UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

FELIPE JOSÉ CARBONE

# Uma Solução de Autenticação Forte para Ambientes de Saúde Baseados em Sensores

Dissertação apresentada como requisito parcial
para a obtenção do grau de
Mestre em Ciência da Computação

Prof[a]. Dr[a]. Liane Margarida Rockenbach
Tarouco
Orientador

Porto Alegre, fevereiro de 2014

**CIP – CATALOGAÇÃO NA PUBLICAÇÃO**

Carbone, Felipe José

Uma Solução de Autenticação Forte para Ambientes de Saúde Baseados em Sensores / Felipe José Carbone. – Porto Alegre: PPGC da UFRGS, 2014.

72 f.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2014. Orientador: Liane Margarida Rockenbach Tarouco.

1. Autenticação forte. 2. Biometria. 3. Localização. 4. Rede de sensores. I. Tarouco, Liane Margarida Rockenbach
. II. Título.

*“A tarefa não é tanto ver aquilo que ninguém viu,*
*mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.”*
— ARTHUR SCHOPENHAUER

# AGRADECIMENTOS

Aos meus colegas do grupo de Redes pelas discussões e pelo companheirismo. A minha orientadora Liane pelo suporte e dedicação. A minha banca examinadora, pelas valiosas dicas e correções. E principalmente aos meus familiares e esposa, pelo apoio incondicional e suporte emocional.

# SUMÁRIO

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| Bpm | Batimentos por minuto |
| CERP | Cluster of European Research Projects |
| DoS | Denial of Service |
| FAR | False Acceptance Rate |
| FRR | False Rejection Rate |
| GHz | Gigahertz |
| IBM | International Business Machines |
| IEC | International Electrotechnical Commission |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| Mbps | Mega bytes por segundo |
| MIT | Massachusetts Institute of Technology |
| PHP | Hypertext Preprocessor |
| RAM | Random-Access Memory |
| RFID | Radio-Frequency Identification |
| RSSI | Received Signal Strength Intensity |
| SBIS | Sociedade Brasileira de Informática em Saúde |
| SHA-2 | Secure Hash Algorithm - 2 |
| SSL | Secure Socket Layer |
| WBAN | Wireless Body Area Network |

# LISTA DE FIGURAS

# LISTA DE TABELAS

# RESUMO

Equipamentos médicos equipados com interface de rede, classificados como sensores, transmitem informações sensíveis sobre a rede, constituindo uma rede de sensores. Essa rede pode ser utilizada para o acompanhamento remoto de pacientes a domicílio, com a finalidade de propiciar comodidade ao paciente. As informações provenientes desses sensores são vulneráveis, necessitando assim de fortes mecanismos de segurança. Devido às vulnerabilidades, métodos mais eficazes de autenticação vêm sendo desenvolvidos. Porém, as soluções de autenticação existentes obrigam a interação direta dos usuários com o sistema, não respeitando suas individualidades. Dessa forma, esta dissertação propõe uma solução de autenticação forte a qual retira a necessidade de interação do usuário com o sistema, baseando-se nos fatores de biometria e localização. O autenticador desenvolvido, foi testado através de estudos de casos distintos para mostrar sua eficiência e viabilidade para utilização em um ambiente real.

**Palavras-chave:** Autenticação forte, biometria, localização, rede de sensores.

**A Solution for Strong Authentication in Sensor-based Healthcare Environments**

# ABSTRACT

Medical devices equipped with network interfaces, classified as sensors, transmit sensitive information through the network and form a sensor network. This network can be used to monitor patients at home remotely. The information from these sensors is vulnerable and requires strong security mechanisms. Because of vulnerabilities, more effective authentication methods have been developed. However, the current authentication solutions require direct interaction of the user with the system, which does not respect their individuality. Thus, this dissertation proposes a strong authentication solution in which the interaction of the user with the system is removed based on biometrics and location factors. The developed authenticator was tested through different case studies to show its efficiency and feasibility before application in a real environment.

**Keywords:** Strong authentication, biometrics, localization, sensor networks.

# 1 INTRODUÇÃO

Medidores de pressão, termômetros corporais, e monitores de batimento cardíaco são exemplos de dispositivos médicos os quais vêm sendo equipados com interfaces de rede, sendo classificados como sensores para monitorar remotamente pacientes através da coleta e troca de informações de saúde sobre redes de computadores (AKYILDIZ et al., 2002). Devido a esses sensores transmitirem informações sensíveis sobre a rede, a segurança se tornou um aspecto fundamental com a finalidade de evitar danos aos pacientes, como por exemplo a exposição de suas informações privadas a terceiros (VARSHNEY, 2007).

A segurança pode ser aplicada através de diferentes mecanismos, como por exemplo, autenticadores, banco de dados de políticas, algoritmos criptográficos, replicação de dados, entre outros. Cada um desses mecanismos poderia assegurar que a comunicação dos sensores apresentará os aspectos fundamentais de segurança, (*i.e.,* confidencialidade, integridade, e disponibilidade) (WALTERS et al., 2007). Entretanto, normalmente estes mecanismos requerem recursos adicionais de hardware, adicionando complexidade na comunicação, resultando em um *trade-off* entre segurança e requisitos de recursos de hardware. Como consequência, esses requisitos representam um grande problema aos sensores no qual são muito mais limitados em hardware do que roteadores, computadores, e outros dispositivos de rede tradicionais no qual já implementam mecanismos de segurança. Dessa forma, a segurança se tornou um gargalo nos sensores, sendo vulneráveis a ataques, tais como personificação, negação de serviço, repetição entre outros.

Devidas essas vulnerabilidades supracitadas, meios de autenticação mais fortes vêm sendo investigados a fim de mitigar ataques contra essas redes de sensores. Autenticação forte geralmente utiliza de múltiplos fatores no qual combinados adicionam mais proteção no processo de autenticação. Senhas, cartões inteligentes e dispositivos biométricos são exemplos de métodos usados para prover autenticação forte em tais redes (CA, 2007). Em ambientes de saúde, os problemas com esses métodos são: (i) a autenticação forte requer interação com o usuário, a qual pode ser uma grande restrição dependendo das limitações físicas ou mentais desse indivíduo; (ii) os métodos de autenticação utilizados sofrem de problemas ocasionados pela interação do usuário; e (iii) devem ser desenvolvidos utilizando as padronizações existentes (*i.e.,* ISO/IEC 27799) (ISO, 2008). Portanto, um novo mecanismo baseado em autenticação forte, no qual retire o usuário do processo direto de autenticação e siga as padronizações vigentes faz-se necessário.

Dessa forma, nesse trabalho é proposto um mecanismo de autenticação forte no qual utiliza-se de fatores nos quais não necessitam da interação direta do usuário e que segue as especificações existentes segundo a ISO/IEC 27799 e a SBIS (Sociedade Brasileira de Informática em Saúde) (SBIS, 2009). O mecanismo realiza a autenticação através da combinação dos fatores biometria (*i.e.,* informações fisiológicas tais como, pressão arte-

rial e saturação de oxigênio) e localização (*i.e.,* a distância dos sensores em relação ao *gateway*), inerentes ao domínio de aplicação pertencente a uma rede de sensores doméstica para monitorar um paciente remotamente. Como prova de conceitos, foi proposto um modelo formal para a comunicação entre os sensores e testes utilizando perfis fisiológicos distintos sobre o autenticador do paciente, com a finalidade de medir seus graus de eficiência da solução proposta. Finalmente, é feita uma discussão sobre os aspectos de segurança que permeiam a solução proposta, os critérios sobre a padronização existente e a viabilidade de utilização da solução em ambientes reais, a fim de responder as seguintes questões.

- Qual é a eficiência de uma solução que combina dois fatores de autenticação pouco usuais para ambientes de saúde?
- Quais variáveis da solução são mais ou menos importantes para a eficiência do autenticador?
- Qual é a viabilidade da solução proposta em um ambiente real?

Esta dissertação foi organizada da seguinte forma. No capítulo 2, alguns conceitos básicos sobre a segurança em ambientes de saúde, autenticação, ambientes inteligentes e padronizações são abordados a fim de facilitar a compreensão do trabalho. Ainda no capítulo 2, alguns trabalhos são apresentados, mostrando as soluções que vem sendo propostas na área. O capítulo 3 contêm a solução proposta desta dissertação, demonstrando o processo de autenticação do paciente. O capítulo 4 demonstra os testes realizados sobre a solução proposta, contendo três estudos de casos no qual retratam três tipos de perfis fisiológicos distintos. Já no capítulo 5, uma discussão é realizada sobre as informações obtidas e observadas nesse trabalho. Finalmente, o capítulo 6 contêm as conclusões do trabalho e os trabalhos futuros.

# 2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS RELACIONADOS

Esse capítulo aborda conceitos que permeiam segurança, autenticação, ambientes inteligentes e padronizações em ambientes médicos baseados em sensores. Possui o objetivo de esclarecer os conceitos fundamentais empregados neste trabalho e apresentar os principais trabalhos relacionados.

## 2.1 Segurança em ambientes de saúde

Ambientes de saúde são projetados a fim de acomodar pacientes para que possam obter algum tipo de serviço médico (*i.e,* consulta, tratamento, diagnóstico), podendo ser aplicados em clínicas, hospitais ou mesmo em casa. Atualmente, esses serviços médicos vem se beneficiando de recursos tecnológicos para melhorar sua eficiência, como por exemplo registros eletrônicos, dispositivos móveis e sistemas especialistas. Porém, a inclusão tecnológica trouxe problemas de segurança que antes não existiam, impondo a necessidade do desenvolvimento de mecanismos de segurança específicos. Estes mecanismos de segurança devem ser capazes de impedir acessos não autorizados, ataques internos e externos, vazamento de informações e vulnerabilidades devido a falhas. Dessa forma, novos métodos e soluções de segurança vêm evoluindo para resolver os problemas presentes, empregando-se nos sistemas eletrônicos responsáveis. No trabalho de Foo Kune *et al*., (FOO KUNE et al., 2012), requisitos para o projeto de um sistema médico seguro são apresentados, incluindo requisitos para sessões seguras, mecanismos de controle de acesso, autenticação, logs, alertas e gerenciamento do usuário.

Os ambientes de saúde vem adotando tecnologias de redes de sensores sem fio, ubíquas (*i.e*, capacidade de estar conectado à rede e fazer uso da conexão a todo o momento), como WSN (Wireless Sensor Network) (SHNAYDER et al., 2005) (MILENKOVIC; OTTO; JOVANOV, 2006) e BAN (Body Area Network) (RAMLI; AHMAD, 2011). Essas tecnologias viabilizam uma grande variedade de aplicações, como por exemplo o monitoramento remoto. O monitoramento remoto permite que profissionais da área da saúde possam tratar de um paciente à distância, evitando riscos e custos vinculados a locomoção. Isso torna possível o tratamento em casa (*homecare*) e minimiza as superlotações em hospitais. Entretanto, o processamento e envio das informações vitais do paciente pela rede traz uma série de riscos, tornando necessários a adoção de diversos requisitos de segurança, tais como:

- Confidencialidade: Nenhum outro indivíduo além dos envolvidos em uma comunicação estabelecida podem reconhecer o conteúdo transmitido. Os dados proveni-

entes dos pacientes são sigilosos e precisam ser mantidos confidenciais durante a transmissão e o armazenamento.

- Integridade: Os dados do paciente não podem ser alterados sem autorização durante transito ou armazenamento. A alteração indevida pode acarretar falsos diagnósticos e falhas nos mecanismos de segurança.

- Confiança: As partes comunicantes devem ter certeza da legitimidade das informações e da comunicação. Também, os dados do paciente devem ser prontamente recuperáveis caso ocorra alguma falha em um dispositivo.

- Controle de acesso: Uma política de acesso bem definida deve ser executada a fim de impedir o acesso não autorizado a bancos de dados e mecanismos pertencentes ao ambiente de saúde. Dessa forma, apenas indivíduos envolvidos com permissões especiais possuem acesso restrito.

- Autenticação: Os participantes devem ser identificados e autenticados garantindo a veracidade dos envolvidos. O processo de autenticação deve ser forte o suficiente respeitando as necessidades requeridas do ambiente envolvido.

Os requisitos fornecem uma base para a implementação de soluções seguras contra ataques. Am redes de sensores sem fio são vulneráveis devido à natureza de transmissão do seu meio, ou seja, em *broadcast*. No trabalho de Padmavathi (PADMAVATHI; SHANMUGAPRIYA, 2009a), uma classificação dos ataques à redes de sensores sem fio foi realizado, seguindo duas categorias, ataques passivos e ataques ativos. Os ataques passivos compreendem escutas e monitoramento do canal de comunicação, afetando diretamente a privacidade. Muita informação pode ser coletada passivamente do canal, utilizando ataques de análise de tráfego, monitoração, espionagem, entre outros. Já os ataques ativos modificam dados trafegantes no canal de comunicação. Existem muitos ataques na categoria de ataques ativos, como negação de serviço, nó falso, ataque de roteamento, alteração de mensagem entre outros.

No geral, as redes de sensores sem fio possuem alguns desafios iminentes devido às suas características (*i.e*, comunicação sem fio, escassez de recursos, comunicação não confiável entre outros). Os recursos limitados dos sensores (*i.e*, hardware, baixo consumo energético) impõem grandes desafios aos mecanismos de segurança. Esses mecanismos normalmente sobrecarregam a rede, pois necessitam de carga adicional de banda, memória e processamento. Outro fator importante é a comunicação não confiável, ou seja, o canal de comunicação fica vulnerável a ataques passivos ou ativos, ou problemas como a perda de pacotes ou de latência, devido à sincronização de vários sensores. Assim, a adoção de tecnologias que utilizem redes de sensores sem fio está limitada à confiança sobre seu funcionamento e segurança do canal de comunicação.

Nos ambientes médicos, a segurança possui grande destaque, incluindo itens como criptografia, autenticação, identificação de intrusos entre outros. O foco deste trabalho é sobre a autenticação realizada nos ambientes médicos. Porém, devido à sensibilidade do ambiente, métodos mais fortes são necessários a fim de garantir os princípios básicos de segurança (*i.e*, privacidade, integridade, disponibilidade).

## 2.2 Autenticação forte

Na ciência da computação, autenticação é o processo no qual associa um cliente a uma identidade virtual, podendo ser descrito como um conjunto de informações relevantes ao sistema, tais como permissões para editar arquivos, diretórios, nomes e endereços. Devido à existência de diversas pessoas durante o processo de autenticação, o sistema deve atribuir desafios às pessoas a fim de validar seu acesso, utilizando-se de perguntas, senhas, coleta de evidências ou solicitando outros fatores. Todorov *et al.,* (TODOROV, 2007) mostrou que a autenticação consiste basicamente em três passos: (*i*) acesso do cliente, no qual será desafiado e proverá diferentes informações a serem validadas; (*ii*) autenticação, onde as identidades serão verificadas pelo sistema para permitir o acesso do cliente; e (*iii*) banco de dados, responsável pela comparação das informações enviadas com as armazenadas a fim de provar as credenciais do cliente.

Em ambientes que lidam com informações sensíveis (*e.g*, envolvendo informações de saúde, transações bancárias, e sistemas militares), é necessário um esquema de autenticação forte para garantir que todos os dados serão protegidos. Para desenvolver uma autenticação forte, são necessários fatores extras para proteger melhor o sistema. Porém, mais fatores resultam em uma maior complexidade na comunicação e em recursos de hardware. Dessa forma, autenticação forte geralmente utiliza de múltiplos fatores no qual combinados adicionam mais proteção no processo de autenticação (TODOROV, 2007). Bishop *et al.,* (BISHOP, 2004) mostra que os fatores podem ser classificados como: i) o que a entidade sabe (*e.g.,* senha e autenticação baseada em conhecimento); ii) o que a entidade tem (*e.g.,* cartão inteligente e certificados digitais); iii) o que a entidade é (*e.g.,* biometria); e iv) onde a entidade está (*e.g.,* geolocalização e localização por IP). Autenticação é considerada forte quando pelo menos dois fatores distintos são utilizados. O uso de autenticação forte reduz os riscos de ataques mais sofisticados pois requer um atacante bastante habilidoso para descobrir todos desafios impostos pelo sistema.

### 2.2.1 Autenticação com base no que a entidade sabe

Essa é a forma de autenticação mais comumente utilizada por sistemas em geral, tendo como base a definição de uma senha. Essa senha é uma sequência de bits à qual apenas duas partes devem ter acesso, a entidade (seja pessoa ou máquina) e o sistema alvo.

A maior vantagem na utilização de senhas é devido à familiaridade das pessoas com este processo, pois é a forma de autenticação mais utilizada no mundo. Além disso, possui fácil integração com diversos tipos de sistemas. Entre suas desvantagens, estão a grande quantidade de ataques disponíveis de fácil obtenção (*e.g*, força bruta, *sniffers*, etc) e a necessidade de memorização de uma sequência de caracteres escolhidos. Ainda, senhas são suscetíveis a serem fracas (*i.e*, de fácil adivinhação ou com poucos bits), uma vez que muitas vezes são os próprios usuários que as escolhem. Dessa forma, as políticas de segurança cada vez mais forçam a utilização de senhas mais complexas, dificultando ainda mais o processo de memorização.

### 2.2.2 Autenticação com base no que a entidade tem

Essa forma de autenticação resguarda-se no uso de dispositivos físicos por parte dos usuários, sendo cada vez mais utilizada como fator extra em conjunto com as senhas. Esses dispositivos podem ser dispositivos de memória, no qual armazenam informações ou dispositivos inteligentes, no qual possuem circuitos integrados que proporcionam o processamento de algumas informações.

Por ser um dispositivo físico, em poder do usuário, possui grande confiabilidade ao sistema. Porém esses dispositivos possuem um alto custo devido a necessidade de hardwares específicos para leitura, o que dificulta sua administração. Ainda, por serem físicos, estão sujeitos a problemas de manipulação, como dispositivos extraviados, ou sua perda (NAKAMURA; GEUS, 2002).

### 2.2.3 Autenticação com base no que a entidade é

Essa forma de autenticação é comumente chamada de biometria, uma vez que autentica um usuário de acordo com as suas características físicas, como iris, digital, voz entre outros. É considerada uma autenticação muito segura, pelo fato do reconhecimento de um usuário ser feito unicamente por aspectos humanos intrínsecos.

Apesar de existir muitas formas de autenticar um usuário através da biometria, sua utilização possui alguns problemas. Aspectos físicos, nos seres humanos, sofrem alterações com o passar do tempo ou devido a acidentes. Porém, a autenticação biométrica é um campo que está constantemente crescendo, com pesquisas e tecnologias sendo desenvolvidas, possibilitando cada vez mais novas formas de autenticação e mais seguras.

### 2.2.4 Autenticação com base onde a entidade está

Muitos autores divergem um pouco sobre o quarto fator de autenticação, onde alguns defendem que esse fator refere-se às características comportamentais de uma entidade. Segundo a definição de Bishop *et al.,* (BISHOP, 2004), essa característica comportamental refere-se à localidade. Portanto essa forma de autenticação utiliza-se de dados geográficos para autenticar uma pessoa. Um exemplo muito utilizado é a tecnologia Geo IP, no qual dependendo da nacionalidade do seu IP, certos serviços e idiomas são executados. Isso mostra de maneira geral a presença da localidade em cada indivíduo, pois seja em um terminal *desktop* ou dispositivo móvel, a localização é um critério existente.

Sua desvantagem fica no fato de serem necessárias tecnologias otimizadas para sua utilização (*i.e*, níveis altos de proximidade). Isso acarreta na necessidade de hardwares especiais e o desenvolvimento de algoritmos ótimos no processo de rastreamento da entidade.

### 2.2.5 Comparação entre os fatores de autenticação

Os fatores de autenticação descritos anteriormente possuem suas vantagens e desvantagens, no qual podem ser melhor visualizados segundo a descrição de Bromba (BROMBA, 2012) na Tabela 2.1.

| | O que a entidade sabe | O que a entidade tem | O que a entidade é |
|---|---|---|---|
| Exemplos | Senhas | Chaves, Cartões Inteligentes | DNA, Digital, Face |
| Cópia | "Software" | Fácil a muito difícil | Fácil a Difícil |
| Perda | "Esquecimento" | Fácil | Muito difícil |
| Roubo | Espionagem | Possível | Muito difícil |
| Mudança | Fácil | Fácil | Fácil a muito difícil |
| Circulação | Fácil | Fácil | Fácil a difícil |

Tabela 2.1: Comparação entre os fatores de autenticação

Essa tabela contêm alguns exemplos para mostrar as características dos métodos de

autenticação. Podemos resumir essa tabela dizendo que os fatores que se referem aquilo que sabe e aquilo que se tem, sofrem de problemas inerentes a situações reais como perda e roubo. A biometria, por sua vez, possui grande variância em cada característica citada, o que oferece eficiência na segurança mediante o custo ao qual se deseja obter. O fator localização não está presente na tabela pois ainda não existem muitos mecanismos para comparação, sendo pouco utilizado.

### 2.2.6 Trabalhos relacionados

Muitos trabalhos estão sendo desenvolvidos no campo da autenticação forte, sendo alguns escolhidos por estarem relacionados ao tópico explorado no presente trabalho. No trabalho de (DAS, 2009), o autor apresenta um protocolo de autenticação utilizando dois fatores (*i.e*, senha e cartão inteligente) e chaves de sessão no qual diz ser resistente a muitos ataques comuns às redes de sensores. Neste trabalho, o protocolo desenvolvido por Das, funciona em duas fases, uma de registro para que o usuário se cadastre e outra de autenticação para acessar os dados da rede. Apesar de demonstrar a eficiência do protocolo desenvolvido, em comparação com outros já desenvolvidos, o esquema proposto por Das necessita da interação do usuário através de seu registro. Esse ponto de interação é compartilhado pela maioria dos trabalhos desenvolvidos na área de segurança sobre ambientes de saúde, não se preocupando com necessidades individuais e passando por cima dos conceitos sobre ambientes inteligentes, foco neste trabalho.

Essas mesmas características são apresentadas no trabalho de Kumar et al. (KUMAR; LEE; LEE, 2012). Os autores desenvolveram um protocolo nomeado E-SAP (*Efficient-Strong Authentication Protocol*) com a proposta de autenticar pacientes em um ambiente de saúde utilizando senha e cartão inteligente. A escolha dos fatores senha e cartão inteligente deve-se a já serem amplamente adotados e possuírem um baixo custo de implantação (CA, 2007). Além dos dois fatores, o protocolo E-SAP provê autenticação mútua entre profissionais e dispositivos, criptografia simétrica nas comunicações e chaves de seção. O trabalho se preocupa em mostrar sua eficiência perante outros protocolos propostos, mas contribui pouco para um ambiente com necessidades especiais.

Na mesma linha de desenvolvimento, destaca-se o trabalho de Pu et al. (PU; WANG; ZHAO, 2012) e de Hsiao et al. (HSIAO et al., 2012). Nestes trabalhos, são desenvolvidos arcabouços utilizando autenticação forte, contendo os fatores senha e cartão inteligente. Igualmente aos trabalhos supracitados, preocupam-se em mostrar serem mais eficientes do que outras soluções existentes. Isso demonstra o descaso por parte das soluções em relação aos pacientes e despreparo em relação aos ambientes de saúde. Apesar de serem fatores bem disseminados, cartões inteligentes e senhas necessitam de habilidades especiais dos usuários. Estes usuários geralmente precisam ser treinados e gozarem de boas condições físicas e psicológicas para lembrar as senhas ou inserir cartões inteligentes no sistema. Isso se agrava ainda mais nos usuários pacientes portadores de necessidades especiais (*e.g*, pessoas com Alzheimer, algum dano cerebral, ou acidente vascular), pois não podem realizar estes requisitos exigidos pela autenticação forte, fazendo necessário esquemas que respeitem suas limitações. Em adição, a maioria dos trabalhos no qual lidam com autenticação forte não seguem as especificações e padronizações disponíveis, no qual servem para um desenvolvimento mais seguro e robusto, como será discutido mais adiante.

Outros trabalhos como os de (HE, 2012) e (YUAN; JIANG; JIANG, 2010), demonstram formas robustas de autenticação sobre redes de sensores. Porém, assim como a maioria dos trabalhos estudados na área de autenticação de redes de sensores, são desen-

volvidas aplicações preocupando-se com a força de apenas um fator, inviabilizando suas aplicações em ambientes de saúde. Dessa forma, a viabilidade da grande maioria dos trabalhos limitam-se a ambientes no qual não existam dados sensíveis cabíveis de um nível extra de proteção. Ou então, quando utilizados fatores extras na autenticação, a preocupação de interação com seus utilizadores é negligenciada, tornando-se um gargalo para sua adoção.

Observa-se assim uma carência em soluções de autenticação fortes para ambiente de saúde no qual explorem a correta utilização dos fatores envolvidos, e levem em conta as necessidades do paciente. Além disso, as soluções desenvolvidas, quando robustas, não podem ser aplicadas nos ambientes de saúde, pois não seguem as padronizações existentes, ocasionando em retrabalho ou adaptação de alguns componentes.

## 2.3 Biometria e localização

Para melhor compreensão sobre a proposta deste trabalho, faz-se necessário explanar sucintamente a respeito dos fatores escolhidos como base para a autenticação.

### 2.3.1 Biometria

Biometria, pela definição da ISO/IEC, é o reconhecimento automático dos indivíduos baseado nos seus comportamentos e características fisiológicas. No reconhecimento biométrico, medindo o comportamento e as características fisiológicas de um indivíduo, a investigação da identidade do indivíduo deve ser comparada com dados de referencia já coletados e armazenados desse indivíduo. Assim uma característica como a face, íris ou digital pode ser submetida a um processo de análise e reconhecimento a fim de reconhecer o indivíduo. As informações cadastradas desse indivíduo, são chamadas de amostras, no qual refletem suas características fisiológicas mas em representação digital. É através dessa representação que um sistema de biometria é construído. A Figura 2.1 mostra o processo de registro e reconhecimento de um sistema biométrico segundo (BROMBA, 2012).

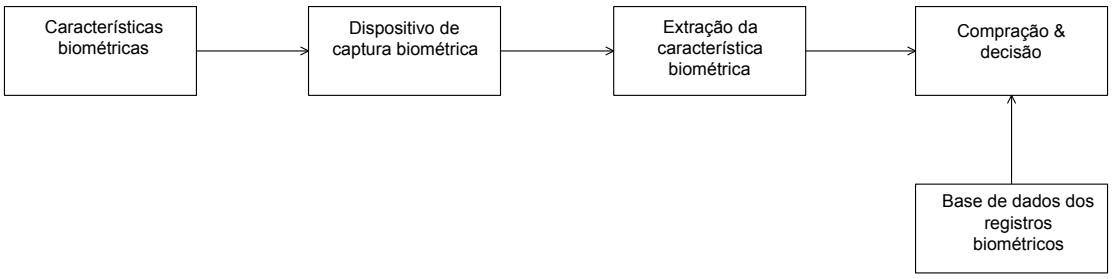


Figura 2.1: Típico processo de registro e reconhecimento biométrico.

