



Programa de Pós-Graduação em

Computação Aplicada

Mestrado/Doutorado Acadêmico

Josué Francisco do Nascimento Júnior

Sistema Baseado em Tolerância a Falhas para o Monitoramento de
Práticas Esportivas de Alto Desempenho

São Leopoldo, 2022

Josué Francisco do Nascimento Júnior

**SISTEMA BASEADO EM TOLERÂNCIA A FALHAS PARA O MONITORAMENTO
DE PRÁTICAS ESPORTIVAS DE ALTO DESEMPENHO**

Dissertação apresentada como requisito parcial
para a obtenção do título de Mestre pelo
Programa de Pós-Graduação em Computação
Aplicada da Universidade do Vale do Rio dos
Sinos — UNISINOS

Orientador:
Prof. Dr. Rodolfo S. Antunes

São Leopoldo
2022

N244s NASCIMENTO JÚNIOR, Josué Francisco
 Sistema baseado em tolerância a falha para o monitoramento de
 práticas esportivas de alto desempenho / Josué Francisco do
 Nascimento Júnior. – 2022.
 51 f. : il. ; 30 cm.

 Dissertação (mestrado) – Universidade do Vale do Rio dos
 Sinos, Programa de Pós-Graduação em Computação Aplicada,
 2022.

 “Orientador: Prof. Dr. Rodolfo Stoffel Antunes.”

 1. Tolerância a falhas. 2. Wearables. 3. Esportes de alto
 desempenho. 4. Monitoramento esportivo. I. Título.

CDU: 004

Resumo

Atualmente, o esporte de alto rendimento tem exigido bastante dos atletas e, portanto, é fundamental ter o monitoramento constante dos treinamentos, dessa forma o desempenho do atleta pode ser analisado dia após dia até a competição. A IoT (Internet das Coisas), através do Wearables, para a coleta de dados, é a melhor opção para o monitoramento por meio das informações coletadas, oferecer de forma rápida, ao treinador uma melhor tomada de decisão baseado no que é percebido no treinamento. Cada vez mais dados são gerados a partir de dispositivos IoT e Wearables nos esportes, e muitos desses dados são perdidos ou mal utilizados. Nesse contexto, o conceito tolerância a falhas é o conjunto de técnicas utilizadas para detectar, mascarar e tolerar falhas no sistema, permitindo um melhor gerenciamento do processo de coleta a partir dos sensores. Desse modo, com o sistema perto de 100% de funcionamento, o atleta terá acesso a informações de desempenho, de forma detalhadas e relevante, a partir de treinamentos e competições. Sendo assim, o presente trabalho tem como objetivo propor um sistema capaz de monitorar o desempenho de atletas, em ambientes distintos, gerenciando a coleta de dados, dos sensores, através de um sistema que seja tolerante a falhas tanto de hardware como de software. Em particular, o sistema tem por objetivo, realizar um levantamento de quais sensores estão aptos para fazer o monitoramento, e dessa forma oferecer um detalhamento preciso das informações coletadas, padronizando os dados, de acordo com a modalidade que será monitorada. Durante todo o processo de monitoramento, o sistema vai verificar o disponibilidade do hardware em tempo real. A contribuição científica deste trabalho surgiu da necessidade de sistemas mais confiáveis, essa necessidade surgiu devido a crescente demanda de serviços de alta confiabilidade. O gerenciamento do monitoramento de atletas de alto desempenho, em diferentes ambientes, e com o objetivo principal, de oferecer dados detalhados, do treinamento de um atleta, para uma tomada de decisão mais assertiva do seu treinador. O sistema proposto foi avaliado, através de um estudo de caso, realizado com um protótipo aplicado aos treinamentos, da modalidade de atletismo. Foram utilizados diversos sensores durante o percurso, e sistema tolerante a falhas, será responsável por em manter o sistema com a maior disponibilidade possível. Os resultados obtidos demonstraram que o sistema computacional, proposto através da tolerância a falhas, obteve êxito nas coletas. Em particular, o sistema avaliado se demonstrou capaz de obter os dados dos atletas durante o treinamento em um tempo aceitável, mesmo com a ocorrência de falhas parciais.

Abstract

Currently, high performance sport has demanded a lot from athletes and, therefore, it is essential to have constant monitoring of training, so the athlete's performance can be analyzed day after day until competition. The IoT (Internet of Things), through Wearables, for data collection, is the best option for monitoring through the information collected, quickly offering the coach better decision-making based on what is perceived in the training. . More and more data is generated from IoT devices and Wearables in sports, and much of this data is lost or misused. In this context, the fault tolerance concept is the set of techniques used to detect, mask and tolerate system failures, allowing a better management of the collection process from the sensors. In this way, with the system close to 100% functioning, the athlete will have access to performance information, in a detailed and relevant way, from training and competitions. Therefore, the present work aims to propose a system capable of monitoring the performance of athletes, in different environments, managing the collection of data from the sensors, through a system that is tolerant to both hardware and software faults. In particular, the system aims to carry out a survey of which sensors are capable of monitoring, and in this way provide accurate detailing. of the information collected, standardizing the data, according to the modality that will be monitored. During the entire monitoring process, the system will check the availability of the hardware in real time. The scientific contribution of this work arose from the need for more reliable systems, this need arose due to the growing demand for high reliability. The management of monitoring of high performance athletes, in different environments, and with the main objective of offering detailed data, from the training of an athlete, for a more assertive decision-making by his coach. The proposed system was evaluated, through a case study, carried out with a prototype applied to training, of athletics. Several sensors were used along the way, and a fault-tolerant system will be responsible for keeping the system as available as possible. The results obtained showed that the computational system, proposed through fault tolerance, was successful in the collections. In particular, the evaluated system was able to obtain data from athletes during training in an acceptable time, even with the occurrence of partial failures.

LISTA DE FIGURAS

Figura 1 – Visão Geral do Sistema	25
Figura 2 – Tela Inicial do Aplicativo	27
Figura 3 – DataSheetGO	32
Figura 4 – Cenário do Estudo de Caso	34
Figura 5 – Cones IoT, visão Externa.	35
Figura 6 – Cones IoT, visão Interna.	36
Figura 7 – Resultado da latência	42
Figura 8 – Smartwatch - Relógio Inteligente Amazfit Bip U Pro (Xiaomi)	43
Figura 9 – Tomadas de tempo dos dia 11/11 e 09/09 de 2022	45

LISTA DE TABELAS

Tabela 1 – Atributos de dependabilidade	11
Tabela 2 – Técnicas para alcançar dependabilidade	12
Tabela 3 – Fases para aplicação das técnicas de tolerância a falhas	14
Tabela 4 – Características	22
Tabela 5 – Comparativo entre Sistemas de Monitoramento	44

SUMÁRIO

1	INTRODUÇÃO	4
1.1	Motivação	4
1.2	Objetivo	6
1.3	Metodologia	6
1.4	Organização do Trabalho	7
2	FUNDAMENTAÇÃO TEÓRICA	8
2.1	Tolerância a Falhas	8
2.2	Técnicas de Tolerância a Falhas	11
2.3	Internet das Coisas	13
2.4	Wearables	15
2.5	Cloud Computing	16
2.6	Fog Computing	17
3	TRABALHOS RELACIONADOS	19
3.1	Estado-da-Arte	19
3.2	Discussão	22
4	MODELO DE SISTEMA COMPUTACIONAL	24
4.1	Visão Geral	24
4.2	Técnicas de Tolerância a Falhas do Sistema	26
4.3	Funcionamento do Sistema	26
4.3.1	Regras da coleta de dados do treinamento	28
4.4	Micro Serviços	29
4.5	Telemetria	29
4.6	Sensores	30
4.7	Microcontrolador	31
4.8	Persistência dos Dados Coletados	32
5	ESTUDO DE CASO	33
5.1	Modalidade Escolhida	34
5.2	Dados Coletados	35
5.3	Cones IoT	35
5.4	Protocolo de Comunicação	36
5.5	Metodologia de Avaliação	37
5.6	Cenário de ambiente controlado	39
5.7	Cenário de teste de falhas no início do treinamento	39
5.8	Métricas	40
5.9	Comparativo com sistemas reais	43
6	CONCLUSÃO	46
	REFERÊNCIAS	47

1 INTRODUÇÃO

O esporte, como fenômeno social, acaba por incorporar as várias faces da cultura, tornando-se um elemento que agrega os acontecimentos sociais, enquanto fonte de produção cultural e um elemento imprescindível para entender os acontecimentos contemporâneos. Portanto, a qualidade de vida como acesso aos bens culturais e incorporação de hábitos saudáveis tem no esporte uma possibilidade ímpar para desenvolver políticas que buscam o movimento e a incorporação de práticas corporais no cotidiano das pessoas (ALMEIDA; JUNIOR, 2010). Com a ajuda da tecnologia, é possível tornar mais interessante a relação do esporte e a sua prática, principalmente com a coleta de dados através da tecnologia vestível (Wearable).

O desenvolvimento tecnológico nas áreas de saúde e esportes, vêm permitindo métodos mais eficientes para a coleta e análise de informações. Dados como saúde do jogador e seu uso na análise tática na partida são muito importantes. Verificar instantaneamente o estado de saúde das pessoas dentro e fora do campo, e a detecção precoce de certos eventos na análise tática tornam a competição melhor. Para isso, aplicativos baseados na Internet das Coisas (IoT) são bastante adequados. A maioria dos aplicativos de IoT usa serviços em nuvem para armazenamento e computação. O uso de computação em neblina melhora a eficiência de uma aplicação de IoT em larga escala envolvendo espectadores, jogadores e outros atores (KARAKAYA; AKLEYLEK, 2021).

O crescimento do software IoT está transformando nosso ambiente de um modo que era considerado impossível. A IoT atenderá nossa comunidade aumentando a eficiência, integridade e conveniência para empresas e consumidores (MAHDI; ALJUBOORI; ALI, 2021). Dado este contexto, o presente trabalho tem como principal proposta explorar a intersecção entre as diferentes tecnologias relacionadas à Internet-das-Coisas para proporcionar um monitoramento mais preciso e a prova de falhas e um detalhamento sobre o desempenho dos atletas.

1.1 Motivação

O poder da computação aplicado a áreas como a captura de movimento e modelos em 3D tem revolucionado o projeto de equipamentos, calçados e roupas. O sistema miCoach da Adidas tem sido utilizado por equipes europeias de rugby e equipes da liga americana/canadense de futebol durante treinos e competições oficiais. O sistema monitora a taxa cardíaca, velocidade, impulsão do salto, distância percorrida e outros dados dos atletas. Isso foi alcançado com o uso de GPS, giroscópios e acelerômetros miniaturizados que foram implantados em um pequeno sistema acoplado à camisa dos atletas e, em alguns casos, nos calçados (DOCUSIGN, 2018).

Dentro deste contexto, o uso de um conjunto heterogêneo de sensores requer mecanismos para garantir a correta operação e coleta de dados, mesmo quando um ou mais destes dispositivos apresenta algum tipo de anomalia. Entretanto, apesar da relevância desse requisito, a literatura não apresenta uma proposta de arquitetura focada em um sistema para monitoramento

de atletas que busque operar mesmo quando existe a degradação dos dispositivos utilizados para monitoramento.

A contribuição científica desta monografia é a aplicação a tolerância a falhas que é utilizada por questões de usabilidade para não gerar uma experiência negativa para o usuário através do gerenciamento do monitoramento de atletas de alto desempenho em diferentes ambientes, tendo como objetivo principal em oferecer dados detalhados do treinamento de um atleta para uma tomada de decisão mais assertiva do seu treinador. A contribuição mais significativa deste artigo é permitir que atletas tenham a possibilidade de registrar dados sobre seu desempenho independente da infraestrutura de sensores presente no ambiente. Essa proposta foi avaliada em uma prova de conceito utilizando um cenário de treinamento intervalado.

Nota-se que a IoT, enquanto inovação tecnológica que envolve questões de privacidade de dados e informações de usuários, ganha espaço nas discussões em meios acadêmicos e profissionais (SANTOS; SALES, 2015). O presente trabalho também leva as questões de privacidade e segurança dos dados de atletas em consideração, em linha com as atuais discussões e regulamentações observadas nesse contexto. Sendo assim, o presente trabalho tem a seguinte questão como principal tema de pesquisa:

Qual seria o modelo de um sistema computacional que aplique o conceito de tolerância a falhas para permitir um monitoramento contínuo e padronizado sobre o desempenho de atletas utilizando arquiteturas IoT heterogêneas.

Além disso, tem-se como um dos desafios deste trabalho o desenvolvimento de um protótipo para validar um pequeno universo da proposta sugerida. Objetiva-se que tal protótipo seja capaz de disponibilizar os dados dos atletas de forma simultânea à sua geração, dados do ambiente onde ocorrem treinos (p.ex., temperatura, umidade do ar, velocidade do vento). Todas essas informações ficam à disposição de cada atleta para acompanhamento de seu desempenho.

Para prover a interação homem-computador (IHC) do atleta com o sistema computacional, será utilizado um aplicativo cuja a sigla será AMA (Aplicativo de Monitoramento de Atleta), que seu objetivo é prover as informações antes do início do treinamento para que o serviço sistema de tolerância a falhas seja executado e o aplicativo também mostrará os resultados do treinamento em tempo real.

O atleta chegando no ambiente de treino, através do seu smartphone, vai logar no AMA e irá selecionar qual será o local de treinamento e qual modalidade pretende treinar. Baseado nessas informações escolhidas pelo atleta, o sistema computacional irá preparar uma infraestrutura de monitoramento baseada nas características da modalidade selecionada pelo atleta utilizando os sensores disponíveis no ambiente. A aplicação informará se o ambiente está apto para monitorar a modalidade selecionada e qual o nível de detalhamento que poderá ser coletado.

1.2 Objetivo

Dada a pergunta de pesquisa definida, o objetivo geral deste trabalho é desenvolver uma metodologia para a aplicação tolerante a falhas em um sistema baseada em redes de sensores sem fio para permitir o monitoramento de atividades de atletas. Tal metodologia explora conceitos como Fog Computing, Edge Computing, Cloud Computing, Wearables dentre outros, permitindo o monitoramento de atletas tanto em sessões de treinamento quanto em competições. Além disso, será desenvolvido um Aplicativo de Monitoramento de Atleta que fornecerá dados coletados e o atleta consulte e compare os dados que foram coletados de seus treinamentos ou competições. Levando em conta o objetivo geral definido, o trabalho terá os seguintes objetivos específicos:

- Proposta de uma arquitetura baseada no conceito de tolerância a falhas para a configuração e coleta de dados de sensores sem fio presentes em ambientes de treinamento ou competição;
- Desenvolvimento de uma prova de conceito da arquitetura proposta a fim de realizar experimentos em cenários de uso reais;
- Validação da arquitetura através da realização de experimentos em cenários reais de utilização por atletas.

