

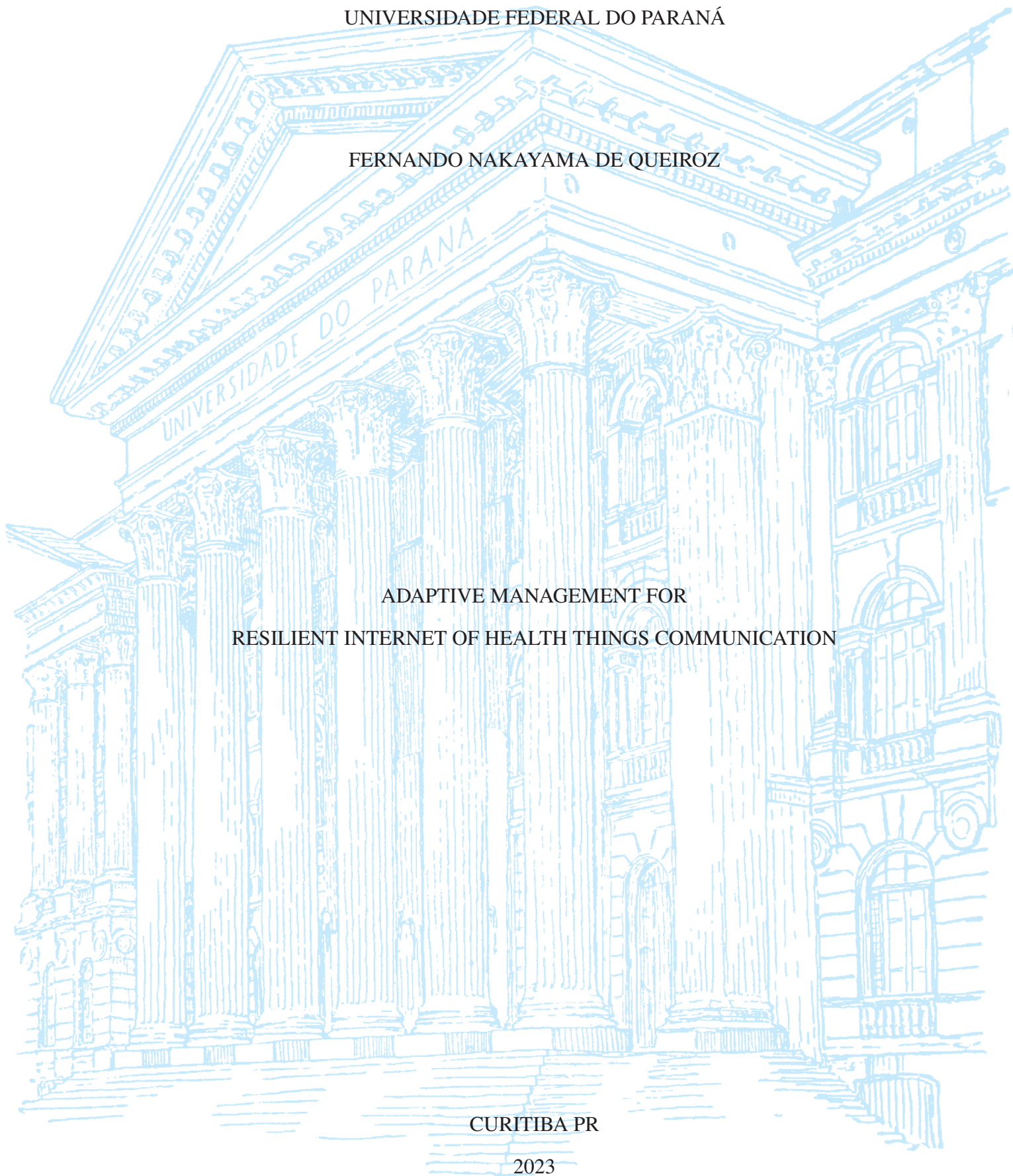
UNIVERSIDADE FEDERAL DO PARANÁ

FERNANDO NAKAYAMA DE QUEIROZ

ADAPTIVE MANAGEMENT FOR
RESILIENT INTERNET OF HEALTH THINGS COMMUNICATION

CURITIBA PR

2023



FERNANDO NAKAYAMA DE QUEIROZ

ADAPTIVE MANAGEMENT FOR
RESILIENT INTERNET OF HEALTH THINGS COMMUNICATION

Tese apresentada como requisito parcial à obtenção do grau de Doutor em Ciência da Computação no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Michele Nogueira Lima.

CURITIBA PR

2023

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA DE CIÊNCIA E TECNOLOGIA

Queiroz, Fernando Nakayama de
Adaptive management for resilient internet of health things
communication / Fernando Nakayama de Queiroz. – Curitiba, 2023.
1 recurso on-line : PDF.

Tese (Doutorado) - Universidade Federal do Paraná, Setor de Ciências
Exatas, Programa de Pós-Graduação em Informática.

Orientador: Michele Nogueira Lima

1. Redes de computadores. 2. Computadores - Medidas de segurança. 3.
Cibersegurança. 4. Saúde (Sistemas de recuperação da informação).. I.
Universidade Federal do Paraná. II. Programa de Pós-Graduação em
Informática. III. Lima, Michele Nogueira. IV. Título.

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da tese de Doutorado de **FERNANDO NAKAYAMA DE QUEIROZ** intitulada: **ADAPTIVE MANAGEMENT FOR RESILIENT INTERNET OF HEALTH THINGS COMMUNICATION**, sob orientação do Prof. Dr. MICHELE NOGUEIRA LIMA, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de doutor está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 14 de Dezembro de 2023.

Assinatura Eletrônica

23/12/2023 16:58:04.0

MICHELE NOGUEIRA LIMA

Presidente da Banca Examinadora

Assinatura Eletrônica

23/12/2023 07:42:33.0

ALDRI LUIZ DOS SANTOS

Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Assinatura Eletrônica

17/01/2024 09:17:16.0

ANELISE MUNARETTO FONSECA

Avaliador Externo (UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ)

Assinatura Eletrônica

23/12/2023 07:23:52.0

ELIAS PROCÓPIO DUARTE JÚNIOR

Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Assinatura Eletrônica

25/12/2023 11:41:36.0

LEOBINO NASCIMENTO SAMPAIO

Avaliador Externo (UNIVERSIDADE FEDERAL DA BAHIA)

To Olivia, Peter, and Ligia. To my family and friends, and all the small things and moments I did not know I needed so profoundly.

ACKNOWLEDGEMENTS

I would like to initially thank Universidade Federal do Paraná for supporting me in the achievement of a goal that once seemed impossible. Despite all the difficulties arising from obtaining a Ph.D., UFPR offered me the resources and structure to complete this journey. Also, I would like to thank Universidade Federal de Minas Gerais for having me for a Doctoral stay in my final year. I also want to thank the funding agencies CAPES grant #88882.382204/2019-01, and CNPQ grant #2022/14299-7, for supporting me throughout my studies and bolstering education in Brazil.

I must thank my advisor, Professor Michele Nogueira Lima, regarding my academic and personal development. As someone told me on the first day in our research lab, she noticed something impressive enough to invest valuable time and effort into my evolution. Thank you very much for this and so many other things. I would also like to thank my lab colleagues Carlos, Danilo, Arthur, Bruno, and Anderson for the partnership.

Finally, I would like to thank my family. The family I left behind at the beginning of this journey, João, Luanna, Maia, Keyla, and Mom, thank you for enduring the distance. The family I made along the way, Gust, Flávia, Agnaldo, Rosângela, Danna, and Paulo, thank you for welcoming me as one of yours. And the family that stood by my side on the adventure of traveling across three cities and two states to pursue my goal. Thank you, Olivia, Peter, and Ligia, for being the most incredible and supportive family; no words can describe how extraordinary you are. Thank you, Dad, for cultivating the seed of knowledge when I was still a kid; we made it.

RESUMO

A Internet das Coisas (IoT) apoiou o desenvolvimento de inúmeras aplicações, contribuindo com o progresso econômico e tecnológico e promovendo benefícios na qualidade de vida dos utilizadores. A IoT representa uma evolução de tecnologias existentes na Internet, compreendendo não apenas computadores e telefones celulares, mas também vários dispositivos heterogêneos em tamanho, tipo e funcionalidade. Mais especificamente, no domínio da saúde, as aplicações IoT levaram ao conceito de Internet of Health Things (IoHT). IoHT refere-se à integração de dispositivos relacionados à saúde conectados entre si e à Internet. A IoHT está revolucionando a medicina, proporcionando fácil acesso a dados relacionados à saúde para usuários e profissionais da área, possibilitando melhorias no monitoramento remoto e desenvolvendo novas aplicações. No entanto, a natureza heterogênea dos dispositivos e tecnologias de comunicação, a sensibilidade dos seus dados e as questões legais e de privacidade tornam a segurança da IoHT uma prioridade. Muitas das práticas de segurança atuais são inadequadas devido à baixa capacidade computacional e às características dinâmicas do ambiente IoHT, tornando-se necessário remodelar os mecanismos de segurança para tornar a IoHT resiliente contra ameaças. Além disso, as aplicações IoHT coletam e transmitem dados críticos, o que torna os requisitos de desempenho muito rigorosos. O foco principal desta tese é buscar soluções resilientes e seguras para resolver problemas de comunicação existentes na IoHT. Esta tese aborda as questões críticas relativas à segurança e ao desempenho para cada nível fundamental de operação relacionado à comunicação IoHT. A hipótese investigada é que ao adicionar gerenciamento adaptativo em todos os níveis fundamentais da comunicação, é possível aprimorar a resiliência geral e preservar o desempenho da rede necessário para aplicações IoHT. O gerenciamento adaptativo é uma abordagem estruturada para tomada de decisões baseada na gestão dos recursos naturais e que habilita fases iterativas de aprendizagem e adaptação do controle para alcançar plenamente os objetivos do gerenciamento. As contribuições feitas nesta tese incluem um novo mecanismo de autenticação baseado em bio-sinais dos usuários e na comunicação intra corporal sem fio, uma arquitetura de gerenciamento resiliente para lidar com a comunicação multi-caminho e, ao mesmo tempo, auxiliar a mobilidade dos usuários em cenários da IoHT, e uma nova abordagem para analisar a resiliência em ambientes de IoHT considerando as múltiplas topologias de comunicação existentes. Estudos adicionais que consideram disciplinas de resiliência em ambientes IoT mostram que as relações entre segurança e desempenho são muito restritas e que os mecanismos de segurança devem ser cuidadosamente adaptados e implementados para alcançar a resiliência.

Palavras-chave: Resiliência. Redes de computadores. Internet das coisas da saúde. Gerenciamento adaptativo. Cibersegurança.

ABSTRACT

The Internet of Things (IoT) has promoted the development of numerous applications, driving economic and technological progress and improving the quality of life for users. The IoT represents an evolution from other Internet technologies, comprising not only computers and cell phones but also various heterogeneous devices in size, type, and functionality. More specifically, in the health domain, IoT applications have led to the Internet of Health Things (IoHT) concept. IoHT refers to integrating health-related devices connected among themselves and the Internet. IoHT is revolutionizing medicine, providing easy access to health-related data for users and professionals in the field, enabling improvements in remote monitoring, and developing new applications. However, the heterogeneous nature of communication devices and technologies, the sensitivity of their data, and legal and privacy issues make IoHT security a top priority for researchers worldwide. Many of the current security practices are inadequate due to the low computational capacity and dynamic characteristics of the IoHT environment, which are necessary to remodel the security mechanisms to make the IoHT resilient against threats. Furthermore, IoHT applications collect and transmit critical data, which makes performance requirements very strict. The main focus of this thesis is to seek resilient and secure solutions to address existing communication problems in IoHT. This thesis tackles the critical issues regarding security and performance for each fundamental level of IoHT communication operation. The hypothesis investigated is about adding adaptive management throughout the fundamental levels to increase overall resilience and preserve the network performance necessary for IoHT applications. Adaptive management is a structured approach to decision-making based on natural resources management that encourages iterative phases of learning and adaptation of control to fully meet the objectives of management. The contributions made in this thesis include a novel authentication mechanism based on users' biosignals and wireless intrabody communication, a resilient management architecture to handle multipath communication while assisting users' mobility in IoHT scenarios, and a novel approach to analyze resilience in IoHT environments considering the multiple communication topologies available. Additional studies considering resilience disciplines in IoHT environments show that the relationships between security and performance are very tight and that security mechanisms must be carefully adapted and implemented to achieve resilience.

Keywords: Resilience. Computer networks. Internet of health things. Adaptive management. Cybersecurity.

LIST OF FIGURES

2.1	Desired attributes for resilient systems	18
2.2	Dependability and security tree	19
2.3	Methods for mitigation and recovery	20
2.4	Tolerance disciplines in communication networks	21
2.5	ICT pillars and paradigms and IoHT paradigms. Figure adapted from (Aceto et al., 2018)	22
2.6	Fundamental levels of operation in IoHT	22
2.7	IoHT essential services, pillars and paradigms	24
2.8	Basic security principles and attacks regarding the IoHT environment	28
2.9	Taxonomy for works on IoHT communication resilience	31
2.10	Adaptive management cycle adapted from (Allen et al., 2011)	34
2.11	Dominant adaptive management schools adapted from (McFadden et al., 2011)	35
2.12	Desired disciplines and techniques for resilient and adaptive IoHT	37
3.1	Tradional AAL vs. portable ALS	41
3.2	PALS integration with AAL and architecture.	43
3.3	A classification of works on IoHT communication resilience	46
3.4	Portable assisted living architecture	50
3.5	Measurement setup	52
3.6	Comparison of PALS implementations under no loss scenarios	53
3.7	Comparison of PALS implementations under random losses	54
3.8	Example of a possible path handover	55
3.9	Handover evaluation	56
3.10	Global evaluations	57
3.11	Europe evaluations	58
3.12	United States of America evaluations	58
3.13	South America evaluations	59
3.14	Evaluation of multipath PALS versions in global scenarios	60
3.15	Communication failure	61
3.16	Delay for PALS versions in failure and continuous scenarios	63
3.17	Retransmissions for PALS versions in failure an continuous scenarios	63
3.18	Induced failures scenarios and data transfer speed per emulation - Global region	64
3.19	Induced failures scenarios and data transfer speed per emulation - South America region	65

3.20	Induced failures scenarios and data transfer speed per emulation - Europe region.	65
3.21	Induced failures scenarios and data transfer speed per emulation - United States of America region.	65
4.1	Taxonomy for biosignal-based continuous authentication systems	68
4.2	The steps of the BEAT authentication system	71
4.3	Optical Sensor.	72
4.4	Main features in a PPG signal waveform	72
4.5	Galvanic coupling model	73
4.6	Register and authentication for the BEAT system	74
4.7	Testbeds	75
4.8	Signals and preprocessing.	76
4.9	Overlapping waves and mean	76
4.10	Authentication threshold	76
4.11	Authentication process	77
4.12	Authentication map	78
5.1	Essential services in IoHT	82
5.2	Possible communication configurations for IoHT	84
5.3	Communication performance baseline evaluation	88
5.4	Communication evaluation - threats regarding the sensing device	88
5.5	Communication evaluation - threats regarding the coordinator device.	89
5.6	Communication evaluation - threats regarding the access gateway.	89
5.7	Communication evaluation - access gateway recovery	90
6.1	Main contributions	92

LIST OF TABLES

2.1	Classification and examples of faults (Avizienis et al., 2004)	19
2.2	IoHT applications criticality	24
2.3	Essential services requirements	27
3.1	Experimental parameters	52
3.2	Bandwidth efficiency	55
3.3	Global and regional speeds for fixed and mobile Internet	57
3.4	Average delay in seconds per region	59
3.5	Bandwidth values for fixed and mobile broadband	62
3.6	PALS average available bandwidth, throughput, and bandwidth use	64
4.1	Overview of the main biosignal-based authentication systems	69
4.2	Comparing results from the NR2/UFPR and Physionet datasets	77
5.1	Topologies evaluation regarding centrality and resilience metrics	86
5.2	Elements and properties of the network simulator	86
5.3	Charaterization of experiments	87

LIST OF ACRONYMS

AAL	Ambient Assisted Living
ACK	Acknowledgment
ANX	Abstract Network Simulator
BEAT	Biosignal Enhanced Authenticator
BP	Blood Pressure
D2D	Device to device
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECG	Electrocardiogram
EEG	Electroencephalogram
eHealth	Electronic Health
FDA	Food and Drug Administration
GC	Galvanic Coupling
GSR	Galvanic Skin Response
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IoHT	Internet of Healthcare Things
IoT	Internet of Things
MITM	Man in the Middle
MPQUIC	Multipath Quick UDP Internet Connections
MPTCP	MultiPath Transmission Control Protocol
NFC	Near Field Communication
OLIA	Opportunistic Linked-increases Algorithm
PALS	Portable Assisted Living
PPG	Photoplethysmogram
QoS	Quality of Service
QUIC	Quick UDP Internet Connections

REST	Representational State Transfer
RTT	Round Trip delay Time
SCTP	Stream Control Transmission Protocol
SIoT	Social Internet of Things
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play

CONTENTS

1	INTRODUCTION	14
1.1	PROBLEM STATEMENT AND GOALS	15
1.2	CONTRIBUTIONS	17
2	BACKGROUND	18
2.1	ATTRIBUTES OF DEPENDABILITY	18
2.1.1	Faults, errors, failures, and attacks	18
2.1.2	Techniques for Resilient IoT-based Concepts	19
2.1.3	Fault Tolerance in Communication Networks	21
2.2	INTERNET OF HEALTH THINGS	21
2.2.1	The IoHT Applications	23
2.2.2	Resilience-driven Requirements	26
2.2.3	Security Principles and Attacks Regarding IoHT.	27
2.3	EXISTING APPROACHES FOR COMMUNICATION RESILIENCE	31
2.4	ADAPTIVE MANAGEMENT PRINCIPLES	33
2.4.1	Adaptive Management and Computing Systems	34
2.5	ADAPTIVE MANAGEMENT AND COMMUNICATION RESILIENCE IN IOHT	35
2.6	LONG-TERM RESILIENCE IN IOHT.	36
2.7	CHAPTER SUMMARY	37
3	A RESILIENCE MANAGEMENT ARCHITECTURE FOR COMMUNICA- TION ON PORTABLE ASSISTED LIVING	38
3.1	RELATED WORK	39
3.2	PORTABLE ASSISTED LIVING SYSTEMS	41
3.2.1	PALS System	42
3.2.2	Communication Protocols	44
3.3	A CLASSIFICATION OF WORKS ON IOHT COMMUNICATION RE- SILIENCE	45
3.3.1	Communication Resilience and Sensing Services	45
3.3.2	Communication Resilience and Connectivity Services.	47
3.3.3	Communication Resilience and End-to-end Communication Services.	48
3.3.4	Discussion.	49
3.4	A RESILIENCE MANAGEMENT ARCHITECTURE FOR COMMUNICATION ON PORTABLE ASSISTED LIVING	50
3.5	PERFORMANCE EVALUATION OF PALS	51
3.5.1	PALS Evaluation in Randomized Scenarios	52

3.5.2	Protocols Evaluation in Specific Scenarios	56
3.5.3	Discussion.	60
3.6	RESILIENCE EVALUATION OF PALS	61
3.6.1	Delay Evaluation	62
3.6.2	Resilience Evaluation	63
3.7	CHAPTER SUMMARY	66
4	A BIOSIGNAL AUTHENTICATION AND INTRABODY COMMUNICATION SYSTEM FOR IOHT	67
4.1	RELATED WORKS	68
4.1.1	Sensors	68
4.1.2	Sources of Biosignals	69
4.1.3	Actions from Users	70
4.1.4	Communication Channels.	71
4.2	THE BEAT AUTHENTICATION SYSTEM.	71
4.2.1	Data Acquisition and Signal Preprocessing.	72
4.2.2	Data Transmission by Galvanic Coupling	73
4.2.3	Authentication Procedure	73
4.3	EXPERIMENTAL DESIGN AND ANALYSIS	74
4.3.1	Implementation of BEAT in an Experimental Environment	74
4.4	CHAPTER SUMMARY	78
5	A RESILIENCE ANALYSIS APPROACH FOR IOHT	80
5.1	BACKGROUND	81
5.2	A NOVEL APPROACH ON IOHT RESILIENCE ANALYSIS	82
5.3	GRAPH-THEORETIC REPRESENTATION AND ANALYSIS	83
5.3.1	Analysis Regarding IoHT Network Configurations.	83
5.3.2	Centrality and Resilience Metrics.	85
5.3.3	Communication Performance Evaluation of IoHT Topologies	86
5.3.4	Discussion.	90
5.4	CHAPTER SUMMARY	91
6	CONCLUSIONS.	92
6.1	MAIN CONTRIBUTIONS	92
6.2	LIMITATIONS AND FUTURE WORK	94
6.3	PUBLICATIONS	94
	REFERENCES	96

1 INTRODUCTION

The Internet of Things has promoted a tremendous number of novel applications, bolstering economic and technological development and improving users' quality of life. The IoT concept represents an evolution from other Internet technologies since it comprises not only computers and mobile phones but also heterogeneous devices of all types, sizes, and functionalities (Atzori et al., 2010). IoT is expected to support a wide range of application domains, such as smart homes, smart cities, industrial automation, logistics, and healthcare. Particularly in the healthcare domain, IoT applications have led to the Internet of Health Things (IoHT) concept. IoHT refers to an infrastructure composed of health-related devices connected to each other and/or the Internet.

IoHT has revolutionized medicine and healthcare, providing users and healthcare professionals easy access to health-related data and opening up countless possibilities. It offers communication between healthcare devices and the Internet, the continuous sensing of personal and environmental data, remote care, and insights into symptoms and treatments, providing high control to patients over their lives and treatments. There is a vast number of IoHT applications towards smart medicine, such as the continuous supervision of cancer treatment and glucose, the automation of insulin delivery, asthma symptoms control, and others. IoHT has gained increasing attention from academia and industry that, motivated by the aging population, shifts care provision from inside traditional care institutions to continuous care anywhere and anytime.

One-third of all IoT devices relate to healthcare (IBM, 2023), and it is estimated that 87% of healthcare organizations will adopt IoHT shortly. The main concerns regarding IoHT relate to communication resilience and performance once healthcare applications require high reliability, security, and safety (Wolf and Serpanos, 2017). People's lives rely on new medical devices and services, requiring special attention to resilience (i.e., continuous connection availability – 99.99 percent reliability, ultra-low latency, and mobility support, even in the advent of faults and threats, that could be unpredictable at design time or could emerge in runtime) (Laprie, 2008; Avizienis et al., 2004). IoT security, privacy, and reliability vulnerabilities have been investigated with many academic results and industry (Zhao and Ge, 2013; Coelho et al., 2019). These vulnerabilities are not different regarding the narrow context of IoHT.

Current IoHT devices are severely vulnerable to the exploitation of weak authentication, poor implementation of communication technologies, and outdated solutions (IBM, 2023). The outcome of attacks and failures includes information loss resulting from IoHT device hijacking, inaccurate treatment for users, the denial of IoHT services, among other (FBI, 2020). Furthermore, given the constrained computational resources (e.g., processing, memory, bandwidth, storage) in IoHT devices and communication channels, IoHT often employs lightweight versions of traditional security mechanisms, which may lead to partial or complete information disclosure (Blasco et al., 2019). Also, communication channels in IoHT are prone to attacks during pairing and data transmission, resulting in failures in the user authentication process (Classen et al., 2018), and poor or no cryptography at all (Wood et al., 2017). Healthcare experiences the highest data breach costs of all industries. It is estimated that a data breach costs, on average, approximately US\$ 4.45 million or US\$ 165 per user record (IBM, 2023).

IoHT has a very complex networking and communication model since its ecosystem comprises a vast number of heterogeneous devices, communication protocols, and processing mechanisms. Therefore, analyzing the information corresponding to an adverse situation becomes complex. Considering the dynamic characteristics of devices and mobile elements, the IoHT environment is constantly and drastically changing. Due to the complex nature of IoHT, the

conventional detection and prevention security mechanisms are not suited to protect it against threats that are becoming increasingly sophisticated (Hassija et al., 2019). Current security mechanisms depend mainly on static information or rely on a particular piece of contextual information monitored in a specific infrastructure domain, needing to be improved to provide security in a dynamic environment like IoHT. Health-related situations as those dealt with by IoHT require fast and dynamic responses to the faced threats. Hence, adaptation is a fundamental property in the IoHT environment (Muccini et al., 2018). Adaptation is a system property that makes regulation and reconfiguration possible according to the faced challenges (Ratasich et al., 2019), being one of the main properties of resilience. Resilience is the ability to provide and maintain an acceptable level of service delivery in the face of faults and challenges that may harm normal operations (Sterbenz et al., 2010a).