A Figura 2.1, exemplifica o processo explicado anteriormente, mostrando o processo de um reconhecimento biométrico. Contendo a captura, a extração da característica e a comparação, a qual beneficia-se de uma base de dados com informação já previamente cadastradas. Desta forma a biometria estabelece o que o indivíduo é para os métodos autenticadores, tornando-se extremamente flexível e, dependendo do método utilizado, eficiente.

Dentre as tecnologias de biometria existentes, existem dois níveis de envolvimento que um indivíduo pode ter, passivo e ativo (REID, 2004). A biometria passiva diz respeito

ao não envolvimento do indivíduo no processo de coleta. Sistemas que utilizam esse tipo de biometria são invasivos, geralmente utilizados em sistemas de monitoramento. Para o uso em sistemas de monitoramento, é necessária uma base de dados conhecida para cada indivíduo e constantes verificações das informações coletadas com as já cadastradas. Normalmente esse tipo de biometria é bastante influenciada pelo ambiente no qual está inserida. Exemplos de biometrias passivas são batimentos cardíacos, voz ou a face. Já a biometria ativa requer a interação direta do indivíduo, forçando-o a interagir com algum tipo de dispositivo biométrico. Esse tipo de biometria é mais amplamente difundido e mais fácil de se desenvolver. Exemplos de biometria ativa são através da digital, da iris ou da geometria da mão. Neste trabalho é utilizada a biometria do tipo passiva.

### 2.3.2 Localização

Localização consiste na identificação de uma entidade em um espaço territorial distribuído. Esse espaço pode ser interno, tais como ambientes pequenos , casas e prédios, ou externo, abrangendo uma extensa área geográfica. A localização utilizada neste trabalho é a interna, também chamada de localização *in-door*. Esse tipo de localização vêm se tornando cada vez mais popular, possibilitando o desenvolvimento de sistemas comerciais para localização de produtos, equipamentos ou pessoas em ambientes de trabalho (LIU et al., 2007). Isso tudo deve-se à crescente utilização de tecnologias sem fio, cada vez mais indispensáveis em diversas aplicações diferentes. Atualmente, três métodos de localização interna estão sendo utilizados:

- Triangulação: Método no qual calcula as coordenadas X,Y de um ponto através da resolução de um conjunto de equações lineares que envolvem vários outros pontos de referência. Triangulação pode ser desenvolvida utilizando angulação, onde são utilizados ângulos entre pontos de referência, ou lateração, no qual utiliza distâncias em linha reta do ponto do ponto a se calcular até múltiplos pontos de referência. Devido às irregularidades do meio de propagação, a técnica de triangulação tradicional se torna inviável.

- Proximidade: Através deste método é possível obter a localização através da proximidade de um nó de posição desconhecida quando em comparação com nós que possuem posições pré-determinadas, ou seja, distâncias já conhecidas. É considerado um método barato e de fácil implementação, muito utilizado quando utilizada a tecnologia de RFID.

- Fingerprinting: Consiste em uma técnica no qual mapeia todo o cenário através das ondas de rádio baseado nas informações de RSSI (*Received Signal Strength Intensity* - Força da Intensidade do Sinal Recebido) provenientes dos diversos dispositivos do ambiente. Assim, os valores das coordenadas X,Y são mapeados em uma matriz no qual pode ser utilizada para calcular o dispositivo mais próximo para predizer sua localização (KAEMARUNGSI; KRISHNAMURTHY, 2012).

Esses métodos de localização utilizam como base o cálculo de RSSI, que mede a força recebida pelo sinal do dispositivo sem fio (KOYUNCU; YANG, 2010). Essa medição utiliza o fato de que a potência com que um sinal chega a um receptor pode ser expressa em uma função, fazendo assim que maiores distâncias tenham menor intensidade de sinal. Esse cálculo de estimativa da distância entre os nós é utilizada na localização interna. O problema do cálculo de RSSI é que necessita de técnicas mais sofisticadas para inferir

corretamente um local, como a utilização de Fingerprinting. Assim, cada um dos métodos explicados anteriormente possui seus graus de eficiência, onde atualmente a técnica de Fingerprinting é considerada a mais precisa, com um erro médio de 1 a 3 metros (SECO et al., 2009), (MARTIN et al., 2009).

No processo de autenticação a localização é um fator ainda pouco utilizado, mas que fornece, quando utilizada de maneira correta, o fator extra de localidade a uma determinada entidade. Se bem empregado, pode fornecer informações únicas da entidade, fornecendo um fator extra muito eficiente.

## 2.4 Ambientes inteligentes

Este trabalho se baseia na utilização de um ambiente inteligente como base para sua aplicação. Ambientes inteligentes vêm crescendo mostrando-se ser extremamente relevante para a sociedade. Pode ser definido, basicamente, como a ideia de enriquecer um ambiente com algum tipo de tecnologia capaz de tomar decisões a favor de seus usuários. Raffler (RAFFLER, 2006) define como um ambiente digital que proativamente, mas sensivelmente, auxilia as pessoas em suas vidas diárias. Normalmente, são utilizados sensores e dispositivos interligados com uma rede de computador, formando um sistema capaz de tomar decisões através da captura de informações do ambiente. Dessa forma, evidenciamos sua multidisciplinaridade, atingindo diversas áreas como por exemplo inteligência artificial, redes de computadores e interação humano computador.

Um aspecto importante nos ambientes inteligentes, segundo Brooks (BROOKS, 2003), é o princípio de design chamado de 5W (Who, Where, What, When e Why), em português, quem, onde, o que, quando e porque. i)Quem: refere-se a identificação dos elementos que possuem papel de destaque no sistema, tal como pessoas e suas relações, animais e objetos. ii)Onde: refere-se ao rastreamento da localização dos elementos que populam o ambiente. iii)O que: refere-se ao reconhecimento das atividades e tarefas dos usuários do sistema. iv)Quando: refere-se à associação das atividades em relação ao tempo, a fim de mapear a dinamicidade do ambiente. v)Porque: refere-se a capacidade de inferir e entender as intenções e objetivos das atividades.

A aplicação de ambientes inteligentes é motivado pela finalidade de trazer autonomia e inteligência em certos contextos do dia-a-dia. Dentre suas aplicações destacam-se aplicações na área da saúde, no setor de transporte público, serviços de educação, serviços emergenciais e monitoramento de espaços públicos (AUGUSTO; MCCULLAGH, 2007). E dentre as tecnologias envolvidas nesses ambientes inteligentes, destacam-se a computação pervasiva ou ubíqua e a Internet das Coisas (IoT - *Internet of Things*), a qual refere-se à capacidade de comunicação de objetos do dia-a-dia através de uma rede de computadores.

Existem soluções específicas sobre ambientes de saúde sendo desenvolvidas. No trabalho de Copetti et al. (COPETTI et al., 2008), um arcabouço para monitoramento ubíquo e inteligente da saúde de uma pessoa em uma casa foi desenvolvido. Nesse trabalho, o monitoramento remoto assistido das pessoas era realizado de acordo com dados fisiológicos e comportamentais, conhecimentos médicos e condições ambientais. Outro trabalho que realiza esse monitoramento remoto de uma pessoa em um ambiente inteligente é Becker et al. (BECKER et al., 2006). Em seu trabalho, motiva a utilização de aplicações para a saúde em ambientes inteligentes. Nele, é introduzido um sistema chamado amiCA, no qual mapeia diversos cenários no ambiente domiciliar, como por exemplo a localização das pessoas e detectores de queda, acoplados à pessoa monitorada. Portanto,

diversas aplicações da área da saúde estão sendo desenvolvidas em ambientes inteligentes, beneficiando-se das redes de sensores, para auxiliar no cuidado com pacientes.

## 2.5 Padronizações

Com a inclusão da tecnologia na área da saúde, o uso de um critério padronizado para sistemas computadorizados tornou-se necessário. Os dados provenientes de ambientes de saúde, são capturados, armazenados, processados e transmitidos por sistemas heterogêneos (*i.e*, diferentes tecnologias, politicas e regulações). Portanto, existe a necessidade de usar uma padronização única para ordenar e organizar as atividades no contexto de segurança e assegurar o processo de desenvolvimento. Assim, a ISO/IEC 27002 foi desenvolvida com a finalidade de fornecer orientações para organizações em como proteger a confidencialidade, integridade e disponibilidade da informação (ISO, 2005). E para englobar os sistemas de saúde nesses critérios de segurança, a ISO/IEC 27799 (ISO, 2008) foi desenvolvida, no qual é uma extensão da ISO/IEC 27002 complementando suas diretrizes de implementação. A padronização ISO/IEC 27799 fornece uma lista de questões em segurança relacionadas à ambientes de saúde, no qual inclui: serviços de certificação, serviços de identificação e autenticação, serviços de contabilização, regras e responsabilidades de todos os envolvidos e várias outras especificações.

Cada país possui suas próprias regulamentações referentes à operação de sistemas em ambientes de saúde. No Brasil, os requisitos para o desenvolvimento de tecnologias em ambientes de saúde são apresentados pelo manual de certificação para sistemas de registros de saúde eletrônicos, desenvolvido pelo SBIS (SBIS, 2009). Este manual de orientação, possui várias padronizações no campo de informática médica e segurança da informação, incluindo as orientações da ISO/IEC 27002 e da ISO/IEC 27799. Assim, no Brasil, qualquer implementação envolvendo dados eletrônicos de saúde precisa seguir as orientações expostas pelo manual de certificação da SBIS.

De maneira a obter uma autenticação eficiente e dentro nas normatizações, é necessário seguir as padronizações exigidas pelo seu país de origem. Muitos trabalhos em autenticação forte não tomam ciência sobre as padronizações existentes, aumentando as chances de um desenvolvimento mais inseguro. As padronizações não ajudam apenas no processo de implementação, mas resultam em uma certificação ao sistema provando ter qualidade suficiente para ser aplicado nos contextos da área médica.

Devido a baixa preocupação da grande maioria das soluções nos trabalhos na área de autenticação de sensores em relação a facilidade de interação do usuário com os mecanismos, a não utilização de um desenvolvimento padronizado e soluções inaceitáveis para ambientes de saúde, faz-se necessário o desenvolvimento de uma solução no qual exista o foco no usuário com uma autenticação forte. O próximo capítulo aborda de maneira geral o funcionamento de uma solução no qual preocupa-se com os itens supracitados.

# 3 PROPOSTA

Neste capítulo, será apresentada a proposta de autenticação forte bem como seu desenvolvimento. Além disso, a infraestrutura abordada será demonstrada e os casos de aplicação serão explicados. Este trabalho faz parte do projeto REMOA (Rede-Cidadã de Monitoramento do Ambiente baseado em Conceitos da Internet das Coisas), no qual consiste no monitoramento remoto de pacientes com doenças crônicas, através de uma infra-estrutura de rede, onde as informações dos pacientes monitorados são enviadas para servidores remotos e posteriormente processadas e avaliadas. O desenvolvimento serve de insumo ao projeto, contribuindo para sua evolução.

A solução proposta por este trabalho é parte integrante de um módulo de segurança sobre um sistema de monitoramento de pacientes a domicilio, implementado sobre uma rede de sensores sem fio. Esse sistema é responsável por extrair e processar as informações provenientes de pacientes, levando-se em conta a capacidade dos sensores disponíveis no ambiente. O objetivo desse sistema é de acompanhar a evolução clínica de um paciente, monitorando-o a fim de identificar problemas de saúde e armazenando seus dados para que possam ser analisados por especialistas. As informações armazenadas, constituem o histórico médico de cada paciente, servindo como dados valiosos para a área da saúde. Neste trabalho, as informações coletadas serão utilizadas como parte integrante da solução de autenticação forte proposta, como será discutido em seguida.

Esse sistema de monitoramento baseado em sensores, faz parte de um ambiente inteligente, possuindo variadas aplicabilidades no ambiente. Esses sensores podem rastrear a movimentação do paciente, analisar se o ambiente está climatizado corretamente, e principalmente monitorar suas condições fisiológicas. Por exemplo, um oxímetro pode ser programado para medir indiretamente a quantidade de oxigênio no sangue de um paciente e enviar os resultados para um dispositivo armazenador. Atualmente, a variedade de dispositivos monitores capazes de extrair informações vitais e se comunicarem com outros dispositivos é bastante variada, obtendo constantes evoluções tecnológicas. Por exemplo, dados da Frost Sullivan (SULLIVAN, 2013), mostram que a comercialização desses dispositivos médicos na Ásia crescerá dos atuais 967 milhões de dólares para 1,21 bilhões de dólares em 2016. Ainda, segundo a Frost Sullivan, isso se deve ao envelhecimento da população e aos incentivos cada vez maiores por parte dos governantes apoiando o *homecare* (cuidados de um paciente à domicílio).

Ainda, durante o monitoramento no ambiente inteligente, uma outra tarefa dos sensores é o rastreamento do paciente. Como já discutido no capítulo anterior, o rastreamento está entre um dos elementos básicos fornecidos pelos ambientes inteligentes. No contexto da monitoração do paciente, constitui uma importante tarefa, monitorando seus percursos no domicílio e mantendo o sistema informado sobre sua localização. Para que tal fato seja possível, existem diversas técnicas que podem ser implementadas, como triangularização

de sinal ou Fingerprinting, já explicadas anteriormente. Dessa forma, um paciente pode ser monitorado em um ambiente interno, englobando assim soluções baseadas em seu comportamento.

Portanto, as informações provenientes dos sensores no ambiente, podem ser classificadas de 3 formas segundo Copetti (COPETTI, 2010): i) Variáveis Fisiológicas, compreendendo informações extraídas dos dispositivos ativos sobre o corpo do paciente, no qual formam a WBAN (Wireless Body Area Network - Rede sem fio sobre o corpo), tais como pressão arterial, frequência cardíaca e capacidade pulmonar. ii) Variáveis Comportamentais, no qual são as ações realizadas no ambiente por parte do paciente, tais como exercícios de rotina, locomoção e atividades domésticas. iii) Variáveis Ambientais, sensores que capturam informações do ambiente, tais como luz, calor e umidade. A presença de mais ou menos sensores referentes a uma dessas três variáveis demonstradas depende do tipo de aplicação. Por exemplo, uma pessoa com bronquite asmática, uma doença nos brônquios que dificulta a respiração, deve possuir mais sensores ambientais para seu monitoramento, tais como sensores de umidade. Neste trabalho, serão englobadas as variáveis fisiológicas e as variáveis comportamentais. Porém, como será demonstrado adiante, a solução seria flexível a ponto de permitir que variáveis ambientais fossem incluídas, dependendo do tipo de aplicação necessária.

A informação proveniente do paciente é enviada a um servidor externo localizado em um hospital. Esse servidor armazena todas as informações coletadas, sendo acessível somente por pessoas autorizadas. Essas pessoas, podem ser médicos especialistas, fisioterapeutas ou enfermeiros que estejam em contato com a evolução clínica do paciente. Para tal, as informações devem ser íntegras e legítimas, precisando assim de fortes esquemas de segurança. Assim, o esquema proposto neste trabalho é uma autenticação forte, sendo abordado na seção seguinte.

## 3.1 O processo de autenticação proposto

O processo de autenticação proposto pode ser observado na Figura 3.1. Este processo baseia-se na obtenção das informações biométricas e de localidade extraídas dos sensores, constituindo os dois fatores para a autenticação forte. O processo de autenticação pode ser resumido basicamente em três etapas: 1) Registro: Os dados do paciente são coletados por uma equipe médica, responsável pelo seu primeiro contato com o servidor do hospital. Essa coleta, deverá ser realizada com os dispositivos disponíveis para seu monitoramento por um período de 24 horas. Esse período de coleta, permite que mais adiante, na autenticação utilizando os dados fisiológicos, seja possível extrair um padrão para verificar com os dados entrantes. Além disso, nessa primeira etapa, as chaves geradas pelo dispositivo *gateway* (*i.e*, um computador na casa do paciente) são distribuídas aos sensores presentes no ambiente, compreendendo os passos 1 e 2 da Figura 3.1. Essas chaves serão utilizadas para as rodadas de comunicação entre sensores e *gateway*, com a finalidade de criptografar as informações. 2) Autenticação dos sensores: através da troca de chaves criptográficas, como será explicado adiante, os sensores são autenticados no ambiente interno e as informações dos sensores são capturadas, englobando os passos 3, 4 e 5 da Figura 3.1. 3) Autenticação do paciente: por fim, os dados do paciente são autenticados no servidor do hospital, compreendendo o passo 6 da Figura 3.1. Cada passo é explicado nas subseções seguintes.

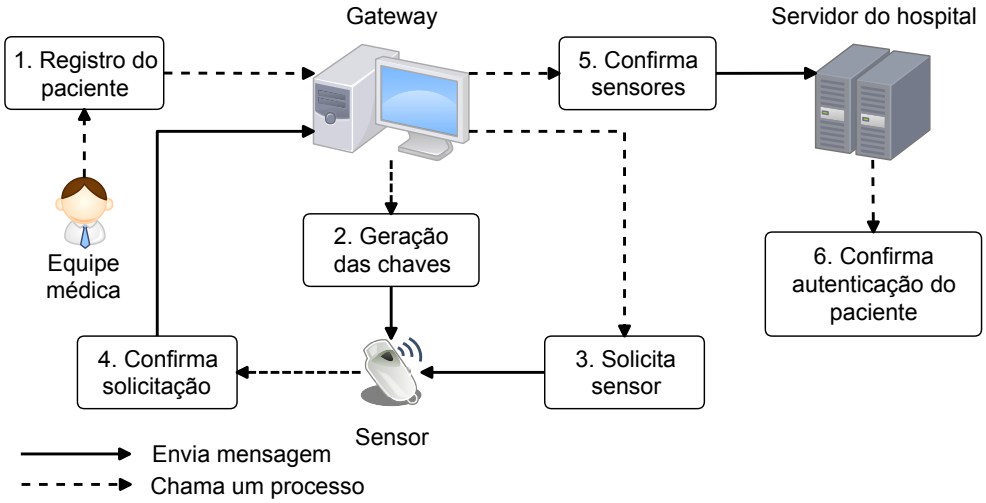


Figura 3.1: Processo de Autenticação Proposto

### 3.1.1 Registro

A primeira etapa da autenticação refere-se ao registro do paciente. Como foi supracitado, uma coleta inicial é realizada pela equipe responsável pelo paciente, referindo-se ao primeiro passo. Esse registro, garante dados ao servidor para futura autenticação. Além disso, é necessário que os sensores sejam autenticados para garantir a integridade e autenticidade das informações trafegantes. Dessa forma, um modelo formal é proposto, a fim de realizar as comunicações iniciais no ambiente. O objetivo de autenticação do paciente no servidor do hospital pode ser satisfeito apenas garantindo que os primeiros passos são seguros. O modelo proposto pretende proteger a comunicação, criptografando-a, para os estágios iniciais de comunicação. Esse modelo formal utiliza-se da criptografia simétrica, do modelo de pré distribuição de chaves e foi baseado nas propostas sobre ambientes de sensores existentes na literatura (LE et al., 2011), (DAS, 2009).

Inicialmente, o *gateway* irá gerar uma chave mestre randômica $X_G$, e para cada comunicação, uma chave de sessão $Y_{SK}$. Estas chaves possuem o tamanho de 256 bits e são utilizadas para calcular $A = h(userID \parallel X_G)$ no qual será mandada aos sensores antes do inicio das comunicações do sistema. Assim, $S$ é enviada aos sensores, onde $S = (userID, A)$. Também, os sensores são registrados (*i.e*, coletadas informações gerais, tais como ID, MAC e modelo) e as chaves armazenadas no *gateway*, no qual é considerado um nó seguro neste trabalho (*i.e*, ameças de ataques ou problemas técnicos não são considerados no dispositivo do *gateway*). Para melhor compreensão, os símbolos e notações são apresentados na Tabela 3.1.

O gerenciamento de chaves é realizado utilizando a abordagem de pré-distribuição. Essa abordagem é baseada na criptografia simétrica, referindo-se a distribuição das chaves entre os dispositivos antes que a rede seja implantada. Esse tipo de distribuição é de fácil implementação e baixo consumo computacional, tornando-se apropriada para ambientes com recursos limitados (KUMAR; LEE; LEE, 2012). As outras abordagens existentes, como a utilização servidores confiáveis para a distribuição ou criptografia assimétrica, requerem muito poder computacional, tornando-se de difícil implantação nesses ambientes.

| Símbolos e notações | Descrição |
|---|---|
| $SID$ | Identificador do sensor |
| $userID$ | Identificador do usuário |
| $X_G$ | Chave mestre |
| $Y_{SK}$ | Chave de sessão |
| $T$ | Parâmetro de tempo |
| $M$ | Mensagem trocada |
| $R$ | Informação capturada |
| $h(.)$ | Função *hash* sem retorno |
| $\|$ | Operador de concatenação de bit |
| $\oplus$ | XOR |
| $D$ | Distância do sensor |

Tabela 3.1: Símbolos e Notações.

### 3.1.2 Autenticação dos sensores

Para uma autenticação eficiente do paciente, é necessário confiar na comunicação dos sensores, pertencentes ao primeiro nível de comunicação. Assim, esse passo tem a finalidade de demonstrar uma comunicação segura entre os sensores e o *gateway*. Para realizar isto, funções *hash* sem retorno e criptografia simétrica utilizando SHA-2 e AES respectivamente são utilizados, no qual são típicas escolhas para aplicações que não comportam a complexidade computacional da criptografia assimétrica (WALTERS et al., 2007). As funções *hash* fornecem autenticidade mapeando uma mensagem e produzindo um único valor à ela. A criptografia simétrica fornece confidencialidade às mensagens para que não sejam legíveis a terceiros durante a troca de mensagens.

Primeiramente, o *gateway* calcula $K_G = h(h(SID_j \parallel A) \parallel T_G) \oplus h(userID \parallel Y_{SK})$, fazendo o *hashing* da identificação do $j^{th}$ sensor com a chave secreta compartilhada $A$ e a chave de sessão randômica gerada $Y_{SK}$. Assim, $K_G$ é criptografado com $userID$, resultando em $C_G = E(K_G \parallel userID \parallel Y_{SK})$. Uma mensagem é enviada ao sensor com o $C_G$ e o parâmetro de tempo (*time stamp*) $T_G$, $M1(C_G, T_G)$.

Nos sensores, após receber a mensagem $M1$, o parâmetro de tempo precisa ser verificado para proceder com a autenticação. Se $\Delta T \geq T_S - T_G$, onde $\Delta T$ é o intervalo de tempo esperado para a transmissão entre o *gateway* e o sensor, a sessão é abortada. Caso não o tempo esperado não for maior, o $C_G$ é descriptografado $\alpha = D(C_G)$ e o sensor calcula $\beta = h(h(SID'_j \parallel A') \parallel T_G) \oplus h(userID' \parallel Y_{SK})$. Calculado o novo *hash* com as informações recebidas e existentes do sensor, $\beta$ e $\alpha$ são comparados, $\beta = \alpha$. Se são iguais, a mensagem é autentica e pode prosseguir para calcular $\gamma = h(h(SID_j \parallel A) \parallel T_S) \oplus h(R \parallel Y_{SK})$, $V_S = E(h(\gamma \parallel T_S))$ e enviar $M2(V_S, R, T_S)$ ao *gateway*. $R$ refere-se a informação capturada do paciente presente no dispositivo presente, e antes de enviar é criptografada $E(R \oplus Y_{SK})$.

Novamente no *gateway*, o objetivo é checar se a resposta do sensor é legitima. Primeiro, o parâmetro de tempo é analisado, executando $\Delta T \geq T_G - T_S$. Se o intervalo está dentro do tempo esperado, calcula $\sigma = h(h(SID''_j \parallel A'') \parallel T_S) \oplus h(R \parallel Y_{SK})$ e descriptografa $V_S$, $\mu = D(V_S)$. Então é analisado se $\sigma = \mu$, se forem iguais, a mensagem é autentica e agora a informação $R$ pode ser armazenada para em breve ser enviada ao servidor do hospital para a autenticação do paciente.

Todas as rodadas de comunicação supracitadas podem ser melhor observadas na Fi-

gura 3.2. Esta figura, ilustra a troca de mensagens realizada nos primeiros passos, antes das informações serem enviadas para o hospital. Como pode ser observado, a primeira rodada de comunicação simboliza o cadastro do cliente e a distribuição das chaves para os sensores. Todas rodadas de comunicação subsequentes ilustram a comunicação realizada entre o *gateway* e os sensores, a fim de sua autenticação. O próximo passo descreve como é realizada a autenticação do paciente.

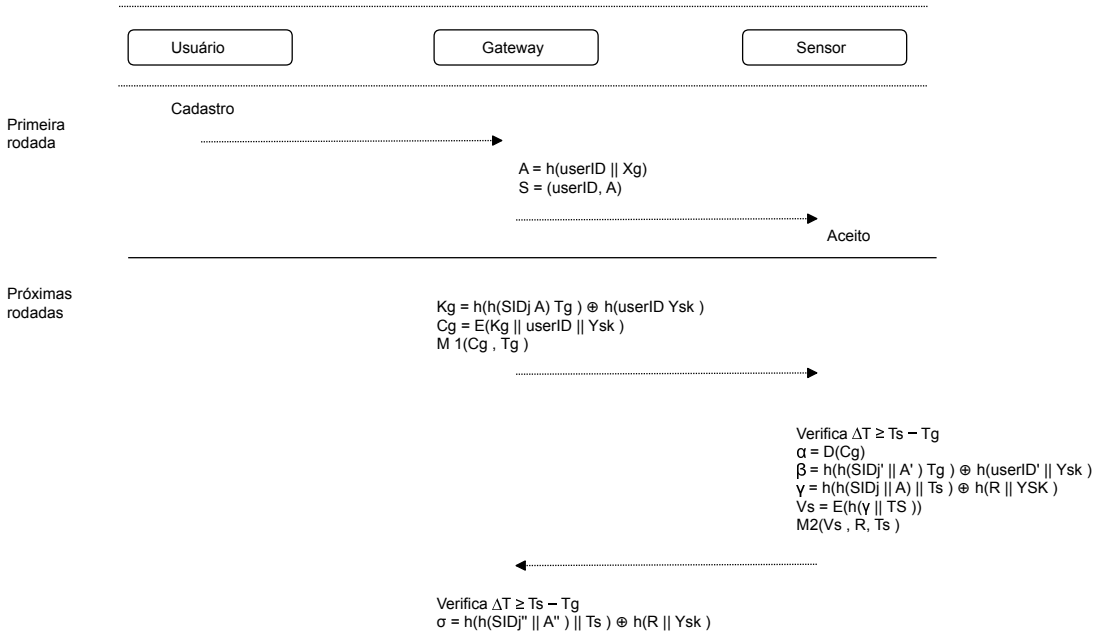


Figura 3.2: Troca de mensagens

### 3.1.3 Autenticação do paciente

O terceiro passo é responsável pela autenticação do paciente no servidor localizado no hospital, ou seja, pertence à autenticação externa do ambiente do paciente. A meta dos primeiros passos, além de cadastrar o paciente e assegurar a integridade das informações dos sensores, é colher informações suficientes dos sensores para que possam ser utilizadas na autenticação do paciente. Como a autenticação possui dois fatores, biometria e localização, um maior esforço é gasto sobre os dados fisiológicos e de localidade, como critérios básicos para a solução.