A contribuição científica deste trabalho é a aplicação da tolerância a falha para o gerenciamento do monitoramento de atletas de alto desempenho em diferentes ambientes, tendo como objetivo principal em oferecer dados detalhados do treinamento de um atleta para uma tomada de decisão mais assertiva do seu treinador. O estudo de caso será importante, pois existirá métricas que foram criadas para avaliar o desempenho do sistema.

1.3 Metodologia

A partir de uma análise inicial da revisão da bibliografia foi verificado a falta de um sistema computacional que utiliza a tolerância a falhas para monitoramento de práticas esportivas. Antes do desenvolvimento do sistema computacional foi necessário identificar todos os cenários possíveis para a implementação do sistema. Com os cenários devidamente identificados, foi definido quais problemas seriam resolvidos. O sistema proposto irá ativar os micro serviços responsáveis por cada fase do monitoramento.

Foi desenvolvido um protótipo (hardware) e um aplicativo para testar em parte o funcionamento do sistema computacional. O monitoramento é iniciado e encerrado pelo atleta. Para iniciar o monitoramento o atleta fornece a informação de qual modalidade será praticada (a localização é fornecida pelo GPS do smartphone), e após alguns segundos, via aplicativo o atleta

recebe as informações de que pode iniciar a sua atividade e quais sensores estão disponíveis para o monitoramento.

O sistema proposto tem como principal foco a tolerância a falhas para o gerenciamento do processo de coleta de dados de treinamento de atletas. Nesse sentido, o foco da avaliação se encontra em identificar o comportamento do mecanismo composto em diferentes cenários de utilização.

1.4 Organização do Trabalho

O restante desta monografia está organizado da seguinte maneira. O Capítulo 2 descreve os conceitos fundamentais explorados ao longo do trabalho. O Capítulo 3 apresenta uma análise do estado-da-arte sobre arquiteturas para o monitoramento de atletas usando conceitos de IoT. O Capítulo 4 descreve o modelo de arquitetura de monitoramento que será desenvolvido ao longo do trabalho. O Capítulo 5 descreve o estudo de caso que será utilizado na avaliação do trabalho. Por fim, o Capítulo 6 apresenta as considerações finais e direções futuras do trabalho em desenvolvimento.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma visão geral sobre os conceitos fundamentais que serão explorados ao longo deste trabalho. Em particular, serão explorados os seguintes conceitos: Tolerância a Falhas, Internet das Coisas, Cloud computing, Fog computing, e dispositivos vestíveis (Wearables).

2.1 Tolerância a Falhas

O termo tolerância a falhas foi cunhado por Avizienis em 1967. Desde então tem sido amplamente utilizado pela comunidade acadêmica para designar toda a área de pesquisa ocupada com o comportamento de sistemas computacionais sujeitos a ocorrência de falhas, sem ter entretanto logrado sucesso como designação popular. Na indústria o termo nunca teve boa aceitação, sendo que desenvolvedores de sistemas de controle preferem usar o termo sistemas redundantes para seus equipamentos. Na comercialização de sistemas computacionais como mainframes e servidores de rede, o termo usual é alta disponibilidade, designando a principal qualidade desses sistemas (WEBER, 2002).

Sistemas totalmente infalíveis são impossíveis, pois falhas são inevitáveis. Componentes físicos envelhecem e sofrem com interferências externas, seja ambientais ou humanas. O software, e também os projetos de software e hardware, são vítimas de sua alta complexidade e da fragilidade humana em trabalhar com grande volume de detalhes ou com deficiências de especificação. Prevenção e remoção de falhas não são suficientes quando o sistema exige alta confiabilidade ou alta disponibilidade. Nesses casos o sistema deve ser construído usando técnicas de tolerância a falhas. Essas técnicas garantem funcionamento correto do sistema mesmo na ocorrência de falhas e são todas baseadas em redundância, exigindo componentes adicionais ou algoritmos especiais. Tolerância a falhas não dispensa as técnicas de prevenção e remoção. Sistemas construídos com componentes frágeis e técnicas inadequadas de projeto não conseguem ser confiáveis pela simples aplicação de tolerância a falhas. (WEBER, 2003).

As principais causas de falhas são problemas de especificação, problemas de implementação, componentes defeituosos, imperfeições de manufatura, fadiga dos componentes físicos, além de distúrbios externos como radiação, interferência eletromagnética, variações ambientais (temperatura, pressão, umidade) e também problemas de operação (WEBER, 2002).

O objetivo de tolerância a falhas é alcançar dependabilidade. Uma das definições diz que dependabilidade do sistema pode ser entendida como a capacidade de oferecer uma funcionalidade específica, que pode ser justificadamente confiável, ou ainda, que o sistema irá executar ações especificadas ou apresentar resultados específicos de maneira confiável e em tempo oportuno. Segundo Dantas (2013), os atributos de dependabilidade são:

- Disponibilidade. A importância de se ter um sistema disponível é observada por grande parte de usuários de sistemas em rede, tais como compras on-line e acesso à sua conta

bancária as quais têm que estar disponíveis sempre que o usuário necessitar das mesmas. Devido a essa necessidade de obtenção de recursos na hora exigida, usuários demandam sistemas que venham atendê-lo a qualquer hora. (DANTAS, 2013)

- **Confiabilidade.** É através da análise da confiabilidade que podemos verificar qual deve ser o melhor caminho a ser seguido na implementação da arquitetura de um sistema computacional. Alta confiabilidade é uma métrica importante quando estamos falando de um sistema cujo as falhas possam causar efeitos catastróficos. As falhas possuem uma tendência de aumentar sua probabilidade de ocorrência ao longo do tempo de funcionamento do sistema. Isso faz com que a taxa de confiabilidade diminua nesse mesmo período de tempo. Vêm crescendo a ocorrência daquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos sistemas. Essas falhas e suas consequências são tratados por técnicas de segurança computacional (security) e não por técnicas de tolerância a falhas. Deve ser considerado, entretanto, que um sistema tolerante a falhas deve ser também seguro a intrusões e ações maliciosas. (MOTA, 2022).
- **Segurança.** É a probabilidade do sistema ou estar operacional, e executar sua função corretamente, ou descontinuar suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam. Segurança é a medida da capacidade do sistema de se comportar de forma livre de falhas (fail-safe). Um exemplo seria um sistema de transporte ferroviário onde os controles de um trem providenciam sua desaceleração e parada automática quando não mais conseguirem garantir o seu funcionamento correto. Em um sistema fail-safe, ou a saída é correta ou o sistema é levado a um estado seguro (WEBER, 2002)
- **Confidencialidade.** Pode ser entendida como a ausência de divulgação não autorizada de informação [8]. As informações devem permanecer secretas e apenas pessoas autorizadas acessam as mesmas. Acesso não autorizado a informações confidenciais podem ter consequências sérias, não só em aplicações de segurança nacional, mas também no comércio e na indústria (DANTAS, 2013).
- **Integridade.** Tenta garantir que os dados não sejam alterados durante uma comunicação. Mecanismos de proteção de integridade podem ser agrupados em duas grandes categorias: (i) Mecanismos de prevenção, tais como controles de acesso que impedem a modificação não autorizada de informação e (ii) Mecanismos de detecção, que se destinam a detectar modificações não autorizadas quando os mecanismos de prevenção falharam.
- **Manutenabilidade.** Significa a facilidade de realizar a manutenção do sistema, ou seja, a probabilidade que um sistema com defeitos seja restaurado a um estado operacional dentro de um período determinado. Restauração envolve a localização do problema, o reparo físico e a colocação em operação (DANTAS, 2013).

Falhas de software e também de projeto são consideradas atualmente o mais grave problema em computação crítica. Sistemas críticos, tradicionalmente, são construídos de forma a suportar falhas físicas. Assim é compreensível que falhas não tratadas, e não previstas, sejam as que mais aborreçam, pois possuem uma grande potencial de comprometer a confiabilidade e disponibilidade do sistema (WEBER, 2002).

As técnicas reativas de tratamento de falhas são aplicadas quando existe a possibilidade de prever a falha antes de sua ocorrência. Ou seja, o local onde ela pode ocorrer possui técnicas de tratamento de falhas implementadas, o que garante maiores chances de tratamento caso venha ocorrer e atesta que o sistema é mais robusto e confiável (TAMASHIRO, 2020).

As principais causas de falhas são problemas de especificação, problemas de implementação, componentes defeituosos, imperfeições de manufatura, fadiga dos componentes físicos além de distúrbios externos como radiação, interferência eletromagnética, variações ambientais (temperatura, pressão, umidade) e também problemas de operação (WEBER, 2003).

As técnicas proativas ou ativas de tratamento de falhas podem ser compreendidas como a utilização de um conjunto de técnicas para prever a ocorrência de falhas e tratá-las antes de sua ocorrência, como por exemplo, a substituição de componentes de hardwares suspeitos e monitoramento da rede de comunicação (TAMASHIRO, 2020).

Por melhor que um sistema tenha sido projetado, especificado e testado, não há como garantir que ele seja totalmente confiável, isto é, que esteja sempre ativo e comportando-se conforme suas especificações. mesmo que se suponha o projeto e implementações perfeitos (o que é difícil), durante a vida útil do sistema podem ocorrer defeitos em componentes de hardware ou situações não previstas no software. Assim em diversas aplicações, independente do tipo de falha, de suas consequências e gravidade, é norma de qualidade, é norma de qualidade que o sistema de computação disponha de mecanismos de tolerância a falhas para impedir que os efeitos destas prejudiquem o seu funcionamento. Existem graus de aplicação de propriedade. Dessa forma, são definidas cinco diferentes categorias de tolerância a falhas, de acordo com os benefícios oferecidos para as aplicações (DENARDIN, 1997).

- Grau 4: Representa tolerância a falhas no nível de ação, ou seja, todas as ações visíveis são executadas com sucesso apesar de defeitos nos componentes. A máxima confiabilidade é garantida (DENARDIN, 1997).
- Grau 3: Ocorre quando a recuperação de uma falha é lenta e, muitas vezes, é necessário abandonar a execução de uma ação visível que foi interrompida devido a ocorrência de uma falha. Entretanto não há perda a nível de hardware (DENARDIN, 1997).
- Grau 2: Resulta em alguma degradação de serviço por que, nesse caso, alguma parte do serviço crítico pode ser sacrificada, resultando em uma recuperação apenas parcial de hardware (DENARDIN, 1997).
- Grau 1: Representa o pior caso do grau 2. Sua finalidade é manter um conjunto mínimo de

funções de serviço críticos, com a recuperação de uma configuração de hardware mínima (DENARDIN, 1997).

- Grau 0: Neste caso, não há tolerância a falhas, pois um serviço crítico não pode ser mantido. Diz-se então que a tolerância a falhas não é fornecida (DENARDIN, 1997).

Caso alguma falha ocorra no sistema, é necessário que o sistema seja tolerante, ou seja, é necessário que ele recupere e volte a operar com o menor ou nenhum impacto nos serviços ofertados. Para que o sistema seja tolerante, várias técnicas podem ser aplicadas, para isso é necessário a sua detecção, recuperação e tratamento (TAMASHIRO, 2020).

2.2 Técnicas de Tolerância a Falhas

O objetivo de tolerância a falhas é alcançar dependabilidade (tabela 1). O termo dependabilidade é uma tradução literal do termo inglês *dependability*, que indica a qualidade do serviço fornecido por um dado sistema e a confiança depositada no serviço fornecido. Principais medidas de dependabilidade são confiabilidade, disponibilidade, segurança de funcionamento (*safety*), segurança (*security*), manutenibilidade, testabilidade e comprometimento do desempenho (*performability*) (WEBER, 2003).

Tabela 1 – Atributos de dependabilidade

Dependabilidade (<i>dependability</i>)	qualidade do serviço fornecido por um dado sistema
Confiabilidade (<i>reliability</i>)	capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período
Disponibilidade (<i>availability</i>)	probabilidade do sistema estar operacional num instante de tempo determinado; alternância de períodos de funcionamento e reparo
Segurança (<i>safety</i>)	probabilidade do sistema ou estar operacional e executar sua função corretamente ou descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam
Segurança (<i>security</i>)	proteção contra falhas maliciosas, visando privacidade, autenticidade, integridade e irrepudiabilidade dos dados

Fonte: WEBER, 2003

Tolerância a falhas é uma questão fundamental de um projeto de computação, pois a tolerância a falhas pode ser relacionada com um sistema que está mascarando uma falha, ou melhor, que não deixa os usuários de um sistema perceberem que algum problema está ocorrendo, deixando o sistema sempre funcionando. Quando um sistema apresenta algum tipo de falha, quer dizer que o sistema não está oferecendo os serviços de acordo com o projetado. Entretanto, nem sempre o problema está nos servidores que estão provendo serviço, pois pode ser que tal serviço dependa de outros servidores para prestar o serviço adequadamente (MARTINS et al., 2014). Segundo o mesmo autor, temos tipos diferentes de falhas que são:

- Falha por queda: ocorre quando um servidor interrompe seu funcionamento prematuramente. Um exemplo de falhas por queda é quando o sistema operacional pára de repente e a única solução é reiniciá-lo;
- Falha por omissão: ocorre quando um servidor deixa de responder a uma requisição. Essa falha pode ser pelo motivo do servidor não ter recebido nenhuma requisição, ou que o servidor enviou uma requisição, mas o outro lado não recebeu;
- Falha de temporização: ocorre quando a resposta se encontra fora de um intervalo de tempo real especificado. Essa falha pode ser classificada como falha de desempenho;
- Falha de resposta: ocorre quando a resposta de um servidor está incorreta. Por exemplo, um mecanismo de busca que retorne sistematicamente páginas Web não relacionadas com qualquer uma das palavras de busca usada;
- Falhas arbitrárias: conhecida como falhas bizantinas, quando ocorrem essas falhas, o cliente deve se preparar para o pior, pois pode acontecer de um servidor estar produzindo saídas que nunca deveria ter produzido, mas que não podem ser detectadas como incorretas.

Segundo (WEBER, 2003) no desenvolvimento de um sistema com os atributos de dependabilidade desejados, um conjunto de métodos e técnicas devem ser empregadas. Esses métodos e técnicas são classificados conforme a tabela 2.

Tabela 2 – Técnicas para alcançar dependabilidade

prevenção de falhas	impede a ocorrência ou introdução de falhas. Envolve a seleção de metodologias de projeto e de tecnologias adequadas para os seus componentes
tolerância a falhas	fornece o serviço esperado mesmo na presença de falhas. Técnicas comuns: mascaramento de falhas, detecção de falhas, localização, confinamento, recuperação, reconfiguração, tratamento
validação	remoção de falhas, verificação da presença de falhas
previsão de falhas	estimativas sobre presença de falhas e estimativas sobre conseqüências de falhas

Fonte: WEBER, 2003

Vem crescendo em frequência aquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos sistemas. Essas falhas e suas conseqüências são tratadas por técnicas de security e não por técnicas de tolerância a falhas. Deve ser considerado, entretanto, que um sistema tolerante a falhas deve ser também seguro a intrusões e ações maliciosas (WEBER, 2003).