Works in the literature address resilience and adaptation in IoHT environments following different perspectives. They generally focus on the broader IoT concept, neglecting IoHT essential and exclusive requirements (e.g., real-time requirements for latency and availability). Additionally, current literature focuses on one or a particular set of security or performance services. Security adaptation models primarily emphasize a particular component without evaluating other non-security parameters, which must be evaluated during the adaptation phase; by analyzing these shortcomings in conventional security solutions, it is clear the need for a computationally reasonable solution for IoHT that should be able to adapt to an optimal trade-off considering resilience and performance.

1.1 PROBLEM STATEMENT AND GOALS

The intricate characteristics of the IoHT environment, *i.e.*, a high diversity of sensors, devices, communication technologies, and processing mechanisms have allowed the development of new applications and promoted improvements on the existing ones. However, because of this dynamic and complex nature, there are drawbacks to enabling resilience measures. Firstly, applications in IoHT have distinct communication performance requirements to be met, including real-time and near-real-time data transmission with high-reliability needs; this mixed criticality environment, along with the unstable Internet characteristics in terms of communication, makes the IoHT requirements very difficult to achieve. The traditional approaches to estimating the quality of communication are inappropriate for IoHT due to the interconnected and independent service layers, which makes it challenging to identify the specific faulty segment considering end-to-end communications. Additionally, regarding the critical applications, response to any unpredicted challenge is desired to be fast and dynamic.

Secondly, numerous threats jeopardize the IoHT environment regarding communication performance and security. The conventional preventive and reactive security controls employed in traditional networks are inadequate to protect the dynamic and constantly expanding IoHT environment (Yang et al., 2012). The provided countermeasures rely primarily on static information, delivering static responses. Current mitigation mechanisms mainly focus on asset protection, prioritizing the closest network segment of the asset and disregarding other critical parameters, such as the impact on user experience and service continuity. Without considering the whole environment, actions from those mechanisms may cause adverse influences, including new security hazards. Furthermore, IoHT services rely on wireless resource-constrained devices, which may not be able to host these conventional controls and mechanisms. Thus, although there are solutions to face threats and communication performance issues for IoHT, they ignore the multiple IoHT configurations required for communication, making it challenging to anticipate issues concerning the performance and security tradeoff.

Considering the existing issues and the adverse conditions against communication resilience in the IoHT environment, the hypothesis investigated in this work is that adding adaptive management throughout the multiple IoHT service stages enhances overall communication resilience and security, and it assists in preserving the minimal required network performance for IoHT applications. Adaptive management is a structured approach to decision-making that encourages iterative phases of learning and adaptation of control to fully meet the objectives of management. The thesis statement relies on the assumption that adaptive management can make security and performance trade-off decisions dynamic as per risk situation. However, for that to happen, the management must occur in a coordinated manner and take into account all essential service layers. This work presents an in-depth discussion about resilience in the IoHT environment. It allowed us to identify open issues, resilience requirements, and their implications regarding each established essential service level and their interaction. This discussion encompasses related works that use adaptability and resilience in IoHT. The intention is to confront the problems in IoHT while observing the manageable adaptive elements and considering three essential matters: the impact on overall resilience, the feasible security approaches, and possible solutions to enhance communication performance. Therefore, these issues are captured in the fundamental research questions as follows.

Main research question: *Can adaptive management increase resilience in complex environments like IoHT?*

In order to consistently answer this fundamental question, it becomes necessary to divide it into sub-questions that address specific aspects, such as communication performance and applications requirements, security versus performance balance, and the feasibility of integrating adaptive management into the current IoHT configurations. These sub-questions and a brief description of the problems they tackle are as follows:

First research question: *How can the techniques that improve communication performance incorporate adaptive management to increase resilience?*

Many techniques that seek to improve communication performance disregard the need for resilience. Most works assume that communication is always available, disregarding all the necessary aspects for this to happen. IoT applications include safety-critical and time-critical applications with increased dependence on communication performance and resilience. Therefore, it becomes necessary to identify the main techniques that seek to maintain or improve communication performance and incorporate adaptive management to satisfy the resilience needs of IoHT applications.

Second research question: *Which security approaches fit adaptive management, and how do they impact resilience versus performance balance?*

The information transferred over IoHT networks is sensitive, demanding efficient security mechanisms. However, approaches that increase security can negatively impact overall communication performance, jeopardizing the IoHT environment unpredictably. Therefore, evaluating which security approaches fit adaptive management and the possible effects on communication performance is required.

Third research question: *Assuming the multiple communication technologies and possible configurations available in IoHT, how can the adaptive management solutions converge with IoHT-based systems, and what is the impact on communication performance?*

The IoT environment encompasses multiple devices, communication technologies, and configurations. Incorporating adaptive management in such a complex and interconnected environment is challenging, particularly considering the numerous configuration possibilities within the wide range of components. Each IoHT communication configuration alone provides distinct levels of resilience, depending on the number of devices and communication links. Therefore, it is essential to investigate how the adaptive solutions can agree with the existing IoHT configurations and their impact on communication performance.

1.2 CONTRIBUTIONS

We summarize the contributions of this work as:

A resilience management architecture for communication and the performance management of multiple communication paths for portable assisted living. IoHT interconnects wearable and portable devices, supporting critical healthcare applications such as Ambient Assisted Living (AAL) that retrieve crucial information from users. These systems have restricted requirements in terms of latency and availability, demanding fast advances in network infrastructure and essential services such as sensing, connectivity, and end-to-end communication. This contribution encompasses a novel resilience management architecture for communication in portable assisted living. IoHT devices have access to multiple access networks, such as fixed and mobile, and the concurrent management of those networks can extend the communication range and enhance communication resilience. In order to improve communication performance and extend the monitoring area of users in the context of Ambient Assisted Living systems (AAL), we have designed and evaluated a Portable Assisted System. PALS improves communication performance and extends the monitoring area for users in the context of Ambient Assisted Living systems by managing the communication paths. The applications supported by the IoHT essential layers are presented and analyzed, and the requirements for each application are classified and organized. As a result, the literature review allows identifying open issues and opportunities to employ adaptive resilience management concepts in the IoHT environment.

A biosignal authentication and intrabody communication system for IoHT. One of the primary challenges for IoHT is offering services that fulfill security and performance requirements. In order to investigate user authentication, one of the security aspects of IoHT, and to evaluate security versus performance tradeoff, the Biosignal Enhanced Authenticator (BEAT) has been proposed. BEAT relies on biosignals to continuously authenticate an allowed user or device. Regarding resilience and security management, the BEAT system employs an intrabody communication technology that can provide redundancy and be a secure alternative to traditional wireless communication technologies.

A resilience analysis approach for IoHT. Estimating IoHT resilience considering multiple possible network configurations and diverse threats is challenging but necessary. Therefore, we propose an approach to analyze resilience in the IoHT that assesses multiple achievable network configurations regarding the devices and communication technologies available and the challenges imposed by threats. Additionally, we propose a discussion considering the possible configurations and evaluations of an IoHT environment in terms of resilience and communication performance.

2 BACKGROUND

This chapter provides background on fundamental topics required for a comprehensive interpretation of this work. It is organized into five sections as follows. Section 2.1 describes the fundamental attributes of dependability. Section 2.2 defines the IoHT concept and presents its essential services, applications, and threats from a resilience perspective. It also provides an overview of the main applications and requirements of IoHT. Section 2.3 illustrates the existing approaches dealing with communication resilience. Section 2.6 defines the main challenges for IoHT, considering long-term resilience. Finally, Section 2.7 concludes the Chapter.

2.1 ATTRIBUTES OF DEPENDABILITY

IoHT is desired to be dependable and secure throughout its entire life cycle. Authors in (Avizienis et al., 2004) define the *dependability* property of a system as a combination of the following attributes: *reliability* (continuity of correct service), *safety* (absence of catastrophic consequences), *maintainability* (ability to undergo modifications and repairs, *availability* (readiness for correct service), and *integrity* (absence of improper system alterations). *Security* adds *confidentiality* (the absence of unauthorized disclosure of information) to the dependability attributes. Figure 2.1 summarizes the relation of system attributes in the context of resilience.

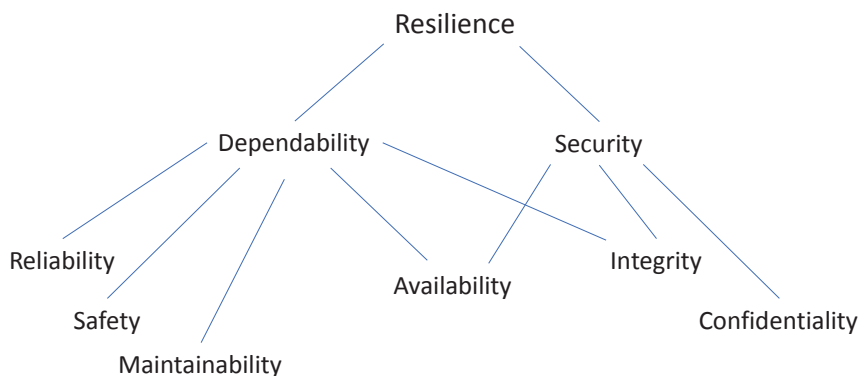


Figure 2.1: Desired attributes for resilient systems

From a *security* perspective resilience can be described as the resistance against attacks (malicious faults), as from a *dependability* perspective resilience is defined as the continuity in proper operation under faults of stochastic nature (non malicious faults). Laprie (2008) defines *resilience* for ubiquitous, large-scale, evolving systems as "The persistence of service delivery that can justifiably be trusted, when facing changes." We consider this resilience definition a good fit to express the needs of an IoHT environment.

2.1.1 Faults, errors, failures, and attacks

A *failure* occurs when a system diverges from its intended behavior. A failure manifests due to an unplanned state of one or more components of the system. This state is known as an *error*. The cause of an error is called *fault*. Possible approaches to deal with faults include prevention, tolerance, removal and forecasting (Laprie, 2008). Figure 2.2 illustrates the dependability and security taxonomy with its attributes, threats, and approaches.

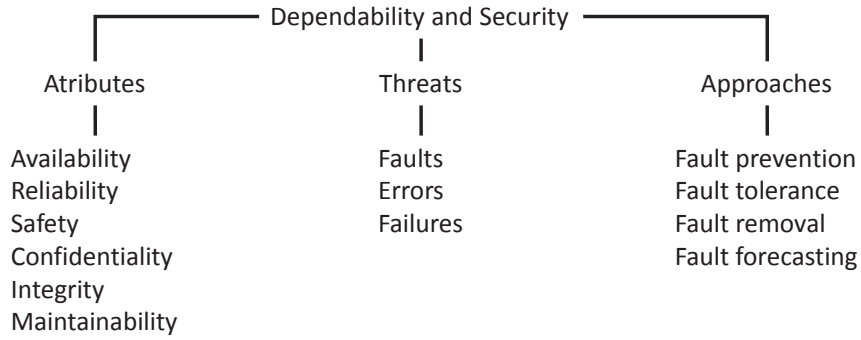


Figure 2.2: Dependability and security tree

The origin of a fault may be internal or external. While internal faults are primarily of physical nature (e.g., component failure, broken connectors), external faults originate from the environment (e.g., noise, radiation) or inputs (e.g., wrong or malicious usage of the system). Faults can also be classified as transient or permanent. Transient faults eventually cause an error and might lead to a permanent failure (Ratasich et al., 2019). Table 2.1 illustrates the faults classification and provides examples for each type of fault.

Table 2.1: Classification and examples of faults (Avizienis et al., 2004)

Fault type	Examples
Physical	Broken connector, radiation, noise, interference, power down and denial-of-service attacks
Development	Production defect, software "bugs", vulnerabilities, memory bloating or leaking
Interaction	Input mistakes, message collision, spoofing, replay attack, flooding, false data injection
Permanent	Design faults, short-circuits, hardware damage
Transient	Radiation, power transients, intrusion attempt via vulnerabilities

2.1.2 Techniques for Resilient IoT-based Concepts

Several online and offline approaches are available to improve resilience in IoT-based environments, such as the IoHT. Developers may try to adapt the traditional dependability and security approaches to prevent faults (e.g., appropriate design, encryption), tolerate faults (e.g., redundancy, multiple setups), remove or mitigate flaws (e.g., isolate faulty components) or forecast faults (e.g., to estimate the consequences of a fault) (Avizienis et al., 2004), specifically for IoHT, the main requirements regarding resilience focus on identifying and diagnosing faulty, attacked or failed components and the mitigation and recovery of the system.

2.1.2.1 Detection and diagnosis

Anomaly detection is the process of identifying an abnormal behavior or pattern (Chandola et al., 2009). Abnormal behavior or service failure (e.g., random failures, design errors, intruders) emanate from a fault (Avizienis et al., 2004). Fault-detecting mechanisms employ different terminologies depending on the application or type of the mechanism. The term *monitoring* is used in the field of runtime verification where information is extracted from a running system to refer to the observation of a finite trace of temporal behavior and the arrangement of a verdict (Leucker and Schallhart, 2009). In the computational security field, the term *intrusion detection* relates to detecting break-ins, penetrations, and other forms of computer abuse (Denning, 1987). Faulty behaviors are detectable through methods of observation and probing (e.g., watchdogs and

timeout monitors). For evaluation purposes, it is essential to compare the faulty behavior against a behavior specification model. This model is usually represented in one of two ways: attack signatures or anomaly-based techniques. Signature-based models compare pre-defined behavior to identify the abnormal event during runtime (Butun et al., 2013). Anomaly-based techniques rely on statistical analysis to identify if the data fits into a model. Using machine learning and data mining techniques in situations lacking domain knowledge has become increasingly popular.

2.1.2.2 Mitigation and recovery

During the development process, it is possible to modify the components, architecture, and parameters of a system (Mendez et al., 2017). If those changes shift from development time to runtime, the system is defined as self-adaptive (Kounev et al., 2017). The actions for runtime reconfiguration of embedded systems are defined in (Papp and Exarchakos, 2016) and adapted for the IoT concept in (Ratasich et al., 2019), Figure 2.3 illustrates the mitigation and recovery methods considering both perspectives. The methods of *re-parameterization* and *runtime enforcement* are standalone approaches, while *restart*, *redirection*, *relocation*, and *replacement* require some degree of redundancy (e.g., hardware, software).

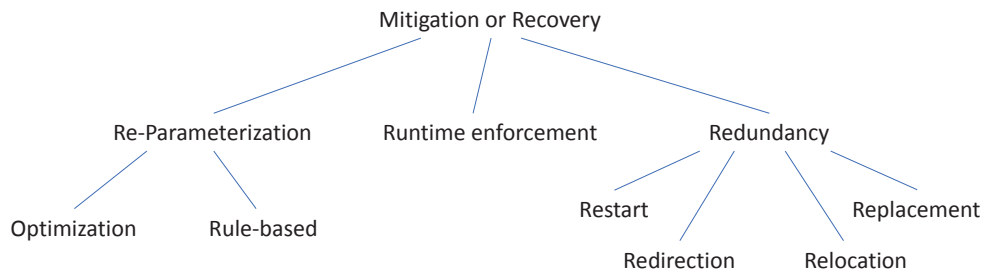


Figure 2.3: Methods for mitigation and recovery

The *re-parameterization* involves reconfiguring one or more components to preserve system functionalities (Papp and Exarchakos, 2016), even if it means reducing the quality of service. The reconfiguration process requires a comprehensive knowledge of the system properties to sustain service delivery with minimal consequences. Therefore, the adaptation of parameters relies on a subsystem. The reconfiguration can occur through optimization by considering the remaining resources or predefined rules. *Runtime enforcement* is a powerful technique to ensure that a program will respect a given set of properties (Falcone et al., 2011); it combines runtime verification with adaptation (Ratasich et al., 2019). In this approach, an enforcer suspends an action whenever it deviates from a safety requirement.

An uncomplicated approach method for fault-tolerance is to *restart* a failed software component to a previously saved checkpoint that represents a healthy state. In some cases, restarts are associated with re-parameterization. One of the most basic approaches to achieving redundancy is the *replacement* of hardware and software components. A substitute spare component is instantiated to replace the failed component and might implicate *redirection* and *relocation*. *Redirection* changes the task flow on a failure to a recovery routine and back to the original flow (Psaier and Dustdar, 2011) being suitable to faulty or broken communication links in IoHT. Task migration is known as *relocation* in the resource optimization field (Ratasich et al., 2019). Relocation of tasks can happen using all the resources in the IoHT environment, including local and distributed applications (e.g., cloud applications).

2.1.3 Fault Tolerance in Communication Networks

Since IoHT relies on multiple communication technologies throughout its information cycle, fault tolerance must encompass the context of communication networks. This work follows the classification proposed by authors in (Sterbenz et al., 2010a) with the organization for tolerance disciplines and how they deal with the challenges that prevent service delivery in communication networks. The organization of challenges is threefold: component and system failures for which *fault tolerance* and *survivability* are concerned, disruptions of communication paths for which *disruption tolerance* is concerned, and challenges due to the injection of traffic into the network, for which *traffic tolerance* is concerned. Figure 2.4 illustrates the disciplines considering tolerance in communication networks.

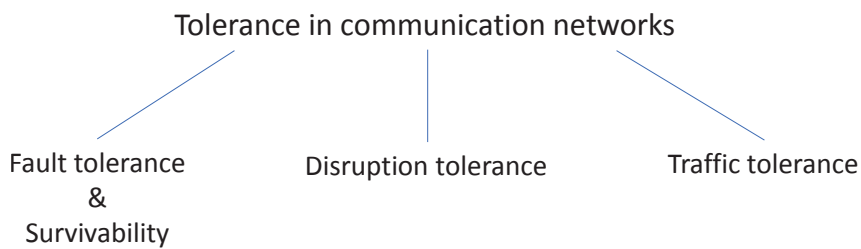


Figure 2.4: Tolerance disciplines in communication networks

Fault tolerance is defined as the ability of a system to continue operation at a defined performance level, even though one or more of its components are malfunctioning (Standard, 2007). Fault tolerance relies on redundancy to compensate for the random uncorrelated failure of components and applies to both hardware and software. Survivability is the capability of a system to fulfill its mission in a timely manner (Avizienis et al., 2004), even in the presence of threats such as attacks or natural disasters. Disruption tolerance is the ability of a system to tolerate intermittent connectivity issues among its components comprising the environmental challenges: weak and episodic channel connectivity, mobility, unpredictably long delay, and tolerance of energy (or power) challenges. Traffic tolerance is the ability of a system to tolerate unpredictable offered loads without a significant drop in carried load (Sterbenz et al., 2010a). Traffic challenges can be legitimate such as from a flash crowd, or malicious such as from a distributed denial-of-service attack (DoS) (Jung et al., 2002).

2.2 INTERNET OF HEALTH THINGS

IoHT comprises implantable and wearable devices (wearables) connected to the Internet supporting and improving healthcare. IoHT includes healthcare and medical-related devices that sense data from the user body and transmit it to healthcare providers (i.e., hospitals and clinics) or healthcare professionals. In addition, IoHT includes the healthcare trackers, such as a smartwatch, a fitness tracker, or even a smartphone. These devices make user tracking possible, continuously reporting about his/her healthcare conditions from different locations. IoHT relies on important information and communication technologies (ICT) and paradigms (Aceto et al., 2018). Figure 2.5 illustrates the ICT pillars and paradigms employed in IoHT that serve as a foundation for the concepts it attempts to accomplish.

Healthcare providers offer a local or cloud infrastructure for computing and storage. This infrastructure assists in data analysis, in learning new insights, and identifying behaviors and trends from users and society. Few works have considered to distribute high-demanding

tasks such as machine learning schemes to fog or edge computing (Isa et al., 2019; Islam et al., 2021). However, computing and storage infrastructures are crucial for IoHT due to the large volume of stored data and the demand for accessing data from multiple distributed locations.

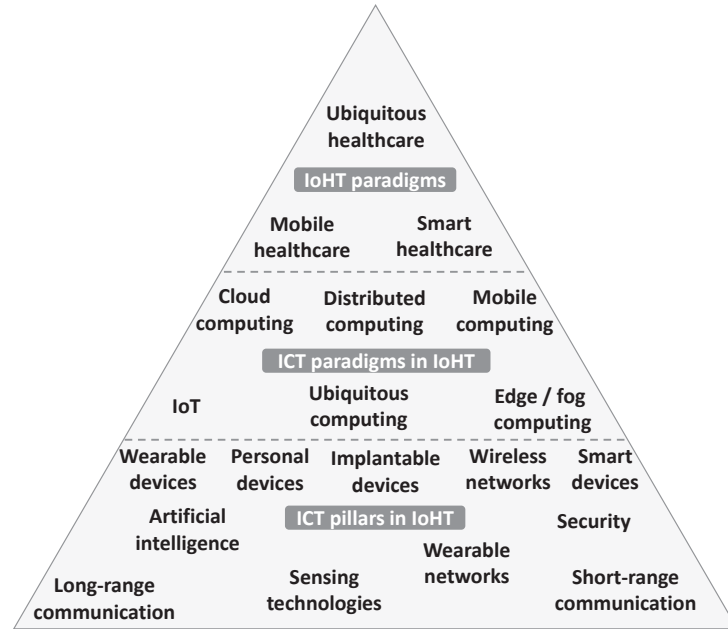


Figure 2.5: ICT pillars and paradigms and IoHT paradigms. Figure adapted from (Aceto et al., 2018)

Figure 2.6 illustrates the three fundamental levels of operation in IoHT as (i) data sensing devices; (ii) Internet; and (iii) the computing and storage infrastructure (e.g., the cloud). End-users interact directly with the devices/sensors collecting their data. Healthcare professionals interact with the computing and storage infrastructure. Figure 2.6 also illustrates the IoHT essential communication services, as **sensing**, **connectivity** and **end-to-end communication**. Sensing operates at the device level; connectivity at the level of direct communication between devices and gateways in houses, vehicles, or held by the user; and the end-to-end communication offers a multi-hop communication between devices and the computing and storage infrastructure.

Sensing services encompass managing data captured from sensors in wearable devices and making it available to connectivity services. Recent researches lean towards non-invasive monitoring of human health as well as activity parameters (Kamišalić et al., 2018). In this sense, a wide range of wearable sensors are available for real-time non-invasive monitoring (e.g., optical, pressure, GPS, accelerometer, gyroscope). Based on the data collected by those sensors, wearable devices can perform significant physiological and activity sensing (e.g., heart rate, body temperature, blood pressure, oxygen saturation, motion and gestures, body acceleration).

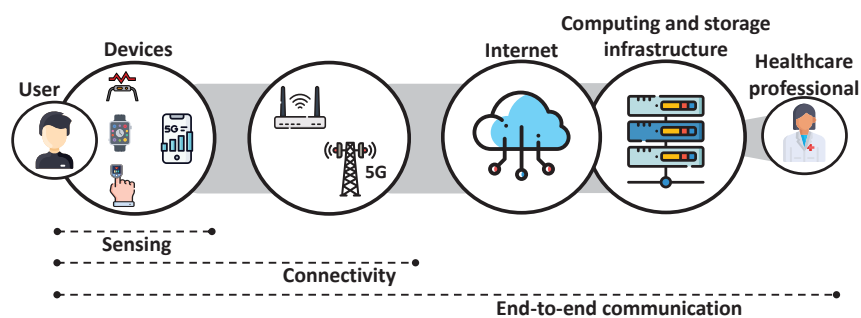


Figure 2.6: Fundamental levels of operation in IoHT

Connectivity services comprise the communication technologies used to transfer data collected from IoHT devices to the Internet. Typically, IoHT devices use the owner's smartphone as an Internet gateway. The most commonly used short-range data transmission technologies for wearables include Bluetooth, Zigbee, and Near Field Communication (NFC). In order to provide Internet connectivity, the smartphone acts as a coordinator, managing the IoHT devices over short-range communication and forwarding data using long-range communication technologies. For example, the coordinator can transmit data using a Wi-Fi access point gateway connected to fixed broadband service or a cellular communication such as 5G. Finally, data reaches a computing and storage infrastructure where the information is processed and stored.

End-to-end services comprise end-node communication through the available communication technologies in essential services. Once the information in IoHT requires a timely delivery to avoid risking users' lives, it becomes necessary to manage communication resilience for all essential services. However, providing reliable performance (e.g., continuous data transmission, low delay) is challenging in IoHT. Random failures regarding communication can happen throughout the essential services reducing the probabilities of attaining end-to-end requirements.

The most common network configuration considering the essential services in IoHT comprises a wearable device collecting data from the user and transferring it to a coordinator device (e.g., a smartphone) with short and long-range communication capabilities (e.g., Wi-Fi and cellular). Supported by those communication technologies, the coordinator forwards the collected data to the computing and storage infrastructure where data is processed and stored. The final step comprises the dissemination of the information to granted users.

