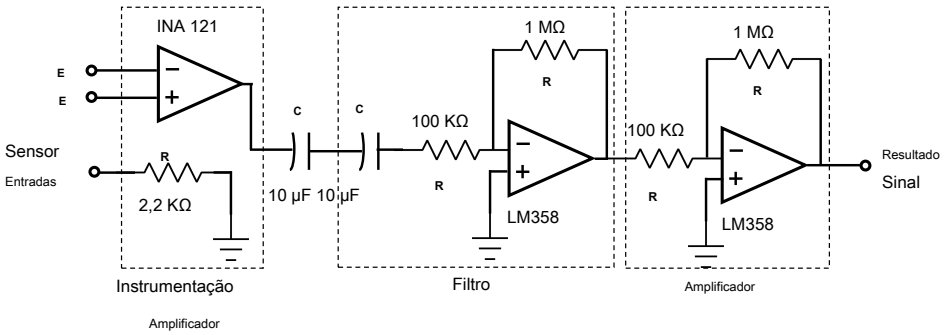

Figura 4. Esquema de nossa placa de processamento do sensor: o amplificador de instrumentação obtém a diferença das entradas do sensor, antes que o sinal único seja filtrado e amplificado.

4.3. Resultados

Um rastreamento de dados coletados com a placa do sensor é mostrado na Figura 5 . O conselho requer 6.0 μ W e tem uma impedância de saída de 1,2 M Ω. Na figura 5 podemos ver que os níveis de saída são claramente distinguíveis e podem ser processados pelo sistema de processamento embutido subsequente. No traçado, os picos da onda PQRST podem ser identificados claramente. Notável também é a estabilidade do nível do sinal, que é importante para o processamento posterior. No entanto, ainda vemos alguns componentes de alta frequência como ruído. É por isso que, na próxima etapa, investigamos o processamento de sinal digital e os algoritmos de detecção de recursos disponíveis para verificar sua adequação para trabalhar com os dados coletados do sensor.

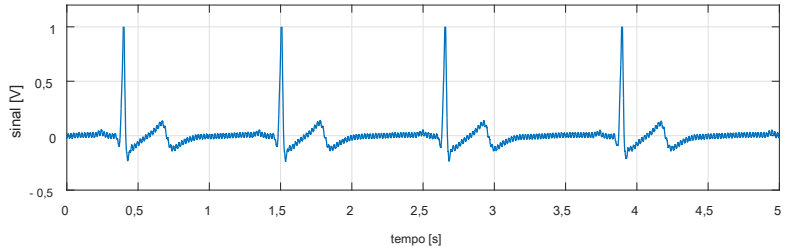

Figura 5. Cinco segundos de dados coletados do sensor após o processamento em nossa placa de sensor. Visíveis estão as características do ECG, mas também alguns artefatos residentes de alta frequência.

5. Processamento de Sinal Digital

Esta seção discute o processamento digital do sinal de ECG coletado. O processo é mostrado na Figura 6 . A entrada é o sinal de ECG de amostra contínua e a saída é uma lista de R-, Q- e S-IPIs. Para processar os dados, as seguintes etapas gerais devem ser executadas:

1 filtragem digital passa-baixa para limpar o sinal de ECG,
2 detecção dos recursos de ECG (picos QRS), e
3 - validação e correção dos valores obtidos, com base no biom.

Descrevemos os detalhes das três etapas no seguinte subse

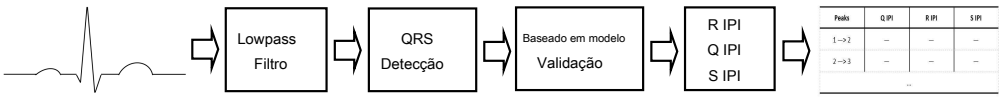

Figura 6. Etapas do processamento digital: o ECG precisa ser filtrado, os picos são detectados e validados. A saída é uma tabela de valores Q, R e S.

5.1. Filtragem Digital

Mesmo que os filtros analógicos em nossa placa de sensor já filtrem o sinal, vários artefatos de alta frequência de fios, hardware e interfaces permanecem. Conforme apresentado na Seção 2,1 , todas as informações importantes do sinal de ECG estão localizadas entre 0,05 Hz a 100 Hz. Essas frequências de corte fixas podem ser filtradas digitalmente com eficiência usando os filtros Butterworth de Resposta ao Impulso In fi nito (IIR) [33] A função de transferência básica de um filtro IIR é dada como:

$$H(z) = \frac{\sum_{i=0} P \; b_{Eu} \, z^{-Eu}}{1 + \sum_{j=1} Q \; uma_j \, z^{-j}} \quad (1)$$

enquanto *uma* e *b* são coeficientes característicos multidimensionais do filtro, e *z* é o sinal a ser filtrado. A geração dos coeficientes para as frequências de corte e a ordem do filtro está bem descrita em trabalhos relacionados [33] O leitor interessado pode encontrar os coeficientes e sua geração no código Matlab e C em [34] A implementação real do filtro depende do

recursos do hardware subjacente e é suspeito de compensações de qualidade para recursos, como discutiremos na Seção 6,3 .

5,2 Detecção de característica de ECG

O sinal filtrado é processado posteriormente para extrair os recursos do sinal de ECG. Esses recursos, que são o tempo dos picos Q, R e S, são os identificadores principais para o esquema de autenticação pretendido descrito na Seção 7 . Para extrair características de ECG, uma série de abordagens foram propostas em trabalhos relacionados [35 , 36] Uma opção de implementação é a detecção de grandes R-peaks. No entanto, devido à falta de informações redundantes, a detecção R simples leva a muitos erros irrecuperáveis e grandes incertezas de tempo.

Aplicamos o algoritmo de detecção de QRS em tempo real Pan – Tompkins (PTA) [36] O PTA extrai o complexo QRS de um determinado sinal de ECG e é adequado para dispositivos com recursos limitados. O PTA também é considerado robusto na presença de ECGs anormais, como arritmias [37] PTA executa uma sequência de etapas de filtragem e comparação, incluindo:

- uma filtragem derivada de cinco pontos para fornecer as informações de inclinação do complexo QRS, usando o função de transferência $H(z) = \frac{1}{8}(-z^{-2} - 2z^{-1} + 2z^{1} + z^{2})$,
- quadratura do sinal, para obter todos os valores de sinal positivos e amplificação não linear para enfatizar as frequências de ECG mais altas características,
- integração de janela móvel fixa para obter informações de recursos de forma de onda, além da inclinação da onda R, e
- uma etapa de comparação para identificar os maiores picos em uma janela para localizar Q, R e S.

A saída do PTA é uma tabela de índices de tempo Q, R e S identificados. O benefício do PTA é que cada etapa pode ser facilmente implementada, mesmo em dispositivos embarcados com severas restrições. No entanto, uma desvantagem do PTA é que o modelo de computação simplificado leva a picos detectados erroneamente se aplicado a sinais de entrada não ideais. Um exemplo de um complexo QRS errôneo é mostrado após 4,8 s na Figura 7 . Neste exemplo, o PTA identificou erroneamente outro complexo QRS apenas na inclinação após o S pico correto. Na verdade, as medições práticas mostraram erros em cerca de 6% dos nossos complexos QRS medidos, que devem ser tratados na seguinte etapa de validação de dados baseada em modelo.

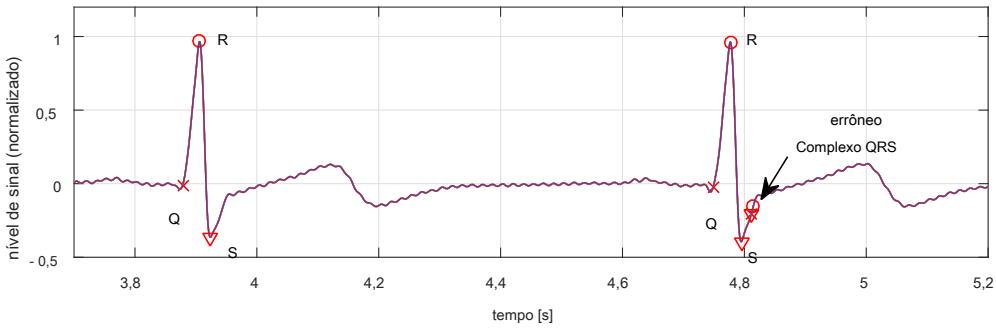

Figura 7. Sinal e picos QRS detectados para dois complexos QRS após Pan-Tompkins. Observe que um terceiro complexo QRS errôneo é detectado no registro de tempo 4,8 s.