Os dados fisiológicos constituem uma parte importante na autenticação. Como o paciente é monitorado por diversos dispositivos no ambiente, a ideia nesse ponto, é tomar vantagem desses dados extraídos. Ainda mais, todas essas informações são específicas de cada indivíduo monitorado, fator necessário para a autenticação em sistemas biométricos (JAIN; ROSS; PRABHAKAR, 2004). A melhor solução utilizaria uma informação fisiológica única presente em cada indivíduo, isto é, uma informação no qual identifique cada pessoa unicamente. Porém, dados como pressão arterial e frequência cardíaca, não são únicos, isto é, vários indivíduos podem compartilhar de informações semelhantes ou idênticas. Isso impõem a necessidade da coleta de não apenas um atributo fisiológico do paciente, mas sim um conjunto deles, a fim de fortalecer a unicidade das informações. Dessa forma, as informações fisiológicas coletadas no ambiente unem-se a fim de fortalecer a unicidade do paciente, formando uma identidade fisiológica. Essa identidade fisiológica é chamada nesse trabalho de vetor identidade, como demonstrado a seguir.

$$Vetor_{userID} = (SID_{j1} \parallel R_{j1}) + (SID_{j2} \parallel R_{j2}) + \ ... + (SID_{jn} \parallel R_{jn}) \quad (3.1)$$

O vetor identidade contém todas informações fisiológicas de cada sensor do ambiente. Como o *gateway* é responsável por centralizar toda informação, é nele que o vetor identidade é montado antes do envio ao servidor externo. Alguns dados, como a frequência cardíaca, possuem uma coleta constante, o que geram muitos dados. Assim, para integrar o vetor, é retirada a média de tempo desde a última medição, para não tornar o vetor demasiadamente grande. Por fim, esse vetor identidade, possuirá dados fisiológicos como os exemplificados na Tabela 3.2. Nesta tabela, a informação capturada pelo sensor $SID_1$ refere-se a saturação de oxigênio, a qual pode ser medida por um dispositivo chamado oxímetro de pulso. A informação capturada pelo sensor $SID_2$ exemplifica uma medida de pressão arterial, podendo ser aferida por um dispositivo chamado esfigmomanômetro. Já a informação do $SID_3$ refere-se a frequência cardíaca, podendo ser obtida pelo mesmo dispositivo da saturação de oxigênio, o oxímetro (SMELTZER; BARE, 2009).

| Sensor ($SID$) | Informação ($R$) | Descrição |
|---|---|---|
| $SID_1$ | 95 % | Saturação de Oxigênio ($SaO_2$) |
| $SID_2$ | 120x80 mmHg | Pressão Arterial (PA) |
| $SID_3$ | 80 bpm | Frequência Cardíaca (FC) |

Tabela 3.2: Exemplos de dados fisiológicos coletados pelos sensores.

Os dados referentes ao outro fator utilizado na autenticação, a localização, necessitam da tecnologia adotada. Como já foi explicado, a localização *indoor* possui algumas técnicas, que dependendo da escolhida, o grau de exatidão da distância do sensor em relação ao *gateway* pode variar bastante. Nesse trabalho, os dados utilizados serão da utilização da técnica de *Fingerprinting*, já explicada anteriormente. Dessa forma, a distância de cada sensor é computada pelo *gateway* a fim de montar o vetor localização, como demonstrado a seguir.

$$Vetor_{SID} = (SID_{j1} \parallel D_{j1}) + (SID_{j2} \parallel D_{j2}) + \ ... + (SID_{jn} \parallel D_{jn}) \quad (3.2)$$

A distância de cada sensor é dada por $D_jn$, assim compondo um vetor onde cada sensor e sua distância do *gateway* são mapeados. É importante notar que o software no *gateway* encarregado por montar os vetores identidade e localização, possui previamente cadastrado os dispositivos no qual participarão da autenticação do paciente. Isso é perfeitamente mutável, dependendo da quantidade de dispositivos presentes. Por fim, esse vetor localização, possuirá dados da distância dos sensores, como exemplificados na Tabela 3.3. Cada distância exemplificada na Tabela 3.3 refere-se a um dispositivo utilizado no ambiente, considerando um grau de acerto de 3 metros, para mais ou para menos, como especificado em (LIU et al., 2007), (SECO et al., 2009) e (MARTIN et al., 2009).

Todas as informações coletadas dos sensores serão centralizadas no *gateway*, com o propósito de iniciar a próxima iteração do processo de autenticação, o envio das informações ao servidor externo. Uma vez reunidas as informações, o *gateway* se comunicará com o servidor externo utilizando-se do protocolo criptográfico SSL (Secure Socket Layer), um protocolo para uma comunicação segura (FREIER; KARLTON; KOCHER, 2011). Essa comunicação entre o *gateway* e o servidor externo, acontecerá em ciclos

| Sensor ($SID$) | Distância ($D$) |
|---|---|
| $SID_1$ | 13 m |
| $SID_2$ | 5.1 m |
| $SID_3$ | 7.8 m |

Tabela 3.3: Exemplos de distâncias dos sensores calculadas pelo *gateway*.

temporais especificados no *gateway* (*e.g*, ciclos de 15 minutos). Cada ciclo depende das necessidades do paciente, ou seja, caso o paciente não tenha nenhum problema mais grave de saúde, seu ciclo pode, por exemplo, ser de 30 - 45 minutos (*i.e*, no momento de instalação do sistema, a equipe médica deve informar esse critério). Além disso, dentre as informações repassadas ao servidor, é necessário as informações do fluxo temporal do paciente, como por exemplo, o que aconteceu durante esse ciclo de 15 minutos. Isso é necessário para que no lado do servidor seja possível analisar as informações corretamente de acordo com as alternâncias das variáveis comportamentais existentes nesse período. No lado do servidor, cada vez que as informações chegam, o modulo de autenticação é acionado dando início ao processo de autenticação do paciente. Esse processo é simplificado na Figura 3.3.

Este diagrama de atividades demonstra o fluxo de atividades para que o paciente seja autenticado no lado do servidor. Basicamente, o servidor está preparado para a análise dos dados provenientes do paciente, chamando o seu processo autenticador. Esse processo é executado utilizando as informações armazenadas sobre os dados fisiológicos do paciente, com adição das informações de localização dos sensores do ambiente. O processamento é realizado mediante um conjunto de regras, escaláveis a cada pessoa individualmente. Cada processo será melhor explicado a seguir.

Inicialmente, quando as informações chegam ao servidor, o módulo de autenticação é chamado. É nesse módulo onde todo o processo de autenticação foi desenvolvido. A primeira etapa quando se chama o módulo de autenticação, é reivindicar as informações existentes cadastradas do paciente no banco de dados local do servidor. Em primeira instância do autenticador, os dados são analisados para ter certeza de que não se trata de uma solicitação falsa. Dessa forma, é verificado se as informações do solicitante provem do determinado *gateway* e paciente. Essa verificação não garante autenticidade do indivíduo envolvido, é apenas uma etapa inicial para garantir que a tentativa é válida. Caso os dados são válidos, a autenticação prossegue para o próximo passo onde as informações fisiológicas são comparadas. Além disso, no caso de êxito, as regras são selecionadas para o paciente específico, a fim de serem utilizadas nas comparações dos dados fisiológicos. Caso a tentativa seja inválida o módulo de alerta é chamado, no qual será explicado mais adiante. As subseções a seguir explicam os componentes principais existentes no autenticador.

#### *3.1.3.1 Regras*

Para que a autenticação utilizando os fatores de localização e biometria possa ser realizada, é necessário que as regras estejam disponíveis. As regras são condições específicas definidas de acordo com as variáveis do monitoramento (*i.e*, variáveis comportamentais, fisiológicas e ambientais) dependentes do monitoramento do paciente no ambiente. Como já foi dito, no início deste capítulo, esse trabalho irá utilizar apenas as variáveis comportamentais e fisiológicas, abstendo-se das variáveis de ambientes. Para a elaboração das regras sobre as informações fisiológicas foram utilizadas fontes bibliográficas da área

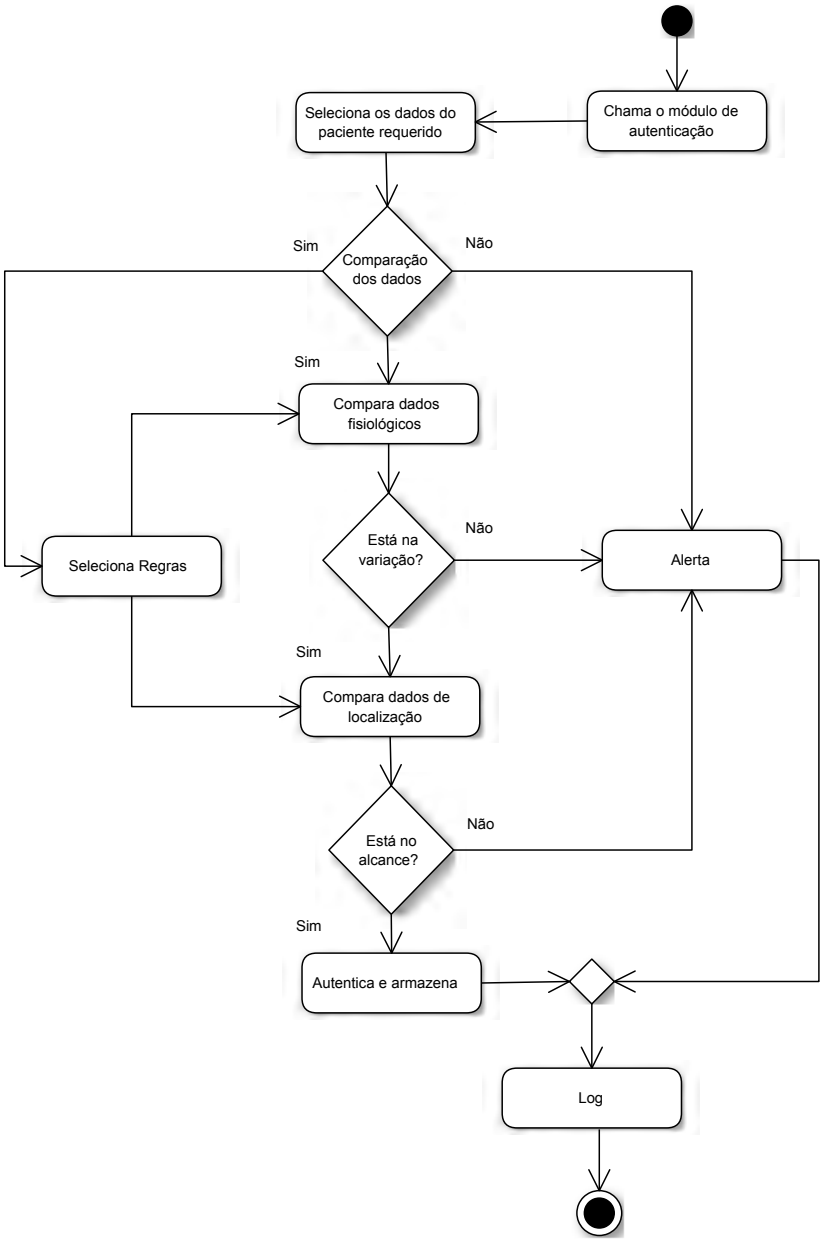


Figura 3.3: Diagrama de atividades do processo de autenticação do paciente no servidor.

da saúde, como (CARDIOLOGIA, 2005), (CARDIOLOGIA, 2006), (POTTER, 2011) e (SMELTZER; BARE, 2009). A seguir algumas regras são demonstradas:

- Durante o sono a pressão arterial sistólica deve diminuir cerca de 10 mmHg e a pressão arterial diastólica deve diminuir 7,6 mmHg;
- Em atividades leves (*e,g*, caminhar) a pressão arterial sistólica deve aumentar cerca 12 mmHg e a pressão arterial diastólica deve aumentar cerca de 5,5 mmHg;
- Em repouso, a frequência cardíaca aceitável deve estar entre 60 e 100 bpm;
- Durante atividades leves a saturação pode ser maior ou igual a 92%;
- A frequência respiratória de um indivíduo adulto quando em prática de alguma

atividade leve, sofre um aumento de 4 a 6 movimentos respiratórios por minuto sobre seus valores basais.

As regras delimitam o comportamento da comparação dos dados fisiológicos, sendo possível assim, identificar corretamente um paciente mesmo que ele esteja executando tarefas variadas em sua residência. A localização também se beneficia das regras, pois suas faixas de aceitação podem variar de acordo com atividades específicas, ou seja, de acordo com as variáveis comportamentais. Porém, neste trabalho, não serão utilizadas regras sobre a localização. Isso se deve a dificuldade de atribuir as atenuações sofridas no sinal de acordo com o deslocamento do paciente na residência. Para que fosse possível uma regra bem elaborada, seria necessário fazer testes no ambiente sobre o algoritmo e o dispositivo escolhido, podendo assim haver variações difíceis de serem mapeadas. Assim apenas as distâncias médias são consideradas neste trabalho, não se preocupando com as irregularidades e dificuldades físicas do ambiente. Ainda, as regras podem ser classificadas em duas categorias:

- Generalista: As regras generalistas dão a base de informações para mapear as ações do paciente, constituindo assim uma classe pai para um paciente.
- Especializada: As regras especializadas são utilizadas para mapear os problemas que afetam especificamente um tipo de paciente. São herdadas da classe generalista, porém com especificações extras, como por exemplo, variações diferenciadas que podem ter em um determinado estado de saúde.

#### *3.1.3.2 Dados fisiológicos*

Utilizando as regras especificadas para cada paciente, os dados fisiológicos podem ser comparados para a autenticação. A comparação se baseia na obtenção de valores mínimos e máximos nas escalas de cada informação fisiológica. Por exemplo, em condições normais qualquer pessoa possui um nível de 95 a 100 % de saturação de oxigênio, assim, quaisquer valores com limite inferior ou superior acima disso estaria com alguma irregularidade. Essa irregularidade pode tanto ser proveniente de um problema de saúde momentâneo do paciente como de uma fraude nos dados, preocupação essa que será discutida adiante no componente de alerta. Dessa forma, com as regras selecionadas, as informações do paciente passariam por um filtro como na seguinte equação:

$$compara(u, w) = \begin{cases} Aceita & \text{se } TH_{min} \geq R_{ju} \leq TH_{max} \\ Rejeita & \text{se } TH_{min} < R_{ju} > TH_{max} \\ Rejeita & \text{se } TH_{min} < R_{ju} \leq TH_{max} \\ Rejeita & \text{se } TH_{min} \geq R_{ju} > TH_{max} \end{cases} \tag{3.3}$$

Considerando que $U$ é o conjunto de pacientes registrados no servidor, e $u$ é a identidade de um indivíduo específico, então $u \in U$. Desta forma, o indivíduo $u$ é colocado a prova sobre a identidade $w$, onde essa por sua vez reflete uma determinada informação biométrica. Para que a comparação seja feita, as informações entrantes do paciente, ou seja, do seu vetor identidade, são comparadas com os limites selecionados pelas suas regras, representados por $TH_{min}$ e $TH_{max}$. A informação $R_{ju}$ do vetor identidade, no qual se refere ao dado fisiológico coletado por um determinado sensor, é colocada a prova a cada tentativa de autenticação. Caso a informação não passe, é gerado um alerta. Além disso, para que o alerta não seja acionado erroneamente muito frequentemente, existe um peso definido para cada paciente segundo a regra, no qual pode gerar estágios distintos de alerta, no qual serão explicados mais a diante.

#### *3.1.3.3 Dados de localização*

A validação da localização, muito semelhante à validação dos dados fisiológicos, deve respeitar alguns valores mínimos e máximos. Esses valores são delimitados pela tecnologia utilizada, como já mencionado anteriormente. Além destes valores pré-determinados, os valores são influenciados pelas regras. A seguir a equação é demonstrada:

$$compara(RD, D_j) = \begin{cases} Aceita & \text{se } Ra_{min} \geq D_j \leq Ra_{max} \\ Rejeita & \text{se } Ra_{min} < D_j > Ra_{max} \\ Rejeita & \text{se } Ra_{min} < D_j \leq Ra_{max} \\ Rejeita & \text{se } Ra_{min} \geq D_j > Ra_{max} \end{cases} \tag{3.4}$$

A equação compara $RD$ no qual é a distância esperada do sensor, com $D_j$ que é a distância obtida pelo *gateway*. Para tal, existem faixas de valores considerados aceitáveis, $Ra_{min}$ e $Ra_{max}$. A comparação entre as distância é rígida, ou seja, as faixas não são mutáveis, podendo variar apenas de acordo com a seleção de alguma regra. Por exemplo, se o paciente está se locomovendo, os limites tornam-se mais flexíveis, devido a dificuldades de difração, reflexão e dispersão presentes nas técnicas que utilizam-se de RSSI (LIU et al., 2007). Essa é a única regra utilizada com a localização, pois de flexibiliza de acordo com o deslocamento do paciente.

#### *3.1.3.4 Alerta*

Toda informação selecionada para a comparação, pode passar ou não pelo algoritmo que serve como filtro. Toda vez que uma informação é rejeitada, significa que algum problema aconteceu, assim fazendo-se necessário avisar a entidade chamada alerta. Um alerta pode ser gerado não necessariamente por uma tentativa de fraude na autenticação, mas sim uma variação fisiológica não esperada do paciente ou um defeito em algum dos sensores no ambiente. Dessa forma, em cada alerta gerado os dados são colocados em um *log* e deixados de lado para a análise de uma equipe responsável. Cada vez que o alerta é chamado, será realizada uma solicitação de volta ao *gateway* para saber se as informações foram provenientes do mesmo. Caso os dados forem exatamente iguais com os informados pelo *gateway*, o hospital deve entrar em contato com a residência do paciente, para checar seu estado. Se os dados forem diferentes, significa que houve uma tentativa de fraude sobre essas informações. Caso foi provado que as informações não são fraudulentas, as informações originais podem ser cadastradas no servidor para futura análise.

Para que alertas não sejam disparados frequentemente, as variáveis fisiológicas necessitam de um ajuste. Por exemplo, a frequência cardíaca de um paciente pode possuir uma variação muito grande, mesmo sobre uma determinada regra. Mas uma variação anormal pode não necessariamente ser passível de alerta. Dessa forma, essas instâncias de variáveis fisiológicas no qual podem possuir muita variação devem possuir níveis de alerta, como a Figura 3.4 mostra a seguir.

Esta figura mostra como as variações de alertas são tratados. Como exemplo para explicar a Figura 3.4, vamos utilizar os valores normais em um adulto de frequência cardíaca (POTTER, 2011). Os valores normais variam de 60 - 100 bpm, equivalentes à variável N. Uma variação aceitável pode ter 10 bpm para mais ou para menos, equivalendo à variável 'a' minúsculo. Caso a variação exceda os valores de 'a', estarão dentro do domínio da variável 'A' maiúsculo, o que determina uma situação onde o componente de alerta deve ser acionado. Cada pessoa possui um tipo de ritmo fisiológico, fazendo com que os valores e as regras criadas sejam específicas para cada paciente.

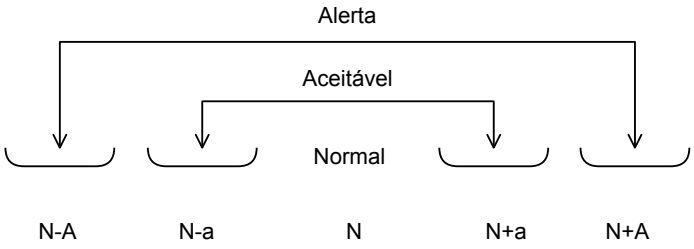


Figura 3.4: Exemplo para calcular as variâncias sobre o alerta.

Existe uma situação particular sobre as variações, em que um alerta é gerado após algum problema fisiológico do paciente. Nessa situação, existem dois casos específicos a serem analisados:

- i) O paciente obteve variações fisiológicas que são legítimas, ocasionadas por algum mal súbito, acidente doméstico ou fatores agravantes sobre sua saúde. Isso ocasionaria na não autenticação do paciente, visto que o algoritmo autenticador não aceitaria os valores recebidos. Neste caso, as informações que não são aceitas, são temporariamente cadastradas em um banco de dados secundário, no qual necessitam de análise (além de serem registrados no log, como citado anteriormente). O módulo de gerenciamento pode descobrir que se tratou de fato de um problema fisiológico do paciente, ocasionando em um falso alerta. Dessa forma, os dados seriam enviados e autenticados no banco de dados original do paciente, com a ressalva que são dados provenientes de algum problema fisiológico do paciente. Caso seja constatado que o paciente não está de fato alterado, existe a possibilidade de um ataque ou de defeito em algum dispositivo do ambiente do paciente. Esses dados não seriam cadastrados e um alerta seria gerado para que medidas de emergência sejam tomadas (*i.e*, medidas essas que seriam especificadas pelas políticas de segurança que regem o sistema).

- ii) Um alerta é gerado somente após determinados valores aceitáveis consecutivos recebidos. Trata-se das mesmas situações descritas no item anterior, porém, dependentes das estratégias adotadas pelo sistema. Por exemplo, após três valores aceitáveis seguidos, um alerta seria autenticado corretamente. Neste trabalho não são incluídas regras como esta, mas são passíveis de estudo, uma vez que retratam possíveis cenários reais.

Se as informações forem legítimas e não acionarem o alarme, significa que podem ser cadastradas no servidor, ou seja, estão autenticadas. Tudo o que acontece no processo de autenticação, seja gerando ou não alarme, é armazenado no log, no qual é responsável para armazenar o status das tentativas de autenticação. Servirá para auditorias e para análise de possíveis alertas.

No próximo capítulo são feitos testes sobre o autenticador, demonstrando seus resultados obtidos. Também, alguns estudos de caso serão realizados testando diferentes perfis fisiológicos de pacientes, mostrando a eficiência da solução proposta.

# 4 ESTUDOS DE CASO E RESULTADOS

Este capítulo é responsável por descrever os testes realizados no autenticador desenvolvido. Estes testes são analisados e discutidos a fim de encontrar seu grau de eficiência no domínio específico. Para auxiliar nesta tarefa, são estudados três casos de uso, com dados e situações distintos refletindo os ambientes reais. Os testes realizados neste trabalho utilizaram-se de simulações, uma vez que um ambiente físico equipado e povoado não se encontra disponível. As próximas seções servem para explicar os testes, os ambientes simulados, os estudos de caso realizados e os resultados obtidos.

## 4.1 Testes e estudos de caso

No sistema proposto de monitoramento do paciente, informações são geradas constantemente e gravadas em um banco de dados específico. E de acordo com essas informações que os testes são realizados sobre o autenticador desenvolvido. Os testes irão se basear sobre três situações diferentes em três pacientes diferentes. As situações referentes às variáveis comportamentais já especificadas neste trabalho, no qual, foi escolhido: i) Repouso: o paciente está em total repouso, não exercendo nenhum tipo de atividade, leve, moderada ou pesada; ii) Comendo: o paciente está se alimentando, o que gera pequenas alterações em alguns atributos fisiológicos; e iii) Atividade leve: o paciente está caminhando, praticando fisioterapia ou qualquer outra atividade leve. A escolha dessas variáveis comportamentais é resultado de estudo sobre materiais na área da saúde que definem as alternâncias sofridas pelo corpo humano nessas condições. Ainda, o escopo foi limitado por se tratar de diversas variáveis comportamentais possíveis em um ambiente real.

Com relação aos pacientes, foram escolhidos três tipos de pacientes diferentes, ou seja, três tipos de pessoas que possuem valores basais fisiológicos distintos. Os tipos de pacientes escolhidos foram: i) Paciente adulto; ii) Paciente idoso (*i.e*, pessoa com mais de 60 anos de idade, segundo os critérios do ministério da saúde brasileiro) e iii) Paciente idoso doente, em que a doença escolhida foi a hipertensão, ocasionada por um acidente vascular encefálico isquêmico. Os dados desses três tipos de pacientes serão submetidos à análise considerando para cada um deles as três variações das variáveis comportamentais especificadas. Isso resultará em três estudos de casos distintos, considerando cada paciente. Todos os valores basais e alterações fisiológicas foram baseados na literatura existente (CARDIOLOGIA, 2005), (CARDIOLOGIA, 2006), (POTTER, 2011) e (SMELTZER; BARE, 2009).

Foram realizados trinta experimentos sobre cada estudo de caso, em que cada experimento consiste da escolha aleatória de uma requisição a ser autenticada pelo algoritmo autenticador. Essa requisição recebe informações provenientes do ambiente do paciente,

bem como os dados fisiológicos e a distância relativa de cada sensor.