Segundo (MARTINS et al., 2014) as técnicas de tolerância a falhas podem ser classificadas em quatro fases: detecção, avaliação, recuperação e tratamento. A tabela 3) apresenta as 4 fases de aplicações para tolerância a falhas. Essas fases estão relacionadas em uma seqüência

de atividades, que devem ser executadas após a identificação de uma ou mais falhas, e são descritos a seguir.

- Fases de detecção de erro: A primeira fase é da detecção de erro, onde uma falha se manifesta inicialmente como um erro, para em seguida ser detectada pelos mecanismos propostos no Quadro 4. Sendo que uma falha não pode ser detectada se o erro não se manifestar; uma falha pode estar em um sistema por toda a sua vida útil se o sistema não entrar em um estado errôneo, dentre os mecanismos nessa fase, destaca-se um pré-diagnóstico do erro detectado, que se confirmará na fase de tratamento da falha;
- Fase de Avaliação: Na fase de avaliação serão levantadas as informações necessárias, para uma correção e futura recuperação do mesmo;
- Fase de Recuperação: São utilizadas técnicas de recuperação por retorno, onde ocorre a condução do estado do sistema para anteriormente ao erro, e técnicas de recuperação por avanço, onde a condução a um novo estado ainda não ocorreu desde a última manifestação de erro, sendo utilizado em sistema de tempo real;
- Fase de Tratamento: Nessa fase é considerado que uma falha única ocorra de cada vez, e a localização da falha é realizada em duas etapas: localização rápida e localização demorada. Para cada um dos tipos são utilizados diagnósticos manuais ou automáticos. Após a localização a falha é reparada pela remoção do componente danificado, e nessa fase é possível informar o diagnóstico da falha corrigida.

2.3 Internet das Coisas

A Internet das Coisas (do inglês Internet of Things (IoT)) emergiu dos avanços de várias áreas como sistemas embarcados, microeletrônica, comunicação e sensoriamento. De fato, a IoT tem recebido bastante atenção tanto da academia quanto da indústria, devido ao seu potencial de uso nas mais diversas áreas das atividades humanas (SANTOS et al., 2016). A Internet das Coisas consiste em objetos, sensores, infraestrutura de comunicação, unidade computacional e de processamento que pode ser colocado na nuvem. (KHAN et al., 2012).

O conceito de uma rede de dispositivos inteligentes foi discutido já em 1982, com uma máquina para venda de bebidas modificada em Carnegie Mellon University se tornando o primeiro aparelho conectado à Internet, capaz de relatar seu inventário e se recentemente as bebidas carregadas estavam geladas. Kevin Ashton (nascido em 1968) é um pioneiro da tecnologia britânica conhecido por inventar o termo "Internet das coisas" para descrever um sistema onde a Internet está conectada ao mundo físico por meio de sensores (GOKHALE; BHAT; BHAT, 2018).

Atualmente, não só computadores convencionais estão conectados à internet, como também uma grande heterogeneidade de equipamentos, tais como TVs, laptops, geladeira, fogão,

Tabela 3 – Fases para aplicação das técnicas de tolerância a falhas

Fases	Mecanismos
Detecção de erros	Duplicação e comparação Testes de limites de tempo Cão de guarda (<i>watchdog timers</i>) Testes reversos Codificação: paridade e códigos de detecção de erros Teste de razoabilidade, de limites e de compatibilidades Testes estruturais e de consistência Pré-Diagnóstico
Avaliação de danos	Ações atômicas Operações primitivas auto encapsuladas Isolamento de processos Regras do tipo tudo que não é permitido é proibido Hierarquia de processos Controle de recursos
Recuperação do erro	Técnicas de recuperação por retorno (<i>backward error recovery</i>) Técnicas de recuperação por avanço (<i>forward error recovery</i>)
Tratamento da falha e continuidade do serviço	Diagnóstico Reparo

Fonte: (MARTINS, 2014)

eletrodomésticos, automóveis, smartphones, entre outros. Nesse novo cenário, a pluralidade é crescente e previsões indicam que mais de 50 bilhões de dispositivos estarão conectados até 2022. Com o uso dos objetos inteligentes será possível detectar seu contexto, controlá-lo, viabilizar troca de informações uns com os outros, acessar serviços da internet e interagir com as pessoas. Em paralelo, uma gama de novas possibilidades de aplicações surge, como, por exemplo, cidades inteligentes (smart cities); saúde (smart healthcare); e casas inteligentes (smart home). Também observa-se o surgimento de novos desafios, tais como regulamentações, segurança, e padronizações. Essas novas habilidades dos objetos inteligentes gerarão um grande número de oportunidades de pesquisas e projetos no âmbito acadêmico e empresarial. Além do desenvolvimento de tecnologias há de se efetuar a pesquisa e o tratamento dos aspectos de segurança aplicáveis em infraestrutura para Internet das coisas (RIBEIRO et al., 2018).

A IoT é capaz de interagir sem intervenção humana. Alguns aplicativos IoT preliminares já foram desenvolvidos em saúde, transporte e indústrias automotivas. As tecnologias de IoT estão em seus estágios iniciais. No entanto, vários desenvolvimentos ocorreram na integração de objetos com sensores na Internet. O desenvolvimento da IoT envolve muitos problemas, como infraestrutura, comunicações, interfaces, protocolos e padrões (GOKHALE; BHAT; BHAT, 2018).

Espera-se que os ambientes SMART se tornem os principais atores da Internet do Futuro, que não serão mais vistos como um meio de conectar as pessoas aos serviços, mas para acessar os recursos disponibilizados por pequenos objetos inteligentes. Esta visão de a Internet se

encaixa no conceito mais amplo da Internet de Coisas (IoT), de acordo com as quais objetos do cotidiano, como aparelhos domésticos, atuadores e sistemas incorporados de qualquer tipo, se tornarão atores pró-ativos da Internet global, com a capacidade de gerar e consumir informações. Explorando as novas possibilidades oferecidas pela IoT permitindo tecnologias, aplicativos inteligentes inovadores podem ser desenvolvidos em muitos cenários heterogêneos, como doméstico e industrial automação, saúde e bem-estar, redes inteligentes, automotivo, e muitos outros (CATARINUCCI et al., 2017).

Aos dispositivos com essas qualidades é dado o nome de objetos inteligentes (Smart Objects). Os objetos, ao estabelecerem comunicação com outros dispositivos, manifestam o conceito de estarem em rede (Santos et al. (2016)). Na Internet das Coisas, eventualmente, a unidade básica de hardware apresentará ao menos uma das seguintes características: (i) unidade(s) de processamento; (ii) unidade(s) de memória; (iii) unidade(s) de comunicação e; (iv) unidade(s) de sensor(es) ou atuador(es).

Um dos desafios mais preocupantes da IoT é a forma como a segurança dos dados e dos próprios consumidores irá ser garantida. Como já acontece com os equipamentos de medição inteligente e automóveis cada vez mais autônomos, haverá um vasto volume de dados fornecendo informações sobre o uso pessoal dos aparelhos que, caso não sejam seguros, poderão abrir caminho para violações de privacidade. Isto é um desafio, pois o volume de informação gerada pela IoT é essencial para trazer melhores serviços e comodidades aos consumidores (Santos e Sales (2015)).

Os avanços significativos em tecnologia nas últimas décadas, caracterizados pela miniaturização de componentes, fontes de energia mais eficientes, redes alternativas, soluções e novos sensores impulsionaram o desenvolvimento de dispositivos vestíveis. Como consequência, uma variedade de fatores foram criados, permitindo que dispositivos vestíveis sejam aplicados para vários fins diferentes. Apesar do grande potencial e benefícios conhecidos de dispositivos vestíveis, seu uso disseminado envolve várias questões de privacidade. Vestuário, continuamente coletando, transmitindo e armazenando dados, lidar com informações que são frequentemente considerados pessoais, privados, sensíveis ou confidenciais. Esta informação pode estar disponível publicamente ou postado nas redes sociais, onde é compartilhado com uma rede de amigos do usuário individual ou mesmo de partes desconhecidas ou não confiáveis. (Motti e Caine (2015)).

2.4 Wearables

Os Wearables são dispositivos vestíveis que possuem tecnologias que são muito importantes e poderão auxiliar bastante, futuramente. Esses dispositivos recolhem informações do usuário, como no caso de batimentos cardíacos, gasto calórico, temperatura do corpo, dentre outros. Tudo que foi coletado é armazenado, podendo chegar aos serviços de saúde ou mesmo ser compartilhados, levando em conta as políticas de privacidade. Alguns dos principais wearables

são os relógios inteligentes, os óculos, as pulseiras, os patches de monitoramento (que são como tatuagens), roupas, colares, bonés, etc. Estes permitem o acompanhamento e armazenamento de dados de atividades diárias, exercícios, sono e muitas outras possibilidades. Um dos pontos fortes está no envio em tempo real de dados relacionados a estas ações. (Verzani e Serapião (2020)).

Dentre as tecnologias computacionais utilizadas atualmente para acompanhamento dos esportistas, destacam-se os Wearable Devices (Dispositivos Vestíveis). Embora a evolução destes dispositivos ocorra rapidamente, consolidando cada vez mais esse tipo de tecnologia no mercado, existem algumas barreiras que ainda impedem a difusão destes produtos. Para algumas equipes, a falta de recursos de tempo, financeiros, ou de recursos humanos para manipulação dos dados são razões para o não monitoramento dos atletas (Oliveira, Carvalho e Bez (2017)). Os wearables, como tecnologias médicas, estão se tornando parte integrante da vida pessoal. Análise, registro de parâmetros fisiológicos, ou informar cronograma de medicação. Esta tecnologia em constante evolução trás plataformas que prometem ajudar as pessoas a buscar um estilo de vida mais saudável e também fornecem dados médicos contínuos para rastrear ativamente o status metabólico, diagnóstico e tratamento. Tais tecnologias têm avançado rapidamente graças a avanços na miniaturização da eletrônica flexível, biossensores eletroquímicos, microfluídica e inteligência artificial. Algoritmos levaram a dispositivos vestíveis que podem gerar dados médicos em tempo real na Internet das coisas. Esses dispositivos flexíveis podem ser configurados para fazer contato conformado com a epiderme, ocular, intracocular e dentária interfaces para coletar sinais bioquímicos ou eletrofisiológicos (Yetisen et al. (2018)).

As tecnologias relacionadas a dispositivos móveis e Internet of Things, ao mesmo passo que evoluem, também se popularizam. Neste segmento tecnológico, os Wearable Devices, já ocupam importante papel na área de monitoramento esportivo. O protótipo construído, assim como o app desenvolvido, é uma iniciativa neste mesmo sentido, com o objetivo promover os benefícios do acompanhamento mais detalhado da saúde e desempenho aos praticantes de esportes (Verzani e Serapião (2020)). Os sistemas vestíveis são os mais usuais atualmente, com soluções diversas disponíveis no mercado. Apesar da grande popularidade que estes dispositivos vêm ganhando, alguns deles podem ser bastante desconfortáveis, dependendo do tamanho ou da posição no corpo (Kronbauer, Luz e Campos (2018)).

2.5 Cloud Computing

Em 1961, o cientista americano John McCarthy, do MIT, criador do termo inteligência artificial, previu o que hoje conhecemos como computação em nuvem: “se os computadores, da forma como eu imagino, se tornarem os computadores do futuro, então a computação poderá ser organizada como um serviço público, assim como a telefonia é. Cada assinante pagará apenas pelos recursos que ele realmente utilizará, mas ele terá acesso a todos os recursos oferecidos pelas linguagens de programação de um grande sistema. Alguns assinantes poderão oferecer

serviços a outros assinantes. A computação como um serviço público poderá ser base de uma nova e importante indústria” (Carissimi (2015)).

A computação na nuvem (Cloud Computing) é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independente da plataforma, bastando para isso ter um terminal conectado à “nuvem” (Pedrosa e Nogueira (2011)). É possível oferecer, por exemplo, serviços de armazenamento de dados sem que o cliente disponha de uma infraestrutura própria dedicada. Portanto, tanto a infraestrutura quanto a interface da aplicação são disponibilizadas pela nuvem. Serviços podem ser adaptados às necessidades do cliente, sem que este participe da instalação, configuração ou manutenção do produto. Além disso, recursos, como máquinas virtuais, podem ser acessados pelo cliente em qualquer lugar, a qualquer momento, também sem a necessidade de envolvimento com o gerenciamento desta infraestrutura (Jacobi et al. (2012)).

O modelo de computação em nuvem foi desenvolvido com o objetivo de fornecer serviços de fácil acesso e de baixo custo e garantir características tais como disponibilidade e escalabilidade. Este modelo visa fornecer, basicamente, três benefícios. O primeiro benefício é reduzir o custo na aquisição e composição de toda infra-estrutura requerida para atender as necessidades das empresas, podendo essa infra-estrutura ser composta sob demanda e com recursos heterogêneos e de menor custo. O segundo é a flexibilidade que esse modelo oferece no que diz respeito à adição e troca de recursos computacionais, podendo assim, escalar tanto em nível de recursos de hardware quanto software para atender as necessidades das empresas e usuários. O terceiro benefício é prover uma abstração e facilidade de acesso aos usuários destes serviços. Com isso, os usuários dos serviços não precisam conhecer aspectos de localização física e de entrega dos resultados destes serviços (Ruschel, Zanotto e Mota (2010)).

2.6 Fog Computing

A Fog Computing (computação de névoa) é definido como "um cenário onde um grande número de heterogêneos (sem fio e às vezes autônomos) onipresentes e dispositivos descentralizados se comunicam e potencialmente cooperam entre eles e com a rede para realizar o armazenamento e processamento de tarefas sem a intervenção de terceiros. Essas tarefas podem suportar funções básicas de rede ou novos serviços e aplicativos executados em um ambiente de área restrita. Os usuários alugam parte de seus dispositivos para hospedar esses serviços recebem incentivos para fazer isso."Embora esta definição ainda seja discutível, concordamos fortemente que precisamos diferenciar a computação em névoa de tecnologias relacionadas uma vez que qualquer uma dessas técnicas subjacentes pode nos oferecer um visão falsa na computação de névoa. (Yi, Li e Li (2015)).

Fog computing é um paradigma com recursos limitados, como computação, armazenamento e serviços de rede de forma distribuída entre diferentes dispositivos finais e computação em nuvem clássica. Ele fornece uma boa solução para aplicativos IoT que são sensíveis à latência

(Atlam, Walters e Wills (2018)). Esse movimento seletivo dos recursos computacionais, controle e tomada de decisões para as extremidades da rede é uma área emergente da engenharia de sistemas e ciência da computação. Seu estudo está no centro de vários domínios de aplicação da Internet das Coisas onde pesquisas vem buscando identificar requisitos, experimentar algoritmos e avaliar arquiteturas para esclarecer problemas relativos à sua implementação (Coutinho, Carneiro e Greve (2016)).