In synthesis, one of the relevant characteristics of IoHT is that the essential services are interdependent. IoHT applications require all three essential services, full or partial operation, to function properly (Cui et al., 2018). Time-critical and safety-critical applications have even more stringent requirements. For example, if the failure of a system could lead to consequences that are determined to be unacceptable, then the system is safety-critical (Knight, 2002). In essence, an IoHT application is safety-critical when a user's well-being depends on it. In addition, some real-time or near real-time applications in IoHT have special requirements considering the delay. In time-critical applications, any interruption throughout the essential services may lead to an increased delay, resulting in poor or faulty service delivery (Ghosh et al., 2019).

From a resilience perspective, increasing the reliability of essential services alone should be enough to guarantee resilience throughout the IoHT environment. However, most of the ICT pillars in IoHT (e.g., communication technologies, sensing technologies, and distributed computing), along with the services they support, overlap at some point, making it difficult to reach the IoHT-based paradigms (e.g., smart healthcare, ubiquitous healthcare), Figure 2.7 illustrates the overlapping of essential services, ICT pillars, and paradigms. Furthermore, most applications in IoHT use essential services as a unique and reliable system. Nevertheless, the IoHT environment is highly segmented and interdependent, which increases the alternatives considering data transmission and makes applying communication resilience mechanisms complex.

In order to identify approaches to apply communication resilience mechanisms in such complex and intricate environments, it is crucial to identify the main IoHT applications and their resilience requirements initially. The following subsections highlight the IoHT applications and their resilience-driven requirements.

2.2.1 The IoHT Applications

IoHT supports multiple applications such as (i) assisted living applications, (ii) vital signs monitoring, (iii) remote drug administration, (iv) physiological data analysis, (v) activity tracking, (vi) telemedicine, and (vii) user authentication by physiological signs. Applications

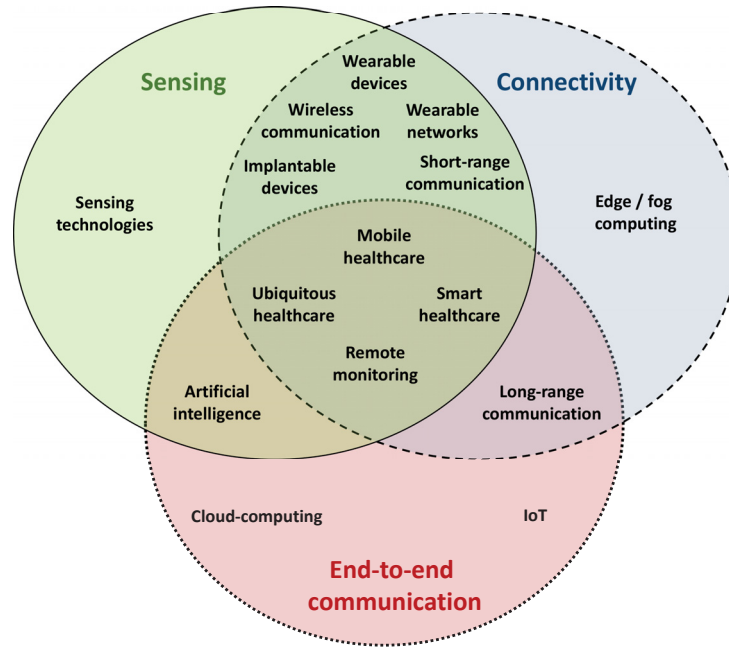


Figure 2.7: IoHT essential services, pillars and paradigms

rely on one or more essential services, demanding resilience in sensing, connectivity, and end-to-end communication.

Table 2.2 highlights the main IoHT applications and their criticality levels. We classify IoHT applications as safety-critical and time-critical. This classification correlates the application risks and urgency for the users' health. If a system failure could lead to consequences that are determined to be unacceptable, then the system is safety-critical (Knight, 2002). As mentioned above, an IoHT application is safety-critical when users rely on it for their well-being. In addition, some real-time or near real-time applications in IoHT have special requirements considering delay and overall quality of service. In time-critical applications, any interruption throughout the essential services may lead to an increased delay in data transfer, resulting in poor or faulty service delivery (Ghosh et al., 2019). Therefore, IoHT applications require low latency in urgent situations where prompt response is essential (e.g., cardiac arrest). Furthermore, low delay is indispensable for the consistent and continuous flow of information (e.g., remote assistance).

Table 2.2: IoHT applications criticality

IoHT Applications	Safety-critical	Time-critical
Assisted living applications	Yes	Yes
Vital sign monitoring	Yes	Yes
Remote drug administration	Yes	Yes
Online data analysis	Yes	Yes
Activity tracking application	No	No
IoHT-based telemedicine	No	Yes
Authentication by physiological signs	No	Yes

Assisted living applications comprises sensors worn by users and sensors in the environment that co-exist and communicate (Abtoy et al., 2020). For instance, ambient assisted living (AAL) assists home care users. The three pillars of AAL are activity recognition, vital sign monitoring, and sensing the surrounding environment. Lately, wearable devices have become a trending technology in ALS systems. By employing those devices, the applications in ALS can offer higher accuracy in situations requiring information about users' body movement and real-

time biosignals (e.g., fall detection and continuous vital sign monitoring). Additionally, wearable devices offer contextual information such as location, which helps track users' displacement, for example, to identify whether an older adult followed a route considering origin and destination.

Vital signs monitoring relies on different sensors to track user information and transmit data to a storage or computing infrastructure through mobile devices and the Internet (Hassen et al., 2020). IoHT devices monitor blood glucose, heart rate variation, blood oxygen levels, and arterial pressure. Variations of those signs might reflect a life-threatening situation and must promptly trigger an alert. A wearable device generally alerts the user through a visual or audio warning. However, in extreme situations such as losing consciousness, a distant person can receive the alert through long-distance communication (e.g., a user contact or a healthcare professional). For this configuration to work appropriately, data sensing, processing, and transmission must occur without delays or losses.

The **remote drug administration** relies on recent technological advances to connect devices such as infusion and syringe pumps to various systems and networks, contributing to IoHT. For example, a healthcare professional remotely accesses an infusion pump device and sets the exact drug dosage by evaluating the sensed data. Aside from the low latency required for the precise data evaluation, this application requires two-way communication to allow IoHT devices to send information to the storage/computing infrastructure and receive commands from the healthcare professional connected remotely. A different type of remote drug administration comes from automatic pill dispensers configured remotely by a healthcare professional (Chavez et al., 2020). In this scenario, the user will always be provided with the correct amount of drugs, avoiding overdoses and improving quality of life.

In order to identify patterns that might represent a health issue, the data collected by the sensing devices require **online data analysis**. A cloud infrastructure, for instance, integrates data from multiple devices and stores it securely. Data collected and previous health-related records allow for establishing a database accessible anywhere by users and healthcare professionals. The online data and health records analysis offer meaningful insights into users' conditions, supporting preventive actions and early diagnosis (Ali et al., 2020).

The **activity tracking application** offers essential information, such as the amount of sleep, step count, and heart rate variation. This application focuses on providing a personalized set of recommendations based on user goals and ongoing health achievements (Cipriano et al., 2021). This user-driven application stimulates users to become proactive partners in healthcare by reinforcing wellness and preventive care concepts.

IoHT-based telemedicine enables remote access to medical care by integrating health systems and telecommunication technologies. In this context, wearable devices add new information that complements and diversify the applications in conventional telemedicine (Angelucci et al., 2020). A remote consultation where a health professional assists a patient can gain new contours using wearables. In addition to the multimedia features of a conventional consultation, the health professional can observe the information collected from the wearable devices, providing a more comprehensive and accurate diagnosis. Based on the information provided by wearable devices and supported by telemedicine, new applications can emerge, including applications aimed at real-time diagnostics, support during the maintenance of chronic diseases, and remote assistance in the recovery of medical procedures.

The **user continuous authentication by physiological signs** is a trending application (Ekiz et al., 2020). Vital signs (e.g., electrocardiogram, photoplethysmography, electroencephalography) have unique patterns suitable for authentication and access control purposes. Vital signs support continuous user authentication rather than one-time authentication alternatives.

2.2.2 Resilience-driven Requirements

IoHT has specific requirements and deals with life-threatening situations, forcing a fast balance among performance, availability, and reliability. This section presents the main IoHT requirements related to safety-criticality and time-criticality. The communication resilience perspective follows the rationale that it is crucial to keep the essential services working, even in the face of unpredicted conditions caused by failures. The following paragraphs discuss the IoHT requirements regarding communication resilience. They follow a perspective based on the primary essential services once they are the foundation for the continuity and availability of the services related to IoHT. Hence, the main focus of communication resilience must be on sensing, connectivity, and end-to-end communication. In addition, there is a set of requirements that are transversal and independent from a specific essential service. Table 2.3 summarizes the communication resilience requirements regarding the essential services.

2.2.2.1 Sensing-related Requirements

The characteristics of devices and communication technologies that support the sensing services provide a complex environment to apply resilience mechanisms. Usually, each device collects data based on the available sensor and transmits it through short-range communication technologies. Conventional resilience techniques based on redundancy are challenging to adopt since the sensors and network interfaces integrate with the devices. In cases of malfunction, these devices must fast adapt to the available communication technology and could be subject to easy replacement. Security is an issue for sensing services. Even though the short-range communication technologies limit the reach for a potential intruder, there are examples of attacks aiming at wearable devices in literature (Shah and Sengupta, 2020; Sethuraman et al., 2020). The redundancy of the collected data is highly desired but hard to achieve with the existing configurations. Wearable devices must preserve data during sudden disconnections or communication failures. The main weakness, in this case, is the limited storage available in the wearable devices.

2.2.2.2 Connectivity-related Requirements

Redundancy at the connectivity level (i.e., the communication between pairs of devices) is necessary. For ensuring seamless data transfer through different communication standards, a high level of interoperability is necessary. Crowded environments make communication interoperability and coexistence very difficult. Also, access control is necessary to avoid unauthorized devices to flood communication channels, resulting in delays or service denial. Alternative communication channels must be available to avoid connectivity denial. It is possible to enable redundancy through multiple devices with the same purpose and different communication technologies, gateways with multiple communication technologies, and different data links to the storage/computing infrastructure. Once the communication technologies have a comprehensive range in connectivity services, they are susceptible to a broader range of attacks.

2.2.2.3 End-to-End Communication-Related Requirements

Communication resilience must happen through the entire communication path providing reliable data delivery and avoiding unauthorized access even when failures and attacks happen. So, measures should mitigate failures and attacks that might disrupt communication. Accordingly, employing multiple communication paths is one of the possible resilience approaches for end-to-end communication services. However, even when multiple data links are available, it is crucial to identify and deal with transmission delays in the storage/computing infrastructure (such as fog

or cloud). Additionally, solutions based on multipath protocols to enhance bandwidth utilization for the available communication paths increases resilience and security and create a better user experience for users and healthcare professionals.

Table 2.3: Essential services requirements

Essential Services	Resilience Requirements
Sensing	Easy, secure, and remote configuration Flexible inclusion of devices Redundancy for the collected signals Local storage in cases of connectivity issues In-device visual or audio warnings
Connectivity	Coexistence of communication technologies Access control mechanisms to devices Redundancy to face connectivity issues Adequate and high reliability bandwidth
End-to-end communication	Integrity, confidentiality and authenticity Using multiple healthcare providers Two-way redundant communication Dealing with edge, fog, and cloud delays

2.2.2.4 Transversal Requirements

Some requirements are recurrent throughout essential services. These requirements create dependency from one service to the next, demanding to achieve them at each service level. IoHT devices present mobility, creating challenges due to the constant changes in network topology and conditions. Furthermore, communication technologies provide different characteristics; some have a limited range (e.g., Bluetooth, Zigbee, NFC), others are highly susceptible to different types of interference, depending on the location (e.g., Wi-Fi, cellular wireless networks), and the operating frequency. Hence, managing mobility and its effects becomes essential for communication resilience. The interoperability among different proprietary devices and services must happen to offer seamless communication between IoHT devices and healthcare providers. The additional data from the growing number of IoHT devices and services can overload the communication channels. In order to prevent shortages of service, the communication channels and computing storage infrastructure solutions must consider scalability. IoHT devices have limited computing resources. Therefore, sensing devices must optimize resources usage by employing resilient-driven and energy-efficient communication protocols. For instance, cross-interference in wireless communication technologies may lead to excessive retransmissions, causing faster battery depletion. In critical situations, interconnected systems should reduce performance and quality of service expectations to focus on service continuity.

2.2.3 Security Principles and Attacks Regarding IoHT

Attacks that harm basic security principles are one of the leading causes of increased communication delays in IoT-based environments (Siddiqui et al., 2021). The lack of security mechanisms or the adoption of overcomplex solutions might also affect communication performance once they facilitate the attacks or overload the low-end devices in IoHT (Tawalbeh et al., 2022). The primary security principles applied to traditional computing systems, such as availability, integrity, confidentiality, and privacy, are even more restricted for IoHT. One of the reasons

for this is the sensitivity of the information collected and distributed. In general, the data existing in these systems represents personal and private information. Therefore, its unauthorized dissemination can negatively impact system users, service providers, and device manufacturers. Even when attacks fail to achieve their primary goal, the outcome is almost invariably increased communication delay and higher processing for IoHT devices, with exceptions for passive attacks. Figure 2.8 illustrates the main security principles associated with the most typical attacks in IoHT.

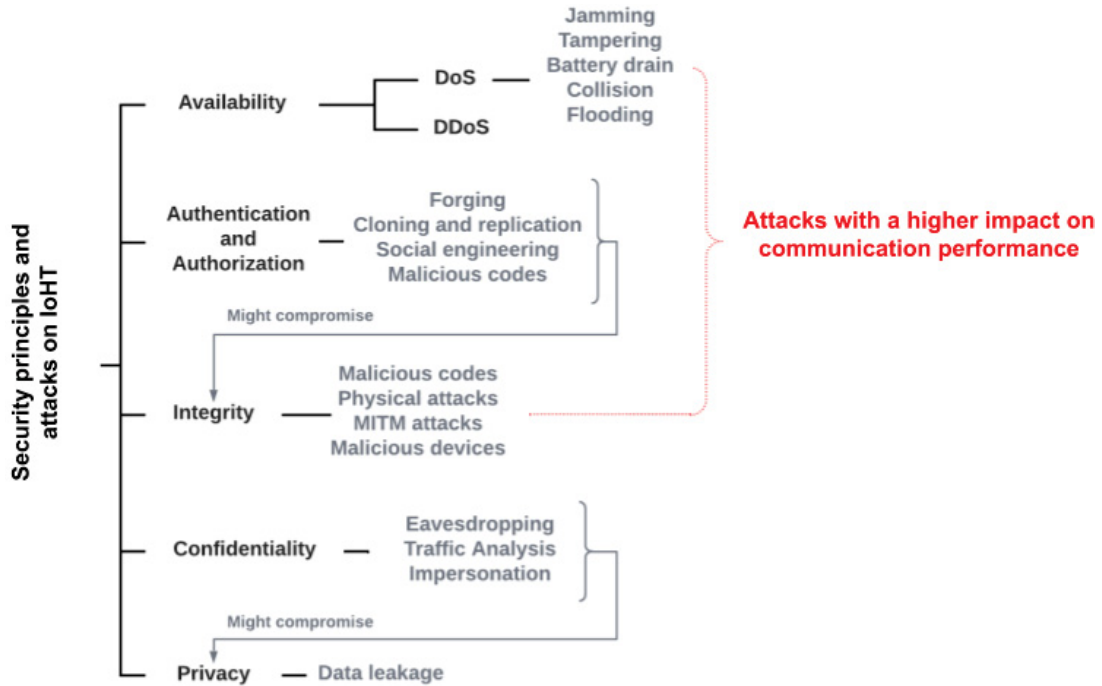


Figure 2.8: Basic security principles and attacks regarding the IoHT environment

2.2.3.1 Availability

The availability security principle ensures that all IoHT components function correctly and that the services provided are available to any authorized user or subsystem (Zaman et al., 2022). Therefore, information in IoHT must be promptly available to a legitimate entity whenever requested. Interruptions in the provision of services or the unavailability of the requested data may lead to situations that put a user in danger, including life-threatening situations. Currently, more IoT devices support healthcare applications. However, the systems employing those devices face issues related to low processing and memory, increasing the challenges when promoting the availability of the services provided. Due to the restricted computational characteristics, it becomes challenging to implement security mechanisms to protect the devices in IoHT, leaving them vulnerable to a series of known security problems. The main security issues are tampering attacks, jamming attacks, battery drain attacks, collision attacks, and flooding attacks.

Figure 2.8 illustrates that the attacks impacting availability in IoHT are tampering attacks, jamming attacks, battery drain, collision attacks, and flooding attacks. This range of attacks is known as denial of service attacks (*Denial of Service* – DoS). Variations of these attacks have gained notoriety in recent years in the form of distributed DoS (DDoS) attacks. DoS and DDoS attacks risk the IoHT environment during data acquisition and storage stages. Attacks directed at IoHT devices aim at temporarily or permanently turning off a device. The unavailability of the device can cause missing data, impair the accuracy and increase the end-to-end delay for applications. In order to deal with DoS and DDoS attacks, the problem is expected to be dealt

with as close as possible to the source of the attack. Thus, if an attack originates locally, an administrator can detect or mitigate the attack. Concurrently, if there is an attack from an external source, it is possible to use external security policies and mechanisms to halt the attack.

2.2.3.2 Authentication and Authorization

The complexity of the IoHT environment makes authentication a demanding operation since it must happen considering several heterogeneous networks and devices. Authentication must occur both for the entities that are part of the system and for the data that will be transmitted. Entity authentication aims to ensure that an authenticated stakeholder in the system connects to another stakeholder if and only if the second party is authenticated. Information authentication is the process by which an entity is verified as the origin of the generated data. One of the main trends for authentication protocols is the so-called lightweight authentication since the memory and processing limitations of IoT devices make the adoption of more robust protocols impractical. The authorization ensures that only recognized entities can access a particular service or resource.

All devices participating in the system must have native authentication mechanisms. However, due to the low computational capacity, IoHT devices often do not have authentication mechanisms or employ simplified versions of traditional mechanisms, which are vulnerable to attacks. Another problem lies in the incompatibility of authentication mechanisms between manufacturers. Since there is no consensus on a unique type of authentication, each manufacturer adopts a security measure, making adding and managing connected devices complex. Additionally, communication technologies for personal networks, such as Bluetooth, have several concurrent versions, some without any authentication mechanism to synchronize a device. The primary attacks aimed at interfering with authentication and authorization mechanisms consist of spoofing or forging attacks, cloning and replication attacks, social engineering attacks, and attacks involving infection through malicious code (Papaioannou et al., 2022).

In forging attacks, an adversary uses an authenticated device or subsystem to construct a valid identity. After accessing the system, the attacker begins to defraud the system with false information or gains access to privileged functions. In cloning and replication attacks, a user compromises a device and creates a significant number of clones to subvert the system. In IoHT, these attacks are not ruled out but are extremely rare since the number of devices and their exclusivity make their execution difficult. Another type of attack aimed at breaking authorization is considerably more direct and effective: social engineering attacks. Many users of IoHT devices have little or no affinity with technology, being relatively easy targets for attackers. If an attacker manages to access a smart device, such as a watch or *smartphone*, he will have access to many applications, including health applications. In this sense, several associated problems exist, such as simplified passwords, default passwords on devices, and a lack of configuration in mechanisms reinforcing security (e.g., two-step authentication and biometrics). Finally, attacks involving infection through malicious code can place an attacker in partial or total control of an IoHT device; later, the attacker can disable sensors, services, and other functions available.

2.2.3.3 Integrity

The principle of integrity aims to ensure that data is not altered or destroyed unauthorizably. In the context of IoHT, the principle of integrity seeks to preserve the accuracy of information about a user, including health-related data, location, or other personal information. Recently, the dissemination IoHT has boosted the debate about the need for greater cautiousness with the integrity of data that transits in this type of environment. The characteristics of devices and communication channels present in IoHT, especially when mobility is a preponderant factor,

create a diversity of vulnerability points that can be manipulated. Corrective measures and using software, devices, and communication technologies aligned with data integrity protection policies are crucial factors for accepting and massively adopting IoHT.

The central menace to data integrity in IoHT relates to improper manipulation of information during transmission. The manipulation can occur through malicious code that infects a device, captures and modifies relevant information, or through a targeted attack on communication channels. Another possibility is a physical attack on the device, in which the malicious user can obtain and manipulate the collected data. This attack generally requires initial information to access the device, such as a username, password, or both. One of the attacks directed at the means of transmission is the *Man-in-the-middle* (MITM) attack, where an attacker manages to impersonate one of the system agents and, from that action, starts to change the information accessed. Finally, a malicious device can be inserted into the system to collect relevant information and forward manipulated data. It is important to note that in the context of IoHT, these attacks are difficult to execute due to the mobility involved and the closeness of devices to the user. Some countermeasures that can be adopted to prevent integrity attacks are using encrypted transport channels, device authentication, authorization mechanisms, and changing default settings, such as username and password.

Integrity concerns are often associated with external sources such as attacks from malicious users. However, the guarantee of integrity also includes aspects such as the correctness and accuracy of the data because, in IoHT, the inaccuracy of the collected data can cause more significant risks than the absence of data. These data accuracy problems can occur for several reasons, such as poor sensor positioning, signal interference, device malfunctions, incorrect date and time settings, and lack of calibration.

2.2.3.4 Confidentiality

The principle of confidentiality within information security defines that confidential information must be unavailable to or shall not be shared with unauthorized entities. In IoHT, confidentiality refers, for example, to protect a patient's medical data that is shared with a doctor or health service provider so that they are not handed to third parties and used improperly. Protection mechanisms should also encompass measures against attackers who scour communication channels for sensitive information. The information stored on devices and infrastructures should also be protected against intrusion. By adopting protection measures that substantiate the principle of confidentiality, identifying a user from improperly collected data becomes more complex, assisting in maintaining data privacy.

2.2.3.5 Privacy

The principle of privacy is the property of a system that seeks to ensure that a user's private data is safe against unauthorized disclosure or attempts to exploit such possible disclosure illegally. The main concerns associated with the breach of privacy in IoHT relate to the misuse of data and its implications, such as the exposure of information on social networks, the use of information for blackmail or schemes, and the unauthorized disclosure of data by service providers. For an IoHT user, any information leak from a participating device may represent the unauthorized disclosure of a health condition, location, a specific behavior or routine, and additional information that might be used in scams or extortion attempts. For equipment manufacturers or service providers, the leak of private information can represent a loss of credibility, causing immeasurable damage.

Sensitive information stored by healthcare service providers is one of the primary sources of data leakage (Alhaj et al., 2022). Therefore, all storage points must have access control

and identity identification mechanisms to ensure the confidentiality of sensitive user information and prevent violation of their privacy. However, as this information is often entrusted to a cloud storage system, it becomes vulnerable to a data leak. As a result, stored data can be obtained through an attack or intentionally exposed by any entity with access to the system. Another trend that requires the same cautiousness concerning data leaks is parsing operations on *Big Data*. To infer valuable health-related information from users, a healthcare provider may entrust the information to a third party to analyze and identify characteristics. In these cases, the entire process must be protected to guarantee the user's privacy (Onesimu et al., 2022). Companies that provide services related to data storage and processing must follow regulations to ensure that the right to privacy is guaranteed. Privacy-related menaces are the least penalizing considering the IoHT environment once the main target is the users' data instead of a system component.

2.3 EXISTING APPROACHES FOR COMMUNICATION RESILIENCE

Given the constrained devices and multiple communication technologies, resilience is challenging for IoT communication (Tsigkanos et al., 2019). Providing a stable system is the main goal for most IoT resilience works, although they tackle isolated attributes while pursuing trustable service delivery. In a comprehensive view, this section organizes the main existing works related to communication resilience. Figure 2.9 presents the proposed classification based on essential services: sensing, connectivity, and end-to-end communication. Considering the essential services, the organization follows a perspective based on the network resilience attributes defined by Avizienis et al. (2004) and Sterbenz et al. (2010a): dependability, security, tolerance, and performability. Additionally, the taxonomy illustrates the solutions available in the literature.