### 4.1.1 Dados

Os dados coletados são armazenados em um banco de dados. Para que fosse possível a execução dos testes sobre o autenticador, uma grande quantidade de dados foi criada através de um algoritmo que gera valores randômicos de acordo com os valores de cada indivíduo. Todos os dados populados no banco de dados estão ajustados de acordo com os padrões basais e variâncias fisiológicas provenientes da literatura supracitada. Já o algoritmo randômico foi necessário pois existem dois grandes problemas quando tratamos de informações fisiológicas de pessoas reais: i) Falta de uma base de dados pública, com informações fisiológicas de pessoas aleatórias anônimas, que facilitaria as pesquisas na área, como por exemplo pesquisas no campo da biometria; e ii) Necessidade de aprovação por um comitê de ética, onde todo dado proveniente de alguma pessoa precisa ser aprovado previamente por esse comitê. Trabalhos que são desenvolvidos na área da saúde, quando possuem interação com pacientes, precisam da escrita de um projeto e submissão a um comitê de ética, que pode aceitar ou negar tais experimentos. Essa burocracia, aliada a falta de base de dados públicas para pesquisa, dificulta muito a experimentação com dados reais, o qual seria o cenário ideal de testes. Dessa forma, o algoritmo desenvolvido para popular o banco de dados foi necessário para dar suporte aos testes realizados, permitindo assim a simulação das informações existentes em um ambiente real. As informações fisiológicas utilizadas neste trabalho estão dispostas na Tabela 4.1.

| Abreviatura | Descrição |
|---|---|
| $FC$ | Frequência Cardíaca, medido em batimentos por minuto ($bpm$). |
| $FR$ | Frequência Respiratória, medido em respirações por minuto ($rpm$). |
| $SAT$ | Saturação de Oxigênio, medido em porcentagem de oxigênio no sangue ($SaO_2$). |
| $TP$ | Temperatura, medido em graus Celsius ($^0C$). |
| $PAS$ | Pressão Arterial Sistólica, medido em milímetros de mercúrio ($mmHg$). |
| $PAD$ | Pressão Arterial Diastólica, medido em milímetros de mercúrio ($mmHg$). |

Tabela 4.1: Informações fisiológicas utilizadas

Essas variáveis foram escolhidas por serem as mais comuns nas medições realizadas em pacientes, facilmente obtidas pela literatura médica existente. Também, são variáveis fáceis de serem obtidas através de sensores, existindo uma grande variedade no mercado, de acordo com a necessidade. Essas variáveis mostradas na Tabela 4.1, constituem as informações básicas existentes em um prontuário médico do paciente. Além das informações fisiológicas, existem os valores simulados para a distância relativa dos sensores. Como já foi explicado na seção de fundamentação teórica, os dados referentes a localização são baseados na literatura existente. A geração desses dados também é realizado através de um algoritmo que gera os valores randômicos. Os valores obedecem as escalas que o algoritmo de *Fingerprinting* produz, de acordo com a literatura, e nenhuma interferência é calculada (*i.e*, ruído, reflexão, falha, etc).

### 4.1.2 Ambiente de teste

O ambiente de teste é constituído basicamente de dois computadores comunicando-se através de uma interface de rede. A comunicação foi realizada utilizando os princípios do modelo cliente-servidor, onde um computador A, referente ao *gateway* do paciente, envia

as informações ao computador B, referente à base de dados do hospital, utilizando SSL. O computador A, possui o sistema operacional Linux, distribuição Ubuntu 13.04, com as seguintes especificações técnicas: processador Intel com 4 núcleos de 3.2 GHz, memória RAM com 4 Gigabytes, dotado com interface de rede cabeada com uma banda de 1 Mbps de download. Já o computador B, servidor pertencente ao hospital, é uma máquina virtual rodando também com o Ubuntu 13.04, utilizando as seguintes especificações técnicas: 2 núcleos de processamento, 2 Gigabytes de memória principal e contém interface de rede cabeada para comunicação com o computador A. Além disso, no computador B, o servidor configurado é o Apache 2.4.6, trabalhando em conjunto com o banco de dados MySQL. Ainda, o autenticador, bem como os algoritmos necessários para execução de todos os testes, foram desenvolvidos na linguagem de programação PHP, em sua versão mais atual, 5.5. A escolha da linguagem PHP foi motivada pela sua grande flexibilidade com aplicações WEB e facilidade de integração com servidores.

## 4.2 Estudo de caso 1: Paciente adulto

O primeiro caso a ser analisado refere-se ao paciente adulto, em que não possui nenhum tipo de doença relevante a ser monitorada. Esse primeiro estudo de caso, refletirá o funcionamento do sistema autenticador sobre variáveis normalmente comportadas, neste caso, um paciente adulto sem nenhum tipo de doença. O teste é realizado sobre uma amostra aleatória deste tipo de paciente, onde as informações coletadas referem-se à tabela 4.1 e o deslocamento dos sensores.

A cada minuto, internamente na residência do paciente, são coletadas informações do seu estado fisiológico. Essas informações podem variar dependendo de sua natureza. Por exemplo, informações sobre a frequência cardíaca são coletadas a cada minuto, enquanto informações sobre sua temperatura podem ser realizadas a cada envio ao servidor externo. Essas informações são importantes para o módulo de gerenciamento, porém, para a autenticação não. Para a autenticação é necessário extrair uma amostra de acordo com os ciclos de tempo pré-determinados. Assim, por exemplo, a cada 60 minutos uma amostra das informações é coletada especificamente para a autenticação. Dessa forma, os testes realizados sorteiam uma amostra aleatória contendo uma instância de informações que chegam ao servidor. Essas informações então são postas à prova, de acordo com as informações já existentes, e as regras, que extraem o padrão de cada paciente. Como já mencionado anteriormente, são escolhidas 30 amostras aleatórias, e esse processo se repete para cada estudo de caso abordado. Assim, a Figura 4.1 mostra a coleta das informações de cada amostra para o paciente adulto.

A Figura 4.1 possui três valores de interpretação. O valor 0 refere-se às informações que passaram pelo autenticador, ou seja, estavam nas faixas corretas de acordo com o paciente, valor normal. Com o valor 1, as informações também passam e são autenticadas normalmente, porém com a ressalva de que houve uma pequena alteração aceitável nos dados coletados, sendo considerados valores aceitáveis. Já o valor 2 pertence a dados que fugiram das escalas normal e aceitável, 0 ou 1 respectivamente, indicando um problema com os dados, um alerta. Como já mencionado, essa amostra seria colocada à prova em uma base de dados separada, enquanto uma equipe entra em contato com o paciente para descobrir o ocorrido. De acordo com o diagnóstico do ocorrido, as informações se tornariam legítimas, e entrariam no banco com a ressalva de que são informações de algum momento anômalo do paciente, ou seja, não podem ser utilizadas como padrão para futuras autenticações. As ações a serem realizadas no momento da descoberta de uma

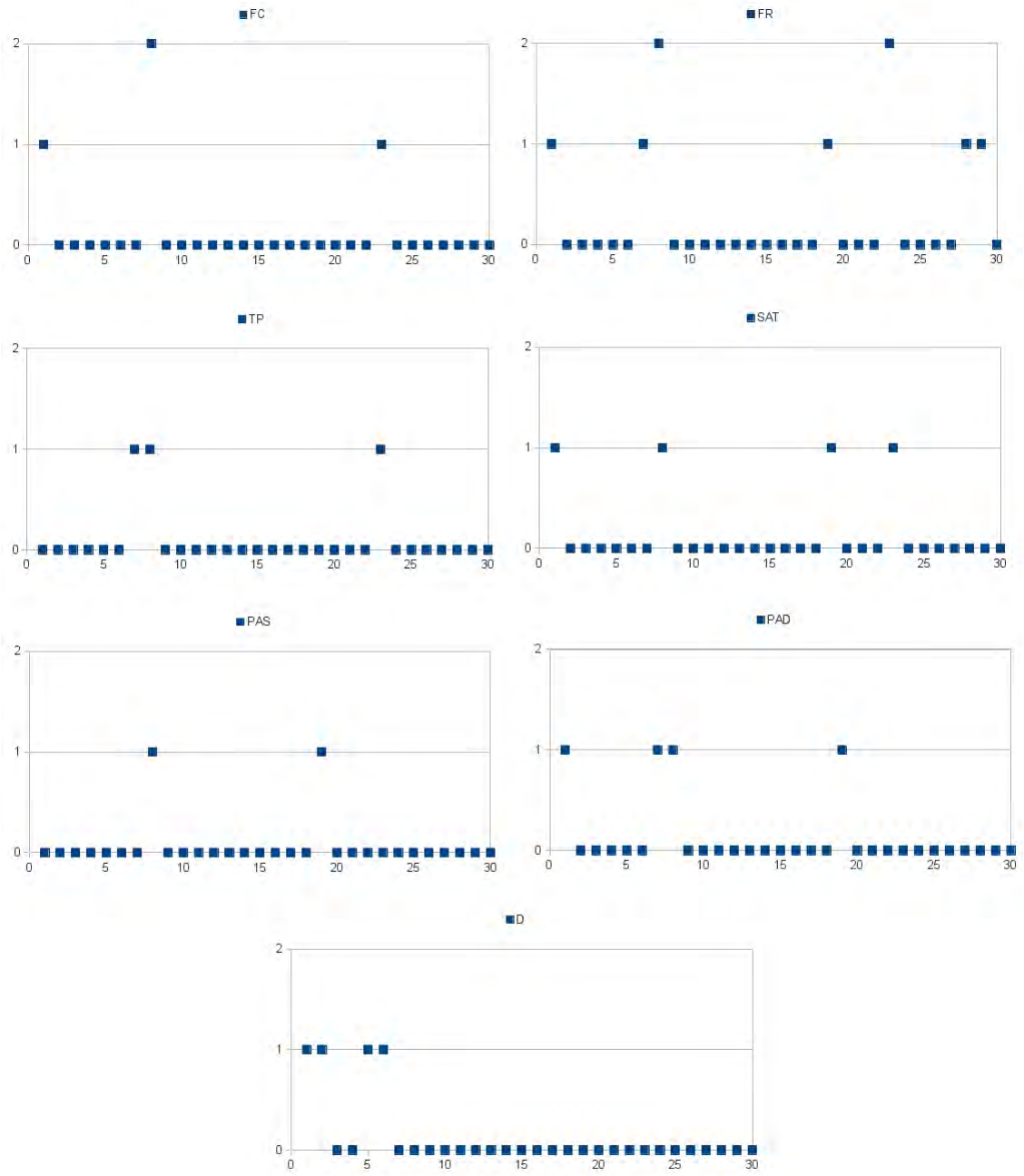


Figura 4.1: Amostras individuais sobre cada variável calculada do paciente adulto.

anomalia não são do escopo deste trabalho, sendo cabíveis de estudo a outros segmentos como o gerenciamento ou tratamento de falhas. Portanto, na Figura 4.1, é possível analisar a amostra colhida, observando o comportamento de cada informação coletada.

É possível verificar que para o paciente adulto, não existe muita alteração nos valores, fazendo com que a maioria seja aceito. Mas algumas variáveis obtiveram variações passíveis de alerta, como a FC e a FR. Tais alterações são explicadas devido à natureza dessas variáveis. Como suas próprias medidas indicam, são coletadas informações a cada minuto sobre essas variáveis, mostrando uma maior tendência sobre oscilações, sendo mais fáceis de fugirem das regras impostas. Essas grandes variações são explicadas pela literatura, onde evidencia-se que pacientes adultos admitem uma faixa de valores muito grande.

Outro fator notável é sobre o comportamento da variável D. Apesar de bastante com-

portada, pode-se observar que nas amostras 1, 2, 5 e 6 houve uma variação, passando da faixa normal para a aceitável. Isso aconteceu pois essas quatro amostras resultaram da variável comportamental de atividade leve, ou seja, amostras calculadas quando o usuário realizava alguma atividade leve (*i.e*, deslocamento pela casa, atividade doméstica ou qualquer outra atividade que não sobrecarregue o físico do paciente). Isso Mostra a sensibilidade da variável D sobre as movimentações do paciente dentro de casa, mesmo que a regra seja flexível sobre seus deslocamentos, é difícil rastrear com precisão por causa da reflexão, ruído e outros fatores de interferência já mencionados anteriormente neste trabalho. As regras utilizadas para a variável D não calculam esses fatorem de interferência, mas admitem faixas maiores sobre as variável comportamentais.

A Figura 4.2, mostra o total calculado sobre cada uma das faixas possíveis.

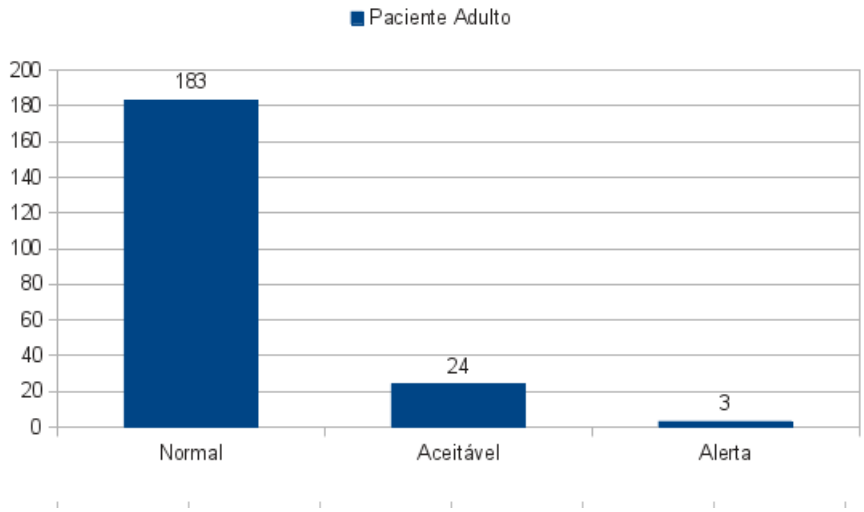


Figura 4.2: Total de dados coletados do paciente adulto.

Com a Figura 4.2, podemos ver os valores totais sobre cada uma das faixas. Onde apenas 3 instâncias coletadas falharam no autenticador. Porém, apesar de 3 falhas existentes, de um total de 210 amostras, apenas 2 amostras do total de 30 é que resultaram em falha, amostras 8 e 23. Isso se deve pois na amostra número 8, tanto a FC quanto a FR geraram alerta, fazendo com que dois alertas ocorressem em uma mesma amostra. Isso pode mostrar que na amostra 8, o alerta pode ser mais legítimo do que o alerta gerado na amostra 23. Porém, apesar de cabível estudo nesse argumento, essa característica não é estudada neste trabalho.

A próxima figura, mostra a eficiência do autenticador, mostrando a porcentagem de falhas e acertos sobre o experimento realizado.

A Figura 4.3 mostra a eficiência da autenticação. Por ela podemos observar que 93,33% das amostras foram autenticadas com êxito, enquanto 6,67% falhou, ou seja, foram consideradas não autênticas.

Sistemas de autenticação que utilizam informações biométricas, utilizam duas medidas como as principais para medirem suas eficiências: Taxa de Falsa Aceitação (False Acceptance Rate - FAR) e a Taxa de Falsa Rejeição (False Rejection Rate - FRR) (JAIN; ROSS; NANDAKUMAR, 2011). A taxa de falsa rejeição se refere quando um usuário legítimo é rejeitado porque o sistema não conseguiu identificar a similaridade entre os dados entrantes e aqueles armazenados na base de dados. A taxa de falsa aceitação se refere quando um impostor é autenticado no lugar de um usuário legítimo, isso pode acontecer

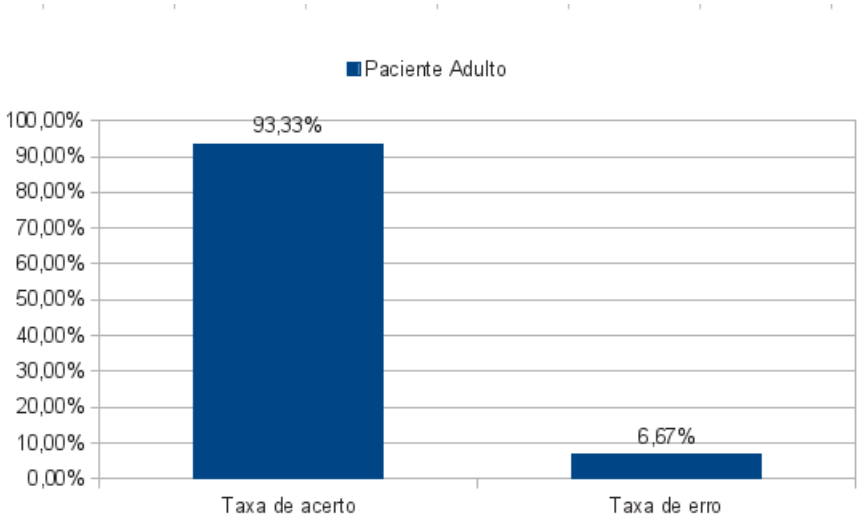


Figura 4.3: Eficiência do autenticador sobre as medidas do paciente adulto.

pois o sistema pode achar os dados biométricos do impostor muito similares ao do usuário legítimo. Dessa forma, para analisarmos a eficiência do sistema utilizado é necessário utilizar essas duas taxas.

As amostras utilizadas nos testes, são provenientes de um gerador legítimo, sem a interferência de um impostor. Assim, as 2 rejeições, referentes aos 6,67%, são consideradas como rejeições sobre valores legítimos, podendo assim dizer que a Figura 4.3 refere-se à taxa de falsa rejeição sobre o sistema.

### 4.2.1 Taxa de falsa aceitação do paciente adulto

Além de calcular a taxa de falsa rejeição, a fim de analisar a eficiência da autenticação, é necessário também que seja calculada a taxa de falsa aceitação. Como essa taxa calcula a possibilidade de um impostor se autenticar no sistema como se fosse um usuário legítimo, foi necessário simular uma violação à integridade das informações entrantes. De acordo com as características do domínio de aplicação, essa violação poderia ser de duas fomas: um ataque bem sucedido, ou uma outra pessoa se passando pelo paciente. Como um ataque é de difícil execução, será adotada a usurpação, onde uma pessoa se faz passar pelo próprio paciente.

Nesse ponto, queremos exatamente o contrário que a Figura 4.3 proporciona, ou seja, a maior quantidade de alertas gerados possíveis. Para realizar esse teste, foram feitas comparações com outros padrões de dados gerados, pertencentes a um outro paciente qualquer. Assim, o algoritmo de geração dos valores foi modificado a fim de estabelecer um outro padrão qualquer, simulando o outro indivíduo envolvido. Novamente foram selecionadas 30 amostras desse novo paciente, mas foram submetidas de acordo com a autenticação do paciente adulto no qual os testes já foram feitos. A Figura 4.4 mostra como foram as amostras das variáveis individuais.

Podemos analisar que a grande maioria das informações ou geraram alerta, ou ficaram na faixa aceitável, por não estarem de acordo com os padrões e regras do paciente legítimo. A exceção está presente na variável do deslocamento, onde todos os valores foram aceitos. Como a localização é igual para os sensores, só aconteceriam alertas caso houvesse muita diferença geométrica entre os sensores e o *gateway*. Em compensação

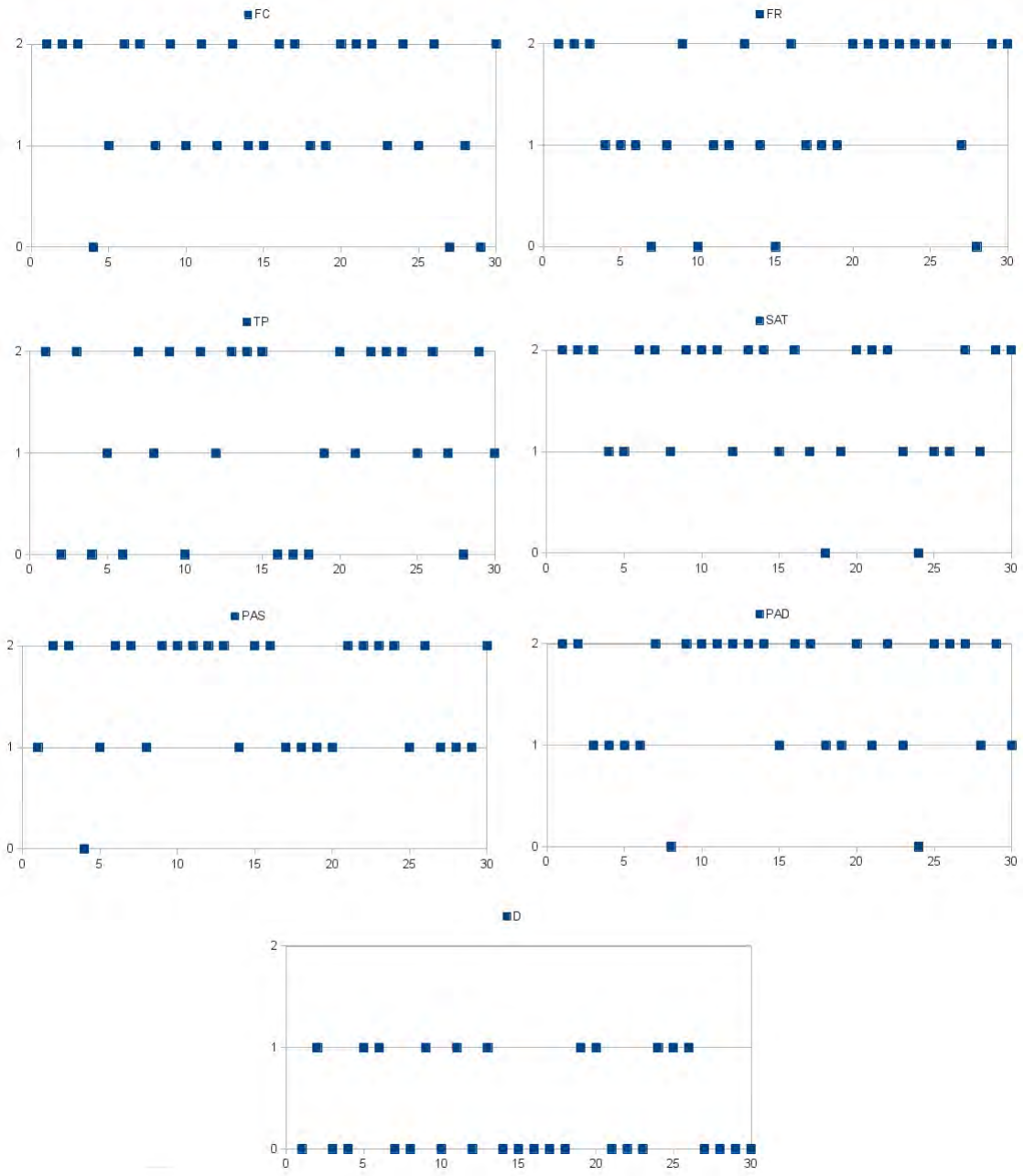


Figura 4.4: Amostras individuais sobre cada variável para o cálculo da FAR no paciente adulto.

variáveis como PAS e PAD obtiveram índice elevado de alertas ou valores aproximados ao alerta, ficando ainda em aceitáveis. Isso mostra PAD e PAS como boas variáveis fisiológicas para comparação, comportando-se com grande unicidade. A Figura 4.5 mostra o total acumulado de cada uma das faixas.

Através da Figura 4.5, podemos notar bastante diferença entre os acumulados de cada faixa para os cálculos da FAR e da FRR, já calculada anteriormente, como esperado. Para a FAR, o acumulado de alertas é superior ao das outras faixas, onde valores 0, ou seja valores na faixa normal, são a minoria, possuindo esse alto número graças a variável D. Pode-se observar que temos um total de 35 dados na faixa normal e 75 dados na faixa aceitável, obtendo um total de 114 dados aceitos pelo autenticador. Isso totaliza 54% de

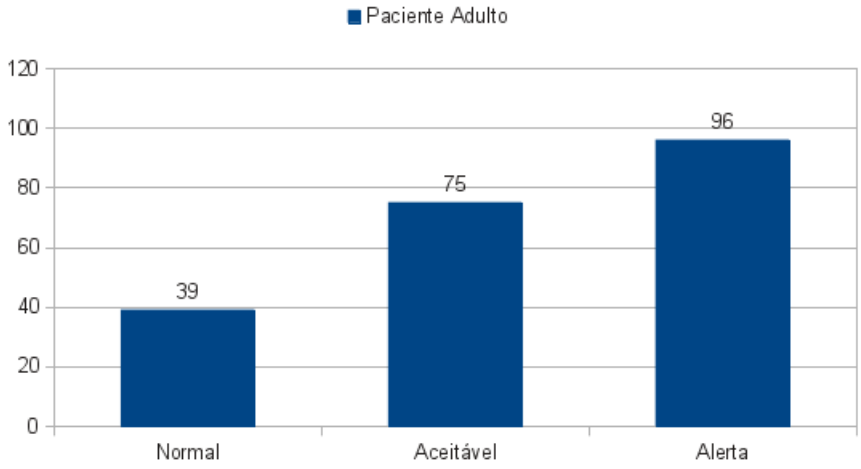


Figura 4.5: Total de dados coletados para o cálculo da FAR no paciente adulto.

amostras aceitas para o paciente adulto, um índice bastante alto.

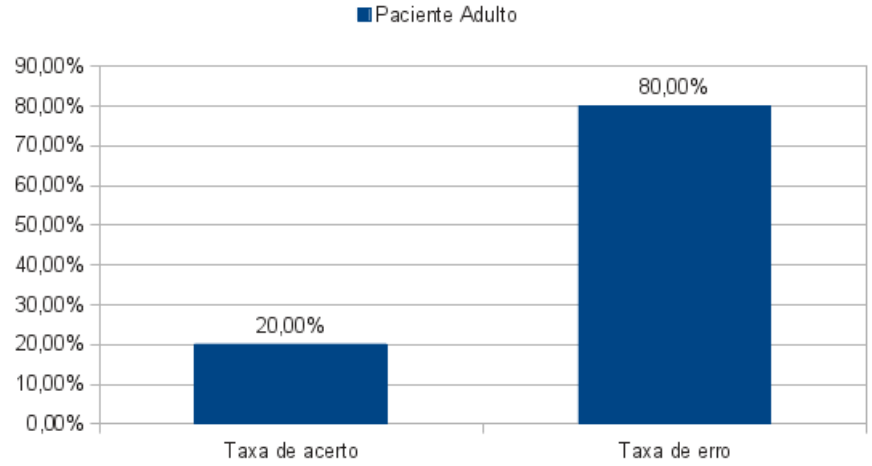


Figura 4.6: Eficiência do autenticador para o cálculo da FAR no paciente adulto.

A Figura 4.6, mostra em porcentagem o cálculo da FAR. Para seu entendimento, vamos relacionar a taxa de acerto como a porcentagem de amostras que foram autenticadas utilizando o autenticador proposto nesse trabalho, e a taxa de erro como a quantidade de amostras que foram rejeitadas pelo autenticador. Pode-se observar que 20% das amostras, ou seja as amostras 4, 5, 8, 18, 19 e 28, passaram e foram autenticadas incorretamente. Também, 80% das amostras não foram autenticadas, ou seja, foram rejeitadas. Isso mostra a sensibilidade das variáveis ao serem comparadas com padrões de outros indivíduos, pois 20% é um número bastante alto e não tolerável a um sistema de autenticação.