3 TRABALHOS RELACIONADOS

Este capítulo apresenta uma análise de propostas que possuem similaridades com o trabalho aqui proposto por terem como foco a Tolerância a Falhas no processo de monitoramento de atividades esportivas utilizando tecnologias IoT. Considerando o foco principal da pesquisa, foram realizadas buscas por trabalhos científicos na base Google Scholar. A busca fez uso do seguinte conjunto de palavras-chave: (i) Fault Tolerance; (ii) IoT; (iii) Monitoring System; e (iv) Sports. A fim de identificar pesquisas relevantes e recentes na área, o intervalo de publicação foi limitado entre janeiro de 2020 a junho de 2022. Tais parâmetros resultaram na obtenção de um corpo literário inicial de 4180 artigos.

Desde ponto em diante, a metodologia seguiu em três etapas: (i) aplicação de critérios de inclusão ou exclusão; (ii) leitura dos títulos e resumos e (iii) leitura completa das obras. Na primeira etapa foram excluídos revisões literárias e artigos com pouco relevância. Na segunda etapa, foram selecionados os artigos no qual o título e resumo estão relacionados com a questão de pesquisa. Por fim, foram selecionados 7 artigos que tratam do assunto de forma mais incisiva a partir da sua leitura completa. Estes artigos serão explorados em mais detalhes no restante deste capítulo.

3.1 Estado-da-Arte

Segundo Li et al. (2020) o rápido desenvolvimento e crescimento na área da Internet das Coisas (IoT) oferece um grande potencial no setor de saúde. Atualmente, a tecnologia sem fio, rastreadores de fitness e sensores corporais no campo esportivo têm um grande impacto na eficiência da vida e na confiabilidade do sistema de saúde. Neste artigo, redes de sensores wearable eficientes computacionais assistidas por névoa foram propostas em sistemas de monitoramento de saúde para esportes atléticos usando IoT. O dispositivo vestível para o monitoramento contínuo em tempo real da frequência cardíaca, frequência respiratória e cadência de movimento durante a atividade física foi analisado. Além disso, os dados coletados pelo sensor são carregados no módulo Ethernet do sistema de conexão IoT, e o Indivíduo Autorizado acessa os dados via internet para rastrear a saúde do atleta. Dispositivos vestíveis tornaram-se cada vez mais interessados em medir fatores fisiológicos, promover a saúde e melhorar a adesão à prática em diferentes populações, desde atletas de elite até pacientes e o artigo propõe:

- (i) Redes de sensores wearable eficientes computacionais;
- (ii) Um modelo de filas e um modelo matemático foram derivados para abordar e prever o desempenho do sistema de monitoramento;
- (iii) Os resultados experimentais foram verificados e realizados;
- (iv) O sistema proposto tem alto desempenho, precisão e baixo custo.

Na visão do Gope et al. (2020) com o desenvolvimento de diversos tipos de produtos e dispositivos eletrônicos de consumo, a vida das pessoas mudou drasticamente. Os dispositivos são conectados por tecnologias avançadas de comunicação à Internet e formam a Internet das Coisas (IoT) para troca de informações. Atualmente, os dispositivos IoT são amplamente implantados para várias aplicações, como casas inteligentes, cidades inteligentes, redes de sensores corporais (BSN) e redes inteligentes. Para alcançar a capacidade de tomada de decisão tolerante a falhas, o sistema proposto usa uma abordagem de aprendizado de máquina. Em particular, ele usa máquinas de vetores de suporte para aprender o comportamento normal do paciente a partir dos dados sensoriais. Este artigo aborda as deficiências do sistema de saúde baseado em IoT existente. Foi proposto um sistema aprimorado, introduzindo um esquema de autenticação baseado em função não clonável física (PUF) e um esquema de tomada de decisão tolerante a falhas orientado a dados para projetar um sistema de saúde moderno baseado em IoT. As análises mostram que o esquema proposto é mais seguro e eficiente do que os sistemas existentes.

Para Qadri et al. (2020) as tecnologias básicas de habilitação incluem os sistemas de comunicação entre os nós sensores, os processadores, e os algoritmos de processamento para gerar uma saída do dados coletados pelos sensores. No entanto, atualmente, essas tecnologias facilitadoras também são apoiadas por vários novos métodos. O uso da Inteligência Artificial (IA) transformou os sistemas Health-IoT em quase todos os níveis. A pesquisa abrange arquitetura, aplicativos, segurança e políticas de IoT em todo o mundo. O artigo propõe uma arquitetura H-IoT e um modelo de segurança. A pesquisa se concentra na segurança da rede IoT, mas não cobre de forma abrangente os riscos de segurança, métodos de mitigação e evolução dos riscos de segurança de acordo com os novos paradigmas. Este artigo investiga as maneiras como essas tecnologias estão transformando os sistemas H-IoT e também identifica o curso futuro para melhorar a Qualidade de Serviço (QoS) usando essas novas tecnologias. H-IoT está evoluindo continuamente de acordo com os avanços nas tecnologias subjacentes em WBANs. Esta evolução visa alcançar os recursos salientes do H-IoT baseado em WBAN. Esses recursos incluem:

- (a) formato compacto para sensores;
- (b) segurança de dados;
- (c) tolerância a falhas;
- (d) Qualidade de Serviço (QoS) como baixa latência com alta integridade de dados;
- (e) interoperabilidade.

Segundo Marandi et al. (2022) as WBANs (Wireless Body Area Network) estão entre as tecnologias usadas nos modernos sistemas de atendimentos baseados em IoT. Essas redes consistem em redes de baixo custo, tamanho, energia limitada, heterogênea e monitorável inteligente que pode ser usado ou implantado no corpo humano. Aplicativos WBAN baseados em IoT, de acordo com sua finalidade são categorizados em formas médicas, não médicas, de implantes

e usáveis. Dados de saúde são informações privadas e consideradas críticas, portanto, a segurança da transmissão de dados em uma WBAN torna-se uma questão importante. O esquema de segurança depende da confidencialidade dos dados, integridade dos dados, autenticidade, não repúdio, disponibilidade, atualização dos dados, localização segura e privacidade. Este artigo apresenta primeiro as WBANs baseadas em IoT, seu mecanismo de roteamento e desafios, após o que fornece uma descrição detalhada dos algoritmos com reconhecimento térmico (temperatura). Por fim, são apresentadas as vantagens e desvantagens desses algoritmos. O protocolo proposto é tolerante a falhas e melhora a vida útil da rede classificando os pacotes. A eficiência energética e a prevenção de aumentos de temperatura não são significativas neste protocolo.

Poongodi et al. (2020) chama atenção sobre a tecnologia IoT que está sendo implantada é especialmente projetada para torná-la invisível, de modo que a tecnologia não manifeste sua presença aos usuários que está monitorando. Para os aplicativos de saúde baseados em IoT, a WBAN está ganhando muita popularidade à medida que os dispositivos vestíveis surgem no mercado. Vários nós de sensores podem ser implantados em diferentes locais do corpo humano para medir os batimentos cardíacos, a distribuição da temperatura corporal e detectar quedas. Além dos sinais médicos, os nós sensores também podem ser colocados para rastrear as condições ambientais ao redor do corpo humano. Assim, os sistemas de sensores vestíveis fornecem informações valiosas sobre o impacto na saúde humana. Os sistemas baseados em sensores vestíveis têm um enorme potencial a ser completamente explorado e prevê-se que o avanço nas tecnologias proporcionará a transformação de como será a saúde no futuro. Este artigo destaca a importância da localização na rede de área corporal e fornece uma visão geral sobre a avaliação do desempenho dos sistemas de localização. Apresenta também os diversos tipos de sensores e metodologias para fundir os dados gerados pelos sensores.

No trabalho do Nguyen e Ha (2022) em sistemas discretos, a confiabilidade é atribuída a propriedades do sistema como disponibilidade, confiabilidade, manutenibilidade, durabilidade e segurança. No contexto de tecnologias para um ambiente sustentável, sistemas confiáveis são importantes para a gestão e processamento de informações em vários aspectos da vida da cidade, melhorando a capacidade de resposta dos cidadãos e facilitando serviços e aplicações para a resiliência de uma cidade inteligente. Em redes de sensores sem fio, a redundância tem sido explorada para aumentar a precisão dos dados, a confiabilidade de detecção, a vida útil do sistema e a segurança. Com a disponibilidade de redes de baixo custo, uma vantagem proeminente resultante da redundância é sua operação segura e tolerante a falhas. Este artigo apresenta uma rede de sensores sem fio de baixo custo habilitada para Internet das Coisas com esquemas confiáveis recém-desenvolvidos para melhorar a confiabilidade no monitoramento da qualidade do ar em áreas suburbanas. O sistema possui unidades de detecção para comunicações do roteador com economia de energia devido à conservação dinâmica.

Moreira et al. (2021) afirma que a extensão dos sensores IoT para incluir dispositivos no domínio médico (Health-IoT) melhorou a qualidade dos cuidados de saúde personalizados serviços. Recentemente, o grande volume de dados gerado pela detecção de Health-IoT dispositi-

vos no ambiente de cuidados de saúde tem sido uma grande preocupação. Este tem criado vários desafios, incluindo a identificação de técnicas eficazes para minerar essa enorme quantidade de dados disponíveis. O objetivo é, portanto, determinar a aplicabilidade ideal de várias novas tecnologias em desenvolvimento de sistemas inteligentes, biossensores vestíveis e para lidar com os dados de saúde sensíveis massivos existentes para o objetivo de fornecer soluções de assistência médica bem-sucedidas e sustentáveis em todo o mundo. Este artigo é uma realização chave na medição nesta área e servirá para ajudar a abordar, unificar e avançar os principais desafios de pesquisa em toda a comunidade científica.

3.2 Discussão

Foi constatado que existem mais projetos focados na área de saúde do que na área de monitoramento de atletas. Uma comparação dos trabalhos relacionados é apresentada na Tabela 4. Estas comparações servem para identificar as similaridades e diferenças entre o trabalho proposto e as literaturas selecionadas. Os critérios de comparações foram:

- Tolerância a falhas: Se o sistema é tolerante a falhas ou seja se possuem a capacidade de continuar provendo corretamente seus serviços mesmo havendo falha tanto de hardware como de software .
- Monitoramento de Atleta: Se o foco do artigo é em atletas.
- Monitoramento de Paciente: Se o foco do artigo é em pacientes.
- Registro de dados individuais: Se o sistema é capaz de identificar vários indivíduos em tempo real.
- Sensor Fisiológico: Utilização de sensores como sensor cardíaco, sensor de temperatura, etc.
- Prova de Conceito: Se houve a utilização de um aplicativo para testes.
- Estudo Real: Se houve a utilização de um protótipo.

Tabela 4 – Características

Artigos	Tolerância a falhas	Monitoramento de Atleta	Monitoramento de Paciente	Registro de dados individuais	Sensor Fisiológico	Prova de Conceito	Estudo Real
LI et al., 2020	Sim	Sim	Sim	Não	Sim	Sim	Não
GOPE et al., 2020	Sim	Sim	Não	Não	Sim	Sim	Não
QADRI et al., 2020	Sim	Não	Sim	Não	Não	Não	Não
JALILI MARANDI et al., 2022	Sim	Não	Sim	Não	Sim	Sim	Não
POONGODI et al., 2020	Sim	Não	Sim	Não	Sim	Sim	Não
NGUYEN; HA, 2022	Sim	Não	Sim	Não	Não	Não	Não
MOREIRA et al., 2021	Sim	Não	Sim	Não	Sim	Não	Não

Fonte: Autor (2021)

A tabela 4 apresenta as comparações considerando critérios como tolerância a falhas, monitoramento de atletas, monitoramento de pacientes, registro de dados individuais, sensor fisiológico, prova de conceito e estudo real. Nenhum dos artigos selecionados atendeu todos os critérios definidos. No sistema proposto neste artigo, atendeu todos os critérios e foi desenvolvido um protótipo como prova de conceito para avaliar na prática a proposta.

4 MODELO DE SISTEMA COMPUTACIONAL

Este capítulo descreve modelo de sistema proposto para o monitoramento flexível de práticas esportivas que prevê um sistema de tolerância a falhas e Internet-das-Coisas. O modelo de sistema toma como base os seguintes requisitos:

- Permitir o monitoramento detalhado de práticas esportivas de diferentes modalidades em um ambiente com sensores heterogêneos;
- Gerenciar de forma automática o nível de detalhes e a estrutura de dados resultante com base nos sensores disponíveis para monitoramento;
- Manter o atleta informado sobre o status do monitoramento e quais informações estarão disponíveis;
- Permitir compatibilidade com sensores genéricos que não sejam específicos de uma modalidade (p.ex., sensores de ambiente).
- Usar técnicas de Tolerância a falhas para manter o sistema em funcionamento a maior parte do tempo para o uso dos atletas.

O modelo de sistema vai se adaptar com base na escolha do atleta (modalidade) e vai verificar quais sensores estarão aptos para fornecer o melhor cenário para o monitoramento do atleta, antes mesmo de começar a sua atividade vai saber quais sensores o monitorarão durante todas as atividades. A tolerância a falhas acontece em vários momentos no sistema, desde o início até o fim da prática esportiva, além do software o hardware também serão monitorados para que o atleta possa realizar sua prática esportiva sem se preocupar com a ocorrência de falhas durante o monitoramento.

4.1 Visão Geral

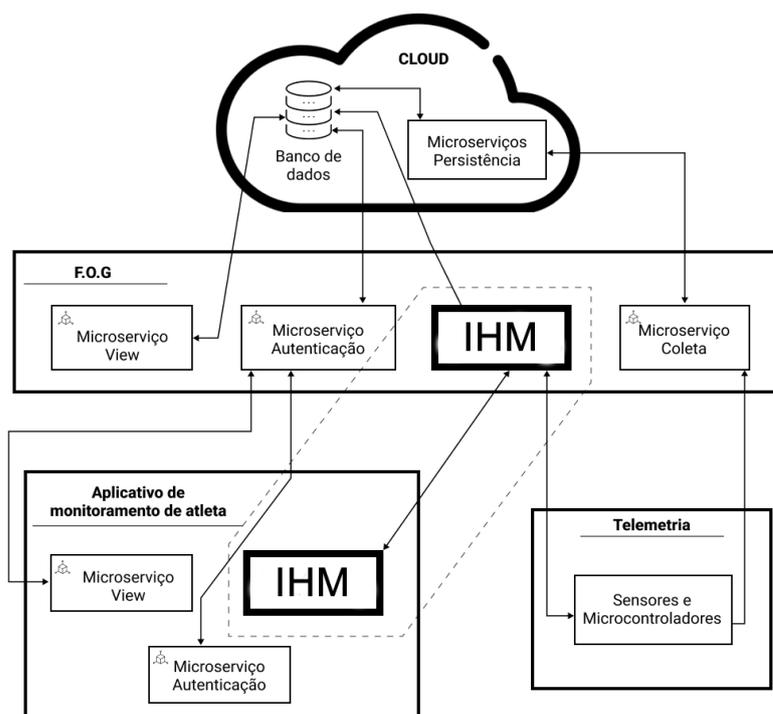
Falhas são inevitáveis, mas as consequências das falhas, ou seja o colapso do sistema, a interrupção no fornecimento do serviço e a perda de dados, podem ser evitadas pelo uso adequado de técnicas viáveis e de fácil compreensão. O conhecimento dessas técnicas habilita o usuário a implementar as mais simples, ou exigir dos fornecedores soluções que as incorporem. Entretanto, as técnicas que toleram falhas tem um custo associado. O domínio da área auxilia usuários e desenvolvedores de sistemas a avaliar a relação custo benefício para o seu caso específico e determinar qual a melhor técnica para seu orçamento (WEBER, 2003).