5,3. Validação de dados baseada em modelo

Para reduzir o impacto de picos detectados erroneamente, exploramos a redundância de dados e o conhecimento sobre o batimento cardíaco típico para identificar e corrigir esses erros. A ideia geral é validar se os valores de QRS detectados estão na ordem QRS esperada e se as magnitudes e diferenças de tempo dos picos Q, R e S detectados estão dentro da faixa teórica esperada para um sinal de ECG normalizado. Uma vez que se espera que a duração de um complexo QRS seja entre 0,06 e 0,1 s, a distância entre dois picos Q, R ou S consecutivos também deve ser maior que 0,06 s. Essas regras básicas levam ao algoritmo 1 .

Algoritmo 1 Validação baseada em modelo em picos QRS detectados

Entrada:

arrays Q, R, S tempo e valores . o tamanho das matrizes pode ser diferente, pode conter valores inválidos

WindowSize = 0,1 *s*

Resultado:

matrizes Q ', R', S 'tempo e valores . tamanho (Q) = tamanho (R) = tamanho (S)

1: *EndWindowTime* = 0;
2: **para todos** $r_{pico} \in R$: *tempo* (r_{pico})> *EndWindowTime* **Faz**
3: *StartWindowTime = time* (r_{pico}) - *Tamanho da janela/* 2
4: *EndWindowTime = time* (r_{pico}) + *Tamanho da janela/* 2
5: $Eu\ iria_R = Eu\ iria_Q = Eu\ iria_S = 0$. ponteiro para identi fi cado Q, R, S
6: **para todos** $r \in R$: *StartWindowTime* ≤ *cronômetro)* ≤ *EndWindowTime* **Faz**
7: **E se** $Eu\ iria_R = 0$ ∨ *valor (r)> valor* (id_R) **então** $Eu\ iria_R = r$
8: **para todos** $q \in P$: *StartWindowTime* ≤ *tempo (q)* ≤ *tempo* (id_R) **Faz**
9: **E se** $Eu\ iria_Q = 0$ ∨ *valor (q) <valor* (id_Q) **então** $Eu\ iria_Q = q$
10: **para todos** $s \in S$: *tempo* (id_R) ≤ *vez (es)* ≤ *EndWindowTime* **Faz**
11: **E se** $Eu\ iria_S = 0$ ∨ *valor (es) <valor* (id_S) **então** $Eu\ iria_S = s$
12: **E se** $Eu\ iria_Q\ 6 = 0 \wedge Eu\ iria_R\ 6 = 0 \wedge Eu\ iria_S\ 6 = 0$ **então**
13: $Q' += Eu$
14: retorno $Q', R'\ d$, $S'_Q; R' += Eu\ iria_R; S' += Eu\ iria_S;$

As entradas para o algoritmo de validação são o *Q, R,* e *S* locais (tempo, valor) entregues pela PTA. O algoritmo itera através dos locais dos picos detectados e copia os locais QRS válidos para as matrizes de saída *Q ', R ',* e *S '.* Para identificar um complexo válido, uma janela de 0,1 s centrada em
Picos R ($r_{pico,}$ linha 2–4) é movido sobre os dados de entrada. Dentro de cada janela, identificamos o R mais alto (linha 6–7), o Q mais baixo (linha 8–9) e o S mais baixo (linha 10–11). Somente se as localizações válidas de Q, R e S forem
encontrados com um intervalo de janela, eles são adicionados às matrizes de saída (linha 12–13), caso contrário, os picos são descartados. O resultado é uma matriz de valores de tempo Q, R e S válidos a partir dos quais os valores de IPI podem ser calculados.

Aplicando o algoritmo apresentado, os falsos picos no exemplo da Figura 7 são removidos porque o falso R aparece dentro da janela de 0,1 s após o R. correto O falso R e seu S adjacente são então descartados porque seus picos são menores do que os corretos, e o Q é descartado porque não segue o padrão esperado . Em nossos testes, que apresentamos a seguir, o algoritmo de validação pode corrigir 100% dos picos detectados erroneamente.

5,4 Implementação Matlab

Nesta seção, descrevemos a configuração e os resultados de um primeiro sistema de protótipo que funciona com a placa do sensor apresentada, mas executa as etapas de processamento digital em Matlab em um PC.

5.4.1. Configuração

Para a implementação do Matlab, duas etapas precisam ser abordadas: primeiro, como fazer a interface com a placa do sensor e, segundo, como executar o processamento digital, discutido na seção anterior.

Para fazer a interface do dispositivo sensor com o PC, exigimos uma conversão analógica para digital que seja facilmente acessível a partir do Matlab. Uma opção de implementação é um conversor AD externo. No entanto, para nossos experimentos, amostramos os dados por meio da porta de microfone do PC, por meio de um conector de áudio padrão. A função Matlab *Gravador de áudio* fornece acesso direto e conveniente aos dados de entrada analógica,

que realiza amostragem contínua entre 1 kHz e 96 kHz com uma precisão de 8 bits a 24 bits. Para nosso experimento, usamos as configurações de 3 kHz e 16 bits.

Uma vez que o Matlab tem suporte nativo para projetar filtros, os filtros Butterworth podem ser facilmente projetados usando funções embutidas, como *manteiga.* A função gera os coeficientes que são utilizados para gerar a resposta ao impulso do filtro usando *impz.* Com a resposta do filtro gerada, podemos realizar a filtragem em qualquer sinal usando *apto.* Da mesma forma, as etapas do algoritmo Pan – Tompkins são implementadas, aplicando as funções Matlab para convoluções e processamento de sinais. Finalmente, o algoritmo de validação de dados é implementado diretamente como o pseudocódigo mostrado em Algoritmo 1 .

5.4.2. Resultados

Para avaliar as etapas de processamento e os algoritmos, conectamos a placa do sensor a um PC (i5, 4 GB de RAM) rodando Matlab. Os resultados para dois sistemas de sensores que rastreiam os IPIs Q-, R- e S são mostrados na Tabela 1 . Na tabela 1 , vemos que ambos os sistemas de sensores obtêm aproximadamente os mesmos IPIs. Além disso, os IPIs Q, R e S combinam entre si para um determinado índice de tempo. Os resultados indicam a adequação da placa do sensor e as etapas de processamento de dados a serem aplicadas para a autenticação fisiológica pretendida de nós sensores anexados à mesma pessoa. O tempo de cálculo para processamento dos oito IPIs em Matlab no PC é em média 0,14 s. O consumo de memória é de 28 MB. Para reduzir o consumo de memória e computação, traduzimos as etapas de processamento digital do PC para um nó BAN na próxima seção.

Tabela 1. Resultados para dois sensores da implementação do Matlab no PC.

IPI em (s)	1º IPI	2º IPI	3º IPI	4o IPI	5º IPI	6º IPI	7º IPI
Sensor 1 R	0,927	0,908	0,880	0,864	0,799	0,828	0,774
Sensor 2 R	0,927	0,908	0,880	0,865	0,799	0,828	0,774
Sensor 1 Q	0,926	0,909	0,880	0,865	0,798	0,829	0,774
Sensor 2 Q	0,926	0,908	0,879	0,865	0,799	0,828	0,775
Sensor 1 S	0,927	0,908	0,879	0,865	0,799	0,828	0,774
Sensor 2 S	0,927	0,908	0,880	0,865	0,799	0,827	0,775

6. Implementação de sistema integrado

Nesta seção, seguimos a metodologia de design baseado em modelo e traduzimos a implementação de processamento de sinal de ECG digital do ambiente PC-Matlab para uma plataforma de sistema embarcado. O principal desafio nesta parte é lidar com as interfaces e recursos de processamento limitados. Descrevemos e comparamos os resultados de uma implementação gerada automaticamente a partir do ambiente Matlab-Simulink e uma implementação manual em C. Devido ao seu desempenho superior, este último é a base para o protocolo de segurança que descreveremos na próxima seção.

6.1. Plataforma Alvo

Como plataforma de destino incorporada neste artigo, escolhemos um Raspberry Pi (RPi). O RPi é um computador de placa única de baixa potência (0,7–1,2 W) com um processador ARM de 700 MHz e 512 MB de RAM. O RPi é um dos nós de BAN mais poderosos e já foi aplicado em uma variedade de aplicações práticas de BAN e e-health [38 , 39] Um benefício particular do RPi é que ele é suportado por Matlab, Simulink e uma variedade de ferramentas de design, o que facilita a prototipagem fácil e rápida.

Para nosso protótipo, usamos o RPi e conectamos nossa placa do sensor através de um ADC externo de 16 bits (ADS1115) aos GPIOs do RPi, resultando em uma resolução de medição efetiva de 9 μ V, que se mostrou su fi ciente para rastrear o sinal de ECG. A configuração do RPi, a placa do sensor e os sensores é mostrada na Figura 8 . A seguir, descrevemos duas abordagens para implementar o software no sistema: primeiro, gerado automaticamente a partir do Matlab / Simulink e, segundo, implementado manualmente em C.