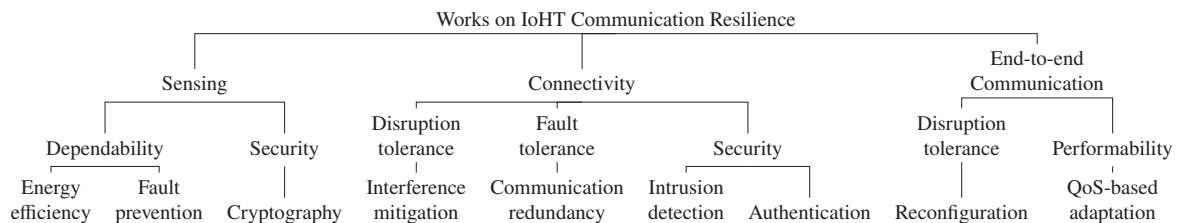


Figure 2.9: Taxonomy for works on IoHT communication resilience

Works focusing on the *sensing essential service* mainly handle issues related to dependability and security attributes of resilience such as device and data security, energy efficiency, and malfunctioning detection. Regarding dependability, works address energy efficiency to strengthen availability in IoHT. The intention is primarily to reduce the energy consumption of devices by optimizing sensing, processing, and data transmission. For instance, Salayma et al. (2018) investigated current and legacy communication protocols that promote device uptime. Regarding malfunctioning detection, there are proposals for failure detection, particularly for IoHT devices. One of the applied approaches lies in constantly collecting and performing anomaly detection on the gathered data, as proposed by Jeong et al. (2014).

Few works concentrate on cryptography-based solutions to address security concerns and promote resilience. Approaches include cryptographic primitives, such as public critical infrastructure, to ensure data confidentiality and privacy. For example, data is encrypted prior to transferring information to the cloud. However, data must be decrypted on arrival, increasing the time and cost of data retrieval. Esposito et al. (2018) proposed a blockchain to protect healthcare data, bringing security and resilience to attacks. The solution inserts health-related data in a

new block for later distribution. If approved by the blockchain participants, it adds the block permanently to the chain.

Works on *connectivity essential service* mainly handle issues associated with disruption, traffic tolerance, and security resilience attributes. The solutions involve interference mitigation, communication redundancy, intrusion detection, and authentication. Regarding interference mitigation among communication technologies (e.g., Wi-Fi, Bluetooth, and Zigbee), the literature reveals that it can result in delays and data damage, directly compromising the resilience of IoHT critical applications. Hence, various works are investigating this issue. For instance, Shao et al. (2020) investigated the effect of Wi-Fi signals in the 2.4GHz band interfering with the Zigbee technology. The outcome is an inaccurate triggering of false alarms to idle Zigbee devices causing considerable energy waste.

The primary example of communication redundancy lies in using multiple communication technologies, providing redundancy, and improving communication resilience. For instance, Cisotto et al. (2020) proposed using 5G cellular communication to attain redundancy while an ambulance moves through multiple locations. Cicioğlu and Çalhan (2019) presented a resilient solution based on communication redundancy that allows IoHT devices to send data to remote locations using device-to-device communication. Finally, some works have proposed new security mechanisms specifically for IoHT demands. In general, the works review security following the perspective of the IoHT requirements and applications. Mainly, they are concerned about identifying threats and resilience against attacks. Security mechanisms have been adapted to IoHT instead of designed with the IoHT requirements in mind.

Benkhelifa et al. (2018), revised traditional IDS solutions and their application to IoHT. Hady et al. (2020) built a real-time healthcare monitoring system and employed machine learning techniques in the collected data to provide intrusion detection. In (Cao et al., 2019), the authors intended to preserve user identities, creating a mechanism to dissociate them from health data. Also, the authors proposed a resilient IoHT architecture to support eHealth, similarly to (Sharma and Kalra, 2019), in which the authors presented a resilient protocol against multiple attacks in IoHT connectivity service. The authors in (Strielkina et al., 2018) developed a Markov model for an IoHT infrastructure considering security issues. They could identify the most frequent failures in connectivity service. Solutions designed specifically for IoHT are also available in the literature. In (Nakayama et al., 2019), the authors proposed an authentication mechanism based on biometric traits to grant access to IoHT devices. The gathered data is transmitted using an alternative intra-body communication channel, increasing the resilience to wireless attacks.

Few previous papers have addressed communication resilience related to the *end-to-end communication service*. The main approaches focus on recovering the service functionality through adaptation or reconfiguration of resources. In (Cicioğlu and Çalhan, 2019), the authors described an architecture to face disaster scenarios involving workers in underground areas. The paper presented a technical solution to control the communication density of the surviving nodes to ensure energy efficiency and increase resilience. The description of the disaster recovery architecture brings no detail regarding the challenges of implementing such a solution.

In (Khan and Yuce, 2010), the authors proposed a new evaluation metric for end-to-end communication resilience that correlates fault tolerance and performability. They also use this metric to provide an adaptive configuration management solution. If a certain QoS level is not achieved within a specific configuration, the communication infrastructure could use redundant devices and communication channels to accomplish the desired level of quality. Despite being related to IoHT, their focus was wireless body area networks, not specifically IoHT.

Observing the proposed taxonomy leads to different features that can improve communication resilience. Resilience solutions focus on maintaining the device's operation for the sensing

services. In contrast, connectivity services aim at improving system tolerance when facing threats and improving resilience through security mechanisms. End-to-end services rely mainly on performance evaluation mechanisms such as QoS measurements to gather the information that assists in the adaptation or reconfiguration of a system. Studies that focus on a system's ability to identify and tolerate unpredicted traffic loads, whether legitimate or from attacks, are absent in IoHT and could contribute to identifying more accurate performance indicators.

One of the most noticeable problems for communication resilience in IoHT is the lack of integration between essential services. Even when solutions emerge from the same attribute of resilience, they serve specific purposes, depending on the essential service to which they belong. This lack of cooperation hinders the implementation of solutions aimed at greater integration between services. The communication resilience mechanisms implemented for an essential service can cause unforeseen inconvenience to the following essential service. Therefore, future solutions seeking communication resilience in IoHT must safeguard the characteristics of the current essential service and consider the communication performance impact they can bring on the IoHT environment.

Therefore, the lack of interaction among the components and services is one of the main problems for inserting adaptive actions in the existing proposals that aim to increase resilience for IoHT. Notably, the solutions are directly connected to essential resiliency principles concentrating more on devices than processes. This strategy proved efficient for specific cases, but considering IoHT and its particularities, broader and more collaborative management is necessary. Current solutions to improve communication resiliency in IoT environments must be adapted or ported to integrate adaptive measures.

2.4 ADAPTIVE MANAGEMENT PRINCIPLES

Adaptive management is a structured approach to decision-making that encourages iterative phases of learning and adaptation of control to fully meet the objectives of management. Adaptive management was initially proposed for resource managers to integrate scientific understanding with managing natural resources. A significant benefit of this approach has been a process that produces new and novel understandings of complex system dynamics and innovative policies and practices. Adaptive management provides a receptacle for innovation because it focuses on integrating scientific understanding, resolving and managing inherent uncertainties, and questioning assumptions, boundaries, and policies (Gunderson, 2015). It is adaptive because it recognizes that managed resources will always change, that surprises are inevitable, and that new uncertainties will emerge (Holling, 1978).

Adaptive management acknowledges that policies exist to satisfy specific objectives but must be continually modified and flexible to adapt to unforeseen changes. It also views policy as hypotheses, meaning that most policies are questions. Because policies are questions, management actions become treatments in an experimental sense. Adaptive management is also an alternative to centralized resource management decision-making techniques (Holling and Meffe, 1996). In adaptive management, chosen strategies are seen as experiments that provide information about the managed system, which will benefit in refining future strategies.

Adaptive management has been employed mainly for natural systems, specifically human relations (McFadden et al., 2011) and ecological systems (Tompkins and Adger, 2004). Over the past few years, adaptive management has become an increasingly popular management-decision tool within the scientific community, employed in multiple domains, such as socio-ecological, psychological, organizational, engineering, and infrastructure. The National Academy of Sciences (NAS) highlights key resilience features applicable to multiple application domains. The features

in common include service continuity, stable systems states, time and scale of events, the memory of previous disruptive events, and adaptive management (Connelly et al., 2017). Thus, along with other essential features, adaptive management is naturally coupled with the resilience of systems.

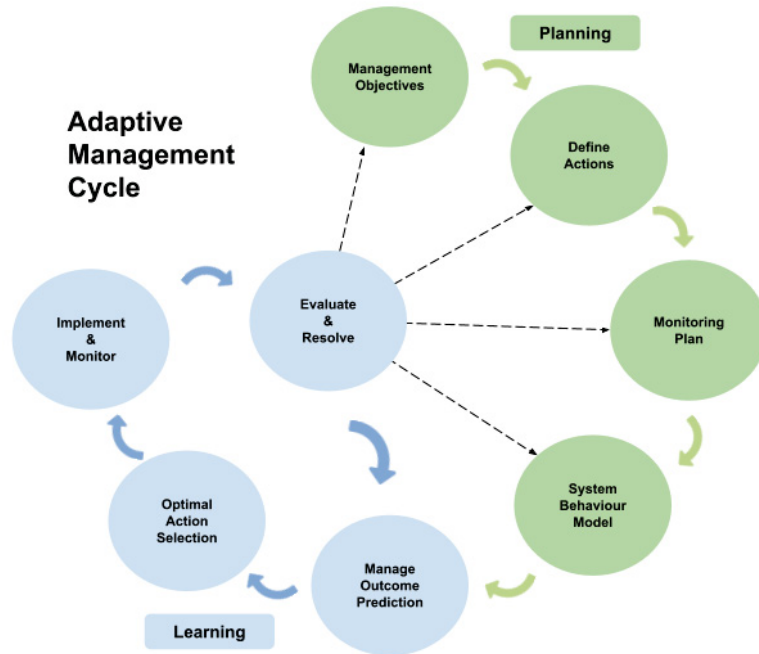


Figure 2.10: Adaptive management cycle adapted from (Allen et al., 2011)

Figure 2.10 describes the Adaptive management cycle. The planning stage (green circles) encompasses pre-defined tasks with input from stakeholders, such as management objectives, possible actions, a monitoring plan, and a system behavior model. In the learning and implementation phase, the components involved (blue circles) aspire to forecast the potential effects of control. The prediction supports a more precise action selection, which benefits the implementation of better solutions. As the cycle completes, the proposed solutions assist in designing new or concurrent behavior models, reducing uncertainty. Finally, dotted black arrows represent the latest information that may lead to changes in the planning components. However, this can eventually harm the ability of adaptive management to select optimal control options.

There are two dominant adaptive management schools of thought that most adaptive management approaches follow: the Resilience-Experimentalist Adaptive Management School and the Decision-Theoretic Adaptive Management School. The Decision-Theoretic School, more heavily influenced by decision theory, utilizes stakeholders' communication to define the management problem, objectives, and actions before developing process models. In Experimentalist Adaptive Management School, there is a high emphasis on obtaining a shared understanding among system stakeholders during the entire process, especially before defining objectives and management actions. In addition, proponents of this school also require active learning about system resilience (i.e., the capacity of an ecosystem to remain within its current state or return to its original state following perturbation) (Walters, 1997; Holling, 2001). Figure 2.11 compares the two dominant adaptive management schools of thought.

2.4.1 Adaptive Management and Computing Systems

Over the last few decades, the adaptive management concept has been applied in some areas of computing systems. Before the propagation of interconnected systems, adaptive management

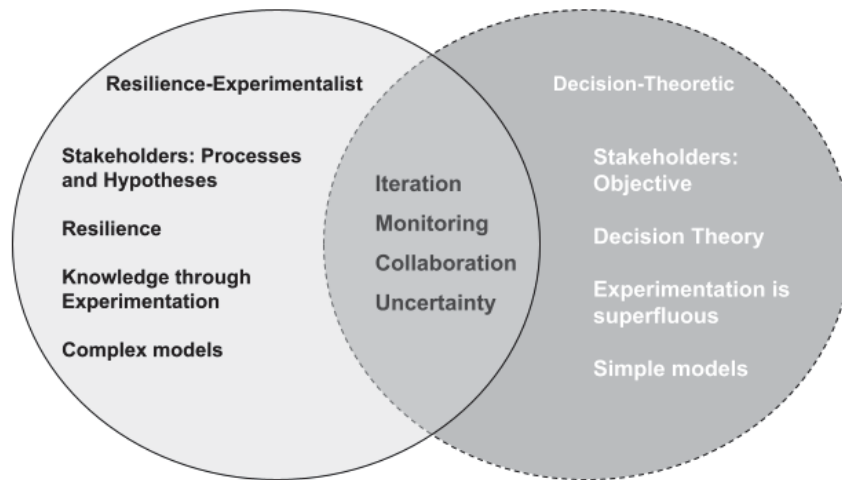


Figure 2.11: Dominant adaptive management schools adapted from (McFadden et al., 2011)

assisted in handling computing resources (Kephart, 2005), user behavior modeling (McTear, 1993), and performance management of local applications (Abdelwahed et al., 2009). With the promotion of networked systems, the initial concept of adaptive management slightly changed to meet new requirements, topologies, services, and applications. Today, most interconnected systems use the Internet to exchange information. These systems exponentially increase the available resources, making management and decision-making more complex. Recent adaptive management techniques attempt to satisfy the interconnected systems requirements with specific objectives, such as providing a better quality of service for Internet services (Gmach et al., 2008), offering self-adaptation for computing services (Paulos et al., 2019), and building artificial intelligence behavior models to face threats (Shandilya et al., 2022).

2.5 ADAPTIVE MANAGEMENT AND COMMUNICATION RESILIENCE IN IOHT

Most strategies inspired by adaptive management schools focus on the Decision-Theoretic school. That is understandable since, considering computational systems, the most typical strategy is to pursue a solution encompassing the concept, design, and implementation, fulfilling all development stages and aiming to insert adaptive management concepts into the process. In this thesis, we follow a hybrid approach mainly founded on the concepts of the Resilience-Experimentalist school, investigating the relationship between the stakeholders of a system and envisioning the possible management actions considering the defined objectives and the autonomy regarding the reach of the systems and subsystems. Additionally, we propose using knowledge gain based on experimentation as active learning to obtain a comprehensive and fresh view of the current IoHT implementations and define possible corrective actions to deal with uncertainties. Since the IoHT environment encompasses more straightforward communication topologies regarding each essential service alone, some of the resulting models mirror the ones proposed by the Decision-Theoretic School. Nonetheless, it is valid to mention that both schools aim for the same goals and deal with common aspects such as uncertainties and collaboration among the stakeholders.

The essence of adaptive management is developing actions designed as much for learning as to meet predefined objectives. The design of adaptive experiments or treatments is one of the outcomes of adaptive evaluations (Walters, 1986). Implementing those experimental or treatment designs has been problematic and can be hindered for several reasons. The reasons include the inability to control critical variables at appropriate scales, unwillingness to risk the results of

outcomes, costs of experiments, inability to monitor fundamental resource responses, and the lack of control (Gunderson, 2015). The adoption of Adaptive management in this thesis aims to integrate a variety of stakeholders within the IoHT system. Stakeholders support a set of isolated services that interact and are conditional, meaning that a problem in one service can affect the other dependent services. In this sense, the evaluations relate to the problem statement and the presented research questions. Also, the experimentation phase evaluates the IoHT systems and subsystems when confronting threats and uncertainties, reinforcing knowledge gain.

Adopting adaptive management in this thesis relies on the main approaches of the experimentalist resilience school. The stakeholders represent IoHT components with a high emphasis on communication representing the information from processes, while uncertainties represent threats to communication resilience. Additionally, experimentation aims to obtain the best conclusions that can, later, act as input for improving the overall system behavior regarding communication performance and security. The significant changes in adaptive management regarding IoHT compared to traditional adaptive management models relate to complexity, once traditional adaptive management deals mainly with a single extensive and complex model. The IoHT design proposed in this thesis comprises three interconnected models defined by the essential services. Finally, the characteristics representing collaboration, iteration among processes, and system monitoring in case of threats will adjust to the components available in the IoHT environment.

2.6 LONG-TERM RESILIENCE IN IOHT

Only a fraction of possible failures and threats can be considered during the design of a system. The impossibility of predicting every unplanned change in such a complex system may lead to new fault situations. Additionally, new attacks can emerge during and after the implementation. In order to achieve long-term dependability and security, the IoHT needs adaptation techniques that work cooperatively with the traditional fault-tolerant techniques. The main techniques envisioned to ensure long-term dependability and security are related to adaptive systems.

Resilience in the IoHT environment is complex and challenging to achieve. The dependency between technologies, devices, and services is more significant than in traditional systems. In reality, this dependency cannot be segmented, and it is necessary to consider the system dependency using a global approach. Dependability and security can be achieved by adaptive systems that can modify their behavior and/or structure in response to their perception of the environment and the system itself and their goals (De Lemos et al., 2013). Many of the traditional resilience techniques fail to handle dynamic or evolving systems. However, the current approaches can be extended using artificial intelligence or new techniques that satisfy IoHT needs. The traditional and static approaches are being replaced by machine learning-based techniques because of their ability to extract additional features from a complex and massive amount of data (Park et al., 2020). Nevertheless, machine learning techniques typically disregard the limited computational resources, the interoperability among the essential services, and the real-time characteristics of some systems. Considering those shortcomings, adaptive techniques for the IoHT environment must be extensively analyzed.

Figure 2.12 illustrates the relationships between resilience, mitigation and recovery, tolerance, and adaptation desired for the IoHT environment. The adaptation process must consider resilience, mitigation or recovery, and tolerance properties as a cooperative process. Regarding resilience, the dependability and security properties are indispensable for a trustworthy system, while performability will assure performance delivery considering a service specification. This specification can be described as a set of metrics such as delay, throughput or goodput,

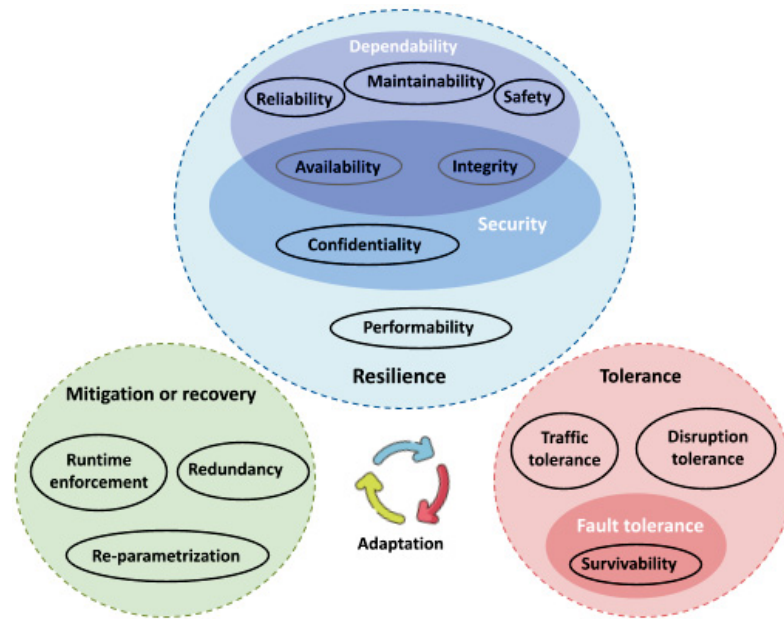


Figure 2.12: Desired disciplines and techniques for resilient and adaptive IoHT

and packet delivery ratio. Performability metrics include formal or informal contracts such as service-level agreements (SLA) and pre-established or online metrics such as quality of service (QoS). Mitigation or recovery techniques involve practices that reduce the impact of threats upon a system or allow full recovery from a failure condition. Tolerance techniques involve the practices that enable a system to continue its intended operation in the presence of failures.

In order to build long-term resilience in IoHT, adaptability is a fundamental property since, during the design time of a system, only a subset of failures and threats are recognized. However, the changes in the system itself or the environment can not be predicted, which may lead to new possible faulty scenarios. Furthermore, over time new attacks can surface, new vulnerabilities in the system can emerge, and attacks may get more elaborated (Ratasich et al., 2019). Therefore, IoHT must encompass adaptation techniques to achieve long-term dependability.

2.7 CHAPTER SUMMARY

This chapter introduced important concepts on resilience for networked computing systems. It presented the definition of faults, errors, failures, and attacks and the main techniques to achieve resilience. This chapter also offered an in-depth view of the IoHT environment and a detailed description of its essential services, applications, and requirements. A review of existing approaches dealing with communication resilience in similar environments was also presented. This chapter likewise presented the Adaptive management concept and schools of thought and explained how they support this work. Finally, we introduced the desired disciplines and techniques to increase resiliency in IoHT environments.

3 A RESILIENCE MANAGEMENT ARCHITECTURE FOR COMMUNICATION ON PORTABLE ASSISTED LIVING

The Internet of Health Things (IoHT) is revolutionizing medicine and healthcare, opening up a myriad of possibilities. It interconnects portable healthcare devices and the Internet; offers continuous sensing of personal and environmental data, remote monitoring, and insights into symptoms and treatments, providing high control to patients over their lives and treatments. A vast number of IoHT applications, such as Ambient Assisted Living (AAL), retrieve valuable information (e.g., user heartbeat rate and temperature), predict and identify falls, for instance, and provide location for urgent care. AAL has a great relevance given the aging of the world population. The Organization for Economic Co-operation and Development countries forecast that 10% of the population of the world will be more than 80 years old by 2050 (OECD, 2019).

IoHT has gained increasing attention from academia and industry on AAL because it shifts care provision from inside traditional care buildings to continuous care anywhere and anytime. Today, one-third of the existing IoT devices is healthcare-related and it is estimated that 87% of health organizations use IoHT. With the popularization of portable healthcare devices and the Internet through high-speed communication technologies, as 5G, new scenarios open to AAL, including scenarios in which AAL becomes portable and the individuals benefit from the continuous monitoring and assistance even when they are not in their conventional ambient.

Providing portability for assisted living systems through IoHT requires particular attention to the resilience of communication between devices. First, AAL deals with demanding requirements in terms of timely data delivery even under scenarios in which multiple communication technologies coexist. Second, IoHT comprises a wide range of heterogeneous devices and communication technologies. Third, the malfunction of crucial elements may lead to unexpected behavior in the network, compromising portable assisted living systems that lean on them. IoHT relies on telecommunication infrastructures, such as cellular and fixed broadband operators, and the Internet. However, operators are susceptible to failures, affecting IoHT applications.

Communication performance and resilience is a primary concern once portable assisted living systems require high reliability for sensing, connectivity, and end-to-end communication, i.e., essential services. The availability of those services is vital once they manage data acquisition from users, communication, and data transfer between end-hosts through the Internet. Thus, potential faults in any essential service can jeopardize the operation of portable assisted living systems. Works considering resilience for portable assisted living systems deal with each essential service separately. Mainly, works handle topics that assist in designing more reliable sensors and devices for sensing services (e.g., energy efficiency and signal redundancy), managing the communication for connectivity service (e.g., mitigate interference and increase security), and enhancing communication performance and availability for end-to-end communication service (e.g., decreasing delay, overcoming network bottlenecks, and data replication).

The heterogeneity of devices and communication technologies in IoHT combined with the autonomy of the services provided by portable assisted living systems expose the limitations of current communication resilience methods. IoHT resilience has been addressed from multiple perspectives. Previous studies focus on (i) the design of resilient systems (Russell et al., 2018; Sagar et al., 2020; Shahbazi and Byun, 2020; Shao et al., 2020), (ii) the capacity of the systems to resist uncertainties (Ullah et al., 2021; Cisotto et al., 2020; Zamanifar, 2020), and (iii) the outcome from failures that affect the interdependent networks (Khan and Yuce, 2010). However, current approaches handle each essential service individually, making a challenge to manage and

achieve reliability in a holistic way. Furthermore, the existing resilience management approaches for IoHT resilience relies on mainstream solutions disregarding the possible configurations available in current and upcoming communication technologies. The advances in healthcare devices and communication technologies compel to create means of efficiently managing the essential services and achieving portable and resilient assisted living systems.

Managing a joint resilience in sensing, connectivity and end-to-end communication is mutually imperative and challenging (Giordani et al., 2020) to portable assisted living systems given their features and requirements. Hence, this chapter introduces an architecture that manages communication resilience in portable assisted living systems by employing redundant communication paths provided by multiple communication technologies. The architecture relies on portable gateways with multipath capabilities, i.e., they employ different communication technologies concurrently to promote redundancy for communication and enhance both resilience and performance. Portable gateways are strategically positioned regarding the essential services, interacting with sensing and connectivity devices and providing valuable information for end-to-end communication. Hence, the main contributions presented in this chapter are described next.

- A clear view of requirements to communication resilience in IoHT with an novel perspective founded on IoHT essential services.
- A Portable Assisted Living System concept aimed at managing communication performance and extend the monitoring area for users in the context of Ambient Assisted Living systems.
- The design of an architecture that manages communication resilience for portable assisted living systems.
- A detailed description and advanced resilience evaluation of a Portable Assisted Living System (PALS) solution, considering time-critical applications and multiple communication paths provided by different communication technologies.
- A meaningful discussion leading to insights, open issues, and pointing out future research opportunities.

This chapter proceeds as follows. Section 3.1 presents the related works. Section 3.2 introduces the concept of Portable Assisted Living Systems, focusing on differentiating Ambient and Portable Assisted Living systems. Section 3.3 shows a classification of the existing works regarding particularly IoHT and communication resilience. Section 3.4 details a resilience management architecture for communication on portable assisted living. Section 3.5 describes the performance evaluation and results. Section 3.6 describes the resilience evaluation and results. Finally, section 3.7 concludes the chapter.