O sistema proposto possui uma interface de interação com o usuário, essa interface é denominada Aplicativo de Monitoramento de Atleta (AMA). Através do AMA, que permite a coleta de informações relevantes para o início da atividade física. Teremos uma Interação Humano-Computador (IHC) através do AMA. A interface vai coletar os dados da arena e da modalidade

onde o atleta vai realizar seu treino, a partir desse momento o sistema verifica quais sensores estão disponíveis através de uma rotina de testes para verificar se os sensores estão funcionando ou estão com falhas e retorna com a resposta que o treinamento pode iniciar e mostra quais sensores estarão disponíveis para aquele monitoramento. O AMA também é a interface responsável por fornecer dados estatísticos dos treinos e por fim fornecer uma análise de desempenho. Dessa forma, o treinamento será monitorado em todo o seu percurso.

O sistema possui quatro ambientes principais. Dentre eles, temos o ambiente da FOG, telemetria, aplicativo e Cloud conforme ilustra a Figura 1. O ambiente do aplicativo é responsável interface entre o atleta e a Fog. A Fog é responsável pelos micro serviço de coleta, micro serviço de autenticação. A Telemetria abriga os sensores utilizados para monitoramento e seus respectivos microcontroladores. Por fim, a Nuvem abriga os micro serviços relacionados à persistência de dados. Estes componentes serão descritos em mais detalhes ao longo deste capítulo.

Figura 1 – Visão Geral do Sistema



Fonte: Elaborado pelo Autor (2022)

O fluxo começa onde o usuário escolhe o local de treinamento (ou o aplicativo reconhece a arena se o GPS estiver ativado) e a modalidade que vai ser monitorada. Em seguida entra em ação as técnicas de tolerância a falhas, onde ela verifica o modelo de dados da modalidade escolhida, verifica quais sensores estão disponíveis para a coleta de dados e retira da hibernação os sensores que serão utilizados. As técnicas acontecem em diversas partes do software e hardware. No início do treinamento é verificado cinco situações.

- Sensores essenciais não aptos (não será possível fazer o monitoramento);

- Sensores essenciais ativos (monitoramento pode ser iniciado);
- Sensores essenciais e sensores ambientes ativos;
- Sensores essenciais e sensores secundários ativos;
- Todos os sensores ativos (monitoramento pode ser iniciado).

4.2 Técnicas de Tolerância a Falhas do Sistema

Redundância é o requisito básico para implementação de sistemas tolerantes a falha. Uma das técnicas de tolerância a falhas utilizado no protótipo foi a redundância de hardware, para detectar uma falha no hardware e alternar instantaneamente para um componente de hardware redundante, seja o componente com falha um processador, uma fonte de alimentação ou um subsistema de armazenamento.

Foi utilizado uma rede mesh, do inglês, significa malha. Isso quer dizer que a rede cria uma malha através dos seus dispositivos para a comunicação entre os microcontroladores. Essa rede é inteligente, então conforme você vai acrescentando ou retirando um dispositivos, ela mesma se organiza para que a rede seja eficiente. Ou seja, ela decide em qual roteador o dispositivo deve se conectar. Essa verificação é feita em tempo real, sempre que um microcontrolador falhar, ele é retirado da rede de forma automática, e se um microcontrolador voltar a funcionar, é colocado na rede de automaticamente.

Utilizamos também watchdog, basicamente esse sistema reinicia periodicamente o sistema para que evite um travamento (Time Out). No caso de um travamento ou mal funcionamento do sistema que esta em execução, o watchdog deixará de ser reiniciado (sistema esta travado), seu temporizador irá expirar, e ele tomará uma decisão, que normalmente é reiniciar o sistema. O watchdog pode ser implementado no hardware ou no software. No caso do sistema que estamos apresentando implementamos um temporizador interno via software que em determinados períodos e somente quando o sistema esta em standby, esse temporizador reinicia o sistema. Caso ocorra um travamento o tempo desse temporizador ira expirar e o watchdog ira tomar a decisão de reiniciar o sistema a fim de se recuperar de possíveis falhas.

4.3 Funcionamento do Sistema

O sistema entra em funcionamento quando o atleta utiliza seu Smartphone e entra de forma autenticada no AMA e escolhe em qual Arena e modalidade irá treinar. A tela inicial do aplicativo consta na figura 2.

O micro serviço de autenticação cria uma sessão e envia uma requisição para o Servidor informando que um atleta quer treinar, por sua vez o micro serviço verifica junto com a telemetria quais sensores estão aptos para fazer o monitoramento e responde a requisição, o atleta é informado que já pode iniciar o seu treinando e quantos sensores serão utilizados para fazer

Figura 2 – Tela Inicial do Aplicativo



Fonte: Elaborado pelo Autor (2022)

o seu monitoramento, e o micro serviço de Coleta estará apto a receber os dados do treinamento. Assim que o atleta inicia o seu treinamento, os sensores responsáveis pela identificação começam a monitorar a atividade, temos também os sensores de ambiente, que irão funcionar 24 horas. A cada leitura de dados será enviada para a FOG onde o micro serviço de coleta será o responsável por validar e enviar para o micro serviço de persistência que fica na Cloud. No AMA, existe uma opção de verificar dados em tempo real. Nesse caso, o micro serviço de autenticação vai informar que existe uma sessão aberta para aquele atleta e será feita uma requisição para a Cloud e o resultado será mostrado no AMA. Mas todos os dados de treinamentos estarão armazenados na Cloud para consulta futura do atleta e será possível fazer a análise de desempenho.

Assim que o atleta inicia o seu treinamento, os sensores responsáveis pela identificação começam a monitorar o tempo das corridas, temos também os sensores de ambiente, que irão funcionar 24 horas e não identifica nenhum atleta. A cada leitura de dados será enviada para a FOG onde o micro serviço de coleta será o responsável por validar e enviar para o micro serviço de persistência que fica na Cloud. No AMA, existe uma opção de verificar dados em tempo real. Nesse caso, o micro serviço de autenticação vai informar que existe uma sessão aberta para aquele atleta e será feita uma requisição para a Cloud e o resultado será mostrado no AMA. Mas todos os dados de treinamentos estarão armazenados na Cloud para consulta futura do atleta e será possível fazer a análise de desempenho.

4.3.1 Regras da coleta de dados do treinamento

Essas regras acontecem dentro da rede mesh. O sistema verifica via hardware se os sensores estão aptos ou inaptos para registrar o monitoramento do atleta. Essa verificação é feita de forma automática e sem interação humana.

As regras são aplicadas após o atleta identificar o local e qual modalidade será monitorada, com essas informações o sistema solicitará o status de todos os sensores que estão aptos ao monitoramento. As regras serão aplicadas nesse momento, entre a resposta da solicitação dos status dos sensores que serão as seguintes:

- Regra 1: Os sensores essenciais não estão aptos e não será feita o monitoramento. Essa regra é a única que não gera dados para a persistência devido a falha em sensores principais da arena.
- Regra 2: Onde somente os sensores essenciais estão aptos ao monitoramento. Nessa regra técnicas avançadas de treinamento (p.ex., treinamento intervalado) não podem ser monitoradas, pois os sensores secundários não estão aptos. Mais o treinamento será monitorado sem as informações das parciais da modalidade e nessa regra os sensores ambientais não estão aptos, ou seja, não são registrados os dados de temperatura e umidade da arena.
- Regra 3: Onde apenas os sensores essenciais e os sensores de ambiente estão aptos ao monitoramento. Nessa regra apenas os sensores secundários não estão aptos, tornando possível apenas o monitoramento básico da modalidade, mais o monitoramento simples da modalidade é acrescido dos dados ambientais (p.ex., temperatura e umidade).
- Regra 4: Onde apenas os sensores essenciais e os sensores secundários estão aptos ao monitoramento. Nessa regra técnicas avançadas de monitoramento da modalidade escolhida podem ser utilizadas. Apenas os dados ambientais não são capturados, mas em nada interfere em nada para que o treinamento intervalado aconteça.
- Regra 5: Onde todos os sensores estão aptos ao monitoramento. Nessa regra além do treinamento intervalado ser monitorado, os dados ambientais são coletados. O relatório de todas as regras, é o mais completa de todos. O atleta poderá verificar a sua performance baseado na temperatura e umidade da arena.

A partir da regra 2 a persistência de dados é realizada com base na regra da coleta de dados do treinamento quando foi definida. Nessa etapa apenas uma regra será executada pelo sistema, sendo a regra 1 a única que encerra o ciclo computacional, pois é a única regra que não pode monitorar nesse evento.

4.4 Micro Serviços

No trabalho proposto, temos a atuação de vários micro serviços. Cada um com sua função específica na arquitetura, são eles:

- O micro serviço de autenticação interage com a AMA e com a FOG. É responsável por criar e destruir a sessão de treinamento do atleta. Além disso, faz uma requisição na FOG que por sua vez, verifica junto a telemetria sobre quais sensores estão disponíveis para o treinamento e exibe essa informações para o atleta pelo aplicativo.
- O micro serviço de coleta é encontrado na FOG, é o responsável por receber os dados da telemetria (via rádio frequência fechada, utilizando o formato JSON na serialização), valida os dados recebidos (verifica se a sessão do atleta está ativa e verifica a tomada de tempo está correta) e após a validação é enviado via JSON (utilizando do webservice) para o micro serviço de persistência que encontra-se na Cloud.
- E temos o micro serviço de Persistência que é o responsável por persistir as informações coletadas. Na fase inicial do processo de autenticação é definido qual é a coleção de dados da modalidade onde as informações serão salvas. Esse micro serviço vai ter uma interação com uma linguagem de programação para fazer as inserções no banco de dados.
- E por fim temos o micro serviço de Visualização, que pode ser acionado pelo atleta ou pelo seu treinador através do aplicativo AMA. Informações do treinamento podem ser consultados e comparados e ainda poderá ser acompanhado o treinamento que está sendo executado em tempo real através da sessão ativa do treinamento.

4.5 Telemetria

No nível da telemetria encontram-se os sensores, os microcontroladores e a comunicação. Temos sensores com identificação e os sensores sem identificação.

- Sensores com Identificação: Esses sensores ficam hibernados até que são requisitados pelo sistema, logo após serem requisitados, os sensores estão aptos a identificar e registrar os dados dos atletas, assim que for registrado o tempo do atleta, os sensores transmitem os dados para o micro serviço de coleta que fica na FOG.
- Sensores sem identificação: Esses sensores ficam transmitindo seus dados a cada 90 segundos para o micro serviço de coleta independente se tem ou não atletas treinando.

Esses dados podem ser utilizados por todos os atletas. A telemetria usa da serialização de bytes através da radiofrequência fechada para se comunicar com o micro serviço de coleta. Onde as vantagens são:

- Alto nível de segurança;
- Baixo consumo de energia;
- Compatibilidade com vários dispositivos e protocolos.

A telemetria usa da serialização de bytes através da radiofrequência fechada para se comunicar com o micro serviço de coleta. Onde as vantagens são:

- Alto nível de segurança;
- Baixo consumo de energia;
- Compatibilidade com vários dispositivos e protocolos. Na arquitetura proposta, ocorre um grande fluxo de pequenos pacotes de dados e operações e a serialização é um excelente recurso neste caso.

Na comunicação entre os sensores será utilizado uma rede mesh. Caso um dos sensores apresente uma falha, o sistema automaticamente muda o caminho dentro da rede mantendo a comunicação entre os outros sensores disponíveis e funcionais.

4.6 Sensores

O sensor basicamente é um dispositivo que tem a função de detectar e responder com eficiência algum estímulo. Existem vários tipos de sensores que respondem à estímulos diferentes. Depois que o sensor recebe o estímulo, a sua função é emitir um sinal que seja capaz de ser convertido e interpretado pelos outros dispositivos (MATTEDE, 2018). Temos vários sensores à disposição na arena de treino como: Sensor de Temperatura e Umidade, Velocidade do Vento, Chuva, GPS (esses sensores são para registrar dados do ambiente) e temos os sensores infravermelhos, RFID, NFC (que são sensores para a tomada de tempo e identificar os atletas) e além desses usaremos os dispositivos vestíveis.

- Dispositivos Vestíveis - Integrados com biossensores eletrônicos e ópticos podem fornecer dados em tempo real sobre o eletrofisiológico ou estado bioquímico de um paciente em configurações de ponto de atendimento ou na clínica. Esses biossensores podem ser incorporados em dispositivos eletrônicos tatuagens / carimbos, remendos, próteses, têxteis, pulseiras e lentes de contato para formar contato conformado com tecido biológico ou fluidos corporais. Esses biossensores podem ser alimentados sem fio ou funcionam com baterias leves que podem ser integradas perfeitamente em dispositivos vestíveis. Os dados físicos e bioquímicos podem ser transmitido sem fio para o paciente ou outro dispositivo vestível para alcançar sistemas terapêuticos de circuito fechado (YETISEN et al., 2018). Dentre várias tecnologias existentes, para esse trabalho proposto podem ser utilizados os sensores para identificar quem é o atleta, qual o tempo percorrido, temperatura e umidade do ambiente, velocidade do vento dentre outros.

- Temperatura - O objetivo do Sensor de Temperatura é aferir constantemente a temperatura do ambiente. Esses dados registrados irão constar nos registros dos dias de treinamento ou competições. Um dia muito quente, ou um dia muito frio vai interferir nos resultados obtidos.
- Infravermelho - O sensor de infravermelho vai detectar o movimento de atletas e dessa forma contabilizar o tempo de saída como o tempo de chegada em alguns esportes (no caso do atletismo por exemplo).
- RFID - É um sensor de Rádio Frequência que vai servir para identificar os atletas de forma individual em diversos lugares na arena.
- NFC - É uma tecnologia de comunicação sem fio entre dois dispositivos fisicamente próximos entre si, a ação é estabelecida automaticamente.
- Sensor Cardíaco - Esse sensor monitora o ritmo cardíaco de diversas atividades.
- GPS - O Sistema de Posicionamento Global é uma tecnologia de navegação baseada em satélite e agora é utilizada cada vez mais nos esportes. O desempenho do atleta é coletado nos treinos e nas competições. Dessa forma os cientistas de dados podem gerar relatórios diversos para técnicos e treinadores.