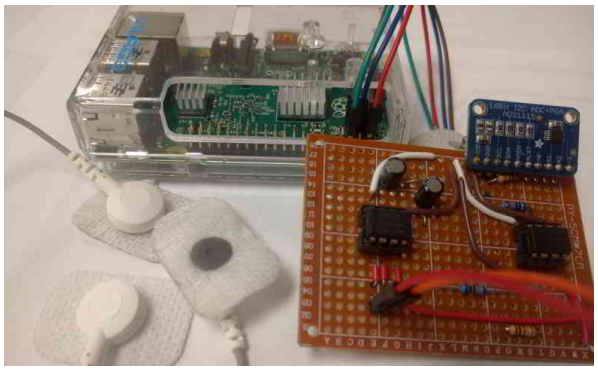

Figura 8. Foto da nossa configuração experimental: eletrodos com placa do sensor na frente, a placa RaspberryPi na parte de trás.

6,2 Simulink

Para a primeira implementação, seguimos ainda a metodologia de design baseada em modelo [19], usando o sistema Matlab para gerar automaticamente o código C que pode ser compilado para o sistema de destino. Aplicamos o codificador Simulink [40], que é uma ferramenta de nível de mercado que gera código C e C ++ a partir de um modelo Simulink. O codificador Simulink ajuda o projetista do sistema avaliando o modelo e os parâmetros do bloco, propagando as larguras dos sinais e os tempos de amostragem e determinando a ordem de execução dos blocos no modelo.

No entanto, o codificador Simulink ainda requer a conversão manual do modelo Matlab para modelos de fl uxo de dados em bloco no Simulink. Muitas partes do nosso sistema podem ser traduzidas diretamente, uma vez que as funções de filtro aplicadas e os blocos de processamento de sinal estão disponíveis no Simulink. O grande desafio diz respeito à medição do tempo. O algoritmo implementado no Simulink calculou os índices de tempo QRS apenas em seus respectivos frames e não para o registro contínuo ao longo de um período de tempo. Conseqüentemente, um temporizador foi necessário dentro do modelo para rastrear os sinais em tempo real. No diagrama do sistema Simulink, mostrado na Figura 9 , o contador de tempo é destacado como bloco **F.** As outras partes do projeto correspondem às etapas de processamento de dados discutidas na seção anterior e são: **UMA:** Aquisição de dados; **B:** Conversão de dados;

C: Resultado; **D:** Filtro passa-baixo; **E:** Detecção de QRS de Pan – Tompkins. O modelo está disponível na página do nosso projeto [34]

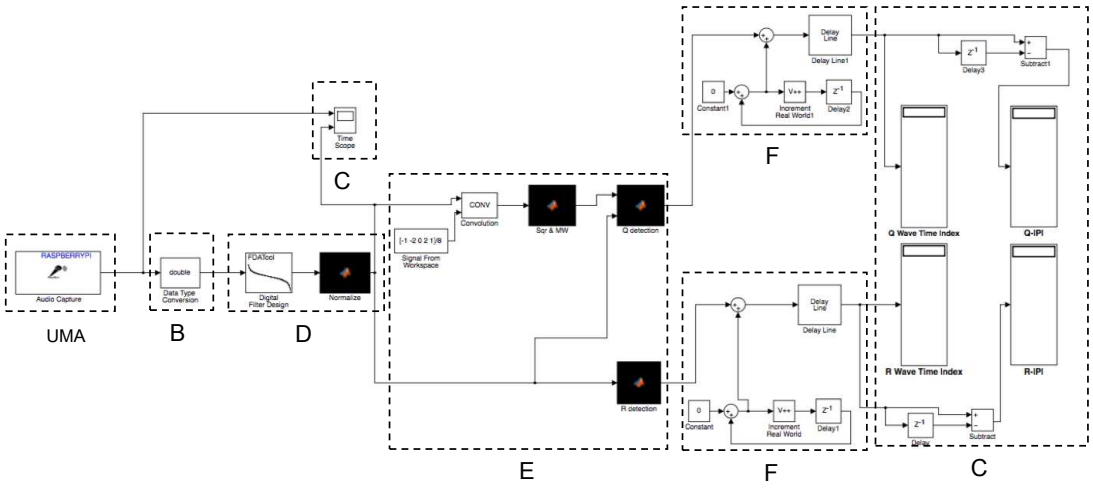

Figura 9. Diagrama de blocos do modelo Simulink. (**A)** aquisição de dados; (**B)** conversão de dados; (**C)** resultado; (**D)** filtro passa-baixo; (**E)** Detecção de QRS de Pan – Tompkins; e (**F)** rastreador de tempo.

Para o código gerado em nossa plataforma de destino, obtivemos os seguintes resultados. Os resultados de Q e R IPI da implementação para dois sistemas de sensores são mostrados na Tabela 2 . Como a implementação Matlab (Tabela 1), esperávamos valores semelhantes para todos os IPIs medidos. No entanto, na Tabela 2 , vemos variações e erros significativos. O principal motivo das incompatibilidades de IPI são atrasos na aquisição de dados e utilização excessiva dos recursos de computação. Na verdade, devido aos recursos de computação limitados, tivemos que desabilitar o rastreamento dos picos S, a fim de obter, pelo menos, R e Q-IPIs. Este resultado mostra a limitação existente do design baseado em modelo. A implementação Simulink traduzida automaticamente do modelo de processamento não é adequada para o nó BAN - mesmo no nó RPi relativamente poderoso. Portanto, precisamos traduzir as etapas de processamento de dados em uma linguagem de implementação de nível inferior como C, manualmente, para abordar os recursos limitados de um BAN.

Mesa 2. Resultados para dois sensores da implementação Simulink.

IPI em (s)	1º IPI	2º IPI	3º IPI	4o IPI	5º IPI	6º IPI	7º IPI
Sensor 1 R	0,927	0,908	0,880	0,864	1.299	0,828	0,774
Sensor 2 R	0,99	0,7737	0,73	0,908	0,8617	1.053	0,977
Sensor 1 Q	0,926	0,909	0,880	0,865	0,798	0,829	0,774
Sensor 2 Q	1,1723	0,828	1.0	1.086	0,9137	0,994	0,9873

6.3. C-Implementação

O ponto de partida da implementação ANSI C manual é o código Matlab gerado. Devido ao uso de design baseado em modelo, fomos capazes de produzir código C com esforço modesto. O design baseado em modelo nos ajudou a traduzir a lógica implementada em Matlab e Simulink para código C. No entanto, tivemos que reduzir a sobrecarga de processamento e o consumo de memória das funções embutidas do Matlab com código C leve e personalizado. As duas funções mais exigentes das etapas de processamento de sinal são a filtragem e a aquisição de dados. Portanto, discutimos a implementação do filtro e a compensação da taxa de amostragem nos parágrafos seguintes.

6.3.1. Implementação de filtro em C

Uma das funções mais utilizadas no fl uxo do processo de dados é a função de filtro do Matlab (*apto). apto* é usado para a filtragem digital dos dados de entrada e para várias etapas do PTA. A função utiliza a característica de fi ltro definida dada pela resposta ao impulso para modelar os dados. No entanto, para alcançar a mesma funcionalidade, precisamos apenas de uma convolução ($y(t) = \sum h(u)\, x(n - você))$ do sinal de entrada x com a resposta de impulso fixa h. A resposta ao impulso do filtro é derivada da função de transferência $H(z)$, de acordo com a Equação (1) $H(z)$ é invariável, de modo que não há necessidade de regenerar $h(n)$

toda vez. Portanto, nosso armazenamento de implementação C h e, eventualmente, reduz a quantidade de memória e poder de processamento, enquanto executa conforme necessário e não perde nenhum componente de frequência essencial.

6.3.2. Taxa de amostragem

As etapas de processamento de dados e o PTA requerem o sinal de entrada por um tempo fixo de vários segundos. Conseqüentemente, as amostras para este período de tempo devem ser armazenadas antes que os dados possam ser processados. A memória necessária para armazenar os dados é determinada pela taxa de amostragem do sinal e afeta significativamente o consumo total de memória. Por exemplo, para um segundo de dados de sinal de ECG com uma taxa de amostragem de 330, um buffer de entrada de pelo menos 1320 bytes é necessário, se tipos de dados de precisão dupla forem usados. Além disso, como o sinal de entrada deve ser manipulado e filtrado por todo o algoritmo, a taxa de amostragem afeta diretamente o tempo e a potência de processamento. No entanto, uma baixa taxa de amostragem pode afetar negativamente a qualidade do processamento. A fim de identificar uma taxa de amostragem preferível e investigar o efeito sobre o consumo de memória e o erro de processamento, aplicamos o algoritmo em sinais com diferentes taxas de amostragem, variando de 150 a 2.000 amostras / s. O fator de erro no experimento é o quadrado do erro de tempo dos picos Q, R e S identificados.