3.1 RELATED WORK

Works in the literature focus on different aspects of the AAL environment, such as improvements in data collection and activity recognition models. In most works, authors assume that data transmission happens without errors or delays, disregarding communication issues. However, performance management for communication in AAL is essential. Different traffic management strategies are available in the literature, such as over-provisioning communication links or reserving bandwidth for applications (Zinner et al., 2017b). More specific solutions to improve

performance are also available, such as management using software-defined networks (SDN), using alternative communication protocols, and applying fog-based solutions.

Authors in (Isravel et al., 2020), used an SDN controller to control traffic flow rules to devices in AAL, avoiding congestions in the communication channel. Authors in (Gomes et al., 2015) used the single path Mobile Reliable User Datagram Protocol (MR-UDP) to improve network performance. The communication using this protocol comprised only mobile devices and the gateway. In (Nikoloudakis et al., 2016) the authors proposed a fog-based approach to avoid communication bottlenecks in the cloud. The solution involved a virtual fog layer that used the cloud timely.

Previous works handling mobility and AAL relate to limited areas, usually indoor buildings. In (Zinner et al., 2017b), the authors have placed distributed devices in a closed environment to monitor users and communicate between themselves and with static communication gateways. In (Laine et al., 2014), a mobile gateway for healthcare systems using 3G cellular communication was proposed. But, the integration with the static AAL environment or the handover among communication technologies were not within its scope. In (Elsts et al., 2018), it was proposed a smart home where static and wearable low-power healthcare devices collect data and transfer it using a 3G/4G communication link. Although, the system achieved a successful deployment and showed good network performance, the system is limited to send only a sub-set of the monitored data through the 3G/4G communication link once the transmission of multiple gigabytes per day over the 3G/4G link, would dramatically increase the costs.

Few previous studies dealt with performance considering communication protocols and critical applications. In (Zinner et al., 2017a), they conducted experiments considering AAL applications and different transport-layer protocols, including the single path QUIC protocol. The measurement-based experiment has compared the performance of multiple transport-layer protocols taking into account as evaluation metric the loading time for different web pages. Results showed better performance from QUIC over HTTP and HTTP2, but the authors provided no information regarding applications and requirements.

In (Mogensen et al., 2019), the authors proposed an algorithm to provide selective redundancy for a critical application using MPQUIC and 5G wireless networks. To achieve redundancy the algorithm identifies the priority traffic and duplicates its packets through redundant paths while background traffic benefits only from single path QUIC features. Employing multiple communication technologies or the transition among the communication paths were outside the scope. One previous work tested the portability in multihomed devices when automatically transitioning among networks. In (De Coninck and Bonaventure, 2019), the authors tested the MultiPath Transmission Control Protocol (MPTCP), that is available in a smartphone to seamlessly handoff from a WiFi to an LTE connection without user interference or losing the initial connection establishment. Despite a successful transmission ratio of 90% for MPTCP in gradual transitions between paths, MPTCP is not present in most portable devices, and its deployment requires complex software changes.

The works available in the literature regarding AAL mostly employ exclusive communication technology, even when they use multipath protocols. Using fixed communication technologies limits the monitoring area for users while employing cellular communication alone brings additional expense to a system aiming to reduce costs. Even though mobility is dealt with in previous works, the main approaches consider classical AAL with limited areas. Transport-layer multipath protocols adoption is gradually increasing, but it still focuses on the communication between high-end hosts and servers, which makes mobility complex. We advocate that embracing AAL systems must provide communication performance and mobility.

Hence, the proposal presented in this chapter advances this research direction, taking into account the AAL characteristics and requirements.

3.2 PORTABLE ASSISTED LIVING SYSTEMS

Modern medicine allows senior citizens to live longer, healthier, and therefore more actively (OECD, 2019). Thus, it is necessary to modernize the concepts of traditional Assisted Living Systems such as AAL to support their benefits without limiting users activities. The existing portable and wearable devices in IoHT and current communication technologies can improve users mobility without losing functionality compared to AAL. The concept of promoting additional freedom by integrating traditional AAL and new IoHT devices and communication technologies is called Portable Assisted Living (Nakayama et al., 2021).

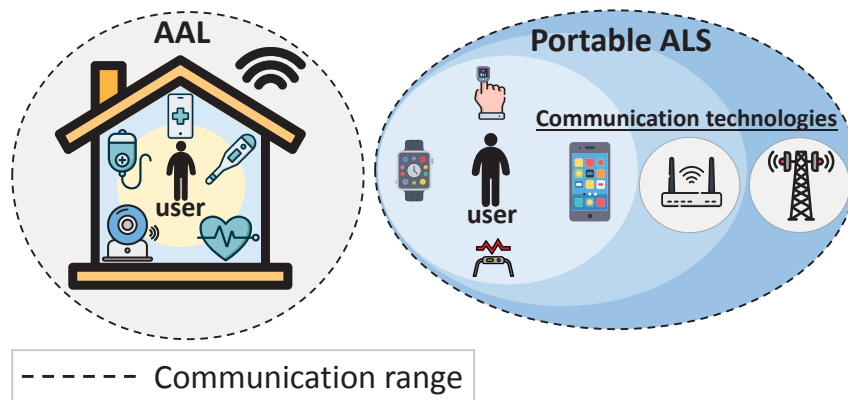


Figure 3.1: Tradional AAL vs. portable ALS

Figure 3.1 compares AAL and portable ALS. The primary idea in AAL is to provide a controlled environment through devices placed on the environment and, more recently, employing wearable devices. However, several issues remain in AAL systems, such as the acceptance of the involved technologies by older adults (e.g., cameras, motion sensors) and privacy and security issues once AAL employs extensive use of personal data to provide context-aware services (Marques et al., 2019). Since AAL highly depends on the environmental settings, the users become restricted to houses or apartments to benefit from the system. Additionally, AAL systems rely on fixed broadband communication technologies, thus restricting user mobility.

In portable ALS, the users rely on wearable devices that constantly collect health-related data independently from their location. User acceptance is not an issue once familiar objects hold the sensors (e.g., watches, clothes, smartphones). Most wearable devices are unable to communicate directly with mobile networks. In this context, portable coordinators such as smartphones can extend the coverage area for being compatible with multiple communication technologies, including short-range technologies (e.g., Bluetooth, Wi-Fi) and long-range communication such as cellular. Portable Assisted Living systems allow continuous monitoring of health-related data by IoHT devices and data transmission through portable communication gateways, encouraging free movement within the communication range.

In order to accomplish the portable assisted living goals, (e.g., seamless remote monitoring, ubiquitous mobile healthcare) the communication technologies must offer high reliability since a hazardous incident concerning users health can happen anywhere oppositely from traditional assisted living systems where users are in a controlled environment. Aside from reliability, communication in portable assisted living must provide delay values accordingly with the requirements of the applications. An advantages of portable assisted living lies in the

communication capabilities of the coordinator device. Usually, the coordinator can communicate with nearby devices employing short-range communication (e.g., Bluetooth, Wi-Fi) and long-range communication such as 5G. Novel communication protocols can enable the coordinator to use multiple communication paths provided by different technologies concurrently, adding a new perspective for communication resilience.

3.2.1 PALS System

This section describes the Portable Assisted Living system (PALS), a multi-layered system. The main functionality of the system is to provide portable assisted living using multiple communication paths and a multi-homed enabled coordinator to transfer data to a remote server. Once mobility is an inherent human behavior, users can be out of the defined AAL sensing area at a particular time. PALS allows a user to take advantage of existing AAL environments, based on static sensors and extends the AAL services to remote locations using applications that collect data from mobile sensors like those found in wearable devices.

Services, such as the continuous monitoring of vital signs and alert provision, remain invariable. The PAL system allows the simultaneous use of paths from multiple communication technologies, such as Wi-Fi and cellular, and it provides seamless transitioning among these paths without user intervention. Figure 3.2(a) illustrates the integration between a traditional AAL and the PAL system. While the user is inside the AAL range, s/he benefits from static and mobile sensors and the coordinator device can use simultaneously the different paths provided by wireless communication technologies, such as WiFi and cellular. Once the user moves away from the AAL environment, the portable coordinator continues to monitor the mobile sensors attached to the wearable devices.

The PAL coordinator keeps sending data to a remote infrastructure by means of the cellular long range communication. The PAL coordinator assists in handover among the paths provided by wireless technologies when the user is transitioning between the AAL and PAL systems. Figure 3.2(b) illustrates the PAL system proposed architecture which consists of four layers: sensing, gateway, network, and remote applications. This architecture encompasses different trending technologies considering the end-to-end communication cycle. For this work, we focus on the communication performance and handover functionalities that occur in the gateway layer. The next paragraphs describe in detail the gateway layer (main focus of this work) and we briefly overview the sensing layer that is responsible for collecting user data.

The sensing layer consists of wearable devices collecting user information such as heart rate variation, body temperature, and blood pressure relevant for healthcare practitioners. Continuous and efficient monitoring of vital signs is a fundamental feature of the system as the collected data serves as a basis for identifying anomalies that may indicate critical condition or disorder (e.g., arrhythmia, fever, high blood pressure). Additional sensors, such as accelerometers, gyroscopes, and compasses, provide relevant data to improve user quality of life. Data from these sensors allows identifying the type and quality of the physical activity, the risk of a potential fall, and other health-related information. Sensors are distributed through different devices or combined in a single device such as a smartwatch. Each sensor provides a different type and amount of data depending on the sensor characteristics and sensing frequency.

A personal mobile device, like a smartphone, is the natural choice for playing a portable gateway role because it provides mobility, communication, and higher computing power than sensing devices. In PALS, this personal mobile device plays the role of coordinator, with three specific functionalities: (i) processing data from the sensing layer, (ii) data transmission using the available communication paths, (iii) assistance to the handover of the available communication

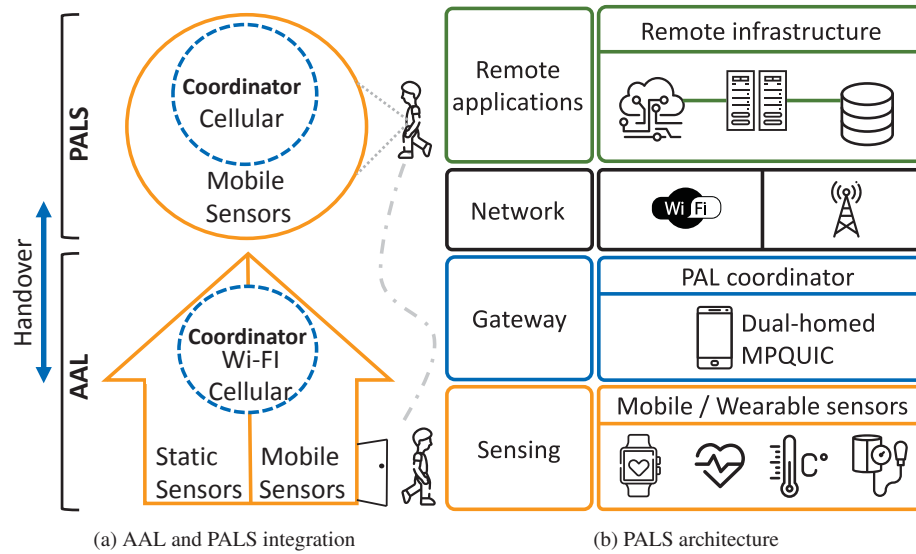


Figure 3.2: PALS integration with AAL and architecture

paths when a user moves away or get closer to the AAL environment. In the next subsections, we describe each of the specific functionalities in detail.

3.2.1.1 Processing Data from Sensing Layer

Each health-related device produces a different type of data depending on the sensor attached to it. The most common vital signs are pulse, temperature, blood pressure, and respiratory rate. Each of these signs provides values that represent the status of a vital function. The coordinator processes the data from each wearable device to identify the values outside a pre-established threshold since it may indicate the presence of a critical medical condition or disorder. The establishment of the threshold includes different factors, such as the identification of sudden variation in the values of the collected signs and also static values supported by medical literature. The deployment of multiple thresholds allows the PAL coordinator to generate alerts with different levels (e.g., low risk, high risk) for several system participants, such as the user himself for low-risk alerts and emergency contacts for high-risk alerts.

3.2.1.2 Data Transmission Using Available Communication Technologies

In order to achieve higher performance and availability in data transmission, the PAL coordinator relies on multipath protocols. We design PALS standalone of a specific multipath protocol, but, particularly for this work, we advocate for the MPQUIC protocol. The MPQUIC protocol is a connection-oriented protocol (De Coninck and Bonaventure, 2017) implemented on top of the User Datagram Protocol (UDP) and circumvents deployment issues as experienced by recent multipath transport-layer protocols like the Multipath TCP and Stream Control Transmission Protocol (SCTP). The implementation of MPQUIC extensions occurs in user space without complex changes to the operational system level.

The main characteristics of the MPQUIC protocol include a fast and secure connection establishment and reliable data transmission. The connection establishment occurs through a secure handshake in which the hosts negotiate the protocol version, the number and identification of paths, and the cryptography material (e.g., configuration, certificates, tokens). Both data and almost all headers are encrypted which prevents middleboxes from interfering with the communication. The information from the initial handshake serves for fast connection establishment

with zero Round Trip delay Time (RTT) latency. MPQUIC uses a connection ID to enable migrations between IP-address/Port tuples. The MPQUIC frame is path specific having a field in the header representing the path ID. The acknowledgment (ACK) frame benefits from this change and it is possible to send a MPQUIC packet through one path and receive the ACK on another path. Additionally, if a stream frame is sent through one path and lost, the lost frames can be retransmitted through another path.

MPQUIC includes a path manager function to handle statistics about loss ratio and RTT as these are adjustment parameters. The congestion control algorithm in MPQUIC maintains fairness, considering the available paths. The basic principle is to make the multipath connections less aggressive to avoid performance degradation of concurrent single path connection when they share the same bottleneck. The congestion control algorithm in MPQUIC is the Opportunistic Linked-Increases Congestion Control Algorithm (OLIA), which controls window size based on optimal resource use and also the responsiveness to packet loss.

3.2.1.3 Assistance to Handover between Available Communication Paths

Assuming that the PALS coordinator is at least a dual-homed device, it associates with different networks, such as cellular and WiFi, simultaneously. The coordinator is also a MPQUIC enabled device, meaning it can use both communication paths provided by the networks at the same time or to switch the paths from one wireless network to another without user intervention. When both paths are available, the MPQUIC protocol optimizes the bandwidth usage by using both paths to send and receive data. The path migration occurs when one of the paths becomes unavailable to the PAL coordinator. This happens when the user moves out of the communication range for one technology or when one path becomes unavailable during transmission. In either case, the PAL coordinator provides fluid transition among paths.

3.2.2 Communication Protocols

Multipath communications have become the subject of significant interest because devices use multiple communication technologies simultaneously. Multipath transport protocols allow the concurrent use of multiple communication technologies, such as Wi-Fi and cellular, for fast and reliable data exchange. Usually, the sender distributes application data onto the available paths provided by the communication technologies, the receiver reassembles and reorders data from different paths, forwarding it towards the application.

Several multipath protocols have been proposed and made available by researchers. The most deployed multipath protocols are the Multipath Transmission Control Protocol (MPTCP), the Multi-path Quick UDP Internet Connections (MPQUIC), the Stream Control Transmission Protocol (SCTP), and more recently, the Multipath Datagram Congestion Control Protocol (MP-DCCP). However, once SCTP has issues facing high-delay paths, and MP-DCCP offers unreliable and out-of-order data transfer (Polese et al., 2019), this chapter focuses on MPTCP and MPQUIC protocols.

MPTCP is a backward-compatible TCP extension that enables simultaneous data transmission from one end-to-end connection using multiple paths. For example, on a smartphone, MPTCP allows applications to concurrently send and receive data over multiple interfaces, such as Wi-Fi and cellular, using one TCP subflow over each interface (Ford et al., 2013). The MPTCP scheduler acknowledges and manages the established subflows for data transmission. When multiple subflows are available, the scheduler will transmit the data on the subflow with a lower round trip time out of all subflows whose congestion window is not full. MPTCP design provides

various benefits, including better resource utilization, higher throughput, and smooth response to failures, and it is suitable to work better with paths that have similar characteristics.

The MPQUIC protocol is a connection-oriented protocol (De Coninck and Bonaventure, 2017) implemented on top of the User Datagram Protocol (UDP). Distinctively from MPTCP, which requires changes on the operating system kernel, the implementation of MPQUIC extensions occurs at the application level and in userspace without complex modifications to the operating system level. The main characteristics of the MPQUIC protocol include a fast and secure connection establishment and reliable data transmission. The connection establishment occurs through a secure handshake in which the hosts negotiate the protocol version, the number, and the identification of paths. The information from the initial handshake serves for fast connection establishment with low Round Trip delay Time (RTT) latency. After a client becomes aware of the server's initial keys, it is possible to establish new QUIC connections with zero round trip time (0-RTT) data delay (Viernickel et al., 2018).

MPQUIC uses a connection ID to enable migrations between IP-address/Port tuples. The MPQUIC frame is path-specific, having a field in the header representing the path ID. The acknowledgment (ACK) frame benefits from this change, and it is possible to send an MPQUIC packet through one path and receive the ACK on another path. Additionally, if a stream frame is sent through one path and lost, the lost frames can be retransmitted through another path. Thus, the congestion control algorithm in MPQUIC maintains fairness, considering the available paths.

3.3 A CLASSIFICATION OF WORKS ON IOHT COMMUNICATION RESILIENCE

A primary concept in IoHT is employing portable devices to perform user monitoring and provide remote assistance regarding activities of daily living. In this context, the works in the literature focus on multiple aspects of the IoHT environment regarding communication resilience, such as advances in sensing technologies to provide continuous data collection and mobility-related issues to allow data transfer while the users are shifting locations. Regarding communication, authors assume that data transmission among IoHT devices and the Internet happens without errors or delays, disregarding transmission issues. However, communication management to improve resilience in IoHT is essential.

Recently, many means have been developed to attain the attributes of dependability to increase communication resilience. Those means relate to IoHT essential services as sensing, connectivity, and end-to-end communication and four major dependability categories: fault prevention, fault tolerance, fault removal, and fault forecasting (Avizienis et al., 2004). Figure 3.3 presents the classification of the existing works on IoHT communication resilience. It focuses on the communication of the essential services and an attribute-driven perspective of dependability.

3.3.1 Communication Resilience and Sensing Services

Sensing services relate to the error-free collection and management of health-related data by IoHT devices. Works focusing on the sensing services comprise fault prevention, fault tolerance, and fault forecastings categories. In addition, the works concentrate on devices and data security, energy efficiency, malfunctioning detection, and models to increase resilience for forthcoming systems. On fault prevention, works address energy efficiency to strengthen availability in IoHT. The intention is to reduce the energy consumption of devices by optimizing data sensing, processing, and transmission.

For instance, the authors of (Sagar et al., 2020) have investigated an energy-aware communication scheme for IoHT devices employing critical data routing code. In (Shahbazi

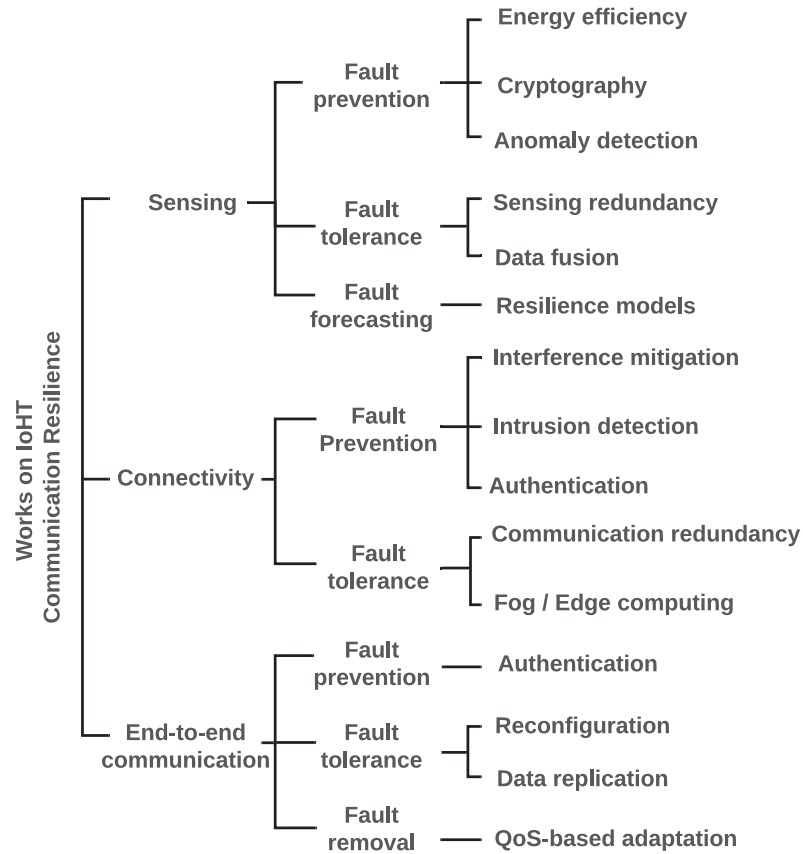


Figure 3.3: A classification of works on IoHT communication resilience

and Byun, 2020), the authors propose a routing protocol for IoHT that increases the lifetime of devices. Additionally, the protocol deals with a different constraint, the overheating due to continuous transmission. Energy harvesting solutions to increase the lifetime of devices are also available in the literature. The authors of (Park et al., 2020) propose a gesture-based technique to optimize energy-harvesting in IoHT devices. In (Khan and Yuce, 2010), the authors propose an energy harvested and cooperative routing protocol that relies on multiple parameters such as residual energy of nodes, congestion levels, and signal-to-noise ratio to choose the correct path.

Few works concentrate efforts on cryptography-based solutions to address security concerns and promote resilience. Approaches include cryptographic primitives, such as public key infrastructure to ensure data confidentiality and privacy, for instance, encryption of data before transferring it to the cloud. However, data decryption upon arrival increases processing time and latency harming time-critical applications requirements. There are works proposing blockchain technology to protect healthcare data which would increase security and resilience to attacks. In (Shahbazi and Byun, 2020) the authors propose a blockchain-based adaptive energy-aware routing protocol for IoHT. The objective is to achieve a secure, transparent, and lightweight solution to promote interoperability of physiological data considering the healthcare professionals and granted users in the IoHT ecosystem.

There are also proposals on failure detection, particularly for IoHT devices. One of the most common approaches to prevent faults in IoHT lies in constantly collecting and performing anomaly detection to identify faulty sensors. The authors of (Gaddam et al., 2020) discuss techniques to detect faults and anomalies in IoT devices, including the ones that support healthcare applications. They also propose an outlier detection model based on reinforcement learning that fits into a specific set of hardware and architecture. In (Safaei et al., 2020) authors propose a

noise and anomaly detection mechanism suitable for IoHT. The anomaly detection algorithm runs on each sensor node individually, avoiding the congestion of the connectivity services. Mainly for this type of solution, the problem lies in the small computational power of the devices to perform concurrent sensing and detection.

Works dealing with fault tolerance consider the redundancy of sensors and data fusion to promote resilience. However, an important goal for IoHT is to promote mobility and usability by combining multiple functions on the same device. Thus, transporting fewer devices improves user experience but decreases possible means of achieving redundancy. The authors of (Peng et al., 2017) propose a network coding-based fault-tolerant mechanism toward healthcare monitoring for proactive data transmission and increased resilience. However, the system design considers a many-to-one stream model, which is unrealistic for IoHT scenarios. A different approach to achieve resilience is employing data fusion of multiple sensors. The authors of (Ullah et al., 2021) propose multisensor data fusion based on the modified belief entropy to merge data from heterogeneous sensors. The authors of (Pollreisz and Nejad, 2020) propose the smart-fusion of frequency domain peaks of photoplethysmogram signals to increase data reliability.

Proposals for fault forecasting are available in literature in the form of resilience models. For example, the authors of (Russell et al., 2018) propose an agile model for critical infrastructure resilience. The model relies on repurposing existing sensors available in the infrastructure to add parallel communication methods and sense additional parameters using existing hardware. Unfortunately, even though the model shares several aspects with the IoHT environment, the possible configurations considering the singularity of the sensors and the lack of device redundancy are limited and make the model impracticable for IoHT.