Cada sensor terá à sua disposição um microcontrolador que será o responsável em enviar os dados coletados para a FOG utilizando um protocolo sem fio. Dessa forma, garantimos uma velocidade no envio de dados, pois o microcontrolador terá o seu uso exclusivo focado no sensor evitando atrasos na transmissão dos dados. Foi utilizado o microcontrolador ATmega328P, conforme a figura 3 podemos ver as portas e os pinos de tensão. No total, existem 23 entradas/saídas programáveis, para uso geral. Estes pinos também podem ser programados para funções alternativas, como comunicação serial, ADC, I2C, Xbee.

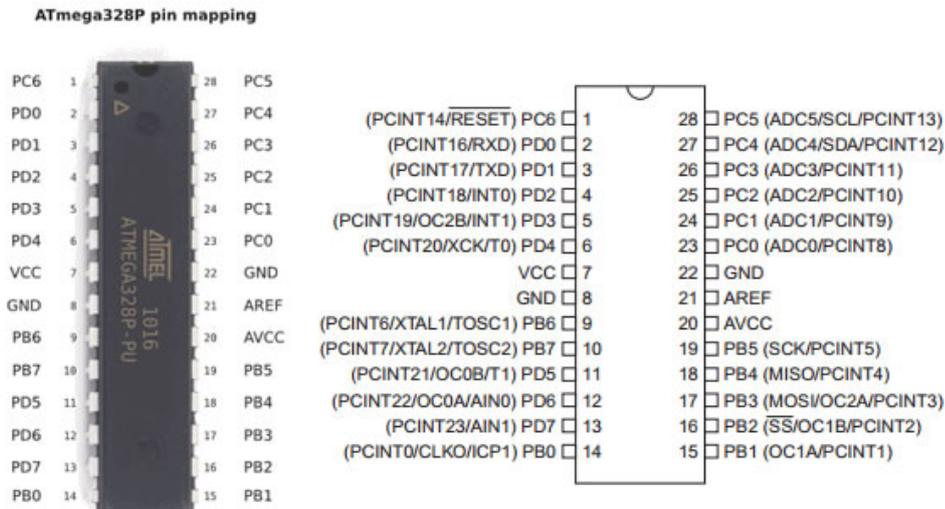
4.7 Microcontrolador

Cada sensor terá a sua disposição um microcontrolador que será o responsável em enviar os dados coletados para a FOG utilizando um protocolo sem fio. Dessa forma, garantimos uma velocidade no envio de dados, pois o microcontrolador terá o seu uso exclusivo focado no sensor evitando atrasos na transmissão dos dados.

Foi utilizado o microcontrolador ATmega328P, conforme a figura 3 podemos ver as portas e os pinos de tensão. No total, existem 23 entradas/saídas programáveis, para uso geral. Estes pinos também podem ser programados para funções alternativas, como comunicação serial, ADC, I2C, Xbee.

Os componentes de hardware só apresentam taxa de defeitos constante durante um período de tempo chamado de vida útil, que segue uma fase com taxa de falhas decrescente chamada

Figura 3 – DataSheetGO



Fonte: <https://datasheetgo.com/atmega328-pdf-8-bit-avr-risc-based-microcontroller> (2020)

de mortalidade infantil. Para acelerar a fase de mortalidade infantil, os fabricantes recorrem a técnicas de burn-in, onde é efetuada a remoção de componentes fracos pela colocação dos componentes em operação acelerada antes de colocá-los no mercado ou no produto final (WEBER, 2003).

4.8 Persistência dos Dados Coletados

Persistência de dados é a garantia de que um dado foi salvo e que poderá ser recuperado quando necessário no futuro (PEREIRA, 2018). Um serviço importante que vai ser executado na Fog é receber os dados dos sensores, processá-los e depois gravá-los na Cloud. Para gerenciar e manipular o banco de dados do protótipo foi utilizado o SGBDs (Sistema Gerenciadores de Banco de Dados) que irá permitir que os dados coletados sejam organizados e persistidos, mas a arquitetura é compatível com outros tipos de banco de dados como, por exemplo, o MongoDB (que é NoSQL). Foi utilizado um banco de dados relacional cuja vantagem é que posteriormente pode ser utilizado para mineração de dados. Um aplicativo será usado para recuperar as informações persistidas. Os atletas deverão ter um cadastro no aplicativo para recuperar seus dados para visualizações futuras.

5 ESTUDO DE CASO

O sistema computacional proposto tem como principal foco a utilização de tolerância a falhas para o gerenciamento do processo de coleta de dados de treinamento de atletas. Nesse sentido, o foco da avaliação se encontra em identificar o comportamento do mecanismo composto em diferentes cenários de utilização.

O estudo de caso desenvolvido utiliza como contexto a modalidade de corrida de 100 metros rasos (atletismo). Em particular, utiliza-se como contexto do experimento a técnica do treinamento intervalado. Este método foi concebido unicamente com o intuito de permitir que uma determinada intensidade de treino (por exemplo, a velocidade de corrida de 12 km/h) seja mantida com maior volume (maior tempo) do que aquele possível de se permanecer de forma contínua. Portanto, em tal modalidade, tem-se como requisito mínimo sensores para capturar os tempos de início e fim da atividade e, para um acompanhamento mais efetivo, sensores para a captura dos tempos parciais da atividade. Somente isso justifica a adoção do método intervalado (MASCARENHAS, 2020). Os benefícios do treinamento intervalado são:

- Treino de corrida mais eficiente em menos tempo;
- Queima de gordura acentuada para os atletas;
- Aceleração do metabolismo;
- Aumento no condicionamento físico.

Dentro do cenário proposto, os sensores de início e fim da atividade compõem o conjunto de “sensores essenciais”, enquanto os sensores de tempo parciais compõem os “sensores secundários”. Um treinamento simples de atletismo pode ser monitorado apenas com o conjunto de sensores essenciais. Mas, caso os sensores de tempo parciais estejam disponíveis no ambiente, torna-se possível o acompanhamento de um treino intervalado. Por fim, o cenário ainda compreende sensores de temperatura e umidade no contexto dos “sensores de ambiente”, que podem conter informações relevantes para um acompanhamento mais preciso do desempenho de práticas esportivas.

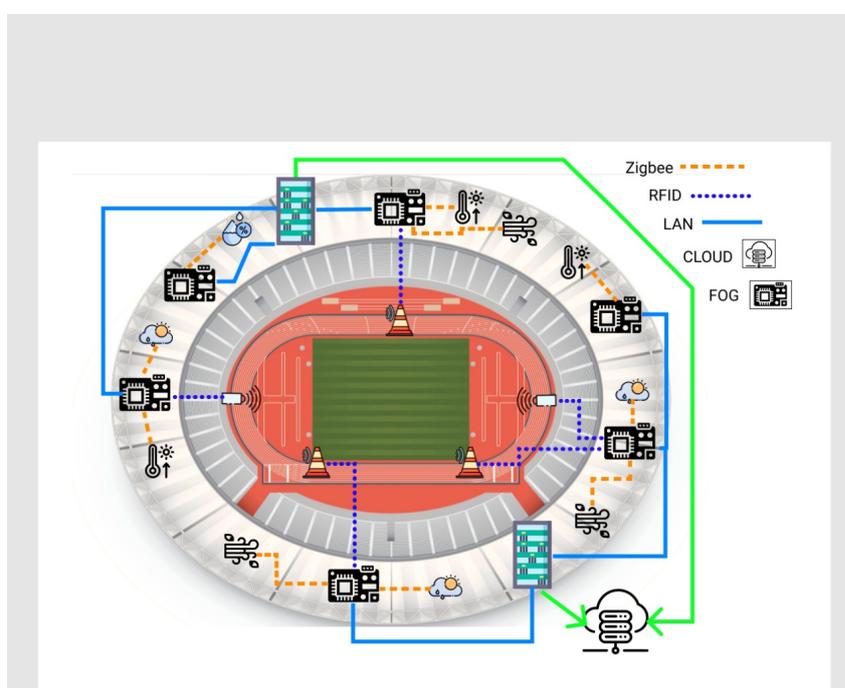
O objetivo do estudo de caso é verificar se a arquitetura descrita é uma solução viável para a questão de pesquisa proposta. Neste estudo de caso, foi implementada uma prova de conceito do sistema computacional proposto, onde é feita a automação do monitoramento do treinamento de atletas de alto desempenho, utilizando recursos IoT. Esse cenário do estudo de caso vem para testar a capacidade da tolerância a falhas em resolver o problema de falta de sensor e mesmo assim permitir o monitoramento do treinamento do atleta.

Nesse sentido, o sistema propõe auxiliar o atleta/treinador com informações importantes do treinamento, além do tempo inicial e do tempo final, as informações dos tempos parciais irão contribuir nas tomadas de decisões sobre o treinamento. O treinamento pode ser prolongado ou

cancelado baseado nas informações fornecidas pela arquitetura e dessa forma evitando fadiga ou até lesões do atleta.

No estudo de caso, serão coletados dados simulado de atletas e o sistema de tolerância a falhas, mitiga todos os problemas com sensores que ocorram durante topo o processo do monitoramento. Dessa forma, as tomadas de tempo, dados do ambiente serão coletados e disponibilizados no Aplicativo (AMA). A figura 4 apresenta um diagrama ilustrando um possível cenário para a aplicação do estudo de caso proposto..

Figura 4 – Cenário do Estudo de Caso



Fonte: Elaborado pelo Autor (2022)

5.1 Modalidade Escolhida

A corrida de 100 metros é uma modalidade olímpica de velocidade no atletismo. A mais curta das distâncias disputadas em eventos ao ar livre, é também uma das mais populares modalidades do esporte. Os atletas largam de blocos firmados no chão ao som de um sinal de partida e correm dentro de raias demarcadas na pista. As solas têm pregos de comprimento máximo fixado em 8,4 milímetros, e a espessura da sola não pode ultrapassar treze milímetros. O vencedor é determinado pelo primeiro a cruzar o torso na linha de chegada; pernas e braços são desconsiderados. Quando a avaliação do vencedor não é possível ao olho humano, é usado um sistema de photo finish para determinar o campeão (OTD (2020)).

5.2 Dados Coletados

O sistema coleta as informações necessárias para avaliar o desempenho do atleta (p.ex., tempo de passagem, distância de saltos, dados ambientais) além do identificador único de sensores a fim de permitir identificar a qual atleta os dados coletados pertencem. Os dados do treinamento serão vinculados no RFID (que será única) e o atleta poderá visualizar seus treinamentos através do AMA. O sistema de tolerância a falhas estão presentes em todas as etapas do monitoramento, mesmo o sistema não estando sendo utilizado pelos atletas. A cada novo atleta que for utilizar o sistema é criado uma sessão do atleta que irá acompanhar o atleta e todo o seu treinamento. Se por algum motivo o atleta desistir do seu treinamento e sair da arena sem finalizar o seu treinamento pelo aplicativo, o sistema irá aguardar por 25 minutos, e se não receber nenhuma informação desse atleta, a sessão desse será fechada e será adicionado que a sessão foi encerrada por "DESISTÊNCIA DO TREINAMENTO". Cabe ressaltar que, no cenário de testes desenvolvido para avaliação da prova de conceito, não houve a coleta de dados reais de atletas. Todas as ativações dos sensores foram realizadas de forma simulada, de modo que os dados coletados em um ambiente similar àquele encontrado em um treinamento, mas sem exigir que atletas reais utilizassem a aplicação.

5.3 Cones IoT

Os cones foram preparado conforme ilustra a figura 5. Temos a opção de alimentação do cone via cabo 110V ou baterias de 9V. Na parte externa do cone temos um sensor infravermelho e três leds (nas cores verde, amarela e vermelha) e um leitor RFID.

Figura 5 – Cones IoT, visão Externa.



Fonte: Autores (2021)

O cone identificado com o Pi é responsável em identificar o atleta e também o responsável pelo seu tempo inicial e envia as informações em tempo real para o cone identificado como Pn que é o responsável por coletar o dado de tempo parcial (podem ser diversos cones, quanto mais cones, maior será o nível de detalhe dos dados coletados pelo sistema) e esses dados são enviados em tempo real para o cone denominado Pf, que além de receber os dados dos cones anteriores é o responsável por fechar o tempo de corrida do atleta e processa o tempo final. Esses dados são enviados para o micro serviço de coleta.

O micro serviço de coleta que vai ser o responsável por receber e validar os dados coletados, além disso será o responsável em adicionar os dados coletados do ambiente, após todo esse processo, os dados serão enviados para o micro serviço de persistência que encontra-se na Cloud. O micro serviço de persistência vai receber os dados validados do micro serviço de coleta, inclusive com a informação de qual coleção de dados da modalidade vai ser utilizada, é será o responsável por fazer a persistência no banco de dados (MySQL).

Dentro dos cones (conforme ilustra a figura 6) temos os seguintes hardwares: Waldunano, Xbee, sensor infravermelho, leds, resistores, receptor NFC/RFID e o sistema de alimentação do dispositivo (os hardwares dos cones são exatamente iguais, o que difere é a programação).

Figura 6 – Cones IoT, visão Interna.



Fonte: Elaborado pelo Autor (2022)

5.4 Protocolo de Comunicação

Para avaliar o estudo de caso proposto, foi desenvolvido o protótipo do sistema computacional proposto na Capítulo 4, incluindo os componentes de software e hardware necessários para a realização do monitoramento de atividades de atletismo através de treinamentos intervalados.

Em termos de hardware, o protótipo utiliza o protocolo ZigBee (radiofrequência fechada). O ZigBee é um protocolo de comunicação sem fios destinado a aparelhos IoT, com foco em dispositivos de baixa potência. Esses, por sua vez, são equipamentos que possuem uma demanda energética limitada, com autonomia que pode chegar a anos com uma única bateria (SOUSA, 2018), é utilizada a serialização de bytes entre os cones e por fim no micro serviço de persistência é utilizado no format JSON (através de Web Services).

Os sensores enviam os dados para o micro serviço de coleta, que é o responsável por receber e validar os dados coletados, além disso, será o responsável em adicionar os dados coletados do ambiente. Após esse processo, os dados serão enviados para o micro serviço de persistência que se encontra na Cloud. O micro serviço de persistência vai receber os dados validados do micro serviço de coleta, inclusive com a informação de qual coleção de dados da modalidade vai ser utilizada, é será o responsável por fazer a persistência no banco de dados (MySQL).