O resultado do processamento de sete segundos de dados de ECG é mostrado na Figura 10 A, B. Os resultados mostrados na figura 10 A con fi rma que o fator de erro diminui com um aumento na taxa de amostragem, enquanto o uso de memória aumenta. Enquanto o consumo de memória cresce linearmente com o aumento da taxa de amostragem, a taxa de erro diminui mais lentamente com o aumento das taxas. Como resultado, aumentar a taxa de amostragem além de 500 Hz melhora apenas marginalmente o processamento. Portanto, para nossa implementação, usamos uma taxa de amostragem de 800 Hz e exigimos uma quantidade de memória de dados de aproximadamente 10 kB por segundo. Como discutiremos na Seção 7,4 , a taxa de amostragem de 800 Hz é preferível para o protocolo de autenticação proposto devido ao seu baixo desvio das leituras do sensor.

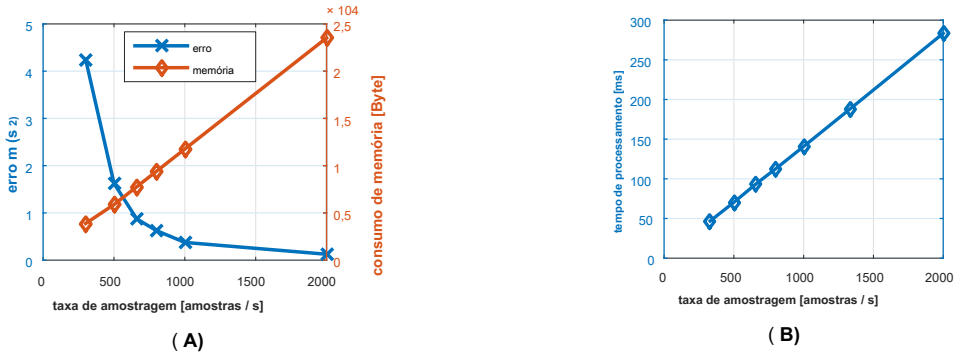

Figura 10. Compromissos de taxa de amostragem: (**A)** memória para taxa de erro; e (**B)** Tempo de processamento.

Figura 10 B mostra os esforços de computação em nossa plataforma de destino para as diferentes taxas de amostragem para processar os dados. Pode-se ver que os esforços de processamento aumentam quase linearmente com taxas de amostragem mais altas, de 23 ms na taxa de amostragem de 150 Hz a 280 ms em 2000 Hz. Como veremos na Seção 7 , o processamento de sinal é o consumidor de processamento dominante em nosso sistema, de modo que os 113 ms necessários para a taxa de amostragem preferencial de 800 Hz estejam bem alinhados com os requisitos do sistema.

6.3.3. Resultados e Avaliação

Usando as técnicas mencionadas, fomos capazes de reduzir o uso de memória de 28 MB necessários para a implementação Simulink gerada para 16 KB para a implementação baseada em C. A utilização média da CPU do RPi caiu de mais de 70% necessário para o Simulink para menos de 5% para a implementação baseada em C.

Nesta seção, descrevemos os resultados da medição para a implementação C no RPi com a placa do sensor (consulte a Figura 8) Para nossos testes, usamos dois sistemas de sensores para reunir os dados necessários para o processo de autenticação. Durante os testes, validamos a funcionalidade geral e a qualidade das medições. Os dados foram coletados dos quatro autores deste artigo. Os dois sensores independentes foram acoplados ao punho esquerdo e direito, respectivamente, com sinais de referência separados na área do tórax. Para os testes, os dados foram sincronizados por carimbos de data / hora, armazenados em arquivos de texto que puderam ser analisados off-line. No total, coletamos 800 amostras de IPI.

Um fragmento de dados medidos para dois nós é mostrado na Tabela 3 . Podemos ver que ambos os sensores entregar picos Q, R e S muito semelhantes, com apenas pequenos desvios. Um histograma dos IPIs obtidos, expresso como batimentos cardíacos por minuto é mostrado na Figura 11 A. Todas as medições estão entre 60 e 100 bpm, sem quaisquer outliers atípicos. Como estatísticas subjacentes para o protocolo de autenticação, rastreamos ainda mais a proximidade dos valores de IPI para pulsações adjacentes e a quantidade de erros de tempo que observamos entre dois nós. Os resultados dos dois estudos são mostrados na Figura 11 B, C, respectivamente. Vemos que os batimentos cardíacos adjacentes estão relacionados entre si, com um desvio padrão de mais de 60 ms. Em contraste, nosso erro de medição entre as placas mostra um desvio padrão

do $\sigma s = 0{,}74$ ms. Duas ordens de diferença de magnitude entre os erros de medição e a incerteza natural do fenômeno subjacente geralmente indicam a aplicabilidade do nosso sistema para uma autenticação fisiológica segura. As medições foram feitas para uma taxa de amostragem de $f = 800$ Hz.

A incerteza do erro de medição aumenta com taxas de amostragem mais baixas. Para uma taxa de amostragem de $f = 666$ Hz, medimos um desvio padrão de $\sigma_S = 6{,}7$ ms, e $f = 500$ Hz resultou em $\sigma_S = 110$ ms. Não foi possível observar melhora na precisão da medição para taxas de amostragem acima de 800 Hz.

Tabela 3. Resultados para dois sensores da implementação C na BAN.

IPI em (s)	1º IPI	2º IPI	3º IPI	4o IPI	5º IPI	6º IPI
Sensor 1 Q	0,965	0,967	0,901	0,964	0,984	0,913
Sensor 2 Q	0,965	0,969	0,905	0,960	0,986	0,910
Sensor 1 R	0,964	0,969	0,904	0,960	0,986	0,910
Sensor 2 R	0,965	0,969	0,905	0,960	0,986	0,910
Sensor 1 S	0,964	0,968	0,901	0,963	0,985	0,913
Sensor 2 S	0,965	0,969	0,904	0,962	0,985	0,910

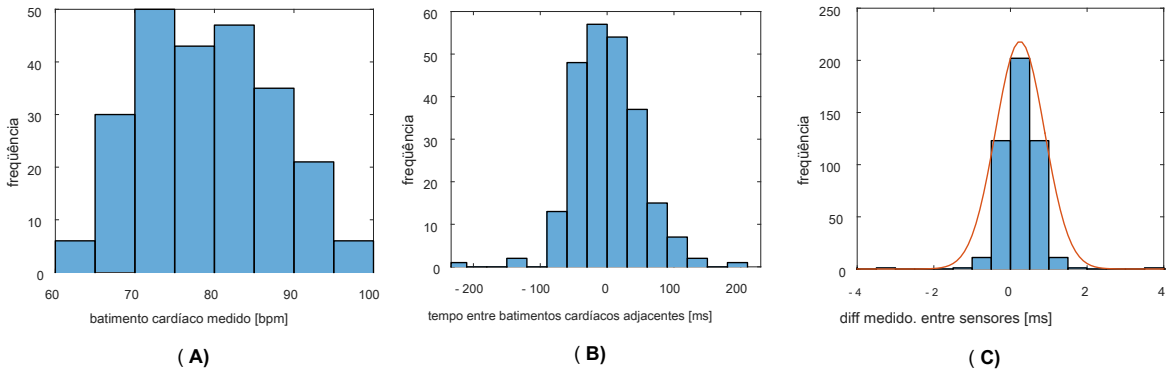

Figura 11. Distribuição de (**A)** IPIs medidos; (**B)** diferença entre duas medições adjacentes; e (**C)** erros de medição entre sensores.

7. Protocolo

Nesta seção, aplicamos os resultados e medições que ganhamos para o sistema, apresentados na seção anterior, para projetar e avaliar um protocolo de autenticação biométrica seguro e robusto. O principal desafio é que diferentes nós sensores medem valores semelhantes, mas não exatamente os mesmos, de modo que uma margem de erro deve ser aceita. No protocolo de autenticação, exploramos o fato de que a distribuição natural de IPIs (ver Figura 11 B) é maior do que a incerteza medida do nosso sistema (Figura 11 C). A hipótese é que podemos decidir se os desvios de um conjunto de pontos de amostragem de diferentes sensores são causados por incertezas técnicas ou por um nó que não está ligado ao mesmo corpo. Além disso, nossas investigações abordam a questão de como o número de amostras e sua resolução afetam a qualidade e a confiabilidade do processo de autenticação.