## 4.3 Estudo de caso 2: Paciente idoso

Agora que analisamos o funcionamento do processo de autenticação em um paciente adulto, vamos repetir as simulações porém para um paciente idoso. Pessoas idosas

possuem sensibilidades diferentes sobre as informações fisiológicas, devido doenças e à fragilidade imposta pela idade. Dessa forma, a ideia nesse segundo estudo de caso é englobar os testes do processo de autenticação sobre uma diferente situação, onde um paciente idoso com padrões e características distintas é submetido ao processo.

Assim como no estudo de caso anterior, serão avaliadas 30 amostras aleatórias geradas para o paciente idoso. A Figura 4.7 mostra as faixas de valores obtidas sobre cada variável.

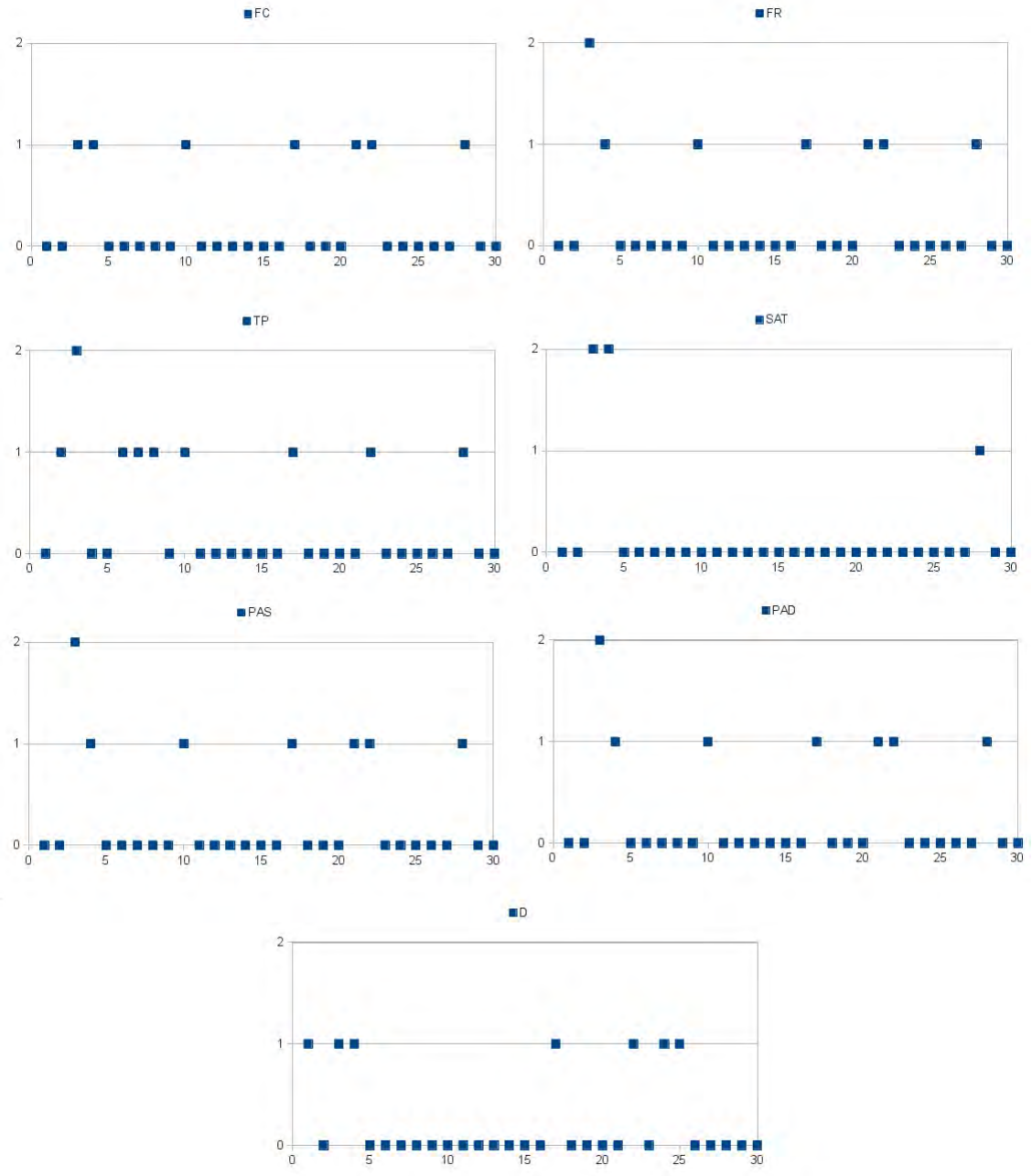


Figura 4.7: Amostras individuais sobre cada variável calculada do paciente idoso.

Pode-se observar que o paciente idoso possui uma maior quantidade de valores nas faixas alerta e aceitável, quando comparado com as amostras do paciente adulto. De acordo com os padrões estabelecidos, a escala de valores aceitáveis de algumas variáveis são muito menores em pacientes idosos, como por exemplo FR e SAT. Como são aceitos menos valores, o índice de falhas aumenta, assim como a quantidade de valores nos

níveis aceitáveis. Esse fato já era esperado para essas variáveis, uma vez que pacientes idosos possuem um ritmo fisiológico mais lento que pacientes mais jovens, explicando uma escala menor de aceitação. Mas dentre as variáveis, destaca-se a variável T, obtendo a maior variação dente todas. Isso mostra a sensibilidade das amostras de temperatura sobre pacientes idosos, o que inclui regras bastante restritas. Já a variável de deslocamento continua com a mesma tendência que já foi demonstrada pelo paciente adulto, ou seja, os valores podem mudar de faixa apenas quando a variável comportamental atividade física leve é utilizada. A seguir a Figura 4.8 mostra o total de dados coletados sobre cada faixa do paciente idoso.

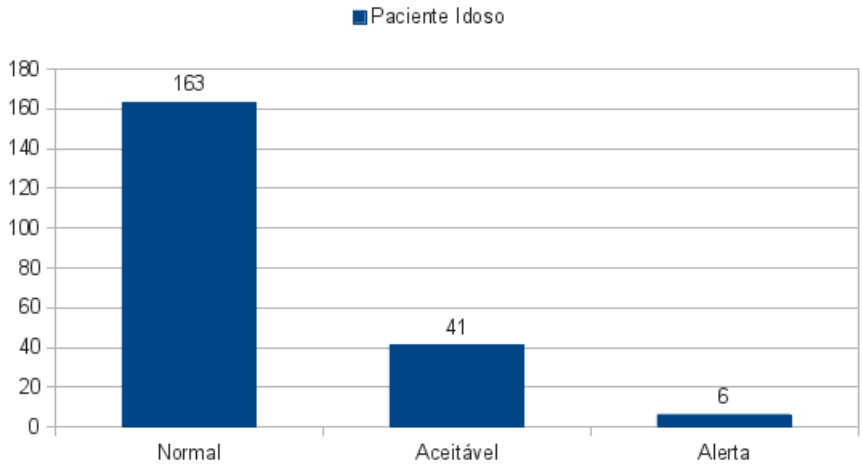


Figura 4.8: Total de dados coletados do paciente idoso.

O acumulado nas faixas aceitável e alerta aumentou em comparação ao paciente adulto. O maior aumento aconteceu nos alertas, possuindo o dobro do que foi obtido no paciente adulto. Apesar desse fato, a quantidade de autenticações falhas se manteve igual, como pode ser visto na Figura 4.9, explicável pela amostra 3, que gerou alerta na maioria das variáveis que foi calculado.

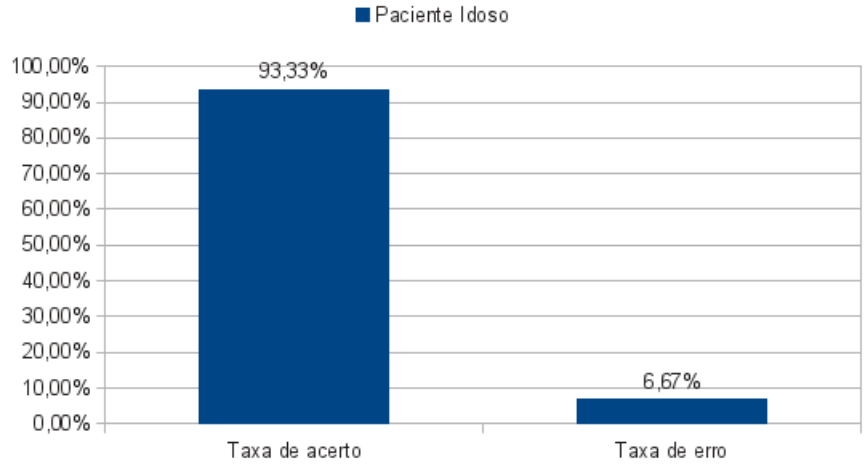


Figura 4.9: Eficiência do autenticador sobre as medidas do paciente idoso.

Apesar de um maior número de valores nas faixas aceitável e alerta, o desempenho

da autenticação do paciente idoso, se manteve igual ao do paciente adulto, com 93,33% de êxito e 6,67% de falhas, segundo a Figura 4.9. Assim as taxas de FRR resultantes de ambos os pacientes adulto e idoso, foram iguais, apesar da diferença dos totais de valores acumulados em cada faixa. Isso mostra que faixas etárias diferentes não possuem grande relevância para o processo de autenticação, pacientes estes que possuam seus valores típicos aos padrões normais.

### 4.3.1 Taxa de falsa aceitação do paciente idoso

Da mesma forma que a taxa de FAR foi calculada para o paciente adulto, o paciente idoso será submetido ao calculo da FAR. O processo é o mesmo ao anterior, simulando um outro paciente qualquer sendo autenticado no lugar do paciente legítimo. A Figura 4.10 mostra as amostras individuais coletadas para o cálculo da FAR.

A grande maioria das informações geraram alerta, ou pelo menos ficaram na faixa de aceitável, como esperado. Mas o destaque ficou para a variável SAT, que obteve um alto índice falsas aceitações, totalizando 8 amostras na faixa normal e 13 amostras na faixa aceitável. Isso demonstra que SAT não é uma boa variável fisiológica a ser considerada para a autenticação no caso do paciente idoso, pois possui uma similaridade muito grande entre indivíduos diferentes. Até mesmo em comparação com outras variáveis comuns entre indivíduos diferentes, como a TP, SAT teve o pior desempenho no total. A Figura 4.11 mostra o total acumulado em cada uma das faixas para o cálculo da FAR.

O total dos dados coletados sobre cada faixa manteve-se muito semelhante ao do paciente adulto. Mostrando mais uma vez que existe pouca diferença entre as autenticações de indivíduos de diferentes idades, não sendo um fator primordial. Pode-se observar que o paciente idoso obteve um acumulado nas faixas normal e aceitável muito semelhante ao paciente adulto, obtendo 40 dados na faixa normal e 72 dados na faixa aceitável, totalizando 112 dados aceitos. Assim, obteve um total de 53% de amostras aceitas, muito semelhante ao paciente adulto. Mais uma vez a variável D alavancou o alto valor da faixa normal, igual ao paciente adulto. Porém no que se refere a quantidade de falsos positivos, ou seja, autenticações falsas que foram aceitas, o paciente idoso se saiu melhor em comparação ao paciente adulto, como pode ser visto na Figura 4.12.

A taxa de falsos positivos obteve 13,33%, enquanto as tentativas que falharam na autenticação obtiveram 86,66%. Apesar de um acumulado total muito semelhante do paciente adulto, o índice de acertos no cálculo da FAR obteve pior resultado, mostrando que na autenticação do paciente idoso, as verificações são mais fáceis. Isso se deve a baixa variabilidade de algumas variáveis, e suas especifidades, como por exemplo PAD e PAS. Diferente da SAT, que possui baixa variabilidade mas com valores muito comuns entre indivíduos diferentes, mostrando-se ser um problema para o método de autenticação sobre os pacientes idosos proposto nesse trabalho.

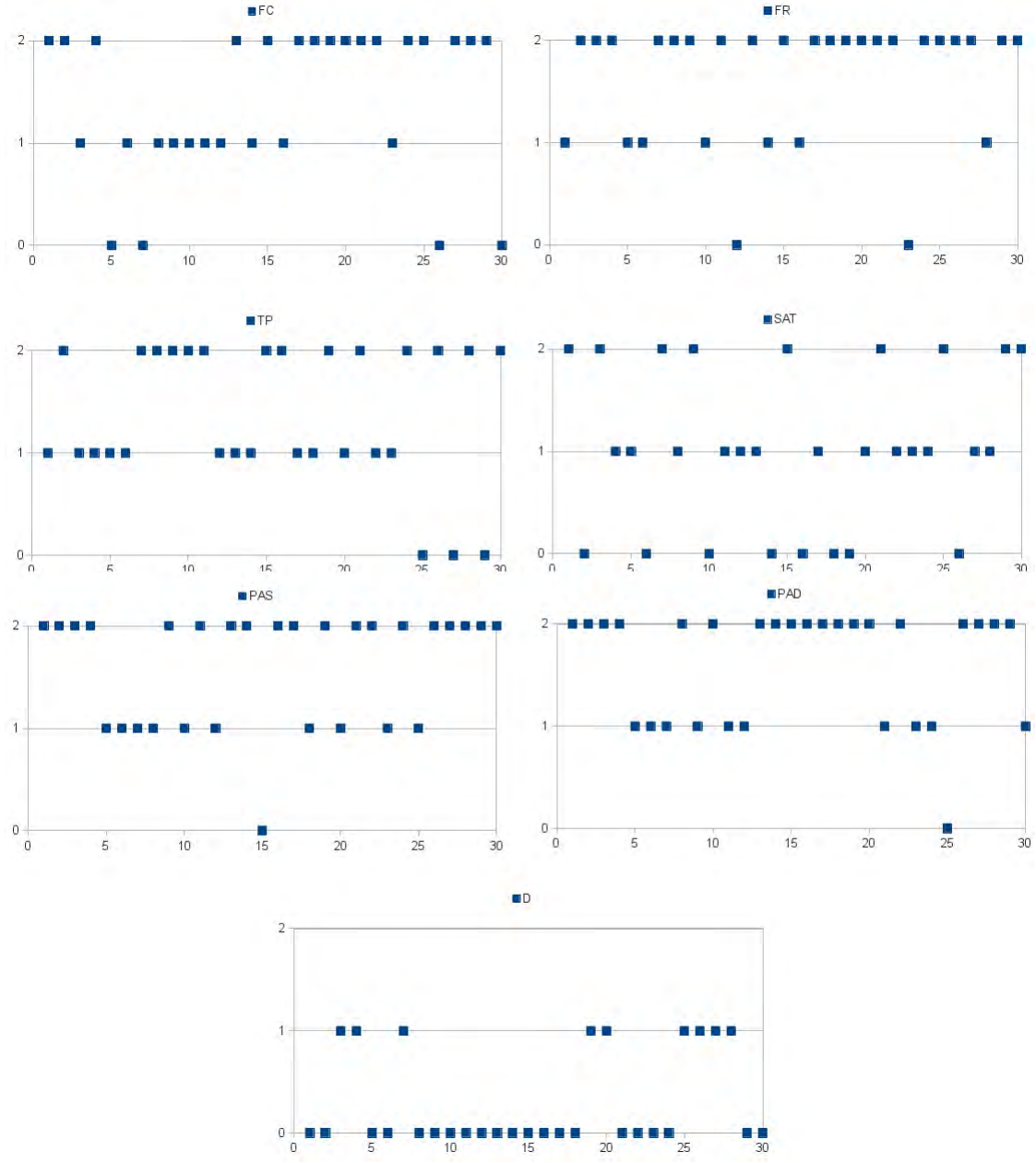


Figura 4.10: Amostras individuais sobre cada variável para o cálculo da FAR no paciente idoso.

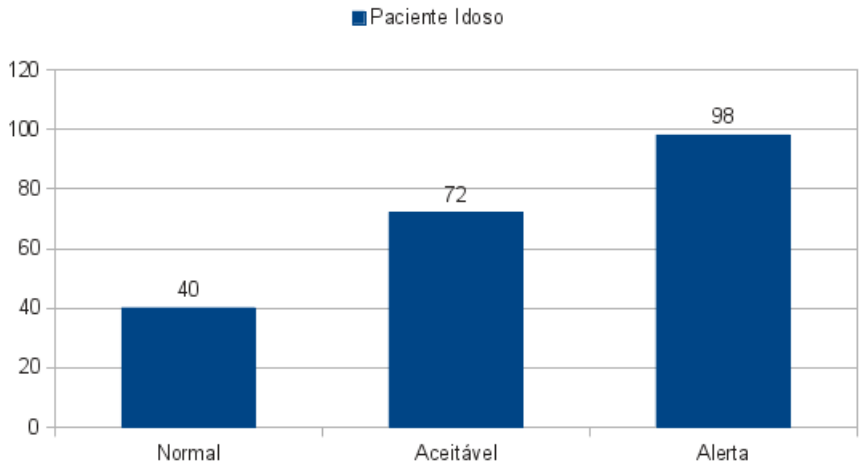


Figura 4.11: Total de dados coletados para o cálculo da FAR no paciente idoso.

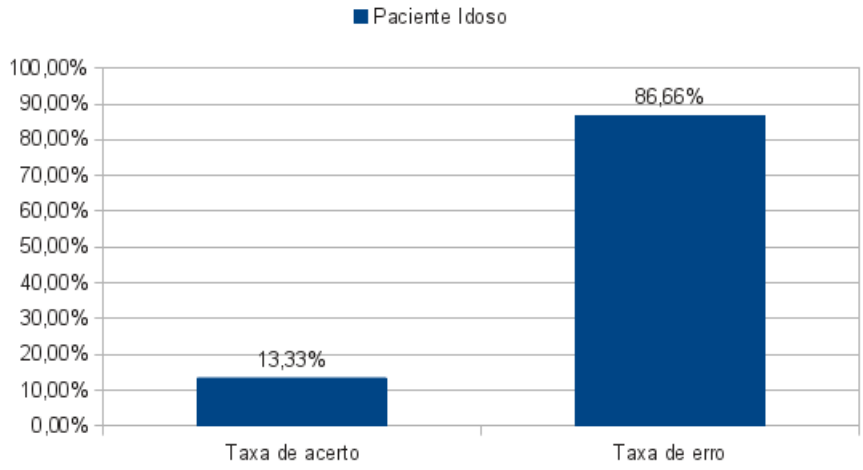


Figura 4.12: Eficiência do autenticador para o cálculo da FAR no paciente idoso.

## 4.4 Estudo de caso 3: Paciente idoso doente

No terceiro estudo de caso, são feitos testes sobre um paciente idoso doente a fim de retratar uma possível realidade em um sistema de monitoramento a domicílio (*i.e*, casos em que pacientes são monitorados devido a doenças). Assim este terceiro estudo de caso visa autenticar um paciente que sofreu um acidente vascular encefálico isquêmico, proveniente de sua hipertensão arterial (acidentes vasculares encefálicos são popularmente conhecidos como derrame cerebral). Um acidente vascular encefálico isquêmico é o tipo de acidente vascular mais comum, presente na grande maioria dos casos, em que se refere à falta de fluxo sanguíneo cerebral causado pela hipertensão, levando ao enfarte (POTTER, 2011). Assim o paciente monitorado possui as características fisiológicas do paciente idoso, mas alterados, de acordo com suas alternâncias devido à hipertensão. A escolha dessa doença, é pela facilidade de encontrar dados na literatura devido a sua grande frequência na população adulto e idosa brasileira (SAúDE, 2011). Um ambiente de monitoramento inteligente remoto, encaixa-se perfeitamente para esses pacientes, uma vez que eles necessitam de acompanhamento contínuo mas não são graves o suficiente para ocupar um leito de hospital. Dessa forma, seguindo a mesma linha dos experimentos anteriores, serão avaliadas 30 amostras coletadas aleatoriamente, geradas seguindo o padrão do paciente idoso e com as especifidades da doença, dando assim origem ao perfil do paciente idoso doente. A Figura 4.13 mostra as faixas de valores obtidas sobre cada variável.

No paciente idoso doente, uma quantidade maior de faixas alerta e aceitável foram obtidas. A explicação é devido à variância das escalas de cada variável fisiológica. Por exemplo, as variáveis PAS e PAD obtiveram uma variância grande em relação aos outros pacientes, devido a grande escala de valores possíveis, mas uma pequena faixa de valores aceitos. Essa pequena faixa de valores aceitos é ocasionada devido à hipertensão do paciente, que apesar de obter valores altos devido a doença, possui uma baixa variedade em sua faixa. As variáveis FC e FR continuaram com a mesma tendência, geram alerta em algumas situações devido à sua variância natural. Já a variável SAT possui índices muito semelhantes aos dos outros pacientes, e bastante comportados. Na Figura 4.14 pode-se observar o total acumulado em cada faixa para as medidas do paciente idoso doente.

O total de valores na faixa normal foi o menor dentre os três pacientes estudados nos estudos de caso, obtendo 18% menor que o paciente adulto e 8,5% menor do que o paciente idoso. A faixa aceitável obteve um aumento no número de valores de 15% em relação ao paciente adulto e 7% em relação ao paciente idoso. Com esses valores já é possível interpretar numa eficiência menor do autenticador quando se tratando de um paciente idoso doente. A faixa de alerta subiu 2,8% em relação ao paciente adulto e 1,4% el relação ao paciente idoso. A eficiência do autenticador pode ser vista na Figura 4.15.

A autenticação do paciente idoso doente foi a pior entre os três casos estudados, obtendo uma taxa de aceitação de 86,66% e uma taxa de rejeição de 13,33%. Nos experimentos realizados, as amostras 9, 11, 22 e 27 falharam, tendo como fator determinante as variáveis PAS e PAD. Isso mostra a necessidade de um treino mais especializado sobre variáveis fisiológicas afetadas por algum fator importante, nesse caso a hipertensão.

### 4.4.1 Taxa de falsa aceitação do paciente idoso doente

Faremos agora os experimentos a fim de obter as taxas de falsa aceitação do paciente idoso doente seguindo a mesma fórmula dos estudos de caso anteriores. Assim, coletando 30 amostras de outros pacientes, a Figura 4.16 mostra as amostras individuais obtidas para

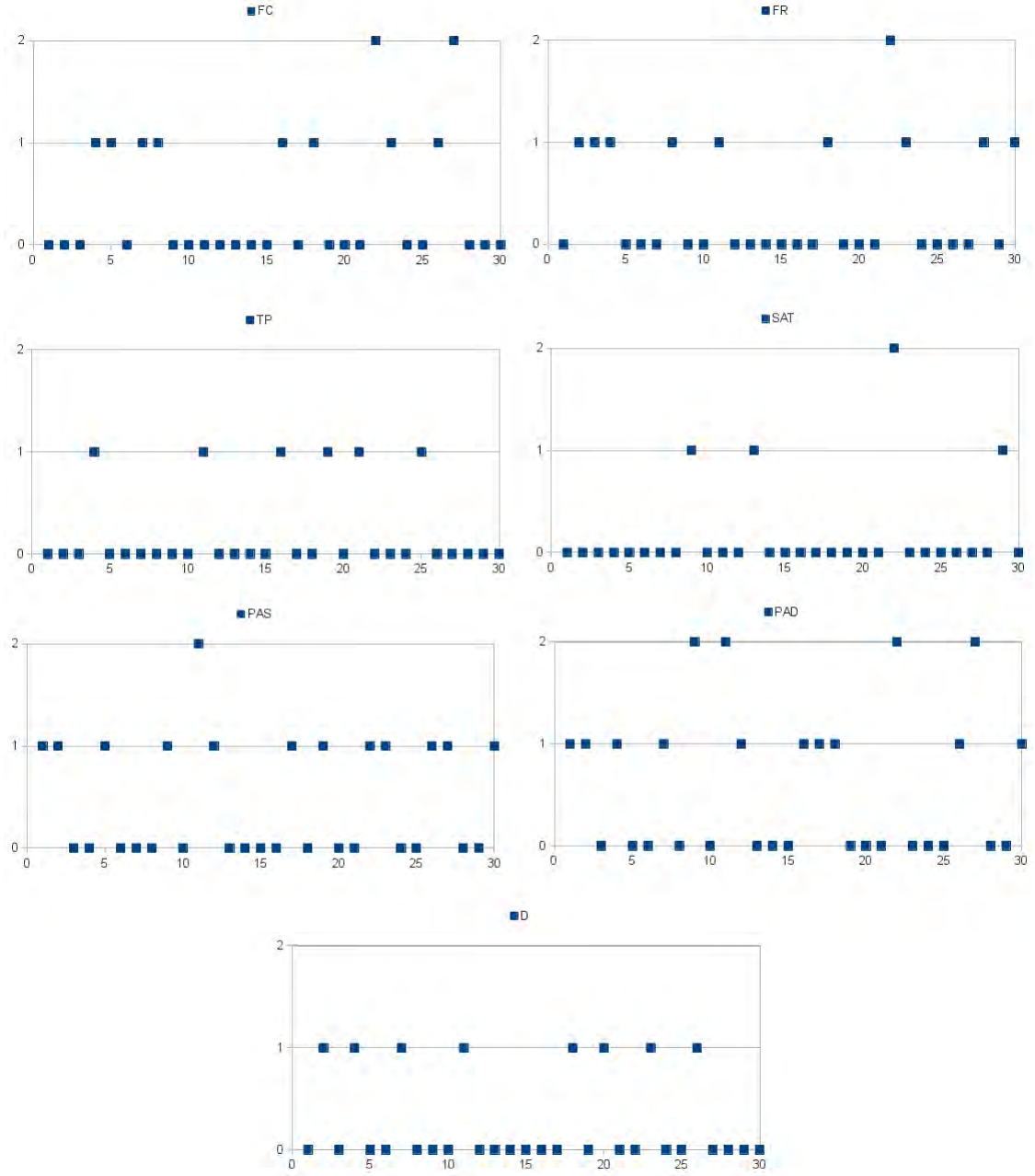


Figura 4.13: Amostras individuais sobre cada variável calculada do paciente idoso doente.

o cálculo da FAR.

Como esperado, a grande maioria das informações geraram alerta, em especial pelas variáveis PAD e PAS, em que para o paciente idoso doente são as mais sensíveis. Na faixa aceitável novamente a variável SAT obteve um alto índice de falsas aceitações. Para o paciente idoso doente a variável TP também se comportou de maneira similar a SAT, aceitando muitas autenticações não legítimas. A Figura 4.17 mostra o total acumulado em cada uma das faixas para o cálculo da FAR.