O cone é alimentado por baterias de 9V, por que o equipamento não requer muita energia para o seu funcionamento (duração de 4 horas sem recarregar). Enquanto o dispositivo não estiver em uso, o sistema estará hibernando. Mas o cone pode ser alimentado por energia convencional e dessa forma as baterias são recarregadas. A vantagem do uso das baterias, é que se por algum motivo haja uma queda da energia, as baterias irão entrar em funcionamento e garantir o funcionamento do sistema sem problema nenhum.

Todos os sensores são verificado constantemente, se por algum motivo, algum sensor não responder a verificação, esse sensor será ignorado pelo sistema e será aberto um chamado para a equipe de manutenção. Assim que o sensor entrar em funcionamento, o sistema irá reconhecer o seu funcionamento e o sensor voltará fazer parte do monitoramento.

5.5 Metodologia de Avaliação

O sistema proposto tem como principal foco a utilização da tolerância a falhas para o gerenciamento do processo de coleta de dados de treinamento de atletas. Nesse sentido, o foco da avaliação se encontra em identificar o comportamento do mecanismo proposto em diferentes cenários de utilização. Para tal, foram definidos cinco cenários principais para avaliação. Cada um dos cenários representa uma combinação diferente de três conjuntos de sensores. Os “sensores essenciais” são aqueles estritamente necessários para o monitoramento de uma modalidade em particular. Os “sensores secundários” permitem um monitoramento mais detalhado de uma modalidade, entretanto, não são obrigatórios para realização de um monitoramento mínimo das atividades. Por fim, os “sensores de ambiente” tem como foco o monitoramento de elementos como a temperatura ou umidade e não são estritamente necessários para que seja possível um monitoramento mínimo de uma modalidade.

Além desses cenários que são testados no inicio dos treinamentos referente a tolerância a falhas, em todo o processo de coleta de dados, os sensores são testados constantemente, para verificar o seu funcionamento. Entre os mecanismos de controle a tolerância a falhas utilizamos

a redundância de hardware, a redundância de software e o watchdog.

O watchdog se trata de um mecanismo baseado em temporizador que é periodicamente reiniciado para garantir que o sistema está operando corretamente. No caso de um travamento ou mal funcionamento da do sistema que esta em execução, o watchdog deixará de ser reiniciado (sistema esta travado), seu temporizador irá expirar, e ele tomará uma decisão, que normalmente é reiniciar o sistema. O watchdog pode ser implementado no hardware ou no software. No caso do sistema que estamos apresentando implementamos um temporizador interno via software que em determinados períodos e somente quando o sistema esta em standbay, esse temporizador reinicia o sistema. Caso ocorra um travamento o tempo desse temporizador ira expirar e o watchdog ira tomar a decisão de reiniciar o sistema a fim de se recuperar de possíveis falhas.

O estudo de caso desenvolvido utiliza como contexto a modalidade de 100 metros rasos. Em particular, utiliza-se como contexto do experimento a técnica do treinamento intervalado. Dentro do cenário proposto, os sensores de início e fim da atividade compõem o conjunto de “sensores obrigatórios”, enquanto os sensores de tempo parcial compõem os “sensores adicionais”. Um treinamento simples de atletismo pode ser monitorado apenas com o conjunto de sensores obrigatórios. Mas, caso os sensores de tempo parciais estejam disponíveis no ambiente, torna-se possível o acompanhamento de um treino intervalado. Por fim, o cenário ainda compreende sensores de temperatura e umidade no contexto dos sensores de “ambiente”, que podem conter informações relevantes para um acompanhamento mais preciso do desempenho de práticas esportivas.

Para avaliar o estudo de caso proposto, foi desenvolvido um protótipo do sistema proposto no capítulo 4, incluindo os componentes de software e hardware necessários para a realização do monitoramento de atividades de atletismo através de treinamentos intervalados. Em termos de hardware, o protótipo utiliza o protocolo ZigBee (radiofrequência fechada). O ZigBee é um protocolo de comunicação sem fios destinado a aparelhos IoT, com foco em dispositivos de baixa potência. Esses, por sua vez, são equipamentos que possuem uma demanda energética limitada, com autonomia que pode chegar a anos com uma única bateria (SOUSA, 2018). É utilizada a serialização de bytes entre os cones e por fim no micro serviço de persistência é utilizado no format JSON (através de Web Services).

Os sensores enviam os dados para o micro serviço de coleta, que é o responsável por receber e validar os dados coletados, além disso, será o responsável em adicionar os dados coletados do ambiente. Após esse processo, os dados serão enviados para o micro serviço de persistência que se encontra na Cloud. O micro serviço de persistência vai receber os dados validados do micro serviço de coleta, inclusive com a informação de qual coleção de dados da modalidade vai ser utilizada, é será o responsável por fazer a persistência no banco de dados (MySQL).

5.6 Cenário de ambiente controlado

O protótipo foi implantado em um ambiente controlado, o qual foi então utilizado para testes do processo de tolerância a falhas e coleta de dados dos sensores. A execução do processo de tolerância a falhas e da coleta de dados dos sensores foi automatizado para permitir a coleta eficiente de dados em múltiplas execuções de “sequências de treinamento” simuladas. Tais sequências de treinamento foram divididas entre cinco cenários.

- O cenário 1 - há falhas nos sensores essenciais, de modo que a arquitetura deve identificar a não possibilidade da realização do processo de monitoramento.
- No cenário 2 - apenas o conjunto de sensores essenciais está operando, sendo possível a utilização de um acompanhamento “degradado” do desempenho do atleta.
- No cenário 3 - além dos sensores essenciais e os sensores ambientais estão operando, nesse cenário não é possível monitorar o treinamento intervalado.
- No cenário 4 - além dos sensores essenciais e os sensores secundários estão operando, nesse cenário o monitoramento do treinamento intervalado é realizado.
- No cenário 5 - todos os grupos de sensores estão operando corretamente, de modo que é possível a utilização do treinamento intervalado juntando com os dados de temperatura e umidade.

Os experimentos realizados visam verificar a correta operação do sistema, no sentido de identificar se o modo de monitoramento adequado para cada um dos cenários de disponibilidade de sensores descritos. Além disso, foram analisados o tempo necessário para a execução do processo de tolerância a falhas em cada um dos cenários. Os resultados obtidos nessas avaliações serão apresentados na próxima seção.

5.7 Cenário de teste de falhas no início do treinamento

O sistema proposto foi implementada conforme descrito nas seções anteriores. Foram também implementados os dispositivos de sensoriamento necessários para o monitoramento da modalidade de 100 metros rasos conforme proposto no estudo de caso. Ressalta-se que os testes realizados com estes sensores utilizaram um ambiente simulado onde não foi necessária a interação dos atletas para a geração dos dados. Entretanto, houve a interação dos sensores com o sistema computacional da mesma forma que seria esperada no caso da utilização do sistema em um ambiente real.

O protótipo foi implantado em um ambiente controlado, o qual foi então utilizado para testes do processo de tolerância a falhas e coleta de dados dos sensores. A execução do processo de

execução de tolerância a falhas e da coleta de dados dos sensores foi automatizado para permitir a coleta eficiente de dados em múltiplas execuções de “sequências de treinamento” simuladas.

Os experimentos realizados visam verificar a correta operação do sistema, no sentido de identificar se o modo de monitoramento adequado para cada um dos cenários de disponibilidade de sensores descritos. Além disso, foram analisados o tempo necessário para a execução do processo de testes de falhas em cada um dos cenários. Os resultados obtidos nessas avaliações serão apresentados na próxima seção.

Em um cenário de utilização normal, o atleta com o RFID colocado no tênis, acessa o AMA apenas colocando o código do RFID para ter acesso da tela principal e selecionar qual modalidade irá iniciar o treino, após alguns segundos o sistema computacional, vai responder quantos sensores estão ativos e que o atleta pode começar o seu treinamento. O atleta passando na frente do primeiro cone acionará o tempo por um infravermelho, os cones secundários irão pegar os dados parciais do percurso e o último cone é responsável por fechar o tempo e fazer o processamento do cálculo e envia esses dados para a FOG, o treinador irá receber essas informações em tempo real, em um ambiente seguro, rápido e gastando pouca energia, podendo ser utilizado por até 4 horas sem precisar recarregar as baterias. Ressalta-se que esse processo de utilização foi simulado durante a realização dos experimentos, porém sem que fosse realizado o monitoramento de dados reais de atletas.

Dependendo do cenário avaliado, alguns dos sensores foram desativados randomicamente a fim de simular problemas na infraestrutura de monitoramento. As métricas propostas foram coletadas de acordo com os cinco cenários descritos acima.

Os cones podem ser movimentados sem problemas, aumentando ou diminuindo a distância percorrida pelo atleta. Fizemos teste de várias distâncias entre 5m até 50m, todos efetuados com sucesso. O processo nem é percebido pelo usuário, esse protótipo terá melhorias que iremos tratar nas considerações finais. Os processos estão bem configurados e a prova de falhas, o sistema vai medir tempos extremamente curtos ou tempos longos. Funciona em área aberta ou fechada (registrando os milésimos de segundos).

5.8 Métricas

A métrica principal foi criada para avaliar o sistema proposto. Tempo de resposta da tolerância a falhas para o início do treinamento; Essa métrica avalia o intervalo de tempo entre a seleção da modalidade e local até que o sistema computacional e os sensores estejam prontos para realizar a coleta dos dados.

Para fins das coletas das métricas da tolerância a falhas foram realizados testes com cinco cenários (ambos cenários foram registrados 500 simulações).

Temos cinco cenário que foram utilizados para gerar a métrica utilizada.

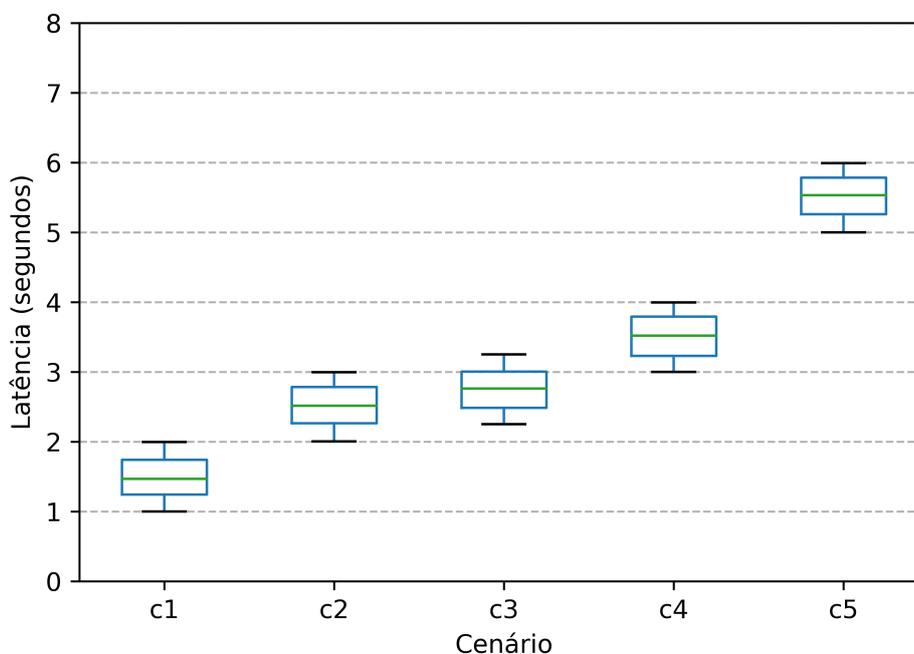
- O cenário 1, considera o caso em que todos os grupos de sensores podem sofrer algum tipo de falha. Em particular, este cenário foi desenhado para que houvesse uma predominância

dos casos em que algum dos sensores essenciais não estaria disponível, de modo que não seja possível a realização do monitoramento de acordo com a especificação da modalidade selecionada. A Figura 7 apresenta o tempo médio para a realização da tolerância a falhas no cenário 1. Neste cenário, observou-se um tempo de execução médio de 1,470 segundos, onde o tempo máximo ficou em 1,995 segundos e o tempo mínimo ficou em 1,000 segundo.

- O cenário 2 considera o caso que somente os sensores essenciais estão aptos para o monitoramento. A Figura 7 apresenta o tempo médio para a realização da tolerância a falhas no cenário 2. Neste cenário, observa-se um tempo de execução média de 2,514 segundos, onde o tempo máximo ficou em 2,996 segundos e o tempo mínimo ficou em 2,006 segundos.
- O cenário 3 os sensores essenciais e os sensores de ambiente irão funcionar perfeitamente, mas os sensores secundários foram programados para reportarem um estado de falha aleatoriamente. Em função de tais falhas, o treinamento intervalado não foi possível de ser executado em alguns casos devido à ausência dos sensores necessários. Entretanto, em todos os casos, pelo menos um acompanhamento mínimo foi possível, pois nenhum dos sensores essenciais sofreu algum tipo de falha. A Figura 7 apresenta o tempo médio de execução da tolerância a falhas para este cenário, no qual foi observada uma média de 2,767 segundos, onde o tempo máximo foi de 3,250 segundos e o tempo mínimo foi de 2,252 segundos.
- O cenário 4 os sensores essenciais e os sensores secundários estão funcionando perfeitamente, mas os sensores de ambiente foram programados para reportarem um estado de falha aleatoriamente. Em função de tais falhas, o treinamento intervalado foi possível de ser executado. Entretanto, os dados ambientais não foram registrado. A Figura 7 apresenta o tempo médio de execução da tolerância a falhas para este cenário, no qual foi observada uma média de 3,518 segundos, onde o tempo máximo foi de 3,997 segundos e o tempo mínimo foi de 3,001 segundos.
- O cenário 5 compreende a utilização dos três conjuntos de sensores para o monitoramento de atividades. Dentro do estudo de caso proposto, torna-se possível a utilização do processo de treinamento intervalado devido à presença dos sensores secundários. Neste cenário, observou-se a correta operação do sistema computacional, tanto durante o processo de tolerância a falhas quanto durante o processo de coleta de dados de todos os sensores. Além disso, foram coletados os tempos de execução do processo de tolerância a falhas. A Figura 7 apresenta a análise dos tempos de execução observados para o processo de tolerância a falhas no cenário 5. Neste cenário, observa-se um tempo de execução médio de 5,535 segundos desde a inicialização do processo até a obtenção da resposta através do aplicativo do atleta, onde o tempo máximo foi de 5,993 segundos e o

tempo mínimo ficou em 5,001 segundos.

Figura 7 – Resultado da latência



Fonte: Elaborado pelo Autor (2022)

A coleta de dados se deu de forma automatizada, de uma forma randômica foi simulada a entrada de um atleta no sistema em um dos cenários existentes. Os sensores foram acionados de forma física e foi mensurado o tempo de resposta do sistema da entrada do atleta no sistema até a resposta do início do treinamento do mesmo.