7.1. Protocolo de autenticação

O protocolo de autenticação que discutimos nesta seção garante que dois nós (S_1 e S_2) concordam que estão ligados ao mesmo corpo, ou seja, sentem os mesmos dados de ECG. Não assumimos nenhum topologia de rede específica ou hierarquia entre S_1 e S_2 Além disso, assumimos que S_1 e S_2 já concordou em uma chave de sessão compartilhada, que é usada em toda a comunicação. Isso pode ser possivel com Dif fi e-Hellman ou outros protocolos de acordo-chave leves [41]

Um diagrama de sequência de mensagem do protocolo de autenticação fisiológica com suas cinco etapas é mostrado na Figura 12 . O protocolo começa com o estabelecimento da sessão e medição dos IPIs. As idéias principais do protocolo são:

1 Os IPIs dos dois pares são comparados com base em propriedades estatísticas no $IPI_1 \approx IPI_2$ operação na Etapa 5. A operação de comparação ($\approx$) compara o desvio padrão das diferenças

entre os dois nós e depende de uma série de incertezas e parâmetros que discutimos na próxima subseção.

2 Cada par envia um valor hash de seus IPIs medidos antes de enviar os dados IPI reais (Etapa 3). Recebendo o valor de hash do par (por exemplo, H_2) antes de enviar os próprios IPIs ($IPI*_1$), impede o colega nó de forjar seu IPI ($IPI*_2$) depois de receber os dados autênticos. Se o IPI recebido não corresponder ao valor de hash recebido (Etapa 4), a autenticação é inválida.

3 - Possíveis ataques de repetição e tentativas de conexão simultâneas são adicionalmente impedidos por aplicando o uso de um único nonce aleatório $N_{Eu,}$ que em nosso caso é um número inteiro aleatório de 32 bits. O nonce é gerado na Etapa 2 e deve ser usado pelo par para o geração de hash (Etapa 3). Portanto, H_{Eu} é o valor hash do nonce recebido concatenado e a matriz de valores IPI medidos.

Um nó de mesmo nível é autenticado como membro da BAN se as duas últimas etapas (4 e 5) forem bem-sucedidas.

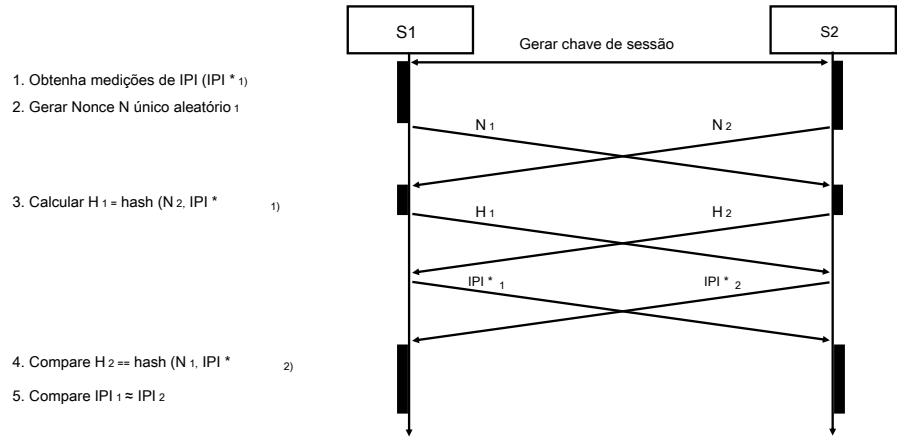

Figura 12. Gráfico de sequência de mensagens para o protocolo de autenticação biométrica entre nós de sensores S_1 e $S_{2,}$ com etapas de processamento para S_1 A autenticação é bem-sucedida se as duas últimas etapas forem bem-sucedidas.

7.2. Parâmetros do protocolo de autenticação

Uma vez que os nós sensores participados podem detectar ou processar diferentes valores de IPI, a comparação função $\approx (IPI*_1, IPI*_2)$ sobre as duas matrizes de IPI de tamanho igual tem que aceitar um grau de incerteza em os valores dos dados. Assim, o objetivo é minimizar o número de autenticações falsas positivas (FPA) e autenticações falsas negativas (FNA).

Autenticações falsas negativas (NFA) é a porcentagem de tentativas de autenticação legítimas que são rejeitadas devido a um alto nível de medição ou erros de processamento.

Autenticações de falso positivo (NPA) é a porcentagem de tentativas de autenticação não legítimas que são aceitas por um nó devido a uma alta tolerância para erros de medição ou processamento.

A função de comparação $\approx (IPI*_1, IPI*_2)$ compara as propriedades estatísticas dos dois vetores IPI. A função e suas propriedades de aceitação e sua pegada podem ser ajustadas por três parâmetros:

Faixa dinâmica (r) medido em dB, expressa a resolução dos valores de IPI amostrados. r é baseado na distância Δ entre dois valores adjacentes de IPI em ms. Desde o fenômeno físico subjacente está em uma faixa de $R = [0, 2000]$ ms, podemos calcular o número necessário de bits por valor por $b = \log_2 |R| / \Delta$, e a faixa dinâmica é $r = 20 \log_{10} |R| / \Delta$. Mesa 4 mostra valores de exemplo para Δ, b, e r. Assumimos que uma faixa dinâmica mais baixa reduzirá o número de falsos positivos, mas aumenta o número de falsos negativos.

Deve-se observar que alterar a resolução também altera as propriedades estatísticas do modelo de referência. Por exemplo, os resultados na Figura 11 foi tirada com uma resolução de $r = 0{,}5$ ms e resultou em um desvio padrão de $\sigma_{0{,}5\ ms} = 1{,}28$, enquanto uma resolução de 2 ms resulta em $\sigma_{2\ ms} = 0{,}45$.

Número de amostras (s) define o número de pontos de dados IPI que usamos para um processo de autenticação. O número de amostras influencia o tempo de medição, bem como o tamanho da mensagem. Mesa 5 mostra os tamanhos das mensagens para uma variedade de configurações. De uma perspectiva de qualidade, podemos esperar que mais amostras compensem os pontos de dados discrepantes e aumentem a confiança na decisão positiva ou negativa.

Desvio permitido (d) medido em número de desvios padrão (σ), determina quanto desvio é aceitável para distinguir medições legítimas de dados que não se originam do mesmo corpo. Portanto, d pode ser considerado um fator de similaridade que decide se um nó é confiável ou não. O valor de σ é baseado nas medições reais (ver Figura 11) e a faixa dinâmica subjacente. Usando o fator de erro $e = \sigma_e$

σ, enquanto $\sqrt{}$ le σ é o desvio padrão da medição esperada

erro (ver Figura 11 C), e σ_e é a distribuição do erro da diferença entre IPI_1 e IPI_2:

$$\sigma_e = \sqrt{\frac{1}{s}\sum_{T=1}^{s}(IPI_{1[Eu]} - IPI_{2[Eu]})} \quad (2)$$

definimos a função de comparação como:

$$\approx (IPI_{*1}, IPI_{*2}) = \begin{cases} verdadeiro & \text{sse } d \leq e \\ Falso & \text{sse } d > e \end{cases} \quad (3)$$

Pode-se supor que um maior d reduz o número de falsos negativos, mas aumenta o número de falsos positivos.

Tabela 4. Quantização por amostra.

Distância Δ (em)	Req. Bits *b*	Dyn. Alcance *r* (dB)
1	11	66
2	10	60
4	9	53
8	8	47
20	7	40

Tabela 5. Tamanhos de assinatura de exemplo.

Distância Δ	Amostras			
[em]	2	4	8	16
2	20	40	80	160
4	18	36	72	144
8	16	32	64	128
20	14	28	56	112

O número de amostras (*s)* e a faixa dinâmica (*r)* têm um efeito mínimo no tempo total de computação do protocolo. O protocolo requer duas operações de hashing (do nonce e das amostras) e o cálculo de um desvio padrão (das diferenças entre as medidas dos dois pares). Dependendo *s* e *r,* o tempo total para essas operações varia entre 130 µ se 160 µ s quando aplicamos MD5 como função hash, e entre 250 µ se 290 µ s quando SHA256 é aplicado. Esses números são insignificantes em comparação com os esforços de processamento de sinal relatados na Seção 6,3 e, portanto, não afetam a busca por combinações de parâmetros preferíveis.

7.3. Análise

Para identificar combinações superiores de parâmetros neste espaço multidimensional - e para validar as suposições de parâmetros expressas na seção anterior - executamos uma variedade de

testes com diferentes parâmetros variáveis e invariantes. Todos os experimentos foram executados em ambiente Matlab utilizando o protocolo de autenticação proposto na Seção 7,1 . A distribuição de erro de referência esperada e seu desvio padrão σ é fornecido por nossas medições práticas de sensor (Figura 11) Na subseção seguinte, investigamos primeiro o impacto dos parâmetros no FNA, depois estudamos o impacto no FPA e concluímos com a seleção de parâmetros combinados e uma análise de sensibilidade.

7.3.1. Autenticações de falsos negativos (FNA)

Figura 13 A, B mostram a taxa de FNAs para diferentes configurações de parâmetros. Nós aplicamos o medido dados para dois sensores e configurações diferentes aplicadas de taxa de amostragem, faixa dinâmica e desvio permitido. O objetivo é identificar a sensibilidade dos parâmetros às tentativas legítimas de autenticação.