O total de valores na faixa normal foi maior no paciente idoso doente do que nos outros dois pacientes estudados, propiciado pela baixa eficiência das variáveis SAT e TP. Assim como nos outros estudos de caso a variável D, continua sendo o fator principal para o acumulado total na faixa normal. Apesar disso as outras faixas se mantiveram com

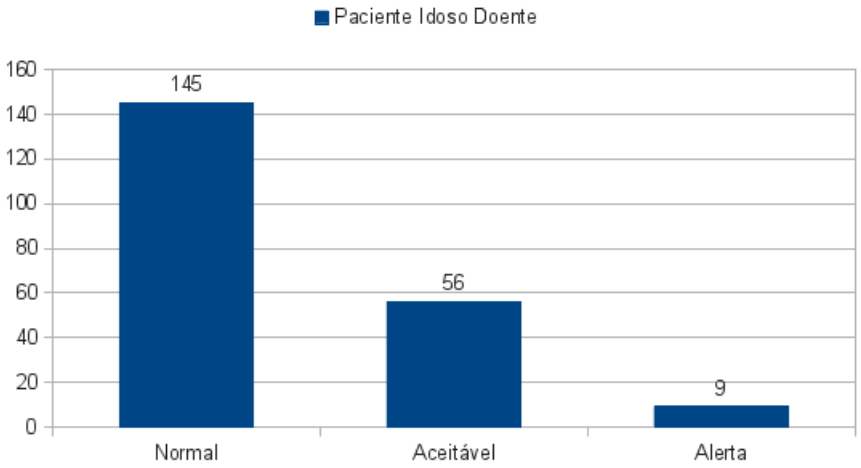


Figura 4.14: Total de dados coletados do paciente idoso doente.

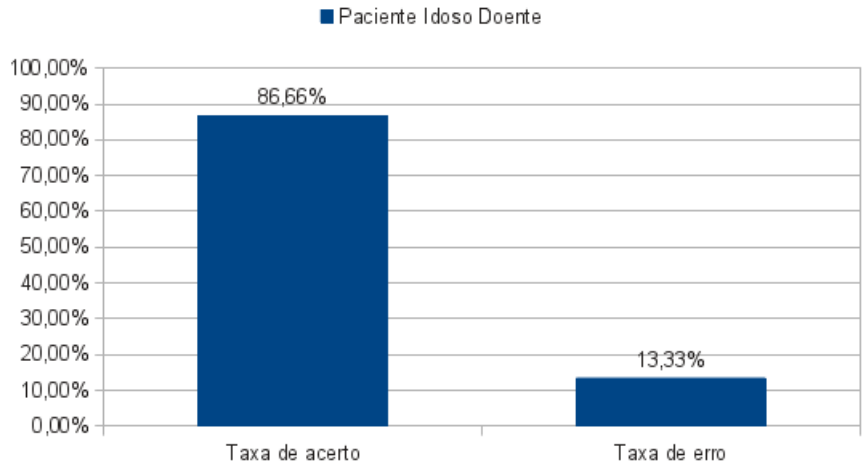


Figura 4.15: Eficiência do autenticador sobre as medidas do paciente idoso doente.

valores similares. Apesar dos valores totais inferiores aos demais pacientes, quanto ao total de falsos positivos, o paciente idoso doente obteve o melhor índice, conforme pode ser visto na Figura 4.18.

Apenas uma das amostras foi aceita nesse experimento, obtendo-se assim o melhor índice de FAR entre os pacientes, com 96,66% de tentativas que não foram autenticadas e 3,33% que foram autenticadas incorretamente. A explicação para esse número está nas variáveis PAD e PAS, que possuem uma unicidade muito elevada para pacientes hipertensos. Isso mostra que pacientes doentes, apesar de serem mais difíceis de serem autenticados, são menos suscetíveis a erros causados por falsas aceitações, graças à combinação das individualidades de suas variáveis fisiológicas e alternâncias sofrido por doenças.

O próximo capítulo se propõe a discutir todos os aspectos técnicos do trabalho, incluindo a segurança, a padronização necessária e a eficiência da solução proposta.

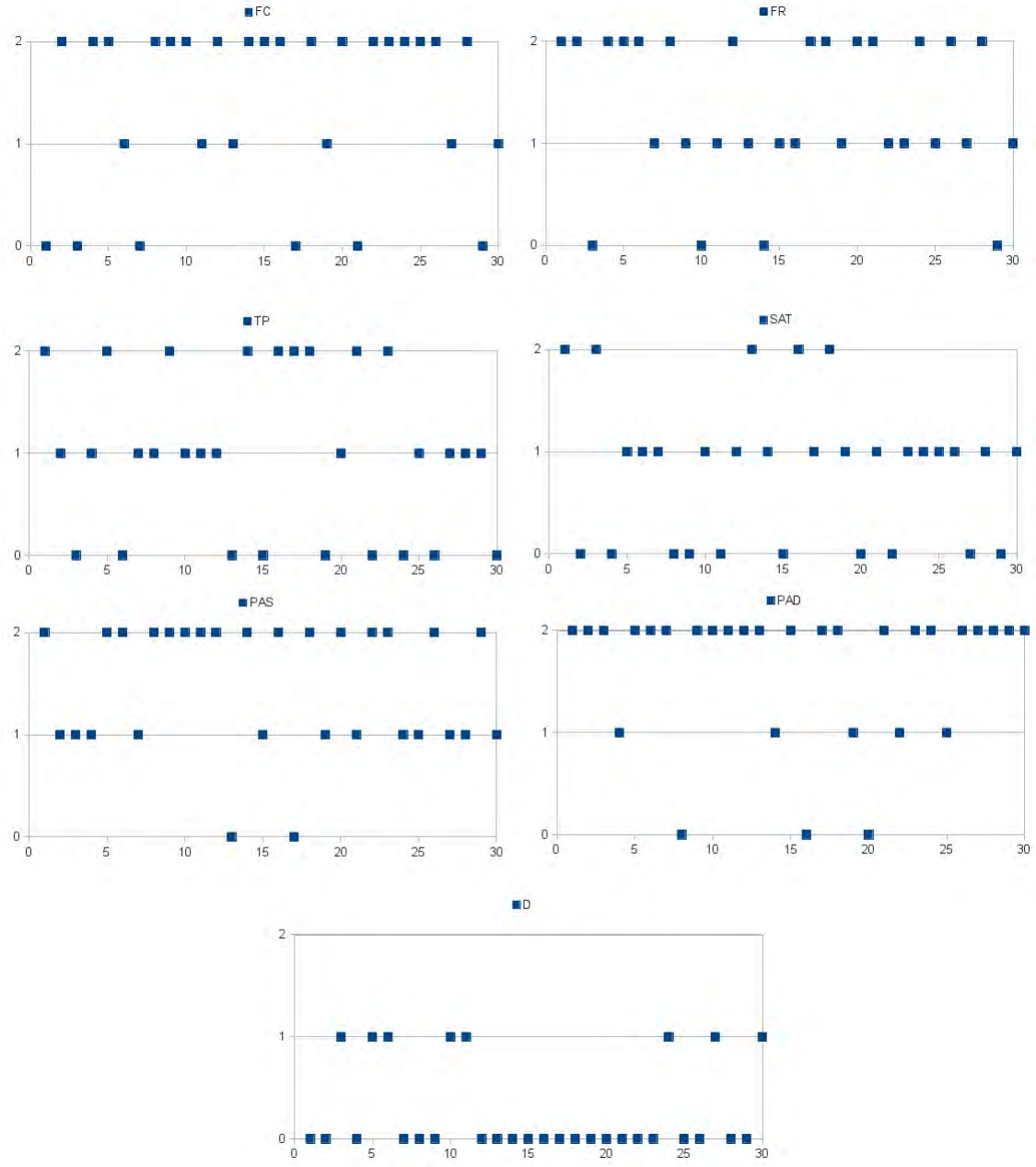


Figura 4.16: Amostras individuais sobre cada variável para o cálculo da FAR no paciente idoso doente.

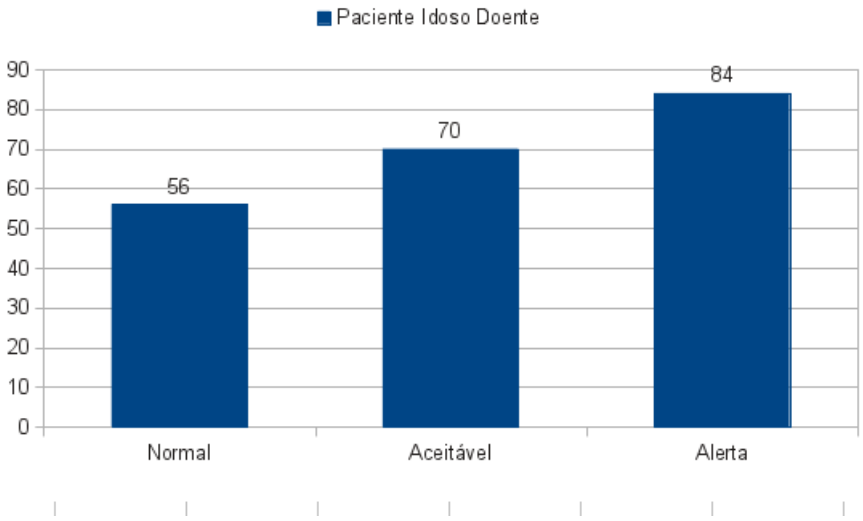


Figura 4.17: Total de dados coletados para o cálculo da FAR no paciente idoso doente.

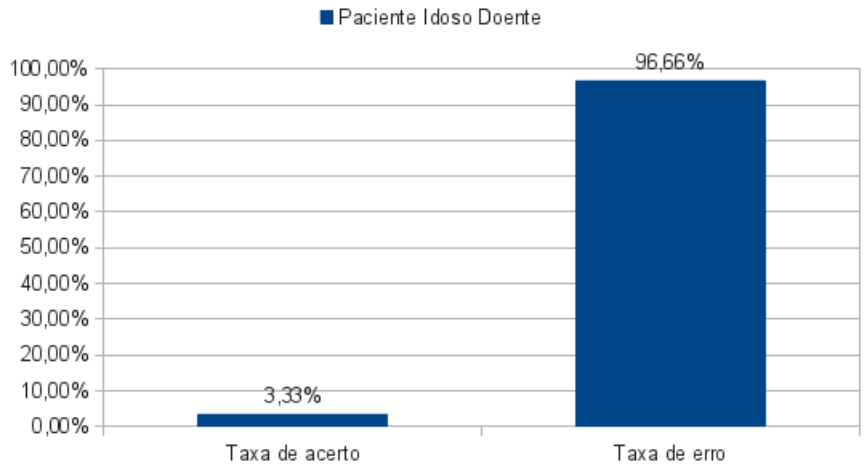


Figura 4.18: Eficiência do autenticador para o cálculo da FAR no paciente idoso doente.

# 5 DISCUSSÃO

Até o momento, foi proposta uma nova solução de autenticação envolvendo um ambiente de saúde dotado de sensores que retira-se o paciente do processo de autenticação direta, muitas vezes impossível para alguns pacientes. Com essa solução, foram feitos experimentos a fim de testar o autenticador, verificando suas características e eficiência. Esses experimentos consistiram de testes sobre diferentes estudos de casos, onde cada estudo de cada retratava uma situação diferente. Nesse capítulo, discutiremos os aspectos de segurança que permeiam a solução proposta, discutiremos sobre seus aspectos que tangem a padronização existente, e por fim a viabilidade de implantação dessa solução em ambientes reais.

## 5.1 Segurança

Na solução proposta, existem três cenários em que podem sofrer com tentativas de ataque: i) o ambiente interno, que se refere a toda comunicação realizada entre os sensores e o *gateway*; ii) a comunicação externa, que se refere a comunicação entre o *gateway* e o servidor do hospital; e iii) o servidor, que se refere aos computadores sobre o domínio do hospital. Qualquer tipo de ataque deverá ser feito contra um desses três cenários.

O primeiro cenário correspondente ao ambiente interno, é o cenário mais crítico em relação à segurança sobre a solução proposta. Devido a características como recursos computacionais escaços, comunicação sem fio e criticidade nas informações que trafegam na rede, a rede de sensores na casa do paciente é um ponto crítico na solução. Diversas ameaças podem afetar a rede, todas referentes as redes de sensores sem fio (PADMAVATHI; SHANMUGAPRIYA, 2009b). Muitas das ameças existentes nas redes de sensores sem fio necessitam de recursos adicionais sofisticados para serem sanados, como por exemplo ataques de negação de serviço (Denial of Service - DoS) ou ataque de Sybil (*i.e*, um nó malicioso ilegitimamente assume múltiplas identidades). Mas existem outros ataques mais comuns que são mitigados pela solução proposta, como o ataque de adivinhação (Guessing Attack), o ataque da representação (Impersonation Attack) e o ataque de repetição (Replay Attack).

No ataque de repetição, um intruso tenta repetir a comunicação recém efetuada e com isso se autenticar no lugar do paciente (UDGATA; MUBEEN; SABAT, 2011). Ataques de repetição podem ser mitigados usando a verificação através do parâmetro de tempo. Quando uma requisição é executada, a primeira verificação será $\Delta T \geq T' - T''$. Se o parâmetro de tempo não se encontra em $\Delta T$, a requisição é terminada e a mensagem irá falhar, pois pode ter acontecido ou uma falha no dispositivo ou uma tentativa de ataque.

Outro ataque que não é possível na solução proposta é o ataque de adivinhação, como foi supracitado. No ataque de adivinhação, segredos mal escolhidos podem ser adivinha-

dos por um atacante e assim comprometer todo o sistema. Isso não é possível na solução proposta pois os pacientes não interagem com o sistema para escolher uma senha, e as chaves existentes são geradas pelo *gateway*. A opção de não deixar o paciente interagir com o sistema aumenta a segurança de todo o processo e retira os erros pertencentes ao fator humano (GEHRINGER, 2002).

Ainda, dentre os ataques, um ataque de representação também não obtêm êxito pois mesmo interceptando um login legítimo, o $C_G$ e $V_S$ das mensagens é encriptado com chaves previamente distribuídas, impedindo os atacantes de obterem as chaves das seções e se registrarem como pacientes legítimos. Outros ataques como o de força bruta também não são factíveis, pois não passam no teste do parâmetro de tempo além de ser fácil de detectar.

Entretanto, ataques como o de DoS e o Sybil, supracitados, continuam sendo um grande desafio nas redes de sensores. O objetivo de um ataque de DoS é esgotar os recursos computacionais de um sensor alvo, a fim de torná-lo indisponível. A defesa contra esse tipo de ataque é muito custosa, necessitando de mecanismos adicionais específicos para mitigá-lo, como demonstrado no trabalho de Gill e Yang (GILL; YANG, 2009). Além disso, os sensores do ambiente podem ser capturados e suas informações internas modificadas, fazendo com que quando volte a acessar a rede, comprometa o sistema inteiro transmitindo mensagens falsas. Isso é conhecido como ataque de comprometimento do nó, difícil de ser prevenido, mas estudos para solucionar esse problema estão sendo conduzidos (LIN, 2009) (CHEN et al., 2007). Já o ataque Sybil necessita de mecanismos de detecção eficientes para encontrar o nó malicioso, como o proposto por Shaohe et. al (LV et al., 2008). Ataques como os anteriores são muito caros para serem incorporados na solução, necessitando assim de um correto projeto das políticas de segurança a fim de mapear os principais desafios do ambiente e suas necessidades.

O segundo cenário, referente à comunicação entre o *gateway* e o servidor, utiliza as linhas de comunicação públicas existentes. Esse cenário, apesar de hostil, não é um problema tratado nesse trabalho, uma vez que a comunicação é confiável, utilizando-se de SSL (*i.e*, comunicação segura e privada utilizando de criptografia assimétrica) (FREIER; KARLTON; KOCHER, 2011). A comunicação utilizando criptografia assimétrica é possível pois não existe nenhum problema com restrições computacionais, já que o *gateway* do usuário é um computador doméstico.

O terceiro cenário pertencente ao lado do servidor também está fora de escopo para estudo de segurança nesse trabalho. Uma vez que as informações são gravadas no banco de dados, é considerado que toda informação proveniente desse banco, sejam os valores das variáveis ou as regras, estão íntegros e não sofreram nenhum tipo de ataque.

Além dos possíveis tipos de ataques que o ambiente pode sofrer, outro importante aspecto de segurança a ser analisado pela política de segurança é o gerenciamento de chaves. O gerenciamento de chaves é fundamental para o desenvolvimento de uma aplicação segura, utilizado para distribuir as chaves criptográficas aos nós de uma rede. A solução proposta utiliza a abordagem da pré distribuição de chaves, onde as chaves secretas são armazenadas após o desenvolvimento da rede, oferecendo assim uma menor complexidade computacional, adequado para redes de sensores que possuem recursos escassos (KUMAR; LEE, 2011). Esse tipo de distribuição de chaves só é possível em pequenos ambientes, onde não exista uma grande quantidade de dispositivos. Ambientes com uma grande quantidade de dispositivos necessitariam de abordagens mais complexas como servidores exclusivos para a distribuição das chaves. O problema sobre o gerenciamento de chaves para a solução proposta é o roubo de seção, pois seções são criadas para as

comunicações. Porém, a cada rodada chaves aleatórias são criadas e as chaves antigas destruídas, requisito para evitar o roubo de seção.

A ISO/IEC 27799 (ISO, 2008) contêm uma lista com 25 tipos de ameaças críticas para a segurança da informação de dados da saúde. Dessas ameaças, as relacionadas ao processo de autenticação são a interceptação das informações, o erro ocasionado pelos usuários e a dissimulação dos usuários internos e externos. Essas são algumas das ameaças que fazem com que a ISO/IEC 27799 solicite uma autenticação forte para esses ambientes de saúde. Portanto, a solução de autenticação proposta, tenta mitigar as ameaças mais pertinentes nas redes de sensores, porém, abstêm-se dos problemas e ameaças mais complexos, estes sendo grandes desafios atuais das redes de sensores.

## 5.2 Vigência com as Padronizações

Como foi dito na seção 2, qualquer sistema eletrônico desenvolvido para a área da saúde deve ser certificado para poder ser utilizado. A SBIS, introduz as especificações para que esses sistemas possam ser aplicados em domínios específicos. Essas especificações envolvem todo o processo de desenvolvimento, englobando diversas padronizações ISO/IEC existentes para fundamentar os requerimentos, tal como a ISO/IEC 27799. Nessas especificações, existem as exigências da área da autenticação, que compõem as especificações NGS1.02 . A solução desenvolvida se preocupou em seguir todas exigências da SBIS, a fim de propiciar uma integração segura ao sistema e pronta para utilização. Assim, seguindo a SBIS, temos as seguintes especificações:

- NGS1.02.01 - Identificação e autenticação do usuário. Antes de qualquer acesso, é necessário que o paciente seja identificado e autenticado, especificação básica para garantir a confiança nas informações. A identificação e autenticação é realizada utilizando a autenticação forte.

- NGS1.02.02 - Método de Autenticação. O método de autenticação utilizado segue os requisitos impostos na ISO/IEC 27799, que solicita uma autenticação que utilize pelo menos dois fatores, sendo esses fatores pertencentes de diferentes tipos (*i.e*, não é possível, por exemplo, utilizar dois fatores biométricos pois são pertencentes ao mesmo tipo). Foram escolhidos então os fatores biometria e localização, com a finalidade de facilitar o processo de autenticação para pacientes que possuam necessidades especiais.

- NGS1.02.03 - Proteção dos parâmetros de autenticação. A proteção pede que algum tipo de criptografia seja utilizado, para que as informações não possam ser legíveis a um atacante ou curioso. Como já discutido, a solução utiliza de criptografia simétrica, devido às necessidades das redes de sensores.

- NGS1.02.04 - Segurança da senha. Essa especificação impõe diversas restrições através de políticas de segurança aos usuários para que escolham senhas consideradas seguras nesses ambientes de saúde. Esse é um grande ganho da solução proposta nesse trabalho, uma vez que devido à escolha de outros fatores de autenticação, a senha não é mais um requisito, não sendo mais um ponto de falha (GEHRINGER, 2002).

- NGS1.02.05 - Controle das tentativas de login. Como última especificação da parte de autenticação, a SBIS solicita um controle sobre tentativas de login no sistema.

Isso seria facilmente obtido no contexto deste trabalho, configurando a periodicidade em que as informações são enviadas do *gateway* para o servidor, sabendo assim cada momento em que uma tentativa de acesso será efetuada. Tal controle não foi realizado durante os testes, mostrados na seção anterior, pois não possuía relevância no que tange à obtenção da eficiência do autenticador.

A solução proposta se preocupou com as especificações existentes no domínio de aplicação do cenário nacional para garantir seu funcionamento. A SBIS propõem ainda várias outras especificações sobre outros componentes de um sistema eletrônico de saúde, porém a preocupação deste trabalho foi seguir o componente de autenticação, que segue as ISO/IEC 27002 e ISO/IEC 27799.

## 5.3 Viabilidade

A autenticação proposta nesse trabalho, baseia-se nos fatores de biometria e localização para seu funcionamento. Além disso, o ambiente que a solução será empregada é considerado crítico e possui limitações computacionais devido à utilização de sensores. Tais informações, remetem a uma pergunta fundamental que tange esse trabalho: qual é a viabilidade da solução proposta no ambiente de saúde demonstrado? É visando responder essa pergunta mais as perguntas de pesquisa propostas na introdução que essa subseção pretender responder e discutir.

A primeira indagação a se fazer é sobre o dinamismo das informações utilizadas no processo de autenticação. Um processo de autenticação tradicional, por exemplo utilizando senha, necessita de constantes alterações como medida de segurança preventiva. Da mesma forma, um cartão necessitaria ser trocado com uma certa periodicidade. Essas alterações fazem parte do requisito de dinamismo, que possuem a finalidade de prevenir que ataques sejam bem sucedidos. Na autenticação proposta, esse dinamismo existe naturalmente nas informações coletadas, sejam elas fisiológicas ou de localidade. Essa variação dificulta ataques de adivinhação ou mesmo intercepção, pois constantemente assumem valores distintos. Esse dinamismo das informações é um desafio para o módulo autenticador, necessitando assim de abordagens extras para seu funcionamento eficiente. Na solução proposta, as regras assumiram o papel de abordagem responsável por interpretar situações comuns dentro das alterações ocorridas com as informações. No trabalho de Copetti (COPETTI, 2010), foi desenvolvido um módulo central para o gerenciamento que utilizava-se de técnicas de lógica difusa sobre as informações, a fim de identificar situações críticas. O trabalho mostrou que a utilização de técnicas de inteligência artificial, aplicadas no contexto de ambientes de saúde, podem ajudar no processo de autenticação.

Outro aspecto importe a discutir é sobre as variáveis fisiológicas. Como descrito no trabalho, os casos de uso utilizaram-se de informações contidas na literatura para montar indivíduos genericamente chamados de adulto, idoso e idoso doente. As informações fisiológicas utilizadas basearam-se nas informações básicas existentes no prontuário de um paciente (*i.e*, frequência cardíaca, frequência respiratória, temperatura, saturação e pressão arterial diastólica e sistólica), devido à facilidade de encontrar esses valores na literatura existente. Mas como se observou através dos testes realizados na seção 4, algumas variáveis não obtiveram boa variação para o processo de autenticação, como é o caso da saturação (SAT). Além disso, outras variáveis, dependendo do contexto, poderiam ter uma variação muito grande, necessitando de flexibilidade por parte do autenticador. Fatores como esses, mostram que é necessário uma análise individual sobre cada variável a fim de descobrir seu grau de significância no processo de autenticação. O trabalho de

Tamura *et al.* (TAMURA et al., 2011), é um bom exemplo de análise individual sobre uma variável, onde nele a pressão arterial é monitorada e avaliada, com a finalidade de demonstrar seu funcionamento no corpo humano. A solução proposta objetivou testar com todas as variáveis em conjunto, mostrando as implicações do mesmo. Com isso obteve valores inferiores aos desejados para um processo de autenticação, 93,33% para o paciente adulto e o paciente idoso, e 86,66% para o paciente idoso doente. Esses valores apesar de altos, são considerados insuficientes para sistemas de autenticação, apesar de que sistemas baseados na biometria aceitam um erro de até 4% em sistemas bem consolidados (WORLD, 2013), (JAIN, 2008). Isso mostra que melhorias devem ser feitas através de novas abordagens de biometria ou a utilização de técnicas de inteligência artificial.

Nesse contexto de novas abordagens sobre a biometria, existem trabalhos sendo desenvolvidos como os de Bao (BAO; ZHANG; SHEN, 2005) e Poon (POON; ZHANG; BAO, 2006). Nestes trabalhos a autenticação biométrica é automática través das medições feitas das variações do batimento cardíaco, obtendo uma eficiência de 95%, operando em uma WBAN. Trabalhos como esses mostram a importância de uma autenticação sem a interação do paciente, de maneira eficiente, viabilizando diversas novas aplicações, assim como a melhoria da solução proposta nesse trabalho, por exemplo.

O fator distância, pertencente ao fator extra da solução proposta nesse trabalho, mostrou ser bastante comportado. Como explicado, tal comportamento é justificado pela ausência da simulação de problemas como ruído ou reflexão em que poderiam dificultar o cálculo da distância. Mesmo assim, a localização se mostra como um fator extra de verificação para a autenticação. No contexto da aplicação deste trabalho, a localização indicaria a distância de cada sensor presente junto ao paciente, possuindo variações de acordo com seu comportamento. No processo final de autenticação, a distância apresentaria resultados valiosos para a validação ou não da autenticação, pois certificaria cada ambiente pela sua característica geométrica única. Nesse campo de localização interna, chamada de localização *in-door*, existem muitas tecnologias e aplicações diferentes possíveis, dependendo do domínio de aplicação.

Como foi dito na proposta, existem 3 formas de se abordar as informações obtidas pelos sensores: variáveis fisiológicas, variáveis comportamentais e variáveis ambientais. Porém, como especificado, as variáveis ambientais não foram abordadas na solução proposta. Seria perfeitamente possível englobar essas variáveis na solução proposta, o que provavelmente fortaleceria o autenticador, colocando outra gama de variáveis a serem analisadas e regras a serem criadas. As variáveis ambientais possuem influência sobre os indivíduos, podendo afetar suas variáveis fisiológicas (*e.g,* a temperatura do ambiente poderia influenciar na temperatura corporal e na frequência cardíaca de um indivíduo). Tal fato resultaria em uma complexidade extra ao autenticador, passível de investigação futura, a fim de analisar se tal complexidade extra trouxe índices de segurança relevantes ao sistema.