3.3.2 Communication Resilience and Connectivity Services

Connectivity services comprise the communication among IoHT devices and the communication between devices and coordinators with short and long range communication gateways. Works regarding connectivity services handle fault prevention and fault tolerance categories. The solutions include interference mitigation, intrusion detection, authentication, communication redundancy, and fog and edge computing. Regarding interference mitigation among communication technologies (e.g., Wi-Fi, Bluetooth, and Zigbee), the literature reveals that it results in delays and data damage (Shao et al., 2020), compromising the resilience of IoHT critical applications directly. Hence, various works are investigating this issue. For instance, in (Shao et al., 2020), the authors have addressed the effect of Wi-Fi signals in the 2.4GHz band interfering with the Zigbee technology. The outcome is an incorrect triggering of false alarms to idle Zigbee devices, causing considerable energy waste.

Works in the literature proposing new security mechanisms relate to intrusion detection and authentication mechanisms. The main issue is that existing security mechanisms have been adapted to IoHT instead of being designed with the IoHT requirements in mind. Some works build a real-time healthcare monitoring system and employ machine learning techniques to detect intrusion (e.g., (Hady et al., 2020)). Few approaches intend to preserve user identities, creating a mechanism to dissociate them from health data (Cao et al., 2019). A resilient IoHT communication architecture supports eHealth in (Sharma and Kalra, 2019), and it presents a resilient protocol against multiple attacks in the IoHT connectivity services. There are also authentication mechanisms based on biometric traits to grant access to IoHT devices (Nakayama et al., 2019). The gathered data is transmitted using an alternative intra-body communication channel, avoiding wireless attacks.

Few works in the literature consider applying multiple communication paths simultaneously to increase resilience and improve communication performance for critical applications.

In (Mogensen et al., 2019), the authors proposed an algorithm to provide selective redundancy for a critical application using MPQUIC and redundant 5G wireless networks. The algorithm identifies the priority traffic and duplicates packets through multiple paths to achieve redundancy, while background traffic benefits only from single-path QUIC features. One previous work tested the portability in multihomed devices when automatically transitioning among networks. In (De Coninck and Bonaventure, 2019), the authors tested a MultiPath Transmission Control Protocol (MPTCP)-enabled smartphone to seamlessly handoff from a WiFi to an LTE connection without user interference or losing the initial connection establishment.

The authors of (Cisotto et al., 2020) propose employing 5G cellular communication to attain redundancy in communication while an ambulance is moving through multiple locations. The Social Internet of Things (SIoT) has recently emerged as a viable alternative to promote communication resilience in IoHT. In SIoT, the devices connect among themselves with one or more types of interdependence levels (e.g., friendship, work, common interest), promoting communication resilience and supporting task allocation (Zamanifar, 2020). However, security aspects such as integrity and confidentiality of data as well as privacy issues are subjects of concern (Rahouma et al., 2020).

Proposals relying on fog or edge computing to increase resilience are available in the literature. The central idea is to use computational nodes at the vicinity of the monitored person to decentralize cloud-based applications, decreasing the communication delay and increasing reliability, availability, and overall resilience. The authors of (Azimi et al., 2017) propose a fog architecture for IoHT-based health monitoring systems. The architecture relies on hierarchical partitioning and execution of machine learning-based data analytics. In (Isa et al., 2019), the authors propose a resilient fog computing infrastructure for health monitoring applications and evaluate its resilience against failures. The authors of (Islam et al., 2021) propose deploying services directly on IoHT nodes to achieve scalability, resource efficiency, and fault tolerance in IoHT scenarios.

The authors of (Isravel et al., 2021) used an SDN controller to manage traffic flow rules to devices in an assisted living system, increasing the resilience to congestion-induced failures in communication channels. In (Dar et al., 2019) the authors proposed a delay-aware accident detection and response system for IoHT, using a fog-based approach to avoid communication bottlenecks in the cloud. Finally, in (Dong et al., 2020) the authors introduce a decentralized health monitoring solution for IoHT that relies on edge computing to overcome delay constraints in communication.

3.3.3 Communication Resilience and End-to-end Communication Services

End-to-end communication services comprise the communication between the end nodes in IoHT and include the communication technologies from all services. Few works have addressed communication resilience related to the end-to-end communication service specifically for IoHT. The main approaches focus on fault prevention, fault tolerance, and fault removal categories and concentrate on promoting security, recovering the service functionality through adaptation, and resource reconfiguration. The authors of (Deebak and Al-Turjman, 2020) have proposed an attack-resilient service authentication framework for cloud-based medical healthcare systems. The formal and informal security analysis shows that the framework ensures adequate security between the patients and the healthcare professionals and is resilient in facing multiple attacks toward medical information systems. Furthermore, in (Liu et al., 2021), the authors propose a resilient replication scheme to improve data availability in cloud storage. The scheme deals with correlated and non-correlated failures that harm data availability.

The authors of (Cicioğlu and Çalhan, 2019) introduced an architecture to preserve communication survivability in disaster scenarios involving underground areas and energy management. The architecture relies on multiple distributed wireless sensor networks that communicate among themselves, promoting end-to-end resilient communication. In (Khan and Yuce, 2010), the authors have proposed a new evaluation metric for end-to-end communication resilience that correlates fault tolerance and quality of service. This metric supports the adaptive configuration management for solutions. If a system fails to achieve a certain QoS level within a specific configuration, the communication infrastructure uses redundant devices and communication channels to accomplish the desired level of quality.

The authors of (Ben Arbia et al., 2017) propose the integration of multiple devices and communication technologies (e.g., WiFi IEEE 802.11n, Bluetooth IEEE 802.15.1) to enable end-to-end network connectivity. A cloud IoT platform monitors and manages communication. However, the authors disregard the resilience aspects considering the multiple communication technologies. Finally, in (Azghiou et al., 2020) the authors propose a framework to assess the reliability of end-to-end communication regarding multi-layer services. However, the evaluation performance comprised exclusively simplified scenarios incompatible with the IoHT environment.

3.3.4 Discussion

The proposed classification leads to important conclusions and highlights research opportunities in communication resilience for IoHT. For sensing services, existing solutions focus on the continuity of its operation (mainly data collection). In some situations, different proposed solutions may conflict, making it impossible to adopt them concurrently. For example, solutions to improve resilience in sensing services through cryptographic mechanisms, anomaly detection, and data fusion will invariably degrade battery life. Sensor redundancy is also questionable because while providing the multiplicity of signals, it also defies the conventional arrangement of wearable devices and networks (e.g., one device with multiple functionalities). Finally, energy harvesting mechanisms to improve the lifetime of devices are promising. However, they still need refinement especially considering the miniaturization aspects. At the current stage, IoHT devices are unable to accommodate the existing solutions.

Regarding connectivity services, the works aim to improve system tolerance when facing failures and enhance resilience through security mechanisms. The main problems considering communication interference relate to the development of devices and the lack of fidelity to existing standards. Regarding security for the essential connectivity service, it is necessary to develop specific tools that take into account the characteristics of IoHT and the sensitivity of the information. Furthermore, although redundancy solutions relying on multiple communication technologies are welcome, it is necessary to evaluate them when dealing with critical applications. Finally, solutions based on edge and fog computing emerge to address resilience problems in the connectivity essential services. However, specific infrastructure requirements for fog computing-based solutions can become an obstacle. Likewise, the low processing power of IoHT devices to directly handle some services can lead to problems such as excessive battery consumption and increased delay in processing and transmitting data.

Finally, for end-to-end services, the works rely on authentication and data replication to increase resilience and performance evaluation mechanisms, such as QoS measurements, to gather the information that assists in adapting or reconfiguring the communication. Solutions to improve security and support data replication are traditional methods of promoting resilience. However, few studies apply these solutions encompassing the information cycle regarding IoHT services. Instead, most studies emphasize generic systems and traditional security aspects (e.g., attack protection, authentication mechanisms). Therefore, evaluating the resilience considering

health-related applications and the essential end-to-end communication service is challenging. Solutions that collect crucial information (e.g., QoS, communication delay) to promote adaptation or reconfiguration on the IoHT environment efficiently improve communication resilience. However, the deployment of such tools seems complex since the information relies on end-to-end measurements, but the required changes might happen in sensing and connectivity services.

One of the most noticeable issues for IoHT communication resilience is the lack of coordination between the solutions for the different services. Even when solutions emerge from the same resilience category, they serve only specific services in general. For instance, relevant information about the status of the communication channels (e.g., delay, congestion) is not shared between solutions to assist other services, making it harder to identify the source of a problem and take precise and efficient measures.

3.4 A RESILIENCE MANAGEMENT ARCHITECTURE FOR COMMUNICATION ON PORTABLE ASSISTED LIVING

In order to provide reliable and timely transmission of health-related data and accomplish the IoHT requirements, this section presents a resilience management architecture for communication on portable assisted living proposed in this work. The goal is to transfer data from IoHT devices that constantly collect health-related data from users and transmit it to a computing and storage infrastructure on the Internet by means of the available communication technologies. Thus, supporting the IoHT applications. Figure 3.4 depicts the layered-based architecture of a portable assisted living system.

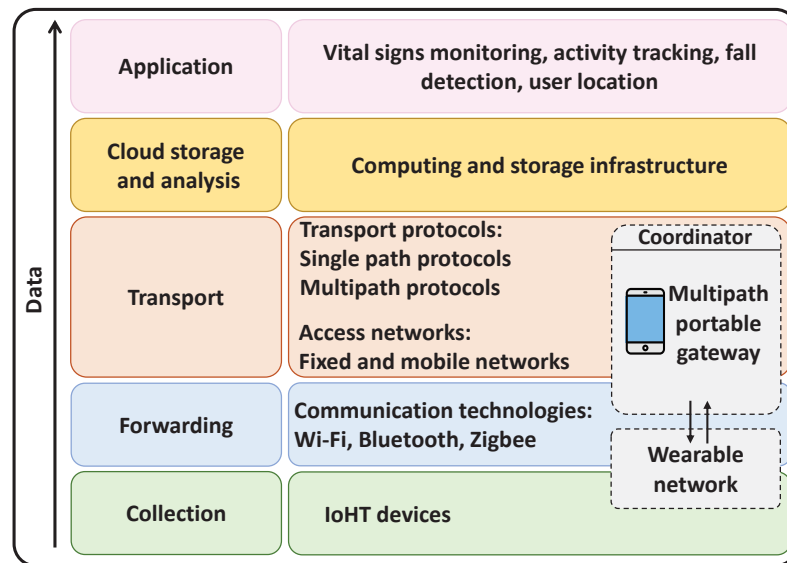


Figure 3.4: Portable assisted living architecture

The proposed architecture is organized in five layers. The first layer is the collection layer responsible for collecting health-related data from users. The second layer is the forwarding layer. It is responsible for forwarding the collected data to the portable gateway using short-range communication technologies like Bluetooth and Zigbee. Multiple IoHT devices can connect to the portable gateway building a wearable network and increasing the resilience against devices failures. The forwarding layer is also responsible for data transmission comprising the coordinator device and a wireless Internet gateway, such as an access point.

The transport layer provides data transmission from the coordinator device to a computing and storage infrastructure on the Internet. The access networks encompass fixed and mobile

networks. The coordinator connects to the fixed networks using the wireless access points in houses, apartments, and commercial establishments. Alternatively, the coordinator can also use mobile networks such as 5G cellular communication to reach the Internet. The communication protocols for data exchange comprise single path protocols (e.g., TCP, QUIC) and multipath protocols (e.g., MPTCP, MPQUIC). The coordinator is capable of single path and multipath communication, depending on the availability of the access networks and, therefore, of paths. Multiple communication paths also contribute to communication resilience since concurrent use increases the probability of constant data transmission.

The cloud storage and analysis layer manages IoHT data and supports the applications in the upper layer. In order to reach the cloud computing and storage infrastructure, the portable assisted living architecture relies on Internet communication. However, the applications in portable assisted living require uninterrupted and timely data exchange between the end nodes. That includes the communication through the Internet core. It is likely to identify specific parameters regarding the communication within the Internet, such as delay, error rate, and available bandwidth. However, it is hard to provide resilient mechanisms due to the distributed and unachievable infrastructure of the Internet. The application layer provides information for end-users employing the information made available by the underlying layers.

It is crucial to notice that the Transport layer encompasses both fixed and mobile access networks once they are vastly available. However, multipath protocols employ the communication technologies in access networks as paths, regardless of the technology. Thus, the architecture is abstract enough to employ different communication technologies. For instance, instead of fixed and mobile communication, it is feasible that the coordinator can employ two mobile interfaces from different carriers to provide resilience. Another possibility is employing device-to-device communication (D2D) as an access network concurrently with a mobile network. In those cases, mobility is kept unaltered. However, the performance evaluation of those configurations should be assessed prior to its deployment.

3.5 PERFORMANCE EVALUATION OF PALS

This section details the performance evaluation of PALS regarding two sets of experiments on the Mininet emulation platform (Handigol et al., 2012). The performance evaluation comprises PALS implementations using single path protocols TCP (PALS+TCP) and QUIC (PALS+QUIC), and multipath protocols MPTCP (PALS+MPTCP) and MPQUIC (PALS+MPQUIC). The first set of experiments evaluates PALS covering a wide range of parameters, which fit the requirements of healthcare applications. This approach enables a comprehensive evaluation of PALS performance using multiple and single communication paths, rather than an evaluation considering a few well-chosen cases. The handover evaluation comprises the multipath implementations and evaluates PALS efficiency in transferring data when one communication path becomes unavailable. The characterization of the second set of experiments relies on real-world information such as data-link speed, packet loss ratio, and delay regarding a fixed and a cellular communication path. This allows us to evaluate the performance of PALS acknowledging the communication channels available in different regions worldwide.

We have conducted the experiments using Ubuntu Linux 16.04 LTS with kernel 4.4 patched with MPTCP v0.92 and running on an Intel i5-6200U @ 2.30 GHz processor. The Mininet emulation platform version is 2.2.1. The network emulation tool, responsible for inserting the link properties, queuing, propagation delay, and packet loss into the emulation, is the NetworkEmulator (Netem) (Hemminger et al., 2005). The iPerf tool acts to generate additional traffic and simulate path competition (Hsu and Kremer, 1998). Finally, the MPQUIC

implementation is supported by the prototype available in (De Coninck and Bonaventure, 2017), which relies on the Go open source programming language.

3.5.1 PALS Evaluation in Randomized Scenarios

We have defined the evaluation scenarios considering bandwidth, delays, and random packet loss for a specific workload. The values for the parameters fit the requirements of healthcare applications as observed in (Cisotto et al., 2020). The parameters and workload are listed in Table 3.1. The emulated scenarios follow a multipath network with two multihomed enabled devices over disjoint paths, as shown in Figure 3.5. The performance of the evaluated protocols indicates the variation of the parameter levels since each emulation is static. The handover evaluations follow the same scenarios with one of the paths being disabled during the experiment. Disabling one of the paths also represents the user mobility when that user is drifting away from a wireless communication device, such as an access point, for instance.

Table 3.1: Experimental parameters

Factor	Parameters	
	Minimum	Maximum
Capacity [Mbps]	0.1	5
End-to-end Latency [ms]	0	250
No Loss [%]	0	0
Random Losses Ratio [%]	1	5
Workload [MB]	20	20

The primary desired characteristics in PALS are performance, mobility, and communication resilience. We have designed experiments to evaluate those attributes considering a wide range of possible scenarios. Because of the multi-factor aspects of the scenario and the multi-leveled factors, we have followed a fractional factorial design approach. Using the parameters available in Table 3.1, we have created three distinct experiments to evaluate PALS: PALS performance evaluation under no loss, PALS performance evaluation under random losses, and PALS handover evaluation. For each experiment, we have assembled 50 scenarios with random values within the range from the experimental parameters. For each scenario and implementation (PALS+TCP, PALS+QUIC, PALS+MPTCP and PALS+MPQUIC), the emulation repeats for 10 times, resulting in 500 emulations per implementation. The performance experiments considering loss and no loss have a total of 2000 emulations each, and the handover evaluation has a total of 1000 emulations since it comprises only the multipath protocols. For the single path protocols the standard congestion control is CUBIC, and since there is no multipath version of this algorithm the congestion control employed in multipath tests is the OLIA congestion control algorithm.

Since fixed and cellular Internet offers different connection characteristics, we have chosen to explore the multiple scenarios provided by those different configurations. At a given

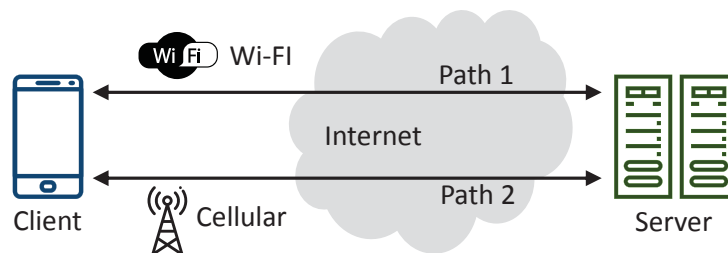


Figure 3.5: Measurement setup

time, the available links can be affected by different levels of end-to-end delay and random losses. Our experiments comprise the addition of random losses in order to evaluate PALS in demanding scenarios. For the handover evaluation, we have considered the success rate in completing the handover process and the efficiency in transferring a file through a high loss and low capacity link when one of the paths becomes unavailable. We have also evaluated the packet delivery ratio in the handover experiment, analyzing the retransmissions values for multipath protocols.

The workload is static and consists of a 20 MB file transferred from a client to a server while we measure the end-to-end delay. We have chosen this specific workload since previous evaluations with short files were conducted pointing out minor advantages in using the MPQUIC protocol (Viernickel et al., 2018). The transmission of short files comprises only a small fraction of traffic types in AAL and PALS. Although multipath protocols are not designed for short file transfers (De Coninck and Bonaventure, 2017), one of the advantages of the QUIC protocol is the single round-time-trip handshake compared to the three times round-trip-times of the TCP protocol. Thus, for small files transfers the QUIC protocol benefits from fewer connection establishments which may benefit the PALS coordinator.

3.5.1.1 PALS evaluation no loss

The experiment illustrates a situation where the user is inside the AAL communication range and has simultaneous access to different wireless technologies. In this experiment, we have inserted no random losses into the emulations. Our first evaluation metric is the ratio between the delay to receive the 20 MB file using the TCP protocol divided by the delay to receive the file using the QUIC protocol. For a perfect equivalence of both protocols, the ratio value is 1, being that the values above 1 indicate better performance for the implementation using QUIC, and the values below 1 indicate better performance for the implementation using TCP.

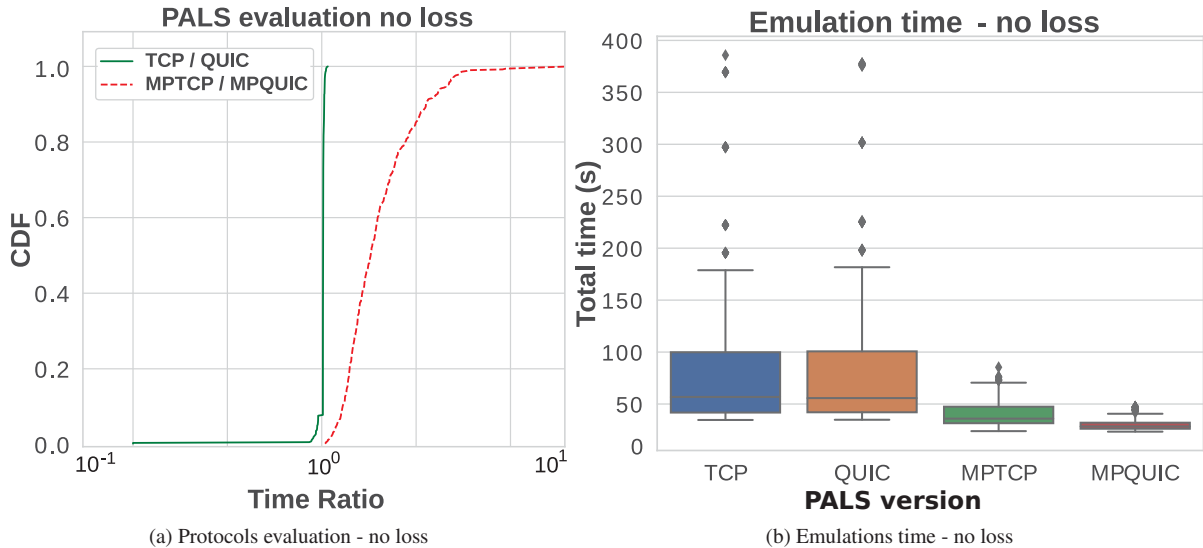


Figure 3.6: Comparison of PALS implementations under no loss scenarios

The results for PALS+TCP and PALS+QUIC are very similar over the course of all emulations results, although, in 91% of the cases, PALS+QUIC was slightly faster than PALS+TCP. This behavior is expected for single path protocols since congestion control becomes a decisive factor, and both protocols use the same algorithm. For the multipath protocols, PALS+MPQUIC has performed better in all emulations results. The packet loss for PALS+MPTCP is higher than PALS+MPQUIC. The probable cause is the more precise latency estimation of the MPQUIC

protocol that contributes to finding the fastest path. The implementations using multipath protocols show better performance than PALS using single path protocols. Figure 3.6(b) shows the boxplots for emulation times over the 500 scenarios for each PALS version. Considering all results, PALS+MPQUIC was 31.4% faster than PALS+MPTCP. Table 3.2 shows how efficiently each PALS version uses the available bandwidth. We have defined bandwidth efficiency as the ratio between goodput and the available bandwidth, regarding the values for each scenario. For the multipath protocols, we have considered the available bandwidth as the sum of the paths capacities. Results show that PALS using single path protocols and PALS+MPTCP have a similar utilization of the available bandwidth. PALS+MPQUIC showed better efficiency than the other protocols, using 88.64% of the available bandwidth.

3.5.1.2 PALS evaluation with random losses

This experiment depicts the same situation from the first one except for the insertion of random losses within a range of 1% to 5% packet loss ratio. Adding random losses to the emulations provides a realistic scenario since wireless communication technologies are prone to random packet loss. Figure 3.7(a) shows the ratio between the delay to transfer the workload using PALS+TCP/PALS+QUIC and PALS+MPTCP/PALS+MPQUIC. The UDP-based versions of PALS show a clear advantage when under low bandwidth and lossy scenarios.

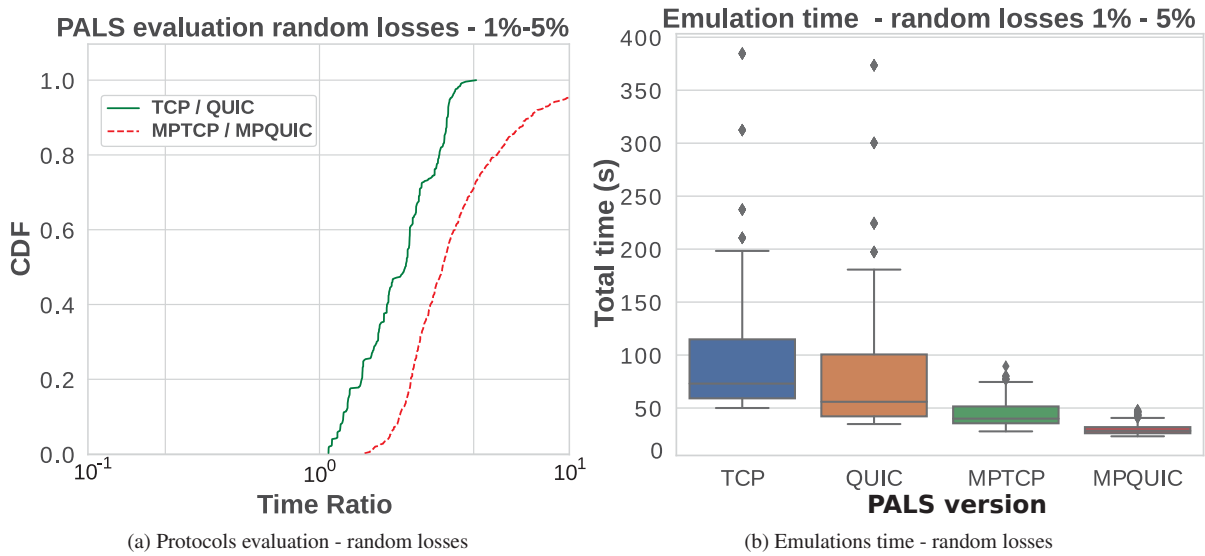


Figure 3.7: Comparison of PALS implementations under random losses

PALS+QUIC is more efficient than PALS+TCP in all emulations. For the implementations using multipath protocols, PALS+MPQUIC performs better than PALS+MPTCP in all scenarios. Figure 3.7(b) shows the boxplots for all implementations considering the emulation times. The results for single path implementation show disperse values as they cannot benefit from the available paths. PALS+QUIC performs better than PALS+TCP. PALS+MPQUIC has dealt better than PALS+MPTCP with the inserted random losses with a 0.29% decrease in performance while PALS+MPTCP has shown 9.54% difference from the previous experiment. PALS+MPQUIC has also presented a lower retransmission rate than PALS+MPTCP. Table 3.2 shows the results for emulations with random losses. In (De Coninck and Bonaventure, 2019), the authors conducted a simulation-based experiment considering the same protocols and variations in the experimental parameters. However, they considered data links with higher capacity (up to 100Mbps) than the ones we have applied in our experiment since we have adjusted our parameters

considering the requirements of healthcare applications. The experimental results diverge explicitly for the scenarios with random losses, due to mainly the demanding characteristics in our scenarios.