Figura 13 A mostra o impacto dos tamanhos de amostra para diferentes desvios padrão permitidos, calculados para um conjunto invariável de faixas dinâmicas. Os resultados desta imagem são:

- Para todos os casos, exceto $d = 1\ \sigma$, um maior número de amostras reduz o número de falsos negativos.
- A razão é que um número maior de amostras ajuda a reduzir o efeito de possíveis outliers. Permitindo apenas um desvio de $d = 1\ \sigma$ é muito restrito para todas as configurações. Na verdade, vemos que um número maior de amostras aumenta a probabilidade de uma autenticação rejeitada. Com um desvio de $d = 4\ \sigma$ e mais, e $s = 4$ amostras e mais, praticamente não podemos identificar quaisquer falsos negativos mais, *ie,* todas as autenticações legítimas são identificadas corretamente.

Figura 13 B mostra o impacto da faixa dinâmica para os mesmos desvios padrão. Os resultados são semelhantes aos resultados anteriores de uma forma que:

- Desvio permitido de $d = 1\ \sigma$ e $2\ \sigma$ resulta em muitos erros, independentemente da faixa dinâmica.
- Com um desvio de $d = 4\ \sigma$ e mais, e uma gama dinâmica de $r = 50$ dB (8 bits) e mais, praticamente não podemos mais identificar nenhum falso negativo, *ie,* as tentativas de autenticação são avaliadas corretamente.

Embora a última observação seja mais importante para nossa seleção de parâmetro, é importante notar que aumentar a faixa dinâmica geralmente não reduz o FNR. Um motivo para esse comportamento pode ser que resoluções muito altas e muito baixas podem enfatizar demais os valores discrepantes e, portanto, rejeitar autenticações válidas.

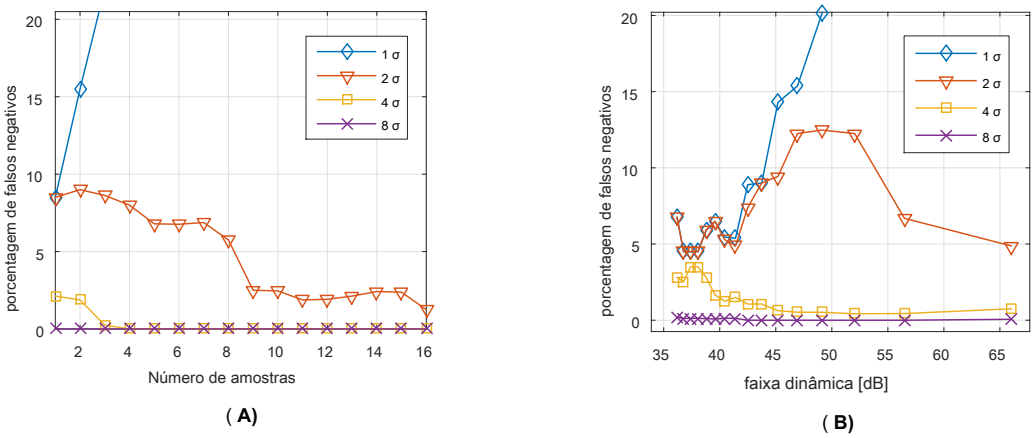

Figura 13. Autenticações rejeitadas (falsos negativos) para tentativas de autenticação verdadeiras medidas, (**A)** para diferentes números de amostras; e (**B)** para diferentes faixas dinâmicas.

7.3.2. Autenticação falso positivo (FPA)

Nesta seção, investigamos o impacto dos parâmetros em tentativas de autenticação não legítimas. Assumimos a ameaça de ataques de similaridade [42] em que um adversário pode explorar que os valores em uma classe de equivalência são distintos, mas semanticamente semelhantes. Em outras palavras, se um adversário pode gerar

ou adivinhe valores de IPI semelhantes, o protocolo apresentado pode estar comprometido. Para gerar IPIs não legítimos, presumimos um modelo de invasor poderoso no qual um invasor conhece a última leitura legítima do sensor e está ciente da distribuição inter-IPI (Figura 11 B). Outros modelos, como adivinhação simples ou aproximações de primeira ordem, não resultaram em autenticações bem-sucedidas observáveis.

Figura 14 A, B mostram o FPA para diferentes números de amostras e faixas dinâmicas, respectivamente.
Os resultados neste caso são:

- Aumentar o número de amostras ou aumentar a faixa dinâmica sempre diminui a chance de um ataque bem-sucedido.
- Desvios permitidos muito altos ($d > 10\ \sigma$) melhorar as chances de um ataque bem-sucedido, enquanto pequenos desvios permitidos ($\leq 8\ \sigma$) proibir ataques.

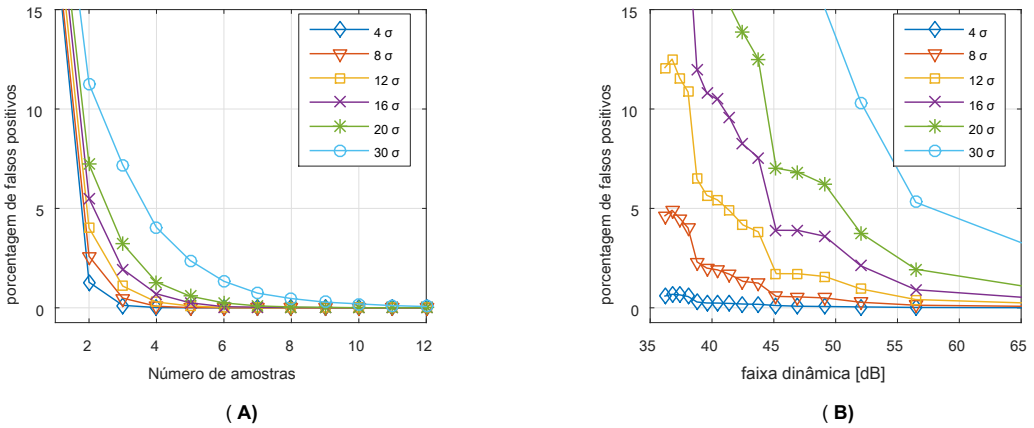

Figura 14. Autenticações aceitas (falsos positivos) para tentativas de autenticação forjada, (**A)** para diferentes números de amostras; e (**B)** para diferentes faixas dinâmicas.

7,4 Seleção de Parâmetros e Análise de Sensibilidade

Com base nos resultados experimentais práticos e analíticos, os parâmetros da função de comparação $\approx$ pode ser definido, de modo que as taxas FPA e FNA sejam reduzidas e os recursos necessários (tamanho do pacote) e o tempo de autenticação (número de amostras necessárias) sejam considerados. Como resultado, para nossa análise dos dados coletados com a configuração BAN apresentada, decidimos por um tamanho de amostra de oito, com codificação de amostra de 8 bits (48 dB) e um desvio permitido de 8 σ. Em nossos experimentos, essa configuração levou a 0% de falsos positivos e 0% de falsos negativos. Na verdade, para a configuração dada, o desvio permitido d pode ser selecionado livremente entre 2 e 14 para obter o mesmo resultado positivo.

Para investigar a sensibilidade da seleção do parâmetro, nos casos em que os nós processam os dados com uma incerteza de tempo maior do que em nosso experimento, executamos testes com um nível de ruído aumentado. Especificamente, estudamos a sensibilidade do desvio aceito d em ambientes com maior incerteza. As possíveis razões para maiores desvios são sensores e processamento de sinal menos precisos, incertezas de tempo no sistema embarcado, mas também pessoas mais velhas ou menos saudáveis [18] Estávamos interessados nos limites exigidos de d limitar o FNR a 1% e limitar o FPR aos níveis de 1% e 5%.

Os resultados são mostrados na Figura 15 . Figura 15 A mostra os limites para nossas configurações selecionadas (oito amostras, 48 dB). Vemos que o limite aceitável para o FNR fica entre 1 σ e 2 σ e não é afetado pelo aumento da variação das medições subjacentes. A razão é que σ é um fator na equação de aceitação (3) e, portanto, um nível de ruído aumentado na distribuição subjacente também aumenta o desvio de aceitação.