Em um sistema como o presente, existem diversas situações que podem ocorrer e propiciar falha na autenticação. Por exemplo, caso o paciente tenha sofrido alguma forte emoção de maneira inesperada, o sistemas não conseguiria descobrir que as variações momentâneas são legítimas. Problemas como esse não são tão graves para a solução proposta pois a autenticação é realizado sobre o cálculo da média das variáveis que são constantemente medidas. Isso significa que mesmo a frequência cardíaca sofrendo um aumento não explicado, a média calculada dos batimentos cardíacos em um tempo predeterminado, iria suavizar o resultado final e não implicar na reprovação da amostra. Problema seria se a emoção permanecesse durante um grande período de tempo, fazendo com que o calculo

da média aumentasse sem motivo aparente. Tal situação foi explicada a fim de mostrar a complexidade de um ambiente como o monitoramento de um paciente à distância. A autenticação desenvolvida baseou-se em apenas três situações simples encontradas na literatura médica: repouso, comendo e atividade leve. Um ambiente inteligente necessitaria de realizar o mapeamento de muitas outras situações e comportamentos, necessitando de uma abrangência maior do sistema de autenticação.

Dessa forma, a solução de autenticação proposta, possui a finalidade de incluir pessoas com deficiências mentais ou motoras no processo de autenticação. Também, se propõe a transgredir os processos de autenticação tradicionais, que vem sofrendo fortes críticas, e devem futuramente entrar em desuso. A autenticação sem interação da pessoa faz parte de um sistema inteligente, que proativamente é capaz de inferir preferências do usuários e ajudá-los nas tarefas rotineiras, tal como um processo de autenticação.

Os resultados demonstraram que pessoas com idades diferentes, apesar de perfis fisiológicos específicos, possuem a eficiência muito semelhante na autenticação. Com os resultados obtivemos os mesmos índices para o cálculo da FRR nos paciente adulto e idoso. A diferença ficou no cálculo da FAR, melhor no paciente idoso, porém com resultados semelhantes ao paciente adulto. Assim, evidenciou-se que o grande desafio está nos pacientes que possuem alguma especifidade devido a doenças, como foi o exemplo do paciente idoso doente, referente a hipertensão, que teve resultado inferior ao desejado.

Um grande mérito da solução apresentada é retirar a interação direta do paciente com o sistema no processo da autenticação. Como já foi demonstrado, as soluções propostas na área das redes de sensores impõem condições aos seus usuários, necessitando assim de gozar de boa saúde para tal. Um ambiente inteligente, que trata de pacientes, não pode limitar suas aplicações. Dessa forma, a solução proposta retira esse paciente da interação com o autenticador, dando um passo adiante nas pesquisas sobre autenticação em ambientes inteligentes, redes de sensores e ambientes de saúde.

Por fim, é possível responder a pergunta referente ao principal problema de pesquisa abordado: sobre a viabilidade da solução proposta em um ambiente real. A resposta não possui um valor único. A solução proposta é viável referente ao domínio de aplicação e aos objetivos requeridos, necessitando de melhorias para atingir o grau de eficiência desejável para os sistemas de autenticação. Porém a solução não é viável no ponto que se refere a utilização imediata, devido aos resultados obtidos estarem abaixo do desejado. De maneira geral, esse trabalho da um passo na evolução dos sistemas de autenticação modernos, que se propõem a buscar soluções inteligentes e seguras. Porém melhorias devem ser feitas no autenticador a fim de obter melhores índices de eficiência, principalmente quando abordados problemas específicos, como é o caso do paciente idoso doente.

# 6 CONCLUSÃO

Nesta dissertação foi apresentada uma proposta de autenticação forte para ambientes de saúde baseados em sensores. Nesse contexto, foi proposta uma solução de autenticação no qual o usuário não necessitasse de interagir com o autenticador, pra isso utilizando os fatores biometria e localização. A biometria consistiu da medição das condições fisiológicas do paciente, tais como frequência cardíaca, frequência respiratória, saturação de oxigênio, temperatura e pressão arterial diastólica e sistólica. A localização consistia no cálculo da distância dos sensores pertencentes a WBAN do paciente, em relação ao *gateway*. Para que tais fatores possam ser medidos, é necessário que o paciente esteja em um ambiente inteligente, dotado de sensores para o seu monitoramento, consistindo de um monitoramento remoto.

Para que a solução fosse possível, foram descritas três etapas principais e suas ações. Essas etapas fornecem a base para apoiar o processo de autenticação, possibilitando a segurança nas operações e as informações iniciais necessárias para o processo de autenticação posterior. A primeira etapa pertence ao registro do paciente no sistema, onde são feitas as primeiras medições para extrair o padrão do paciente, utilizado para o processo de autenticação biométrica. Ainda, as chaves devem ser geradas e distribuídas nos sensores, para que as futuras comunicações possam ser feitas com segurança. A segunda etapa consistiu em uma modelagem teórica sobre a comunicação dos sensores no ambiente interno para propiciar segurança entre as comunicações. Essa etapa mostrou como seria a troca de mensagens utilizando as chaves geradas na etapa anterior. A terceira e última etapa, pertencia a autenticação do paciente, propriamente dita. Nela os dados coletados do ambiente eram enviados a um servidor responsável pela autenticação do paciente para salvar os dados na base de dados responsável.

Toda requisição oriunda de um paciente ao servidor, invocava o método autenticador que agia sobre os vetores identidade e localização. Esse método autenticador, utilizando-se das regras criadas para cada paciente, calculava se as informações fisiológicas e de distância estavam de acordo com valores preestabelecidos. Esses valores possuem três níveis possíveis: normal, para quando as informações do paciente estavam dentro das faixas esperadas; aceitável, para quando os valores por algum motivo acabavam saindo um pouco da faixa esperada; e alerta, para quando anomalias eram encontradas nos valores obtidos. Assim toda requisição ao servidor passava pelo método autenticador para avaliar a vericidade das informações.

Foram feitos alguns testes sobre o autenticador desenvolvido, a fim de medir a sua eficiência. Os testes consistiram em trinta medições sobre três estudos de caso diferentes, onde cada estudo de caso retratou um perfil fisiológico distinto, tais como paciente adulto, paciente idoso e paciente idoso doente. Cada amostra coletada de cada perfil fisiológico foi obtida através de um simulador que gerava os valores aleatórios mas respeitando as

faixas de cada perfil de paciente, que foi baseado na literatura existente. Foram feitos testes para mostrar a eficiência do autenticador através do índice de falsas rejeições. Também foram feitos testes para calcular a probabilidade de um impostor se autenticar no sistema como se fosse um usuário legítimo, através do índice de falsa aceitação.

Com os resultados, foi possível observar um comportamento diferente das variáveis sobre cada perfil fisiológico escolhido. Através dos resultados, obteve-se uma eficiência de 93,33% das amostras autenticadas com êxito para o paciente adulto e idoso, e 86,66% de êxito para o paciente idoso doente. Além disso, através dos totais de dados coletados sobre cada variável, obteve-se para cada faixa: I)A faixa normal obteve maior ocorrência no paciente adulto, superando em 9,5% o paciente idoso e 18% o paciente idoso doente. Tal ocorrência explicada pela grande flexibilidade dos valores possíveis dentro da faixa normal, ocasionando também flexibilidade para o cálculo das regras. II) A faixa aceitável obteve maior ocorrência no paciente idoso doente, superando em 15% o paciente adulto e 7% o paciente idoso. Essa ocorrência segue a tendência dos alertas, que no paciente idoso doente foi maior, devido suas restrições nos valores. III) A faixa alerta obteve maior ocorrência no paciente idoso doente, novamente, superando em 2,8% o paciente adulto e 1,5% o paciente idoso. Apesar da baixa diferença entre o acumulado da faixa alerta entre o paciente idoso doente para os pacientes adulto e idoso, a porcentagem da eficiência, referente ao índice de acertos, foi de 7% menor aos outros dois paciente. Tal fato foi resultado de um maior índice de amostras diferentes que geraram alarme.

Pode-se obter também, através dos resultados dos testes, os índices de falsa aceitação. Dessa forma, obteve-se uma taxa de 20% de acerto do paciente adulto, 13,33% do paciente idoso e 3,33% do paciente idoso doente. As taxas de acerto consideram a porcentagem de tentativas que foram autenticadas, mesmo sendo provenientes de outros indivíduos. Os pacientes adulto e idoso, mesmo obtendo a maior eficiência de autenticação, obtiveram os piores resultados no cálculo da FAR, devido a suas flexibilidades nos valores. O paciente idoso doente, por outro lado, obteve o melhor resultado na FAR, explicado pela sua restrição e unicidade de valores fisiológicos.

O fator localização utilizado na solução proposta, estabeleceu-se como fator extra com a proposta de confirmar a veracidade das informações, idealmente para constituir a autenticação forte. A localização, não influencia nos resultados da autenticação, mas pode se tornar um fator crítico dependendo do tipo de canário existente no domicílio do paciente. Um paciente que possa se locomover em um ambiente muito espaçoso, om diferentes níveis, necessitará de maior infraestrutura de hardware para comportá-lo sem perdas no sinal. Além disso, a localização minimiza o problema de uma tentativa de invasão por uma fonte externa da residência, pois o RSSI de um atacante seria muito diferente de uma fonte interna, dificultando esse tipo de invasão.

Assim, através dos resultados obtidos, pode-se concluir que a solução proposta necessita de melhorias em alguns aspectos, como uma análise sobre cada variável a fim de provar sua eficiência em algum paciente específico. Soluções de autenticação que utilizam da biometria sofrem com taxas de erro que variam entre 4%, mas a autenticação proposta ficou um pouco mais abaixo do que o normal obtido, sendo menos eficiente ainda para casos mais complexos (*i.e*, paciente idoso doente). Mas a solução proposta mostrou-se factível e viável, podendo ser melhorada através de otimizações na técnica atual ou utilização de outros mecanismos biométricos bem consolidados, desde que mantenham o mesmo foco (*i.e*, soluções em que o paciente não interaja com o sistema)

Como trabalhos futuros, pretende-se inicialmente trabalhar sobre cada variável fisiológica utilizada na proposta a fim de descobrir sua unicidade, além de suas implicações

sobre perfis fisiológicos diferentes. Também, seria de grande valia a utilização de técnicas de inteligência artificial para melhorar o processo de análise na autenticação, como por exemplo a utilização da lógica difusa para decisão das faixas normal, aceitável e alerta. E por fim englobar as variáveis ambientais, como tentativa de melhorar a eficiência da solução apresentada nesse trabalho.

# REFERÊNCIAS

AKYILDIZ, I. F. et al. Wireless sensor networks: a survey. **Computer Networks**, [S.l.], v.38, p.393–422, 2002.

AUGUSTO, J.; MCCULLAGH, P. Ambient Intelligence: concepts and applications. **Computer Science and Information Systems**, [S.l.], v.4, n.1, p.1–27, 2007.

BAO, S.-D.; ZHANG, Y.-T.; SHEN, L.-F. Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems. In: ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY, 2005. IEEE-EMBS 2005. 27TH ANNUAL INTERNATIONAL CONFERENCE OF THE. **Anais...** [S.l.: s.n.], 2005. p.2455 –2458.

BECKER, M. et al. Approaching Ambient Intelligent Home Care Systems. In: PERVASIVE HEALTH CONFERENCE AND WORKSHOPS, 2006. **Anais...** [S.l.: s.n.], 2006. p.1–10.

BISHOP, M. **Introduction to Computer Security**. [S.l.]: Addison-Wesley Professional, 2004.

BROMBA, M. **Bioidentification**. 2012.

BROOKS, K. The context quintet: narrative elements applied to context awareness. In: IN PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON HUMAN COMPUTER INTERACTION (HCI 2003). **Anais...** Erlbaum Associates, 2003.

CA. **Managing Strong Authentication: a guide to creating an effective management system**. [S.l.]: CA Technologies, 2007.

CARDIOLOGIA, S. S. B. de. **IV Diretriz para uso da Monitorização Ambulatorial da Pressão Arterial**. [S.l.]: SBC - Sociedade Brasileira de Cardiologia, 2005.

CARDIOLOGIA, S. S. B. de. **V Diretrizes Brasileiras de Hipetensão Arterial**. [S.l.]: SBC - Sociedade Brasileira de Cardiologia, 2006.

CHEN, X. et al. Node Compromise Modeling and its Applications in Sensor Networks. In: COMPUTERS AND COMMUNICATIONS, 2007. ISCC 2007. 12TH IEEE SYMPOSIUM ON. **Anais...** [S.l.: s.n.], 2007. p.575 –582.

COPETTI, A. **Monitoramento Inteligente e Sensível ao Contexto na Assistência Domiciliar Telemonitorada**. 2010. Tese (Doutorado em Ciência da Computação) — Instituto de Computação, Universidade Federal Fluminense, Niterói, RJ, Brasil.

COPETTI, A. et al. Monitoramento Inteligente e Sensível ao Contexto na Assistência Domiciliar Telemonitorada. **Anais do XXVIII Congresso da SBC**, [S.l.], 2008.

DAS, M. Two-factor user authentication in wireless sensor networks. **Wireless Communications, IEEE Transactions on**, [S.l.], v.8, n.3, p.1086 –1090, march 2009.

FOO KUNE, D. et al. Toward a safe integrated clinical environment: a communication security perspective. In: ACM WORKSHOP ON MEDICAL COMMUNICATION SYSTEMS, 2012., New York, NY, USA. **Proceedings...** ACM, 2012. p.7–12. (MedCOMM '12).

FREIER, A.; KARLTON, P.; KOCHER, P. **The Secure Sockets Layer (SSL) Protocol Version 3.0**. [S.l.]: IETF, 2011. n.6101. (Request for Comments).

GEHRINGER, E. Choosing passwords: security and human factors. In: TECHNOLOGY AND SOCIETY, 2002. (ISTAS'02). 2002 INTERNATIONAL SYMPOSIUM ON. **Anais...** [S.l.: s.n.], 2002. p.369 – 373.

GILL, K.; YANG, S.-H. A scheme for preventing denial of service attacks on wireless sensor networks. In: INDUSTRIAL ELECTRONICS, 2009. IECON '09. 35TH ANNUAL CONFERENCE OF IEEE. **Anais...** [S.l.: s.n.], 2009. p.2603 –2609.

HE, D. Robust biometric-based user authentication scheme for wireless sensor networks. **IACR Cryptology ePrint Archive**, [S.l.], v.2012, p.203, 2012.

HSIAO, T.-C. et al. An Authentication Scheme to Healthcare Security under Wireless Sensor Networks. **Journal of Medical Systems**, [S.l.], v.36, p.3649–3664, 2012. 10.1007/s10916-012-9839-x.

ISO. **Information technology – Security techniques – Code of practice for information security management**. 2005. n.ISO/IEC 27002:2005.

ISO. **Health informatics – Information security management in health using ISO/IEC 27002**. 2008. n.ISO/IEC 27799:2008.

JAIN, A. K. Biometric authentication. , [S.l.], v.3, n.6, p.3716, 2008.

JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. **IEEE Transactions on Circuits and Systems for Video Technology**, [S.l.], v.14, n.1, p.4–20, Jan. 2004.

JAIN, A.; ROSS, A.; NANDAKUMAR, K. **Introduction to Biometrics**. [S.l.]: Springer, 2011. (SpringerLink : Bücher).

KAEMARUNGSI, K.; KRISHNAMURTHY, P. Analysis of WLAN's received signal strength indication for indoor location fingerprinting. **Pervasive Mob. Comput.**, Amsterdam, The Netherlands, The Netherlands, v.8, n.2, p.292–316, Apr. 2012.

KOYUNCU, H.; YANG, S. A survey of indoor positioning and object locating systems. **IJCSNS International Journal of Computer Science and Network Security**, [S.l.], v.10, n.5, p.121–128, 2010.

KUMAR, P.; LEE, H.-J. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: a survey. **Sensors**, [S.l.], v.12, n.1, p.55–91, 2011.

KUMAR, P.; LEE, S.-G.; LEE, H.-J. E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. **Sensors**, [S.l.], v.12, n.2, p.1625–1647, 2012.

LE, X. H. et al. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare. **Journal of Networks**, [S.l.], v.6, n.3, 2011.

LIN, X. CAT: building couples to early detect node compromise attack in wireless sensor networks. In: GLOBAL TELECOMMUNICATIONS CONFERENCE, 2009. GLOBECOM 2009. IEEE. **Anais...** [S.l.: s.n.], 2009. p.1 –6.

LIU, H. et al. Survey of Wireless Indoor Positioning Techniques and Systems. **Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on**, [S.l.], v.37, n.6, p.1067 –1080, nov. 2007.

LV, S. et al. Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks. In: COMPUTATIONAL INTELLIGENCE AND SECURITY, 2008. CIS '08. INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2008. v.1, p.442–446.

MARTIN, H. et al. Experimental Evaluation of Channel Modelling and Fingerprinting Localization Techniques for Sensor Networks. In: CORCHADO, J. et al. (Ed.). **International Symposium on Distributed Computing and Artificial Intelligence 2008 (DCAI 2008)**. [S.l.]: Springer Berlin Heidelberg, 2009. p.748–756. (Advances in Soft Computing, v.50).

MILENKOVIC, A.; OTTO, C.; JOVANOV, E. Wireless sensor networks for personal health monitoring: issues and an implementation. **Computer Communications**, [S.l.], v.29, n.1314, p.2521 – 2533, 2006. <ce:title>Wirelsess Senson Networks and Wired/Wireless Internet Communications</ce:title>.

NAKAMURA, E.; GEUS, P. **Segurança de Redes em Ambientes Cooperativos**. [S.l.]: Berkeley, 2002.

PADMAVATHI, G.; SHANMUGAPRIYA, D. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. **CoRR**, [S.l.], v.abs/0909.0576, 2009.

PADMAVATHI, G.; SHANMUGAPRIYA, D. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. **CoRR**, [S.l.], v.abs/0909.0576, 2009.

POON, C.; ZHANG, Y.-T.; BAO, S.-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. **Communications Magazine, IEEE**, [S.l.], v.44, n.4, p.73 – 81, april 2006.

POTTER, P. **Fundamentos de Enfermagem**. [S.l.]: Elsevier Health Sciences, 2011.

PU, Q.; WANG, J.; ZHAO, R. Strong Authentication Scheme for Telecare Medicine Information Systems. **J. Med. Syst.**, New York, NY, USA, v.36, n.4, p.2609–2619, Aug. 2012.

RAFFLER, H. **Other perspectives on ambient intelligence**. 2006.

RAMLI, S.; AHMAD, R. Surveying the Wireless Body Area Network in the realm of wireless communication. In: INFORMATION ASSURANCE AND SECURITY (IAS), 2011 7TH INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2011. p.58 –61.

REID, P. **Biometrics for Network Security**. [S.l.]: Prentice Hall PTR, 2004. (Prentice Hall series in computer networking and distributed systems).

SAúDE, M. da. **Implantando a linha de cuidado do acidente vascular cerebral - AVC na rede de atenção às urgências**. [S.l.]: Ministério da Saúde, 2011.

SBIS. **Manual de Certificacao para Sistemas de Registro Eletronico em Saude (S-RES)**. 2009. n.Version 3.3.

SECO, F. et al. A survey of mathematical methods for indoor localization. In: INTELLIGENT SIGNAL PROCESSING, 2009. WISP 2009. IEEE INTERNATIONAL SYMPOSIUM ON. **Anais...** [S.l.: s.n.], 2009. p.9 –14.

SHNAYDER, V. et al. Sensor networks for medical care. In: EMBEDDED NETWORKED SENSOR SYSTEMS, 3., New York, NY, USA. **Proceedings...** ACM, 2005. p.314–314. (SenSys '05).

SMELTZER, S.; BARE, B. **Brunner & Suddarth tratado de enfermagem médico-cirúrgica**. [S.l.]: Guanabara Koogan, 2009.

SULLIVAN, F. . **Analysis of the Asia-Pacific Home Care Devices Market**. 2013.

TAMURA, T. et al. Monitoring and Evaluation of Blood Pressure Changes With a Home Healthcare System. **Information Technology in Biomedicine, IEEE Transactions on**, [S.l.], v.15, n.4, p.602–607, 2011.

TODOROV, D. **Mechanics of user identification and authentication**: fundamentals of identity management. [S.l.]: Auerbach Publications, 2007.

UDGATA, S.; MUBEEN, A.; SABAT, S. Wireless Sensor Network Security Model Using Zero Knowledge Protocol. In: COMMUNICATIONS (ICC), 2011 IEEE INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2011. p.1 –5.

VARSHNEY, U. Pervasive healthcare and wireless health monitoring. **Mob. Netw. Appl.**, Secaucus, NJ, USA, v.12, n.2-3, p.113–127, Mar. 2007.

WALTERS, J. P. et al. Wireless sensor network security: a survey, in book chapter of security. In: DISTRIBUTED, GRID, AND PERVASIVE COMPUTING, YANG XIAO (EDS. **Anais...** CRC Press, 2007. p.0–849.

WORLD, A. **Authentication Biometrics**. 2013.

YUAN, J.; JIANG, C.; JIANG, Z. A biometric-based user authentication for wireless sensor networks. **Wuhan University Journal of Natural Sciences**, [S.l.], v.15, n.3, p.272–276, 2010.

# SUBMISSÃO

Este apêndice apresenta o artigo submetido a revista JBHI - IEEE Journal of Biomedical and Health Informatics, intitulado A Solution for Strong Authentication in Sensor-based Healthcare Environments. Essa revista é o carro chefe da IEEE para os assuntos de informática médica, sendo avaliado com o Qualis A2 pela CAPES.

- Título: A Solution for Strong Authentication in Sensor-based Healthcare Environments
- Nome: IEEE Journal of Biomedical and Health Informatics
- Data de submissão: 30/11/2012

# A Solution for Strong Authentication in Sensor-based Healthcare Environments

Felipe Jose Carbone, Marcelo Antonio Marotta, Lisandro Zambenedetti Granville, Liane Margarida Rockenbach Tarouco

***Abstract*—Medical devices equipped with network interfaces, classified as sensors, transmit sensitive information over the network. This information need to be secured applying security mechaninsms, in order to mitigate vulnerabilities. Because of the vulnerabilities, strong means of authentication have been investigating. However, existing strong authentication solutions require user interaction, not respecting their individuality. This paper proposes an strong authentication solution on sensor-based healthcare environments in order to support the authentication process of patients with special needs. The authentication was based on a combination of two methods acquired from sensors of a healthcare environment: biometrics and location. In addition, standardizations provided by ISO/IEC 27799 and SBIS was followed for a safe development.**

***Keywords*-Strong Authentication, Biometry, Location, Wireless Sensor Networks.**

## I. Introduction

Blood pressure meters, body thermometers, and heart monitors are examples of medical devices that have been recently equipped with network interfaces, being classified as sensors to remotely monitor patients by gathering and exchanging health information over computer networks [1]. Because these sensors transmit sensitive information over the network, security became a fundamental concern to avoid patients harm and exposure of private data [2].

Security may be applied through different mechanisms, for example, authenticators, policy databases, cryptographic algorithms, and source replication. Each of these mechanisms may assure that sensors communication presents fundamental aspects of security, *i.e.,* confidentiality, integrity, and availability [3]. However, these mechanisms also require hardware resources and add communication complexity to be applied, presenting a trade-off between security and hardware resource requirements. As a consequence, these requirements represent a major problem to sensors that are much more limited in hardware than routers, computers, and other traditional network boxes that already implement security mechanisms. Therefore, sensors become a security bottleneck being vulnerable to attacks, such as impersonation, denial of service, and replay.

Because of the aforementioned vulnerability, stronger means of authentication have been investigated to mitigate attacks to sensor networks. Passwords, smart cards and biometrics are examples of methods used to provide strong authentication in such networks [4]. In health care environments, the problem with these methods is twofold: (i) strong authentication requires user interaction, which, depending on the physical or mental limitations of patients, can be a major restriction; and (ii) they are not in accordance with existing standardization *i.e.,* ISO/IEC 27799 [5]. Therefore, a new mechanism based on both strong authentication and existing standardizations that remove patient interaction in the authentication process still lacks.

In this paper we propose a strong authentication-oriented mechanism that follows ISO/IEC 27799 to mitigate attacks on sensor-based healthcare environments in order to support the authentication process of patients with special needs. Our mechanism does authentication based on a combination of two methods acquired from sensors of a healthcare environment. As a proof of concepts, perform patient authentication based on biometrics (*i.e.,* physiological information, such as blood pressure and respiration rate) and location (*i.e.,* position of the sensors relative to gateway). In addition, we define a formal model to represent our solution using cryptographic mechanisms. Finally, we discuss our solution in regards to security analysis and compliance with security regulations.

The remainder of this paper is organized as follows. In Section 2, we briefly introduce the basic concepts and some works regarding strong authentication and standardizations. Then, in Section 3, the proposed solution is explained, showing the authentication process of the patient. Section 4 provides a discussion about the proposed solution in order to analyze security, legal and feasibility issues. Finally, section 5 take the conclusions regarding the proposed solution.

## II. Background and Related Works

In this section, we present fundamental concepts to understand our solution. Afterwards, we describe current strong authentication based work, showing their pros and cons. Finally, we discuss some problems unsolved by current state of art solutions.

### A. Strong Authentication

In computer systems, authentication is the process that associates one client to a virtual identity, which may be described as a set of relevant informations to a system, such as permissions to edit files, home directories, names, and addresses. Because there are different persons that may want to impersonate others by accessing a system with different identities, authentication process have to challenge these persons to validate their access, for example, asking questions, requiring passwords, collecting biometric information or requiring other factors. Todorov *et al.,* [6] state that the authentication process consists basically of three steps: (*i*) client access, who will be challenged and will provide different informations to be validated; (*ii*) authentication, in which system identities will

be verified to enable client access to the system; and (*iii*) database, this step will compare previously stored informations with client provided ones.

In environments that deal with critical information (*e.g*, healthcare, banking, and military systems), a strong authentication scheme is require to ensure that all data will be protected. To develop a strong authentication, a tradeoff must be take in concern, *i.e.,* it is necessary extra factors to better protect the system, however, extra communication complexity and hardware resource are also required. Strong authentication typically uses multiple factors, in which combined add more protection for the authentication [6]. Bishop *et al.,* [7] state that factors can be classified as: i) what the entity knows (such as passwords); ii) what the entity have (such as smart cards); iii) what the entity is (such as biometrics); and iv) where the entity is (*e.g.,* geolocation and IP location). Authentication is considered strong when at least two distinct factors are used. The use of strong authentication reduces the risk of more sophisticated attacks, requiring more ability from an attacker to discover more information of your target.