Table 3.2: Bandwidth efficiency

Bandwidth efficiency no loss				
Version	PALS+TCP	PALS+QUIC	PALS+MPTCP	PALS+MPQUIC
Goodput	1.82 Mb/s	1.91 Mb/s	3.81 Mb/s	5.23 Mb/s
Bandwidth	2.90 Mb/s	2.90 Mb/s	5.90 Mb/s	5.90 Mb/s
Efficiency	62.76%	65.86%	64.58%	88.64%
Bandwidth efficiency random losses - 1% - 5%				
Version	PALS+TCP	PALS+QUIC	PALS+MPTCP	PALS+MPQUIC
Goodput	1.60 Mb/s	1.88 Mb/s	3.59 Mb/s	5.19 Mb/s
Bandwidth	2.94 Mb/s	2.94 Mb/s	5.90 Mb/s	5.90 Mb/s
Efficiency	54.42%	64.22%	60.86%	87.37%
Handover bandwidth efficiency random losses - 1% - 5%				
Version	PALS+TCP	PALS+QUIC	PALS+MPTCP	PALS+MPQUIC
Goodput	–	–	2.27 Mb/s	2.33 Mb/s
Bandwidth	–	–	3.5 Mb/s	3.5 Mb/s
Efficiency	–	–	64.91%	66.66%

3.5.1.3 PALS handover evaluation

The handover among paths is one of the main reasons to follow multipath protocols in PALS. For the handover evaluation, we have considered the same experimental design used in the performance evaluation with random losses added through all emulations. For each experiment, we have disabled one of the communications interface automatically 15 seconds after the beginning of the emulations. Figure 3.8 illustrates an example of a path handover.

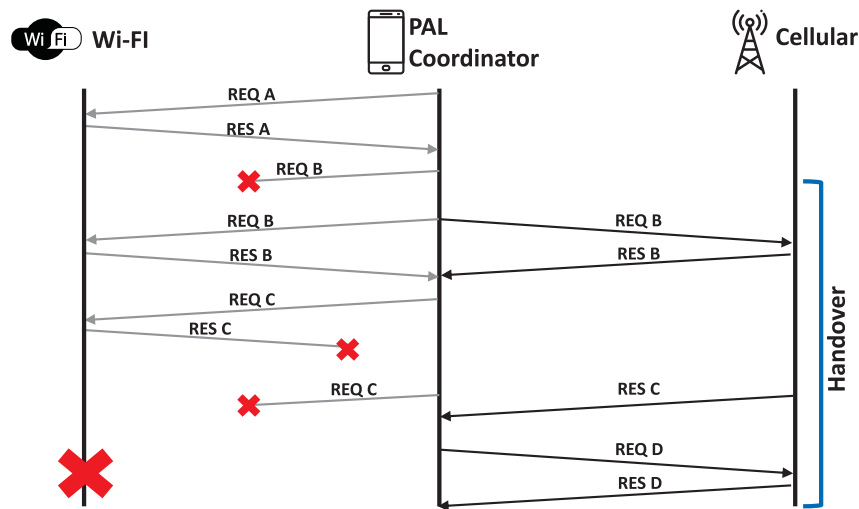


Figure 3.8: Example of a possible path handover

As the PAL coordinator has access to both paths, it benefits from both communication technologies, simultaneously, even in the presence of losses. As the PAL coordinator moves away from the Wi-Fi access point, the transport-layer protocol shifts the connection to the path

provided by cellular technology. For this experiment, we have evaluated retransmissions for each protocol once a high number of retransmissions may indicate the attempt to use the disabled path by the PAL coordinator.

PALS+MPTCP and PALS+MPQUIC have completed the emulations in 98.6% of the scenarios. Failures have occurred mostly when both paths presented low capacity and high end-to-end latency. Figure 3.9(a) shows the ratio between the delay to transfer the workload with PALS+MPTCP divided by the time required by PALS+MPQUIC considering handover scenarios with losses. PALS+MPQUIC outperforms PALS+MPTCP in 78.6% of the experiments, although the time to complete the emulations was similar in most cases. Results were also comparable to the performance of the PALS implementation using single path protocols. This is expected because despite the emulations start with redundant paths, the multipath protocols benefit from them only for 14% of total time, in average. As observed in Figure 3.9(b), PALS+MPQUIC needs fewer retransmissions than PALS+MPTCP. This is particularly important to spare the restrained resources of the PALS coordinator considering processing power and energy. Finally, PALS+MPQUIC has obtained 66.1% of bandwidth efficiency. Both implementations offer handover capabilities and are similar in performance, enabling the deployment in a portable coordinator. Results for performance and uncomplicated deployment make MPQUIC the most suitable candidate for implementation. Our experimental results are in agreement with others (De Coninck and Bonaventure, 2019), where the authors have also tested the handover considering MPTCP and MPQUIC protocols.

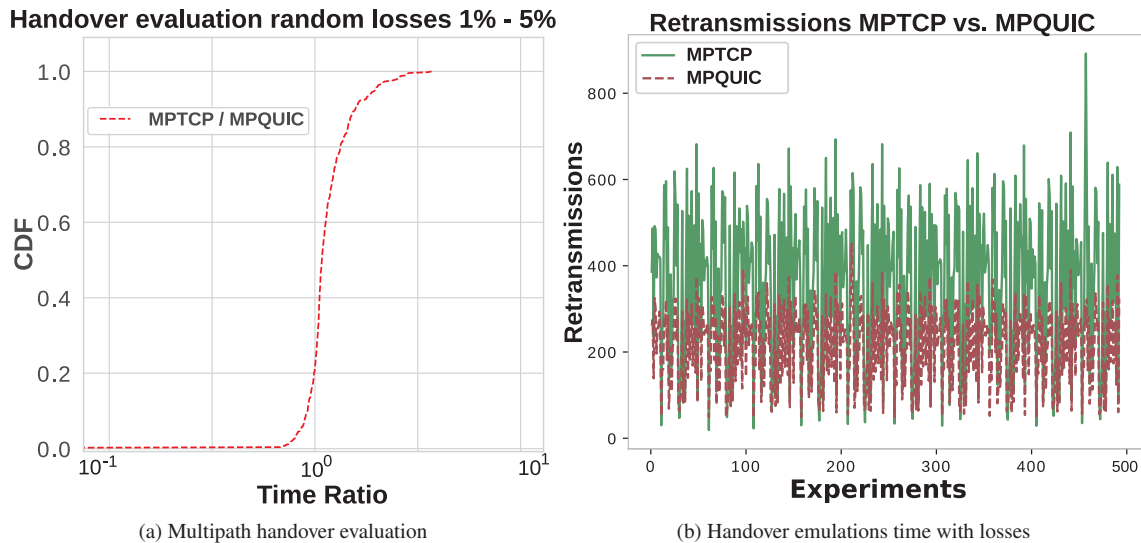


Figure 3.9: Handover evaluation

3.5.2 Protocols Evaluation in Specific Scenarios

The availability of communication technologies and bandwidth is different depending on the geographical location. To investigate the applicability of PALS in real-world scenarios, we have conducted additional experiments considering the average global Internet speeds and also in Europe, in the United States of America, and South America, for fixed and cellular communication links. Table 3.3 shows the global and regional values for fixed and mobile Internet speeds. This experiment relies on the 2019 reports provided by (SPEEDTEST, 2019) with throughput tests carried out by users worldwide. *Speedtest.net* is a bandwidth and performance evaluation platform. The reports from 2019 comprise 500 million individual evaluations.

The European region comprises Germany, United Kingdom, Belgium, Spain, and France, and the South America region comprises Brazil, Peru, and Argentina. Each of the regions has provided two distinct scenarios, a best-case scenario that represents the download speeds and a worst-case scenario that depicts the upload speeds considering fixed and cellular communications. For increasing fairness to the protocols, we have included a global average of latency (24ms) and data loss ratio (5%). The evaluation of the scenarios comprises 50 repetitions for each PALS version considering the delay time to transfer a 20 MB file. The results are presented and discussed in the next sections.

Table 3.3: Global and regional speeds for fixed and mobile Internet

Global	Best-case (Download)	Worst-case (Upload)
Fixed bandwidth	76.9 Mbps	41.09 Mbps
Mobile bandwidth	33.71 Mbps	10.89 Mbps
Europe	Best-case (Download)	Worst-case (Upload)
Fixed bandwidth	50.16 Mbps	9.96 Mbps
Mobile bandwidth	26.36 Mbps	11.05 Mbps
USA	Best-case (Download)	Worst-case (Upload)
Fixed bandwidth	96.25 Mbps	32.88 Mbps
Mobile bandwidth	33.88 Mbps	9.75 Mbps
South America	Best-case (Download)	Worst-case (Upload)
Fixed bandwidth	23.64 Mbps	10.57 Mbps
Mobile bandwidth	18.50 Mbps	7.52 Mbps

3.5.2.1 Global Evaluation

The UDP-based implementations PALS+QUIC and PALS+MPQUIC were faster in transferring the 20 MB file than the TCP-based versions in both scenarios. Considering the best-case scenario, PALS+QUIC and PALS+MPQUIC had similar performance while in the worst-case scenario QUIC has outperformed MPQUIC in 77% of the emulations. Figure 3.10 presents the boxplots for global evaluations.

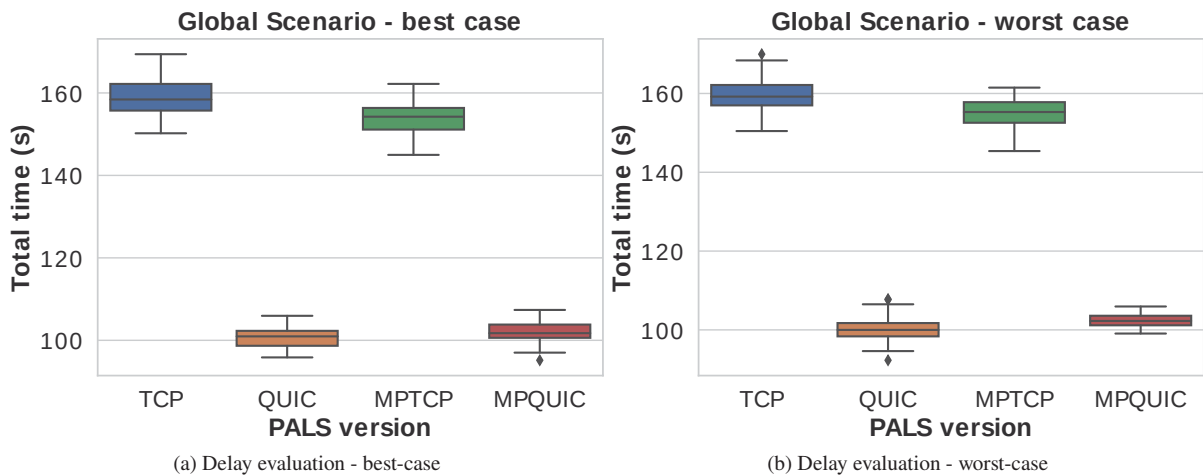


Figure 3.10: Global evaluations

3.5.2.2 Europe Evaluation

Once again UDP-based implementations have outperformed TCP-based implementations. The PALS+QUIC and PALS+MPQUIC results were very close considering the number of times each protocol were the fastest through the repetitions and the total delay for each repetition. Figure 3.11 presents the boxplots for Europe evaluations.

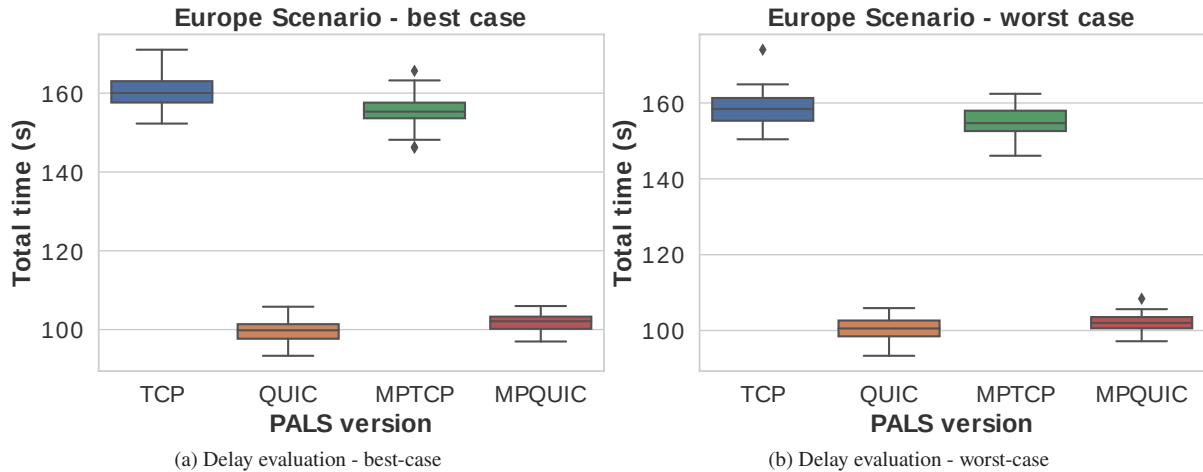


Figure 3.11: Europe evaluations

3.5.2.3 United States of America Evaluation

In this scenario, the PALS+MPTCP implementation has achieved the best performance considering all regional tests, approaching the performance of the PALS+TCP version. However, TCP-based versions have performed worse than UDP-based versions of PALS implementation. Considering only the UDP-based versions protocols, again the PALS+QUIC and PALS+MPQUIC implementations have performed similarly, being the PALS+QUIC protocol marginally better in most emulations. Figure 3.12 presents the boxplots for the United States of America evaluations.

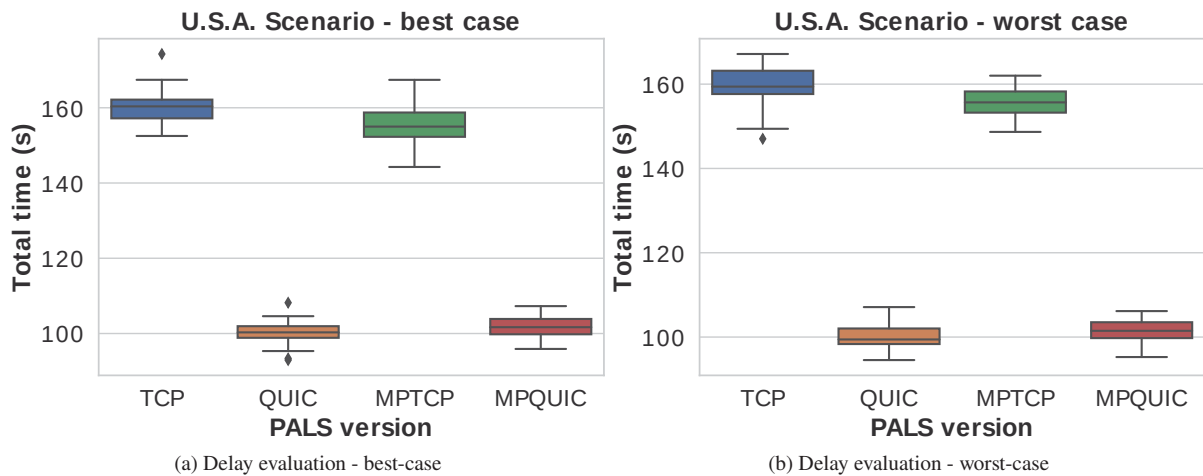


Figure 3.12: United States of America evaluations

3.5.2.4 South America Evaluation

This scenario exhibit similar results compared to the previous evaluations, even though it presents the lowest bandwidth values considering all the regional scenarios. The PALS+TCP and PALS+MPTCP implementations performed similarly, with PALS+TCP being faster when transferring the workload. The PALS versions based on UDP were faster than those based on TCP, with PALS+QUIC being faster than PALS+MPQUIC. The worst-case scenario presented better results than the best-case scenario, showing that UDP-based PALS implementations can perform well even under adverse conditions. Figure 3.13 presents the boxplots for South America evaluations.

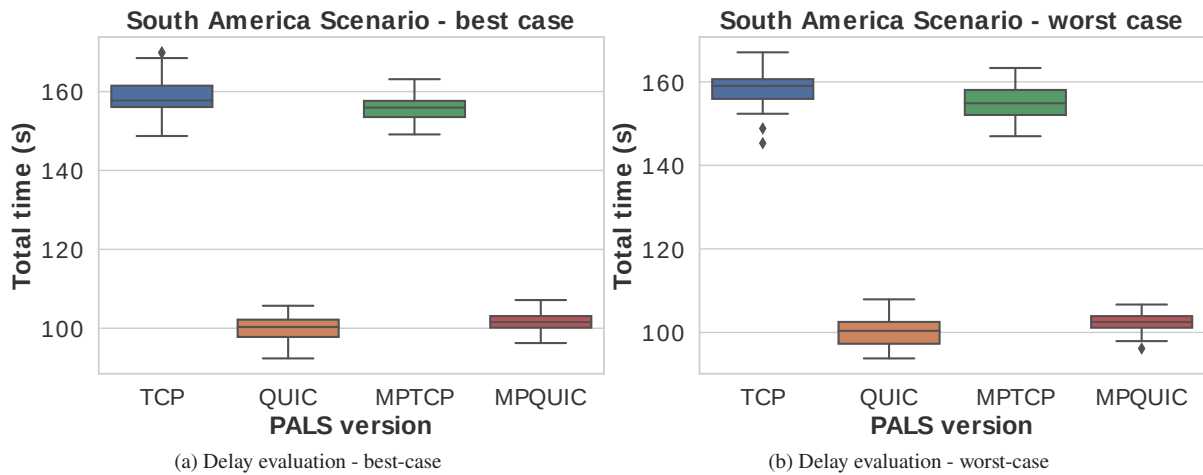


Figure 3.13: South America evaluations

Table 3.4 summarizes the results for all specific scenarios experiments. The UDP-based version of PALS has shown better performance than TCP-based versions in every scenario and all repetitions. PALS+QUIC has outperformed PALS+MPQUIC in most experiments, although the average time to transfer the workload was similar. Considering only the multipath protocols, PALS+MPQUIC has shown better performance than PALS+MPTCP in these specific scenarios. The PALS+QUIC implementation has considerably outperformed PALS+MPTCP. The probable cause is the additional delay caused by the TCP handshake, and the different congestion control schemes employed in the tests.

Table 3.4: Average delay in seconds per region

Version	Protocol			
	PALS+TCP	PALS+QUIC	PALS+MPTCP	PALS+MPQUIC
Global best	158,83	100,70	153,98	102,09
Global worst	159,71	100,25	154,86	102,39
Europe best	160,64	99,46	155,30	101,81
Europe worst	158,54	100,55	154,68	102,02
USA best	160,85	100,05	154,88	101,74
USA worst	159,56	99,83	155,79	101,52
S.A. best	159,60	100,52	155,80	102,01
S.A. worst	158,40	100,30	154,76	102,74

3.5.3 Discussion

Regarding both experiments and considering the scope of this work, the PALS+MPQUIC implementation meets the requirements that can handle multiple communication paths to enhance performance and assist in extending the monitoring area in assisted living systems. However, the effectiveness of employing multipath protocols should be further studied and applied in specific situations. Below, we discuss results and insights regarding the use of multipath protocols.

For the randomized scenarios, the purpose was to compare PALS versions regarding performance and mobility in a broad range of cases. The capabilities for the disjoint paths were selected at random, enabling multiple combinations of speed, delay, and packet loss rate. This allows the multipath versions of PALS to have a broader range of resources available. PALS versions implemented over single path protocols must deal with the characteristics of the exclusive path. The impacts of the path characteristics are even more apparent in scenarios of high delay and packet loss ratio. Even though the results were favorable for the multipath implementations, we have noticed that in specific situations, the performance was comparable to the single path implementations. Those situations specifically involved the scenarios with higher bandwidth available. These observations have encouraged us to develop further tests considering a realistic approach. The evaluation of specific scenarios has brought a sharper interpretation of the feasibility of using multipath.

To provide the desired design characteristics, PALS must rely on a multipath protocol. However, considering exclusively the performance in the specific scenarios evaluation, the PALS+MPTCP implementation offered no notable advantages. In this case, PALS+MPTCP still benefits from using multiple communication technologies and provides smooth transitioning among those technologies, but offers no performance improvements when compared to the single path implementations or the PALS+MPQUIC implementation. Fig 3.14 illustrates the time ratio regarding multipath PALS implementations in global scenarios. PALS+MPQUIC shows considerably better performance in specific scenarios than PALS+MPTCP. The superior performance persists throughout all emulations and for every region evaluated.

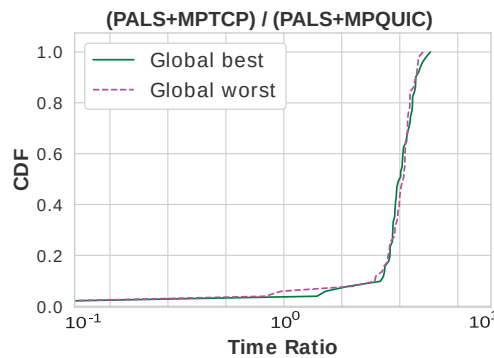


Figure 3.14: Evaluation of multipath PALS versions in global scenarios

Future solutions relying on multipath protocols must be carefully planned. They must acknowledge the resources and characteristics of the implementation environment and also evaluate the availability of the multipath protocol. For instance, MPTCP requires complex changes at the operating system level while (MP)QUIC runs in user-space, being easily deployed. Additionally, topics that were not within the scope of this work must be examined, such as the security aspects of multipath protocols, the consequences of the additional overhead because of multiplexing, and improvements on congestion control considering those protocols.

3.6 RESILIENCE EVALUATION OF PALS

In order to evaluate the performance and resilience to communication failures we have extended the evaluation of the Portable Assisted Living System (PALS) including induced communication failures. PALS acts on the Transport and Cloud storage and analysis layers of the portable assisted living architecture proposed in Section 3.4. The experiment encompasses the communication regarding a coordinator device and a computing and storage infrastructure on the Internet. The evaluation includes multiple access networks (Fixed and Mobile) and protocols (Single path and multipath). The Internet core is characterized regarding available bandwidth, error rate, and delay considering worldwide scenarios.

The emulated scenarios follow a multipath network with two multihomed enabled devices, i.e., a sender and a receiver, over disjoint paths, as shown in Figure 3.15. When an individual communication path is available, the evaluations consider the single path versions of PALS, and when both paths are available, the evaluations employ the multipath versions of PALS. The evaluations regarding the uninterrupted transmission (without induced failures) of PALS involve transferring a fixed workload through the available paths while measuring the transfer delay, the number of retransmissions, and the bandwidth usage.

The resilience evaluations consider the same experiments regarding the uninterrupted transmission. However, it includes induced failures into the emulations to assess resilience. The induced failures include disabling and re-enabling a communication path for short periods while transferring the workload, representing a random communication failure. By evaluating the outcome of this new configuration it is possible to identify the resilience offered by single and multipath PALS regarding communication. Figure 3.15 represents a failure in a communication path. In a single path configuration, the data transmission would cease temporarily, while in a multipath configuration, the transmission continues through the second path.

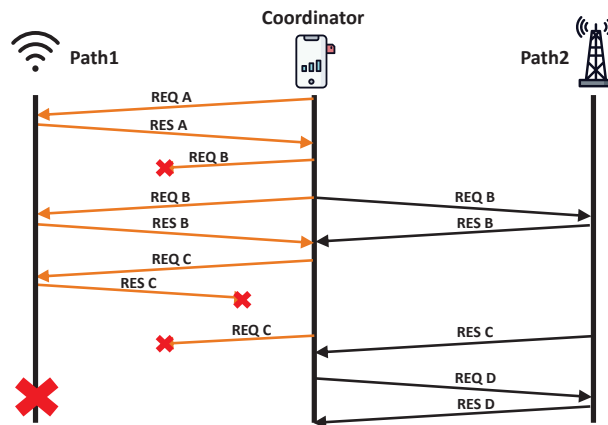


Figure 3.15: Communication failure

The availability of communication technologies and bandwidth is different depending on the geographical location. To investigate PALS applicability, the experiments rely on the average global Internet speeds and from South America (S.A), Europe, and the United States of America (U.S.A.) for fixed and cellular communication links. Table 3.5 shows the global and regional values for fixed and mobile Internet speeds. The European region comprises Germany, United Kingdom, Belgium, Spain, and France, and the South American region comprises Brazil, Peru, and Argentina. The experiments rely on the 2020 reports provided by (SPEEDTEST, 2019) with throughput tests carried out by users worldwide. *Speedtest.net* is a bandwidth and performance evaluation platform. The reports from 2020 comprise over 500 million individual evaluations.