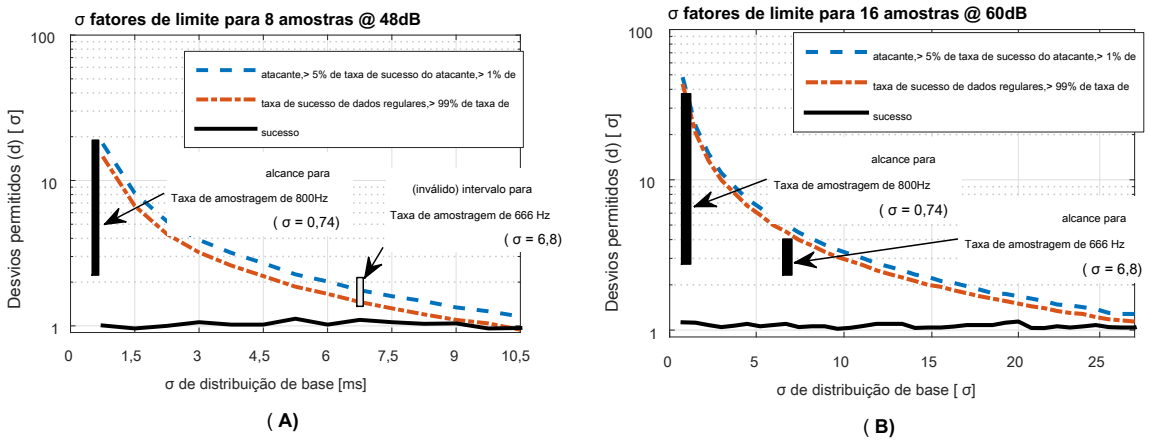

Figura 15. Impacto do aumento da variância da base (por exemplo, mais ruído) nos limites permitidos para limitar falsos positivos e falsos negativos, para (**A)** 8 amostras a 48 dB, e (**B)** 16 amostras a 60 dB.

No entanto, Figura 15 A, B mostram que os limiares para FPR diminuem com um aumento do desvio na distribuição do erro de referência. Esse efeito é plausível, porque se um alto nível de ruído tem que ser tolerado, é mais difícil diferenciar entre desvios devido a ataques e ruído natural.

Nossas configurações padrão do protocolo, mostradas na Figura 15 A, pode tolerar incerteza de medição até $\sigma = 4$ ms, se exigirmos 1 σ entre os limiares FPA e FNA. Níveis de ruído mais altos aumentariam os FPAs, uma vez que os ataques não podem ser claramente distinguidos de tentativas de autenticação legítimas.

Incerteza maior do que $\sigma = 4$ ms requer uma adaptação dos parâmetros do sistema. Figura 15 B mostra os limites para 16 amostras e faixa dinâmica de 60 dB (11 bits). O gráfico mostra que, neste caso, um desvio de base 20 vezes maior ainda fornece espaço suficiente para diferenciar entre tentativas autênticas e falsas. No entanto, o custo para essa confiança aprimorada é o tempo de amostra estendido (16 em vez de 8 batimentos cardíacos) e os tamanhos de pacote maiores (160 em vez de 64 bytes).

Para validar os resultados da simulação, aplicamos medidas práticas coletadas com diferentes taxas de amostragem. Os intervalos efetivos para uma confiança de 99% de FPA e FNA são destacados como os retângulos na Figura 15 A, B. Mostramos apenas as taxas de amostragem de 800 Hz e 666 Hz, porque taxas mais altas não foram distinguíveis de 800 Hz. Taxas mais baixas, como 500 Hz, resultam em um desvio padrão de $\sigma >$ 100 ms, o que não é prático. As medições mostram que o limite prático FNA é cerca de 1 σ superior ao estimado nas simulações, enquanto o limiar de FPA corresponde às simulações. Como resultado, mostrado na Figura 15 A, os dados coletados em 666 Hz não podem ser distinguidos com sucesso, porque com $\sigma = 6.8$, o limite prático para evitar ataques é inferior ao limite para identificar tentativas legítimas. Com a configuração estendida (Figura 15 B), ainda temos um intervalo válido para d entre 2,5 σ e 4 σ. Os resultados mostram que os parâmetros de protocolo com uma relação qualidade-recurso preferível podem ser encontrados se a incerteza do sistema implementado for conhecida.

8. Conclusões

A combinação de sensores reais, protocolos sofisticados e parametrização do sistema nunca é fácil. Este artigo mostrou como um protocolo de autenticação fisiológica para redes de área corporal pode ser projetado, implementado e parametrizado para trabalhar com as incertezas do mundo real de nós sensores de área corporal de baixo custo. A chave para o protocolo de autenticação apresentado é a análise estatística das medições reais do sensor, que permite a um projetista adaptar os parâmetros do sistema de acordo com as propriedades das implantações de BAN do mundo real.

Como base reproduzível de nosso trabalho, na primeira parte deste artigo, descrevemos como projetar e implementar a placa do sensor de ECG e seu sistema de processamento. Nesta parte, descobriu-se que o ruído e a qualidade do sinal tinham que ser tratados em todas as etapas de projeto e processamento, começando do pré-processamento analógico até a etapa de validação baseada em modelo dos sinais de pico de ECG detectados. Durante o projeto, observamos ainda que os fl uxos de projeto baseados em modelo são úteis nos estágios iniciais do projeto. Contudo,

para obter um desempenho de sistema su fi ciente, foram necessários esforços de projeto manual, tanto na parte analógica quanto na parte digital do sistema. O sistema de sensor resultante é o primeiro sistema de sensor BAN relatado para facilitar o rastreamento em tempo real dos dados IPI de ECG para autenticação entre nós.

Medidas práticas com os sistemas apresentados são a chave para o projeto e a parametrização do protocolo de autenticação atual. Com os dados estatísticos do comportamento prático, poderíamos definir as margens de desvio permitidas para que autenticações honestas fossem permitidas e tentativas falsas pudessem ser evitadas. Exploramos o fato de que os desvios da propriedade biométrica subjacente são maiores do que os desvios de detecção e processamento de dados para otimizar e ajustar os parâmetros da função de autenticação e para reduzir a sobrecarga de detecção e processamento. A configuração de sistema recomendada requer oito amostras de precisão de inteiro de 8 bits cada, resultando em 100% de autenticações corretas e uma probabilidade inviável de uma autenticação de falso positivo.

Embora os resultados desse primeiro sistema BAN biométrico do mundo real sejam promissores, também identificamos uma série de possíveis trabalhos futuros. Um trabalho futuro é a validação estendida do protocolo para mais pessoas em diferentes situações e possíveis propriedades anormais de ECG. O objetivo seria uma combinação de fontes biológicas de incerteza, conforme discutido em [18] e os aspectos tecnológicos, discutidos em nosso artigo, para uma estrutura para determinar as configurações de sistema preferíveis para minimizar a probabilidade de erros. Outra questão de pesquisa aberta é como podemos tornar o design baseado em modelo mais eficaz, sem a necessidade de reimplementação de algoritmos em linguagens de implementação de nível inferior. O objetivo é a adaptação da configuração apresentada a uma plataforma de computação ainda menor de 8 ou 16 bits. Para atingir esse objetivo, estender o esquema de autenticação apresentado para gerar chaves de sessão seguras, em vez de aceitar chaves de sessão pré-acordadas, poderia melhorar ainda mais a eficiência e aplicabilidade do sistema de autenticação biométrica apresentado.

Agradecimentos: Este trabalho foi apoiado em parte pela National Science Foundation sob o número de concessão NSF 1136146.

Contribuições do autor: Neste manuscrito, Steffen Peter contribuiu com o projeto experimental, análise de dados e redação; Bhanu Pratap Reddy contribuiu com a configuração e redação experimental; Farshad Momtaz contribuiu com a programação e análise de dados e redação; e Tony Givargis contribuiu com a análise e redação dos dados.

Conflitos de interesse: Os autores declaram não haver conflito de interesses.

Referências

1 Movassaghi, S .; Abolhasan, M .; Lipman, J .; Smith, D .; Jamalipour, A. Redes sem fio de área corporal: uma pesquisa. *IEEE Commun. Surv. Tutor.* **2014,** *16,* 1658–1686.

2 Constant, N .; Douglas-Prawl, O .; Johnson, S .; Mankodiya, K. Pulse-Glasses: um monitor de RH discreto e vestível com funcionalidade de Internet das Coisas. Em Proceedings of the 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN), Cambridge, MA, USA, 9-12 junho de 2015. Piotrowski, K .; Sojka, A .; Langendoerfer, P. Body area network for first responders: A case study. Em

3 - Proceedings of the Fifth International Conference on Body Area Networks, Corfu Island, Greece, 10-12 setembro de 2010; pp. 37–40.

4 - Kumar, P .; Lee, HJ Problemas de segurança em aplicativos de saúde usando redes de sensores médicos sem fio: uma pesquisa. *Sensores* **2011,** *12,* 55–91.

5 Sametinger, J .; Rozenblit, J .; Lysecky, R .; Ott, P. Security challenge for medical devices. *Comum. ACM* **2015,** *58,* 74–82.