In the IoT, some works have developed strong authentication in sensor-based environments [8][9][10][11]. In these works, the chosen factors was password and smart card, that are widely adopted and have low deployment costs [4]. Despite being well disseminated factors, smart cards and passwords require users skills. These users usually need to be trained and have good physical and psychological conditions to remember passwords or insert smart cards into a system. Users with special needs (*e.g*, people with Alzheimer, a brain injury, or had a stroke) cannot accomplish these requirements imposed by strong authentication, making necessary schemes that respect their limitations. In addition, the majority works that deal with strong authentication do not follow available specifications and standardizations in order to develop more reliable solutions.

### B. Security Regulations

With the inclusion of technology in healthcare area, the use of a common criteria for computerized systems has become necessary. This criteria may be captured, stored, processed and transmitted by diverging systems (*i.e*, different technologies, policies and regulations). Accordingly, there is a need to use a single standard to sort and organize activities in the security context to trust in the development process. Thereby, ISO/IEC 27002 was developed to provide guidance to organizations on how protect the confidentiality, integrity and evaluability of information [12]. Then, to encompass healthcare systems the ISO/IEC 27799 [5] was developed, which is an extension of ISO/IEC 27002 that complements the implementation guidelines. The ISO/IEC 27799 standard provides a checklist of security issues in healthcare, which includes: certification services, identification and authentication services, accountability services, rules and responsibilities of all partners and several other specifications.

Each country has its own regulations for healthcare systems operation. In Brazil requirements for the development of technologies on healthcare are presented by certification manual for systems of electronic health record, developed by SBIS (Brasilian Society of Health Informatics) [13]. This guidance manual has inherited several standardizations in the field of medical informatics and information security, including the ISO/IEC 27002 and 27799. Thus, in Brazil any implementation involving electronic healthcare data needs to follow orientations exposed by the certification manual of SBIS.

In order to obtain an efficient and legal strong authentication, it is necessary to follow standardizations concerned by the origin country. Major works on strong authentication do not concern about standardizations or the adopted common criteria was demonstrated, leading to an unsecured development. Standards not only helps the implementation process, but results in a certificate that proves the efficiency and quality of deployed solutions.

Thereby, new strong authentication mechanisms in which encompasses patients with special needs must be proposed. These mechanisms should follow existing guidelines for standardization and be adapted to not require any skill of a patient. The next section describes the solution presented in this paper to authenticate patients with special needs.

## III. Proposal Solution and Design Considerations

The proposed solution is part of a security module in a homecare monitoring system deployed over a wireless sensor network. This system is responsible to measure and process the patient information leveraging the collection capability of sensors, aiming accompany his clinical evolution to treat it at home. In addition, through these sensors capabilities, the system has the ability to infer the patient activity at home with an analysis module. Thus, the information is sent to a certified Hospital Federated Server (HFS) to be authenticated and stored. This HFS is part of a federation that provide the stored information for any healthcare professional belonging to it involved with the patient treatment.

The authentication process can be viewed in Figure 1. This authentication relies in biometric and location informations extracted from the sensors. These informations are the factors for the strong authentication scheme. So, the proposed solution is resumed in three main steps: 1) Registration: the patient is registered and generated keys are shared, comprising steps 1 and 2 of Figure 1; 2) Authentication of sensors: the sensors are authenticated and physiological data are obtained, comprising steps 3, 4 and 5 of Figure 1; and 3) Authentication of patient: in the HFS side, the information captured of patient are authenticated using the two factors chosen, comprising step 6 of Figure 1. The details of each step are discussed below.

### A. Registration

Initially, when the system is deployed, the gateway (*i.e*, a desktop computer at patient house) will generate a master random key $X_G$ and a random session key $Y_{SK}$ for every communication. These keys have size of 256 bits and are used to compute $A = h(userID \parallel X_G)$ that will be sended to the sensors node before starting the system. Thus, $S$ is sent to sensors, where $S = (userID, A)$. Also, the sensors are registered (*i.e*, collected information about sensors ID, MAC and type) and the keys stored in the gateway, considered a

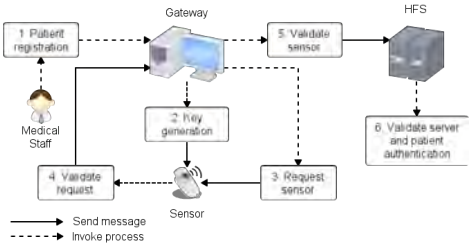


Figure 1. Authentication process

secured node. In addition, the patient need to be registered in the HFS. This responsibility is from medical staff, that also measure the initial physiological data and sets the normal behaviors for patient activities. For clarity, the symbols and notations used in this paper are listed on Table I.

| Symbols and Notations | Description |
|---|---|
| $SID$ | Sensor identification |
| $userID$ | User identification |
| $X_G$ | Master key |
| $Y_{SK}$ | Session key |
| $T$ | Time parameter |
| $M$ | Exchanged message |
| $R$ | Captured information |
| $h(.)$ | One-way hash function |
| $\|$ | Bit concatenation operator |
| $\oplus$ | XOR |

Table I
THE SYMBOLS AND NOTATIONS

### B. Sensors authentication

For the correct patient authentication it is necessary to trust in the sensors communication. So this step will demonstrate a securely communication between sensors and the gateway node. To achieve this, one-way hash function and symmetric encryption using SHA-2 and AES respectively was used, typical choices for applications that cannot afford the computational complexity of asymmetric cryptography [3]. Hash functions provide authenticity mapping a message and producing an single value for it. Symmetric encryption provide confidentiality to messages that cannot be readable during the message exchange.

First, the gateway node calculate $K_G = h(h(SID_j \parallel A) \parallel T_G) \oplus h(userID \parallel Y_{SK})$, hashing the identification of the $j^{th}$ sensor with shared secret key $A$ and the random session key generated $Y_{SK}$. Then, $K_G$ is encrypted with the $userID$, resulting in $C_G = E(K_G \parallel userID \parallel Y_{SK})$. A message is send to the sensor node with de $C_G$ and the time stamp $T_G$, $M1(C_G, T_G)$.

In the sensor side, after receiving the message $M1$, the time stamp need to be checked in order to proceed the authentication. If $\Delta T \geq T_S - T_G$, where $\Delta T$ is the expected time interval of the transmission between gateway and sensor, the session is aborted. Otherwise, the $C_G$ is decrypted $\alpha = D(C_G)$ and sensor compute $\beta = h(h(SID'_j \parallel A') \parallel T_G) \oplus h(userID' \parallel Y_{SK})$. Calculated the new hash with the received and existent information by the sensor, $\beta$ and $\alpha$ are compared, $\beta = \alpha$. If are equal the message is authentic and can proceed to calculate $\gamma = h(h(SID_j \parallel A) \parallel T_S) \oplus h(R \parallel Y_{SK})$, $V_S = E(h(\gamma \parallel T_S))$ and send $M2(V_S, R, T_S)$ to gateway. $R$ is the captured information of the patient, and before sending is encrypted $E(R \oplus Y_{SK})$.

Again in the gateway node, the goal is to check if the response of the sensor node is legitimate. First the time stamp is checked, performing $\Delta T \geq T_G - T_S$. If the interval is in the expected time, compute $\sigma = h(h(SID''_j \parallel A'') \parallel T_S) \oplus h(R \parallel Y_{SK})$ and decrypt $V_S$, $\mu = D(V_S)$. Then check $\sigma = \mu$, if are equal, the message is authentic and now the information $R$ can be stored to soon be sended to the HFS for patient authentication.

### C. Patient authentication

The third step is responsible to authenticate the patient information to HSF in order to provide trust in medical process. This authentication is performed through the two factors biometrics and location using data collected during the monitoring process. Biometrics will take advance by the sensors measurements, that provide useful physiological information about patient condition (*e.g*, such as blood pressure, electrocardiogram, respiration rate, pulse and oxygen saturation). The location factor calculate through the RSSI (Received Signal Strength Intensity) the position of the sensors relative to gateway in the environment [14]. This step proves the authenticity of the patient to HFS.

Data collected from sensors have physiological information about the monitoring patient, also called biometrics. This information compose an identity vector

$$Vector_{userB} = (SID_{j1} \parallel R_{j1}) + (SID_{j2} \parallel R_{j2}) + ... + (SID_{jn} \parallel R_{jn}) \quad (1)$$

. This vector contains identification $SID_j$ and information $R_j$ (*i.e.,* physiological information) of sensors measures. If some measurement have a lot of data, like heartbeat, the mean is obtained before integrated the vector.

Location is the another factor to be used in the authentication process, where gateway receives the signals of sensors in known locations, and has the capability to compute its location based on the measured signals. This measured can be obtained through RSSI, including several existing techniques and algorithms [15]. The results will be the distance in meters, composing the location vector

$$Vector_{sensorD} = (SID_{j1} \parallel D_{j1}) + (SID_{j2} \parallel D_{j2}) + ... + (SID_{jn} \parallel D_{jn}) \quad (2)$$

. where $D_j$ is the distance of the respective sensor.

Thus, after all data is gathered, the gateway can communicate with HFS. This communication is done using SSL (Secure Socket Layer) protocol, that provides a secure communication with server [16]. The communication is established after a

predefined time, imposed by system (*e.g*, cycles of 15 minutes). In each interaction, the HFS invokes the authentication module, responsible with the patient authentication, as can see in Figure 2.

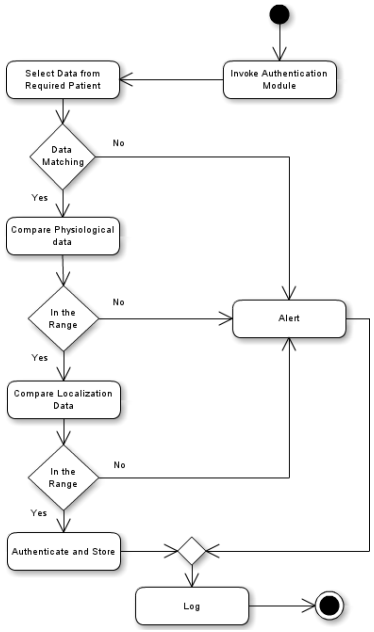


Figure 2. Activity diagram from patient authentication step

In Figure 2, the activity diagram shows the execution flow performed by patient data to be authenticated. In the first step, authentication module is invoked and data already stored is selected to be compared with the new values. This data have biometric and location information of each sensor and also the created rules based on the patient thresholds. So, if some patient coming data are missed, a problem may be happened (*i.e*, an attack or defect in some sensor). If this happens, the alert is invoked. Alert is an entity that report the unusual situation to a responsible sector with the objective to investigate the occurred, checking the patient situation.

Then, if all data are present, the validation can proceed. The next step will check the correctness of biometric data analyzing identity vector $Vector_{userB}$. A set of predefined rules are selected according to patient activity measured by analysis module in the patient gateway and patient physiologic patterns. These rules have the aim of set limits for thresholds (*i.e*, minimum and maximum values for the physiological data), $TH$, according to environment variables, $EV$, (*i.e*, variables that explain the patient activities). Considering $U$ as the set of registered patients in HFS, $u$ is the identity of an individual, then $u \in U$. If $EV = \theta$, then select rule $\theta$. Thus, to prove an identity $w$, the matching process is described as follows:

$$match(u, w) = \begin{cases} accept & \text{if } TH_{min} \geq R_{ju} \leq TH_{max} \\ reject & \text{if } TH_{min} < R_{ju} > TH_{max} \\ reject & \text{if } TH_{min} < R_{ju} \leq TH_{max} \\ reject & \text{if } TH_{min} \geq R_{ju} > TH_{max} \end{cases} \quad (3)$$

The rule $\theta$ is an arbitrary choice selected according to the pacient activity. This rule will dictate values of $TH_{min}$ and $TH_{max}$ to check the validity of patient biometric data, $R_{ju}$, using the matching algorithm. If the data are accepted, the authentication can proceed to location validation. Otherwise, if is rejected, alert is invoked.

In the location validation process, the distance from gateway is calculated, obtaining $D_j$, checking the correctness of the vector $Vector_{sensorD}$. Each sensor, $SID_j$, has ranges , $Ra$, that are considered acceptable. The validation process is obtained by the following matching process:

$$match(RD, D_j) = \begin{cases} accept & \text{if } Ra_{min} \geq D_j \leq Ra_{max} \\ reject & \text{if } Ra_{min} < D_j > Ra_{max} \\ reject & \text{if } Ra_{min} < D_j \leq Ra_{max} \\ reject & \text{if } Ra_{min} \geq D_j > Ra_{max} \end{cases} \quad (4)$$

$RD$ is the range distance that are required for verification. If the match is accepted, the authentication is completely successful, otherwise alert is invoked. At this point, the two factors are validated and the patient identity is proven. Thus, all data is stored in the HFS and hereafter can be used to validate the next requisitions and for medical purposes. Also, all the process is registered in a log, representing the last step of activity diagram, responsible to provide useful information for auditing.

## IV. Discussion

This paper propose an authentication solution for patients over wireless sensor networks. This solution explores the necessity of a strong authentication using two factors in order to strengthen the requirements of confidentiality, integrity and authenticity. Also, the solution was developed to encompass patients with special needs, removing patient interaction with system in the authentication process. The contribution focus on wireless sensor networks security, showing a protection model that combines sensors authentication and strong user authentication. To demonstrate the contribution, this section will discuss about the compliance of the solution with the security regulations, the feasibility of this kind of solution and perform a security analysis to encompass related threats.

### A. Secutiry Analysis

Due to scarce resources, wireless communication and critical information presented by sensors, a variety of threats may affect the proposed solution [17]. Some of these threats require more sophisticated mechanisms, like Denial-of-service (DoS) and Compromise Node attacks. Others can be mitigated by the

proposed solution, like Guessing attack, Impersonation attack and Replay attack. In the gateway-HFS communication, due to use of SSL connection (*i.e*, reliable and private connection with asymmetric cryptography), the communication can be securely established [16].

In the Replay attack, an intruder tries to replay the earlier communication and authenticate itself instead the patient [18]. Replay attacks can be mitigated using the time stamp verification. When a request is performed, the first verification will be $\Delta T \geq T' - T''$. If the time stamp does not lies in $\Delta T$, the request is terminate and messages will fail. Guessing attack is another comprehended attack that are not feasible in the proposed authentication process. In Guessing attacks, poorly-chosen secrets can be guessed for an attacker and compromise the system. This is not feasible because the patients do not interact with system to choose a password, and keys are generated by the gateway. Also, one-way hash function is used for password transmissions and other confidential components, using SHA-2 512 bit long output, safely and efficiency proven [19]. Users often choose weak passwords and have difficulty to remember it, causing a good choice to leave the human out of the process [20].

In this way, Impersonation attacks are not successful because even intercepting a legal login, the $C_G$ and $V_S$ in messages are encrypted, precluding attackers to derive the keys in order to forge patient registration. Also, attempts to brute force attack in hash functions will be unsuccessful, requiring a long time to make a collision, being determined in order of $2^{n/2}$ (*i.e*, the hash code strength) [21].

However, attacks of DoS and Node Compromise are big challenges in the wireless sensor networks, introducing complexity to the solution. In a DoS attack, the objetive is to exhaust the sensor resources in order to making it unavailable. To defend against DoS some overhead is required, like introduced in [22], adding entities with specific features to mitigate these attacks. Also, nodes around the environment can be captured and accessed to tamper with the internal settings. When rejoin in the network, can compromise the entire system transmitting tampered informations. This attack is known as Node Compromise and is rather difficult to prevent, but some works has been studying this problem [23] [24].

Other important security consideration must be done in key management. Key management is fundamental to develop a secure application, used to distribute cryptographic keys to nodes in the network. The proposed solution uses the Key pre-distribution approach, where secret keys are stored before the network deployment, offering relatively less computational complexity, more suitable for resource constrained sensor networks [25]. But, this approach is not feasible in an hospital sensor-based network (*i.e.,* a large network with ad hoc characteristic), requiring stronger and expensive approaches, like key distributions servers. In addition, session hijacking may be a major problem for the shared session keys. Therefore, keys are generated by fresh random numbers, being destructed immediately after a round of communication, for every requisition.

Also, ISO/IEC 27799 [5] provide a list of 25 threats to health information security. The threats related to the authentication process are: Masquerade by insiders, service providers and outsiders, communications interception, embedding of malicious code and user error. Weak authentication provides an easy point of entry for a masquerade, further motivating the strong authentication. Communication interception is a problem in wireless communication, but the use of cryptography and one-way hash functions make the sensitive information unreadable for third parties. Embedding of malicious code increase with the use of mobile technology, and is a big challenge to solve, like node compromise. Finally, user errors are not possible in our solution, as aforementioned system have no interaction with patient in the authentication process.

### *B. Compliance with Security Regulations*

Standardizations need to be followed in order to have a more reliable development. Thus, the proposed solution focus on follow the existing guidelines presented by ISO/IEC 27799 and the security specifications of SBIS. Following the SBIS requirements for identification and authentication (*i.e*, NGS1.02 requirement), the proposed solution comprises:

- NGS1.02.01 - User identification and authentication: Before any access, patient need to be identified and authenticated. This is the basic requirement to guarantee trust in patient information, being invoked by system in the first instance.
- NGS1.02.02 - Authentication method: For this requirement, the guidelines of ISO/IEC 27799 was used, where health information systems shall authenticate users and should do involving at least two factors [5]. So, fallowing the specifications and concerning patients with special needs, biometrics and location were chosen.
- NGS1.02.03 - Protection of authentication parameters: Requires protection to all data parameters using SHA-1 or SHA-2. In all the process of the proposed solution, important data, like the secrets $Y_{SK}$ and $X_G$, are protected using SHA-2 512 bit longer. None of the exchanged secrets are legible for third parties, protecting against unauthorized access and modification.
- NGS1.02.04 - Password security: This requirement imposes passwords restrictions for users. But in our solution, password is no more a patient choice, using others factors for authentication. As already mentioned, passwords are problematic because of human interaction [20].
- NGS1.02.05 - Control of login attempts: Requests for authentication in the HFS are performed according to the previous time interval configured in the gateway side. This time interval will vary depending the patient necessity, having short times (*e.g*, 5 minutes) or large times (*e.g*, 1 hour). Any attempt out of the time interval will have high chance to be an attack. This control assure more reliable login attempts and minimizes the bandwidth.

Also, ISO/IEC 27799 guidelines were followed for deployment of authentication process, taking into account cryptographic controls, access control, logging and user access management.

### C. Feasibility Analysis

Authentication relies on factors biometrics and location of the patient. But these factors have some limitations to be considered. In location, the accuracy and precision depends on the RSSI technique used (*i.e*, triangulation, scene analysis or proximity), thus necessitating careful consideration in the choice of positioning system [15]. Currently, the most adopted mechanism for track is RSS-based location fingerprinting, belonging to scene analysis technique, providing accuracy about 3 meters [26] [27].

In biometrics, the choice of collect physiological data is motivated by patients limitations. But this data have high variability and have poor biometric uniqueness, may resulting in a insecure analysis. In this way, to strengthen this factor the ideal is some well established biometrics (*e.g*, fingerprint, iris recognition) [28], but one that does not require patient interaction. In the works of [29] and [30], patients are identified automatically by the heart rate variability in a BASN (Body Area Sensor Network). These works are going toward an efficient automatic authentication using strong biometrics characteristics.

Symmetric cryptography and one-way hash function have low computational consumption, and used with some appropriate key management and session keys can provide high security. The technique to be chosen can vary according to available hardware and software resources, but following well established mechanisms [31][25] and legal issues [32].

Thereby, the proposed solution may encompass any patient with mental and physical restrictions, due to remove patient interaction in the authentication process. This characteristic can be included in an inteligent environment, being defined as an environment that pro actively, but sensibly, supports people in their daily lives [33][34]. In the world, about 1 billion people suffer from neurological disorders, such as Alzheimer and strokes [35], and Elderly population are growing [36]. Such examples, motivates the need for solutions which encompass patients with special needs in healthcare environments. This paper provides sight in the field of automatic authentication in order to benefit patients with special needs and increase the researches in security for intelligent environments.

## V. Conclusion

In this paper, we presented a strong authentication solution over wireless sensor networks in order to authenticate patients with special needs. This solution utilizes biometrics and location as authenticator factors, extracted from sensors. The authentication process is performed in the gateway-sensor round, using symmetric cryptography and one-way hash function and in the gateway-server round, using biometrics and location information. Data authenticated in the server side will be used for medical purposes (*i.e.,* diagnoses, monitoring, medical history) [37]. Also, development process follow guidelines of ISO/IEC 27799 and authentication specifications of SBIS, ensuring security issues. In terms of security, the sensors communication is secure against attacks like impersonation and session hijacking, but still lack for mechanims to mitigate DoS attacks.

The proposed solution may have impact on the wireless sensor networks security and strong authentication field. This solution is feasible for healthcare environments, caring with existing standard guidelines, providing an adaptable strong authentication solution for patients with special needs.

## References


[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.

[2] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mob. Netw. Appl.*, vol. 12, no. 2-3, pp. 113–127, Mar. 2007. [Online]. Available: http://dx.doi.org/10.1007/s11036-007-0017-1

[3] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey, in book chapter of security," in *in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds*. CRC Press, 2007, pp. 0–849.

[4] CA, "Managing Strong Authentication: A Guide to Creating an Effective Management System," CA Technologies, Tech. Rep., 2007.

[5] I. O. for Standardization, *Health informatics – Information security management in health using ISO/IEC 27002*, Std. ISO/IEC 27 799:2008, 2008.

[6] D. Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*, 1st ed. AUERBACH, Jun. 2007. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/1420052195

[7] M. Bishop, *Introduction to Computer Security*. Addison-Wesley Professional, 2004.

[8] M. Das, "Two-factor user authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 3, pp. 1086 –1090, march 2009.

[9] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012. [Online]. Available: http://www.mdpi.com/1424-8220/12/2/1625/

[10] T.-C. Hsiao, Y.-T. Liao, J.-Y. Huang, T.-S. Chen, and G.-B. Horng, "An authentication scheme to healthcare security under wireless sensor networks," *Journal of Medical Systems*, vol. 36, pp. 3649–3664, 2012, 10.1007/s10916-012-9839-x. [Online]. Available: http://dx.doi.org/10.1007/s10916-012-9839-x

[11] Q. Pu, J. Wang, and R. Zhao, "Strong authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 4, pp. 2609–2619, Aug. 2012. [Online]. Available: http://dx.doi.org/10.1007/s10916-011-9735-9

[12] I. O. for Standardization, *Information technology – Security techniques – Code of practice for information security management*, Std. ISO/IEC 27 002:2005.

[13] SBIS, *Manual de Certificacao para Sistemas de Registro Eletronico em Saude (S-RES)*, Std. Version 3.3, 2009.

[14] H. Koyuncu and S. Yang, "A survey of indoor positioning and object locating systems," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 5, pp. 121–128, 2010.

[15] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 37, no. 6, pp. 1067 –1080, nov. 2007.

[16] A. Freier, P. Karlton, and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0," RFC 6101 (Historic), Internet Engineering Task Force, Aug. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6101.txt

[17] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *CoRR*, vol. abs/0909.0576, 2009.

[18] S. Udgata, A. Mubeen, and S. Sabat, "Wireless sensor network security model using zero knowledge protocol," in *Communications (ICC), 2011 IEEE International Conference on*, june 2011, pp. 1 –5.

[19] T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, and B. Schott, "Comparative analysis of the hardware implementations of hash functions sha-1 and sha-512," in *Information Security*, ser. Lecture Notes in Computer Science, A. Chan and V. Gligor, Eds. Springer Berlin Heidelberg, 2002, vol. 2433, pp. 75–89.

[20] E. Gehringer, "Choosing passwords: security and human factors," in *Technology and Society, 2002. (ISTAS'02). 2002 International Symposium on*, 2002, pp. 369 – 373.

[21] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.

[22] K. Gill and S.-H. Yang, "A scheme for preventing denial of service attacks on wireless sensor networks," in *Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE*, nov. 2009, pp. 2603 – 2609.

[23] X. Lin, "Cat: Building couples to early detect node compromise attack in wireless sensor networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 30 2009-dec. 4 2009, pp. 1 –6.

[24] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Node compromise modeling and its applications in sensor networks," in *Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on*, july 2007, pp. 575 –582.

[25] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011. [Online]. Available: http://www.mdpi.com/1424-8220/12/1/55

[26] H. Martin, P. Tarrio, A. Bernardos, and J. Casar, "Experimental evaluation of channel modelling and fingerprinting localization techniques for sensor networks," in *International Symposium on Distributed Computing and Artificial Intelligence 2008 (DCAI 2008)*, ser. Advances in Soft Computing, J. Corchado, S. Rodriguez, J. Llinas, and J. Molina, Eds. Springer Berlin Heidelberg, 2009, vol. 50, pp. 748–756.

[27] F. Seco, A. Jimenez, C. Prieto, J. Roa, and K. Koutsou, "A survey of mathematical methods for indoor localization," in *Intelligent Signal Processing, 2009. WISP 2009. IEEE International Symposium on*, aug. 2009, pp. 9 –14.

[28] A. Cavoukian, A. Stoianov, and F. Carter, "Biometric encryption: Technology for strong authentication, security and privacy," in *IFIP International Federation for Information Processing*, vol. 261, 2008, pp. 57–77.

[29] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, 2005, pp. 2455 –2458.

[30] C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *Communications Magazine, IEEE*, vol. 44, no. 4, pp. 73 – 81, april 2006.

[31] T. Huston, "Security issues for implementation of e-medical records," *Commun. ACM*, vol. 44, no. 9, pp. 89–94, Sep. 2001. [Online]. Available: http://doi.acm.org/10.1145/383694.383712

[32] J. Jensen, I. Tondel, M. Jaatun, P. Meland, and H. Andresen, "Reusable security requirements for healthcare applications," in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, march 2009, pp. 380 –385.

[33] J. Augusto and P. Mccullagh, "Ambient Intelligence: Concepts and applications," *Computer Science and Information Systems*, vol. 4, no. 1, pp. 1–27, 2007. [Online]. Available: http://dx.doi.org/10.2298/CSIS0701001A

[34] A. Coronato and G. De Pietro, "Formal design of ambient intelligence applications," *Computer*, vol. 43, no. 12, pp. 60 –68, dec. 2010.

[35] W. H. Organization., *Neurological disorders : public health challenges*. World Health Organization, Geneva :, 2006.

[36] D. Bloom, A. Boersch-Supan, P. McGee, and A. Seike, "Population aging: Facts, challenges and responses," *Benefits and Compensation International*, vol. 41, no. 1, p. 22, 2011.

[37] M. Ogawa, T. Tamura, and T. Togawa, "Fully automated biosignal acquisition in daily routine through 1 month," in *Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE*, vol. 4, oct-1 nov 1998, pp. 1947 –1950 vol.4.