De forma geral, observa-se uma redução consistente no tempo necessário para o processo de tolerância a falhas comparando-se os resultados do Cenário 5 até ao Cenário 1. Tais resultados ocorreram devido ao menor tempo necessário para o processo de testes de falhas realize a configuração dos sensores ativos no ambiente. Isto é, quanto maior o número de sensores necessários para o processo de monitoramento da prática esportiva, maior o tempo necessário para o processo de testes de falhas. Portanto, em cenários com um maior número de sensores, é esperado que haja um tempo respectivamente maior para que a teste de falhas seja completada. Da mesma forma, com a falta dos sensores secundários permite apenas que o monitoramento simples da prática seja realizado, o processo testes de falhas é mais rápido, já que o processo de coleta de dados a ser preparado também se torna mais simples. Por fim, o Cenário 1 apresenta o menor tempo de execução justamente porque o sistema de computação detecta a falta dos sensores necessários para o monitoramento e, portanto, o monitoramento do atleta é interrompida sem que seja possível criar um ambiente para o monitoramento.

A título de complemento, foram observados os tempos necessários para a realização do processo de coleta de dados pelos sensores em cada um dos cenários válidos, isto é, os cenários

1, 2, 3 e 4. O comportamento observado nesses cenários refletiu as observações realizadas durante o processo do teste de falhas. Ou seja, nos casos em que a tolerância a falhas permitiu o monitoramento através de mais sensores e de uma técnica mais complexa, houve uma leve amplificação do tempo necessário para a realização do processamento dos dados. Entretanto, em nenhum dos cenários, o tempo necessário para a aquisição dos dados foi prejudicial ao desempenho do sistema no sentido de não permitir a análise do desempenho do atleta durante a realização do treinamento.

5.9 Comparativo com sistemas reais

Foi realizado testes comparativos com um sistema já consolidado no mercado. Nesse caso, fizemos um comparativo com o Smartwatch da Xiaomi (conforme a figura 8).

Figura 8 – Smartwatch - Relógio Inteligente Amazfit Bip U Pro (Xiaomi)



Fonte: Foto de Arquivo do Autor (2022)

No teste foi realizado a tomada de tempo e percurso longo durante 10 dias (não consecutivos). Nesses dias foram utilizando os softwares da ZEPP da Xiaomi e do AMA para registrar o monitoramento dos atletas. Foi coletado os seguintes dados:

- Data do treinamento;
- Como foi a cobertura da disponibilidade;
- O tempo do percurso;
- A distância;

- Coleta de tempos parciais;

A disponibilidade em ambos os sistemas foram de 100%. Se houve falha, os sistemas conseguiram através das técnicas de tolerância a falhas mitigá-los. Todos esses dados estão na tabela 5.

Tabela 5 – Comparativo entre Sistemas de Monitoramento

Data	Xiaomi				AMA			
	Disponibilidade	Tempo	KM	Tempo Parciais	Disponibilidade	Tempo	KM	Tempo Parciais
25/11/2022	100%	34:13	4.29	Não	100%	34:11	4.50	Sim
06/11/2022	100%	36:00	4.33	Não	100%	35:57	4.50	Sim
11/11/2022	100%	36:12	4.35	Não	100%	36:08	4.50	Sim
02/10/2022	100%	34:04	4.52	Não	100%	34:02	4.50	Sim
25/09/2022	100%	41:05	4.42	Não	100%	41:03	4.50	Sim
12/09/2022	100%	39:14	4.41	Não	100%	39:10	4.50	Sim
10/09/2022	100%	35:37	4.15	Não	100%	35:35	4.50	Sim
09/09/2022	100%	39:37	4.40	Não	100%	39:36	4.50	Sim
08/09/2022	100%	44:19	4.45	Não	100%	44:17	4.50	Sim
26/08/2022	100%	37:41	4.44	Não	100%	37:39	4.50	Sim

Fonte: Autor (2021)

O tempo houve uma pequena diferença entre os sistemas, na questão do sistema da Xiaomi, existiu um delay, por tratar de uma ação humana em acionar o relógio para encerrar o monitoramento, e no caso do AMA, o encerramento do monitoramento foi automático através do cone que coleta os dados. No quesito tempo parcial, apenas no sistema do AMA que está disponível essa informação e no quesito distância, é onde tem uma diferença importante. No caso do sistema do AMA, os cones são fixos, a distância sempre é a mesma e no sistema da Xiaomi, como precisam das informações do GPS, houve uma variação grande do percurso, mesmo sendo corrido um percurso de 4.5 km (conforme demonstra a figura 9). Nessa mesma figura percebe-se que é o mesmo percurso, mas com a variação da distância gerada pelo GPS, deu uma diferença de 5 metros entre as corridas e mais 10 metros da distância correta.

A variação foi de 4.15 km até 4.52 km, ou seja uma diferença em 370 metros. Nesse quesito o dispositivo do AMA foi preciso, pois não depende dos satélites para determinar a localização do atleta ao ar livre.

Figura 9 – Tomadas de tempo dos dia 11/11 e 09/09 de 2022



Fonte: Foto de Arquivo do Autor (2022)

6 CONCLUSÃO

A IoT está cada vez mais presente em diferentes contextos da sociedade, dentre os quais se encontra o monitoramento de práticas esportivas. O avanço da tecnologia permite o monitoramento de um conjunto cada vez maior de dados para acompanhamento da evolução de atletas. Nesse sentido, torna-se necessária um sistema que permita fazer uso de conjuntos heterogêneos de sensores para o monitoramento de modalidades específicas de esportes. Neste contexto, o presente artigo apresentou a proposta de um sistema baseada em tolerância a falhas para realizar o monitoramento da prática de esportes. Em particular, o sistema permite que diferentes técnicas de monitoramento e treinamento sejam aplicadas dependendo da modalidade e dos sensores disponíveis no local escolhido para treinamento sem interrupções em seu monitoramento.

Baseado nos testes feitos na metodologia de avaliação, ficou evidente que o tempo de resposta da tolerância a falhas do sistema proposto foi adequado levando em conta os diferentes cenários concebidos para avaliação do sistema. Além disso, observou-se que o tempo de coleta e processamento de dados permanece adequado para acompanhamento do desempenho durante a realização das atividades, mesmo em cenários requerendo técnicas de monitoramento mais complexas. Vale ressaltar que o estudo de caso testado abrange uma pequena fração do potencial do sistema proposto. Esse trabalho foi submetido em forma de artigo para o XXII Simpósio em Sistemas Computacionais de Alto Desempenho (WSCAD 2022).

Como trabalho futuro, planeja-se expandir os cenários de avaliação para outras modalidades de esporte, preferencialmente requerendo técnicas complexas de coleta e análise de dados e principalmente fazer os testes com atletas reais.

REFERÊNCIAS

- ALMEIDA, M. A. B. de; JUNIOR, D. de R. Fenômeno esporte: relações com a qualidade de vida. **QUALIDADE DE VIDA**, UNIVERSIDADE FEDERAL DO CEARÁ, p. 11, 2010.
- ATLAM, H. F.; WALTERS, R. J.; WILLS, G. B. Fog computing and the internet of things: A review. **big data and cognitive computing**, Multidisciplinary Digital Publishing Institute, v. 2, n. 2, p. 10, 2018.
- CARISSIMI, A. Desmistificando a computação em nuvem. **ROSE, Cesar de**, p. 3–24, 2015.
- CATARINUCCI, L. et al. An iot-aware architecture to improve safety in sports environments. **Journal of communications software and systems**, Udruga za komunikacijske i informacijske tehnologije, Fakultet . . . , v. 13, n. 2, p. 44–52, 2017.
- COUTINHO, A.; CARNEIRO, E. O.; GREVE, F. G. P. Computação em névoa: Conceitos, aplicações e desafios. **Minicursos do XXXIV SBRC**, p. 266–315, 2016.
- DANTAS, J. R. **Modelos para análise de dependabilidade de arquiteturas de computação em nuvem**. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2013.
- DENARDIN, F. K. Software tolerante a falhas para aplicações tempo real. 1997.
- DOCUSIGN, J. **6 maneiras como a tecnologia está transformando o esporte no mundo**. 2018. Disponível em: <<https://www.docusign.com.br/blog/6-maneiras-como-a-tecnologia-esta-transformando-o-esporte-no-mundo>>. Acesso em: 10 maio 2021.
- GOKHALE, P.; BHAT, O.; BHAT, S. Introduction to iot. **International Advanced Research Journal in Science, Engineering and Technology**, v. 5, n. 1, p. 41–44, 2018.
- GOPE, P. et al. A secure iot-based modern healthcare system with fault-tolerant decision making process. **IEEE Journal of Biomedical and Health Informatics**, IEEE, v. 25, n. 3, p. 862–873, 2020.
- JACOBI, E. B. et al. O modelo de computação em nuvem e sua aplicabilidade. In: . [S.l.: s.n.], 2012.
- KARAKAYA, A.; AKLEYLEK, S. A novel iot-based health and tactical analysis model with fog computing. **PeerJ Computer Science**, PeerJ Inc., v. 7, p. e342, 2021.
- KHAN, R. et al. Future internet: The internet of things architecture, possible applications and key challenges. In: **10th International Conference on Frontiers of Information Technology**. [S.l.: s.n.], 2012. p. 257–260. ISBN 978-1-4673-4946-8.
- KRONBAUER, A.; LUZ, H. D.; CAMPOS, J. Mobile security monitor: A wearable computing platform to detect and notify falls. **IEEE Latin America Transactions**, IEEE, v. 16, n. 3, p. 957–965, 2018.
- LI, S. et al. Computational efficient wearable sensor network health monitoring system for sports athletics using iot. **Aggression and Violent Behavior**, Elsevier, p. 101541, 2020.
- MAHDI, M. J.; ALJUBOORI, A. F.; ALI, M. H. Smart stadium using cloud computing and internet of things (iot): Existing and new models. **International Journal of Computer Applications Technology and Research**, v. 10, p. 111–118, 2021.

- MARANDI, S. J. et al. Iot based thermal aware routing protocols in wireless body area networks: Survey: Iot based thermal aware routing in wban. **IET Communications**, Wiley Online Library, v. 16, n. 15, p. 1753–1771, 2022.
- MARTINS, H. P. et al. Tolerância a falha em um ambiente de computação em nuvem open source. Universidade Estadual Paulista (Unesp), 2014.
- MASCARENHAS, P. D. C. **O que é o Treinamento Intervalado?** 2020. Disponível em: <<https://blog.bodymetrix.com.br/o-que-e-o-treinamento-intervalado/>>. Acesso em: 10 janeiro 2022.
- MATTEDE, H. **O que são sensores e quais as suas aplicações?** 2018. Disponível em: <<https://www.mundodaeletrica.com.br/o-que-sao-sensores-e-quais-as-suas-aplicacoes>>. Acesso em: 10 junho 2021.
- MOREIRA, R. S. et al. Combining iot architectures in next generation healthcare computing systems. In: **Intelligent IoT Systems in Personalized Health Care**. [S.l.]: Elsevier, 2021. p. 1–29.
- MOTA, D. F. M. Robust obc: um sistema de computação de bordo tolerante a falhas. 2022.
- MOTTI, V. G.; CAINE, K. Users' privacy concerns about wearables. In: SPRINGER. **International Conference on Financial Cryptography and Data Security**. [S.l.], 2015. p. 231–244.
- NGUYEN, H. A.; HA, Q. P. Wireless sensor network dependable monitoring for urban air quality. **IEEE Access**, IEEE, v. 10, p. 40051–40062, 2022.
- OLIVEIRA, A. C. de; CARVALHO, J. V. de; BEZ, M. R. Wearable device for athletes: An approach to individual and collective sports. In: SBC. **Anais Estendidos do XXIII Simpósio Brasileiro de Sistemas Multimídia e Web**. [S.l.], 2017. p. 174–178.
- OTD. **100m masculino**. 2020. Disponível em: <<https://www.olimpiadatododia.com.br/toquio-2020/jogos-olimpicos/atletismo/100m-masculino>>. Acesso em: 15 maio 2022.
- PEDROSA, P. H.; NOGUEIRA, T. Computação em nuvem. **Acesso em**, v. 6, 2011.
- PEREIRA, W. **Persistência de dados: tudo que você precisa saber sobre conceito, tipos e técnicas**. 2018. Disponível em: <<https://www.take.net/blog/tecnologia/persistencia-de-dados/>>. Acesso em: 10 junho 2021.
- POONGODI, T. et al. Iot sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (wban), data acquisition. In: **Principles of internet of things (IoT) ecosystem: Insight paradigm**. [S.l.]: Springer, 2020. p. 127–151.
- QADRI, Y. A. et al. The future of healthcare internet of things: a survey of emerging technologies. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 2, p. 1121–1167, 2020.
- RIBEIRO, R. M. O. et al. Segurança em iot: simulação de ataque em uma rede rpl utilizando contiki. In: . [S.l.]: Universidade Federal de Uberlândia, 2018.
- RUSCHEL, H.; ZANOTTO, M. S.; MOTA, W. d. Computação em nuvem. **Pontifícia Universidade Católica do Paraná, Curitiba, Brazil**, 2010.

SANTOS, B. P. et al. Internet das coisas: da teoria à prática. **Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**, v. 31, p. 16, 2016.

SANTOS, C. C.; SALES, J. D. de A. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, Universidade Federal de Pernambuco, v. 13, n. 3, p. 282–290, 2015.

SOUSA, F. **O que é ZigBee? Saiba tudo sobre o protocolo para IoT e casa conectada**. 2018. Disponível em: <<https://www.techtudo.com.br/noticias/2019/12/o-que-e-zigbee-saiba-tudo-sobre-o-protocolo-para-iot-e-casa-conectada.ghtml>>. Acesso em: 10 junho 2021.

TAMASHIRO, C. B. O. Modelagem de falhas em nuvem. Universidade Estadual Paulista (Unesp), 2020.

VERZANI, R. H.; SERAPIÃO, A. B. d. S. Technological contributions for health: outlook on physical activity. **Ciência & Saúde Coletiva**, SciELO Brasil, v. 25, n. 8, p. 3227–3238, 2020.

WEBER, T. S. Um roteiro para exploração dos conceitos básicos de tolerância a falhas. **Relatório técnico, Instituto de Informática UFRGS**, 2002.

WEBER, T. S. Tolerância a falhas: conceitos e exemplos. **Apostila do Programa de Pós-Graduação–Instituto de Informática-UFRGS. Porto Alegre**, p. 24, 2003.

YETISEN, A. K. et al. Wearables in medicine. **Advanced Materials**, Wiley Online Library, v. 30, n. 33, p. 1706910, 2018.

YI, S.; LI, C.; LI, Q. A survey of fog computing: concepts, applications and issues. In: **Proceedings of the 2015 workshop on mobile big data**. [S.l.: s.n.], 2015. p. 37–42.