6 Gold, RD Considerações de segurança e confiabilidade. *VLSI Med. VLSI Electron. Microstruct. Sci.* **2014,** *17,* 247. Rushanan, M .; Rubin, AD; Kune,

7 DF; Swanson, CM SoK: Segurança e privacidade em dispositivos médicos implantáveis e redes corporais. Em Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 18-21 de maio de 2014; pp. 524–539.

8 Peter, S .; Langendoerfer, P .; Piotrowski, K. Pó inteligente habilitado para criptografia de chave pública é acessível. *Int. J. Sens. Netw.* **2008,** *4,* 130–143.

9 Karlof, C .; Sastry, N .; Wagner, D. TinySec: Uma arquitetura de segurança de camada de link para redes de sensores sem fio. Em Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, EUA, 3–5 de novembro de 2004; pp. 162–175.

10 Toorani, M. Criptoanálise de dois protocolos PAKE para redes de área corporal e ambientes inteligentes. *Int. J. Netw. Secur.* **2015,** *17,* 629–636.

11 Ele, DD; Winokur, ES; Sodini, CG Um monitor cardíaco contínuo, vestível e sem fio usando balistocardiograma (BCG) e eletrocardiograma (ECG). Em Proceedings of the 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Boston, MA, USA, 30 agosto – 3 setembro 2011; pp. 4729–4732.

12 Takano, C .; Ohta, Y. Medição da frequência cardíaca com base em uma imagem de lapso de tempo. *Med. Eng. Phys.* **2007,** *29,* 853–857. Al Taradeh, N .;
13 Bastaki, N .; Saadat, I .; Al Ahmad, M. Detecção piezoelétrica não invasiva de freqüência cardíaca e pressão arterial. *Elétron. Lett.* **2015,** *51,* 452–454.

14 Shu, Y .; Li, C .; Wang, Z .; Mi, W .; Li, Y .; Ren, TL A Sistema de detecção de pressão para monitoramento de frequência cardíaca com sensores de pressão baseados em polímero e um circuito de pós-processamento anti-interferência. *Sensores* **2015,** *15,* 3224–3235. Zhang, Z .; Wang, H .; Vasilakos, A .; Fang, H.
15 ECG-Cryptography and Authentication in Body Area Networks.
IEEE Trans. Inf. Technol. Biomed. **2012,** *16,* 1070–1078.
16 Yao, L .; Liu, B .; Sim OK.; Wu, G .; Wang, J. An ECG-Based Signal Key Establishment Protocol in Body Area Networks. Em Proceedings of the 2010 7th International Conference on Ubiquitous Intelligence & Computing e 7th International Conference on Autonomic & Trusted Computing (UIC / ATC), Xi'an, China, 26-29 de outubro de 2010; pp. 233–238.

17 Venkatasubramanian, KK; Banerjee, A .; Gupta, SKS PSKA: Esquema de acordo de chave utilizável e seguro para redes de área corporal. *IEEE Trans. Inf. Technol. Biomed.* **2010,** *14,* 60–68.
18 Poon, CC; Zhang, YT; Bao, SD Um novo método biométrico para proteger redes sem fio de sensores de área corporal para telemedicina e saúde m. *IEEE Commun. Mag.* **2006,** *44,* 73–81.
19 Jensen, J .; Chang, D .; Lee, E. Metodologia de design baseada em Amodel para sistemas ciber-físicos. Em Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC), Istambul, Turquia, 4–8 de julho de 2011; pp. 1666–1671.

20 Jeon, C .; Awtry, EH; Ware, MG *Cardiologia de projetos;* Lippincott Williams & Wilkins: Filadélfia, PA, EUA, 2006.

21 Li, M .; Lou, W .; Ren, K. Segurança de dados e privacidade em redes corporais sem fio. *IEEE Wirel. Comum.*
2010, *17,* 51–58.
22 Hu, C .; Cheng, X .; Zhang, F .; Wu, D .; Liao, X .; Chen, D. OPFKA: Acordo de chave baseado em recursos fisiológicos ordenados seguro e eficiente para redes corporais sem fio. Em Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 abril de 2013; pp. 2274–2282.

23 Wang, W .; Wang, H .; Hempel, M .; Peng, D .; Sharif, H .; Chen, HH Secure Stochastic ECG Signals Baseados no Gaussian Mixture Model for-Healthcare Systems. *IEEE Syst. J.* **2011,** *5,* 564–573.
24 Dodis, Y .; Reyzin, L .; Smith, A. extratores fuzzy: como gerar chaves fortes a partir de dados biométricos e outros dados ruidosos. *Advances in Cryptology-Eurocrypt 2004;* Springer: Berlin / Heidelberg, Alemanha, 2004; pp. 523–540. Moody, GB; Mark, RG O impacto do banco de dados de
25 arritmia do MIT-BIH. *IEEE Eng. Med. Biol. Mag.* **2001,**
20, 45–50.
26 Bao, SD; Poon, CC; Zhang, YT; Shen, LF Usando as informações de tempo de batimentos cardíacos como um identificador de entidade para proteger a rede de sensores corporais. *IEEE Trans. Inf. Technol. Biomed.* **2008,** *12,* 772–779.
27 Banerjee, A .; Gupta, SK; Venkatasubramanian, KK PEES: Segurança ponta a ponta baseada em fisiologia para mHealth. Em Proceedings of the 4th Conference onWireless Health, Baltimore, MD, USA, 1–3 de novembro de 2013. Denning, T .; Kramer, DB; Friedman, B .; Reynolds, MR; Gill, B .;
28 Kohno, T. CPS: Além da usabilidade: Aplicando métodos baseados em design sensíveis a valores para investigar características de domínio para segurança de dispositivos cardíacos implantáveis. Em Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8-12 dezembro de 2014; pp. 426–435.

29 Maye, O .; Peter, S. Como o estabelecimento-chave em redes de sensores médicos se beneficia da tecnologia de comunicação de campo próximo. Em Proceedings of the 2010 IEEE / ACM International Conference on Cyber, Physical and Social Computing (CPSCom), Green Computing and Communications (GreenCom), Hangzhou, China, 18-20 de dezembro de 2010; pp. 566–571.

30 Nie, Z .; Liu, Y .; Duan, C .; Ruan, Z .; Li, J .; Wang, L. Autenticação biométrica wearable baseada na comunicação do corpo humano. Em Proceedings of the 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN), Cambridge, MA, USA, 9-12 junho de 2015; pp. 1-5. Ali, J. Economical ECGMachine. *Int. J. Appl. Phys. Matemática.* **2012,** *2,* 179.

31

32 Medline. Eletrodos de espuma de monitoramento geral da MedGel. 2015. Disponível online: http://www.medline.com/ sku / item / MDPMDSM611505 (acessado em 19 de abril de 2016).

33 Proakis, JG; Manolakis, DG *Processamento de Sinal Digital: Princípios, Algoritmos e Aplicativos, 4 / e;* Pearson Education: New York, NY, USA, 2007.

34 CPS Design Group na UC Irvine. Página da Web: Autenticação biométrica em redes de sensores corporais. Disponível online: http://tiny.cc/bioauth (acessado em 19 de abril de 2016).

35 Mehta, S .; Lingayat, N. Detection of P and T-waves in Electrocardiogram. Em Proceedings of the World Congress on Engineering and Computer Science, San Francisco, CA, USA, 22–24 de outubro de 2008; pp. 22–24. Pan, J .; Tompkins, WJ Um algoritmo de detecção de QRS em tempo real. *IEEE*

36 *Trans. Biomed. Eng.* **1985,** 230–236. Patel, AM; Gakare, PK; Cheeran, A. Extração de recursos de ECG em tempo real e detecção de arritmia em

37 uma plataforma móvel. *Int. J. Comput. Appl.* **2012,** *44,* 40–45.

38 Tomtsis, D .; Kontogiannis, S .; Kokkonis, G .; Kazanidis, I .; Valsamidis, S. Proposta de infraestrutura em nuvem de serviços médicos vestíveis e onipresentes. Em Proceedings of the 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), Sierre, Switzerland, 7-9 outubro 2015; pp. 213–218.

39 Villarrubia, G .; Bajo, J .; De Paz, JF; Corchado, JM Plataforma de monitoramento e detecção para prevenção de situações anômalas no atendimento domiciliar. *Sensores* **2014,** *14,* 9900–9921.

40 MathWorks. Simulink Coder - Gere código C e C ++ a partir de Simulink e State fl owModels. Disponível online: http://www.mathworks.com/products/simulink-coder/ (acessado em 19 de abril de 2016).

41 Ali, A .; Khan, FA Principais esquemas de acordo em redes sem fio de área corporal: Taxonomia e estado da arte. *J. Med. Syst.* **2015,** *39,* 1-14.

42 Li, N .; Aceso.; Venkatasubramanian, S. t-Closeness: Privacy além de k-anonimato e l-diversidade. Em Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, 15-20 April 2007; pp. 106-115.