For each region and PALS version, the emulation repeats 50 times considering the uninterrupted transmission scenarios and induced failures scenarios, resulting in 1600 emulations. The induced failures scenarios include two failure intervals of five seconds each. The failures happen ten seconds after the emulations begin. The purpose is to distinguish the behavior of single and multipath configurations when facing unexpected changes in communication. The workload is static and consists of a 50 MB file. For the single path protocols, the standard congestion control is CUBIC, and since there is no multipath version of this algorithm, the congestion control employed in multipath tests is the OLIA. To increase fairness, all emulations included a global latency average (24ms) and data loss ratio (5%) (SPEEDTEST, 2019).

3.6.1 Delay Evaluation

The health-related data collected by wearable devices must respect the time-critical characteristics of IoHT applications. Thus, maintaining a low delay while transferring data is crucial. The delay measurement evaluations comprise the transmission of the workload considering all regions and protocols, and with and without the insertion of failures. Figure 3.16 summarizes the delay values for all regions and protocols.

As expected, PALS consumes more time to transfer the workload in the induced failures scenarios (TCP-F, QUIC-F, MPTCP-F, and MPQUIC-F) than in the continuous transmission scenarios (TCP, QUIC, MPTCP, and MPQUIC). In the induced failure scenarios, the multipath protocols were faster than the single path to transfer the workload, with the MPQUIC being the fastest. The multipath protocols were also faster in the uninterrupted transmission scenarios, and MPQUIC was the fastest. This behavior recurred in all regions, with minimal differences in delay due to the different bandwidth values for each region.

Low retransmission is essential, especially for a portable communication gateway with limited processing and battery. Figure 3.17 shows that the multipath protocols require more retransmissions, mainly in the presence of communication failures. In all regions, with minor differences, the multipath protocols retransmitted more data than the single-path counterparts. This behavior is not unusual once the multipath protocols demand error management and face losses in both paths. However, it is necessary to keep retransmissions managed to avoid battery drains and processing issues.

Table 3.6 shows the average bandwidth, throughput, and bandwidth usage for PALS considering all regions and uninterrupted and induced failures scenarios. Multipath protocols provide better average throughput speeds since they rely on both communications paths concurrently. The communication failures highly impact the throughput rate and the bandwidth use percentage. Since the throughput speeds are similar for all regions, the bandwidth usage is higher in regions with lower bandwidth values, such as South America. The average round trip time for all PALS versions considering each path is below 1ms, matching the requirements of end-to-end delay for wearable devices and healthcare applications proposed in (Cisotto et al., 2020).

Table 3.5: Bandwidth values for fixed and mobile broadband

Global		Europe	
Fixed bandwidth	76.90 Mbps	Fixed bandwidth	50.16 Mbps
Mobile bandwidth	33.71 Mbps	Mobile bandwidth	26.36 Mbps
South America		U.S.A.	
Fixed bandwidth	23.64 Mbps	Fixed bandwidth	96.25 Mbps
Mobile bandwidth	18.50 Mbps	Mobile bandwidth	33.88 Mbps

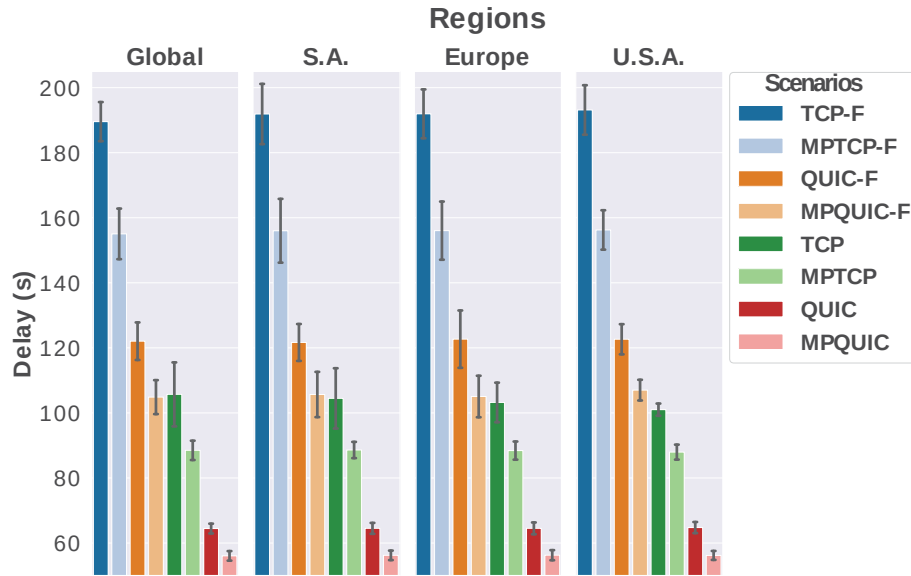


Figure 3.16: Delay for PALS versions in failure and continuous scenarios

PALS shows good performance in multiple bandwidth configurations regarding the delay evaluation, even when dealing with lower bandwidth values. QUIC based versions were faster and provided higher throughput rates, with the cost of a higher number of retransmissions.

3.6.2 Resilience Evaluation

The experiments regarding resilience focus on the scenarios with induced failures. The goal is to identify how failures on the communication paths impact data transmission considering the single path and the multipath protocols. The evaluation comprises three different cases, (i) PALS relying exclusively on fixed broadband, (ii) PALS relying solely on cellular broadband, and (iii) PALS employing both communication technologies concurrently. The analysis also comprises TCP vs. MPTCP and QUIC vs. MPQUIC to assess all protocols. Additionally, the resilience evaluation comprises the average values for data transfer speeds achieved in each emulation round.

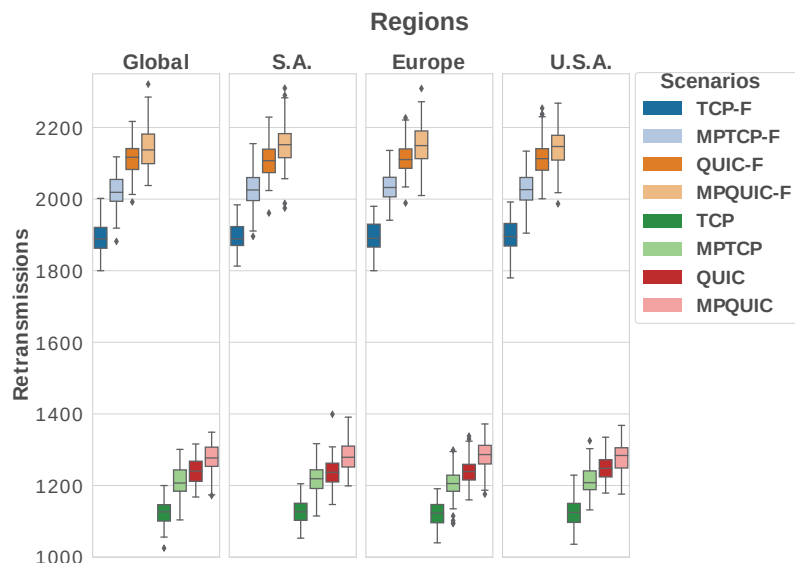


Figure 3.17: Retransmissions for PALS versions in failure and continuous scenarios

Table 3.6: PALS average available bandwidth, throughput, and bandwidth use

	TCP-F	MPTCP-F	QUIC-F	MPQUIC-F	TCP	MPTCP	QUIC	MPQUIC
Global scenario								
Bandwidth (Mb/s)	55.31	55.31	55.31	55.31	55.31	55.31	55.31	55.31
Throughput (Mb/s)	2.12	2.58	3.25	3.81	3.77	4.53	6.21	7.14
Bandwidth use (%)	3.83	4.66	5.87	6.89	6.82	8.19	11.22	12.90
South America scenario								
Bandwidth (Mb/s)	21.07	21.07	21.07	21.07	21.07	21.07	21.07	21.07
Throughput (Mb/s)	2.08	2.57	3.28	3.84	3.80	4.52	6.20	7.12
Bandwidth use (%)	9.85	12.19	15.57	18.21	18.04	21.44	29.43	33.77
Europe scenario								
Bandwidth (Mb/s)	38.26	38.26	38.26	38.26	38.26	38.26	38.26	38.26
Throughput (Mb/s)	2.06	2.56	3.25	3.88	3.82	4.53	6.20	7.11
Bandwidth use (%)	5.39	6.69	8.50	10.14	9.99	11.85	16.21	18.58
U.S.A. scenario								
Bandwidth (Mb/s)	55.31	55.31	55.31	55.31	55.31	55.31	55.31	55.31
Throughput (Mb/s)	2.07	2.56	3.28	3.86	3.81	4.54	6.20	7.12
Bandwidth use (%)	3.75	4.63	5.93	6.97	6.89	8.21	11.21	12.87

Data transfer values are essential to identify if any of the protocols sustained sub-par values throughout the emulations, indicating possible issues regarding the safety-critical requirements.

Figure 3.18 shows the resilience evaluation results for the Global region. Figure 3.18(a) depicts the results considering TCP and MPTCP. The communication failures highly compromise the single path technologies (Fixed broadband and Cellular broadband), causing the complete lack of data transmission during the period of induced failures. The induced failures also affect one of the paths considering the multipath scenario. However, since there are two available paths, data transmission halts on one path (MP Path 2) and continues on the other (MP Path 1). As a result, MPQUIC is faster in transferring the workload. However, the main advantage of MPQUIC lies in the continuous data transmission regardless of the communication faults.

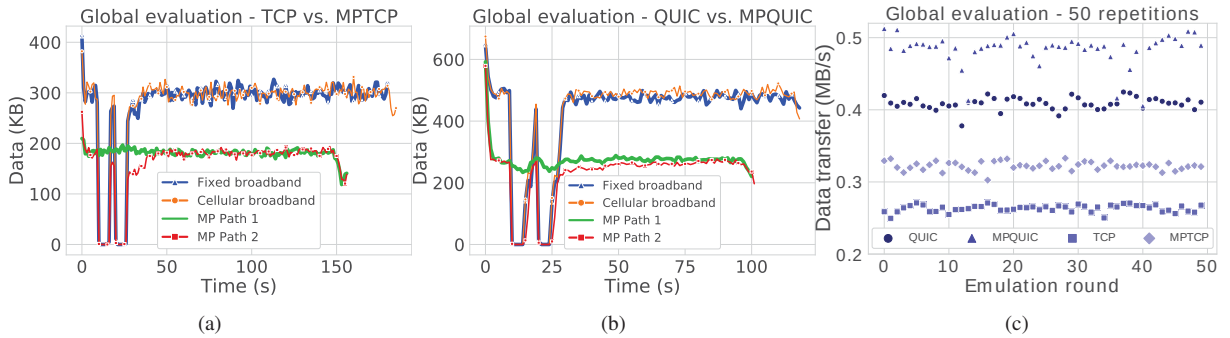


Figure 3.18: Induced failures scenarios and data transfer speed per emulation - Global region

Figure 3.18(b) shows the results for QUIC and MPQUIC protocols. Once again, the multipath protocol handles the communication failures better than the single path one. Similar to the delay evaluations, QUIC and MPQUIC provide better performance considering transfer delay and bandwidth usage. Regarding all protocols, the single path protocols achieve higher absolute transfer rates due to the characteristics of the CUBIC congestion control (e.g., good bandwidth use). The OLIA algorithm in the multipath protocols uses both paths concurrently and seeks fairness regarding possible simultaneous connections and subflows. Thus, even though the transfer rate speeds are lower considering each path individually, the combined speeds are

higher. As a result, the multipath protocols offer higher average data transfer and resilience to communication failures.

Figure 3.18(c) compiles the results from the Global region and the data transfer values achieved by multipath and single path protocols across the emulation rounds. QUIC and MPQUIC achieve higher values in all emulations. However, only the multipath protocols offer adequate performance levels and continuous data transmission in the presence of communication failures. Thus, even though QUIC is faster than MPTCP considering average transfer delay and data transfer speeds, MPTCP provides resilience against communication failures.

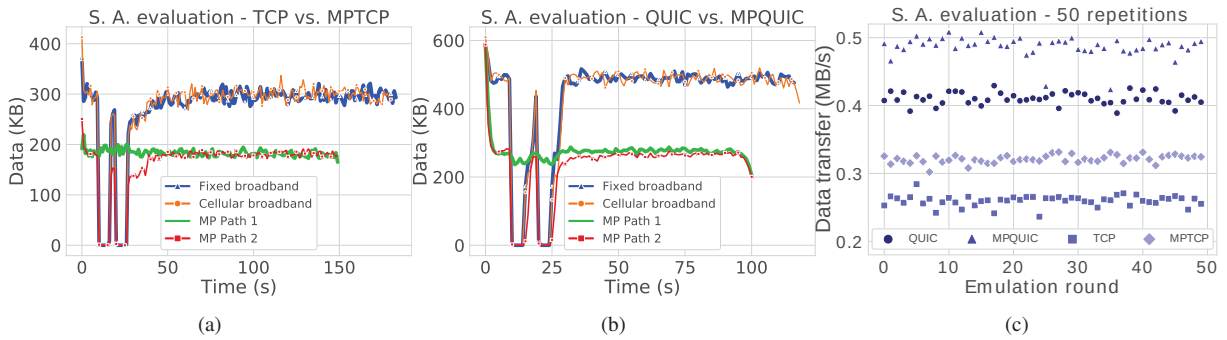


Figure 3.19: Induced failures scenarios and data transfer speed per emulation - South America region

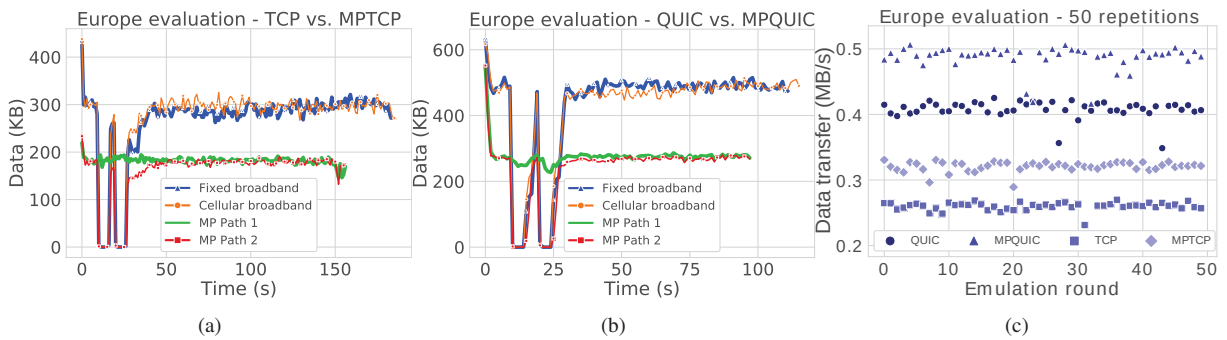


Figure 3.20: Induced failures scenarios and data transfer speed per emulation - Europe region

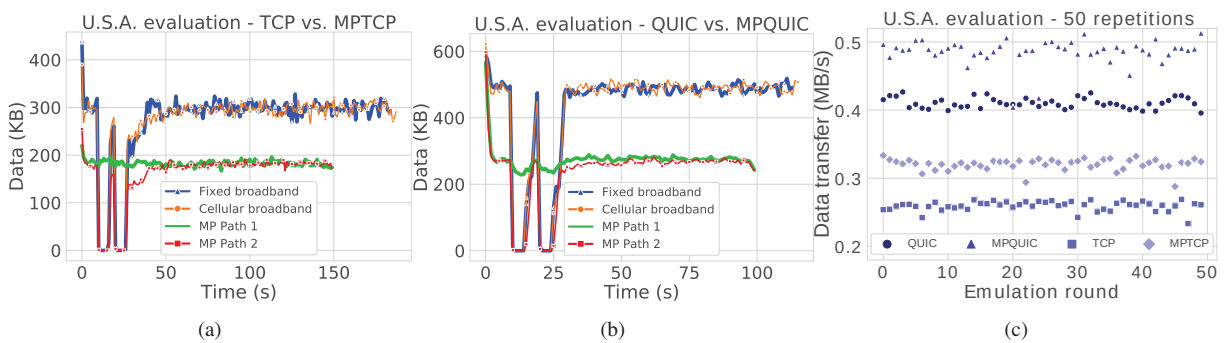


Figure 3.21: Induced failures scenarios and data transfer speed per emulation - United States of America region

PALS behavior considering communication resilience and data transfer speeds repeat throughout the evaluated regions. Figures 3.19, 3.20, and 3.21 depict the induced failures graphs and transfer speed per emulation for South America, Europe, and United States of America regions. MPTCP and MPQUIC managed the communication paths to overcome the communication failures offering continuous data transmission and higher transfer speeds. MPTCP shows a linear

behavior in the first communication path (MP Path 1) when the failures occur in the additional path (MP Path 2). The first communication path in MPQUIC suffers minor oscillations when failures happen in the second path. However, the recovery is fast, preventing interruptions in transmission. Nevertheless, once the speed rates are higher in MPQUIC, it finishes the emulations faster than MPTCP. Data transfer speeds were also similar across the regions regardless of the different throughput speeds available. PALS with MPQUIC protocol provided lower delay, higher transfer rates, and constant data transmission in all emulations.

3.7 CHAPTER SUMMARY

This chapter introduced a resilience management architecture for communication on portable assisted living. The purpose of the architecture lies in increasing communication resilience in IoHT environments and assisting in reaching performance requirements regarding safety and time-critical applications. In order to assess the feasibility of increasing resilience through multiple communication technologies, a resilience-driven experiment was conducted employing a previously proposed Portable Assisted Living System (PALS) solution. The results showed that the multipath versions of the system satisfy the performance requirements regarding the delay and offer resilience against communication failures. This chapter also contributes to reviewing and classifying existing works on IoHT communication resilience and a meaningful discussion on the topic.

4 A BIOSIGNAL AUTHENTICATION AND INTRABODY COMMUNICATION SYSTEM FOR IOHT

Smart healthcare (s-health) applications have great potential to positively impact many people's daily lives, contributing to early detection, prevention, and long-term management of health conditions. Health monitoring is a vital topic and an essential research field supported by sensors in wearable devices, either in direct contact with the human body (invasive) or indirect (non-invasive). Healthcare is moving from a reactive approach to a proactive one, promoted mainly by continuously monitoring health conditions and applying data analytics techniques to the collected data. Monitoring systems allow individuals to monitor their vital signs and provide real-time feedback, which helps maintain optimal health status.

Data privacy is the primary concern in s-health (Abdellatif et al., 2019), given the vulnerabilities found in wearable devices related to data collection, resource constraints, and vulnerabilities in communication technologies, such as wireless communication (Kay et al., 2011). Recent attacks against healthcare providers have exposed an increasing number of security and privacy breaches, as pointed out by CynergisTek on its 7th Annual Breach Report (CynergisTek, 2017). Also, worldwide regulatory institutions (e.g., the U.S. Food and Drug Administration (FDA)) have been requesting public and private companies to develop high-quality and secure healthcare devices and applications (FDA, 2018) by acting as the Health Insurance Portability and Accountability Act (HIPAA). However, preserving data privacy and access in the s-health environment without affecting usability is challenging.

In this context, user authentication systems are crucial to grant data access for authorized professionals (Sandhu and Samarati, 1994). Traditional methods follow one-time event authentication and demand the user to intentionally engage with the system, such as scanning a fingerprint or inserting a password every a certain period (Lin et al., 2017). However, the offered security of one-time event authentication solutions lasts for short periods, being prone to malicious actions and requiring regular attention and interaction from users (Lin et al., 2017). Also, data transmission in current authentication systems relies on wireless technologies. These technologies are susceptible to eavesdropping during the pairing stage, being necessary to design a distinct and secure communication channel.

Hence, the significance and the challenges of s-health applications have led to the exploration of new forms of human-computer interactions and communication technologies for designing continuous and seamless user authentication (Sitová et al., 2015). A set of recurrent biosignals is available in the literature (e.g., electrocardiogram – ECG), electroencephalogram – EEG), galvanic skin response – GSR) (Sancho et al., 2018), and experimental communication channels (e.g., galvanic coupling (GC)) (Tomlinson et al., 2019) applied to continuous authentication and less interaction from users. Furthermore, advances in micro and nano-electronics have assisted the development of different types of sensors that provide real-time vital signs acquisition. Thus, it becomes necessary to rethink current authentication systems to encompass new biometric traits and communication technologies that can protect data and provide continuous authentication.

This chapter presents BEAT (Biosignal Enhanced Authenticator), an original continuous authentication system based on photoplethysmography (PPG) signals and data transmission through a secure Galvanic Coupling (GC) channel. The GC channel deals with one of the main issues regarding the communication between wearable devices once there is a wide variety of security vulnerabilities affecting wireless communication technologies (Celebucki et al., 2018;

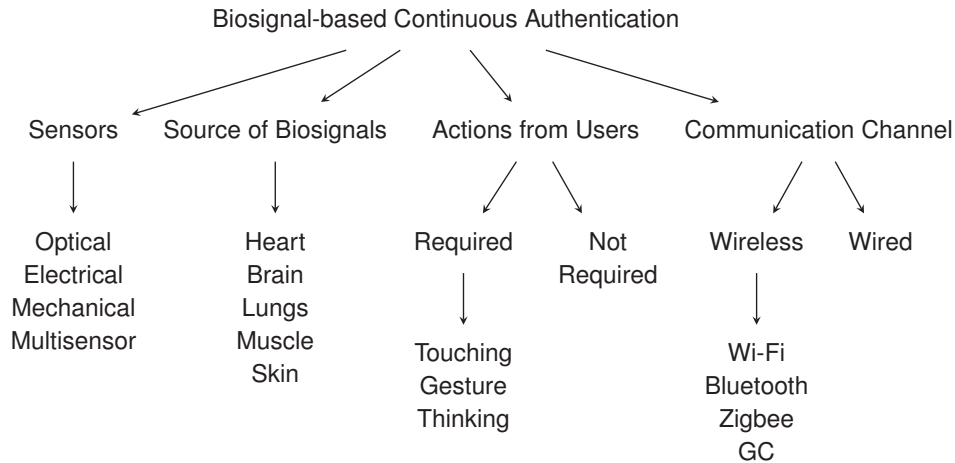


Figure 4.1: Taxonomy for biosignal-based continuous authentication systems

Lonzetta et al., 2018). The PPG biosignal is one of the easiest to collect, becoming prevalent in commercial wearable devices like fitness trackers. This chapter also fills a gap in overviewing and organizing the state-of-the-art biosignal-based and continuous user authentication systems. Its purpose is to build a holistic view of future research directions in this crucial topic. The feasibility of the system has been evaluated by a prototype using PPG as biosignal and synthetic skin as a transmission medium. The results show the system's accuracy in preserving data integrity during transmission and up to 98.66% of true positive authentications.

This chapter proceeds as follows. Section 4.1 presents the literature review of existing biosignal-based continuous authentication systems. Section 4.2 details the proposed PPG-based user authentication system. Section 4.3 describes its performance evaluation and results. Finally, Section 4.4 shows future directions in this topic and concludes the chapter.

4.1 RELATED WORKS

This section presents a literature review and a classification of authentication systems that employ biosignals. Although various works in the literature use biosignals as user credentials for continuous authentication systems, no previous works have categorized and classified the existing works. Observations from this study have led to identifying recurrent features, such as diversity in the type of sensors; focus on a single part of the body as the source of biosignal; the requirement or not of specific actions from users; and the heterogeneity in the explored communication channels. Based on this, Figure 4.1 summarizes a classification of these works, following four main categories: (i) sensors, (ii) sources of biosignals, (iii) actions required from users, and (iv) communication channels. Each category is explained, offering an overview of the main existing works. Table 4.1 compiles the major biosignal-based authentication systems and their primary characteristics.

4.1.1 Sensors

This category highlights the type of sensors employed in continuous user authentication systems, focusing on biosensors, which collect vital signs from users and are the basis for different services in the context of s-health. As detailed next, the biosensors commonly applied in continuous authentication systems are mechanical, electrical, and optical. Continuous authentication systems, such as the one proposed by Yeh et al. (2018), rely on mechanical sensors that utilize mechanical force or pressure to identify the response of a muscle contraction, the push of a button, or the

Table 4.1: Overview of the main biosignal-based authentication systems

Study	Biosignal	Sensor	Source	Action	Communication
(Belgacem et al., 2015)	ECG	Electrical	Heart	Touching (different body sides)	Bluetooth
(Singh and Singh, 2012)	ECG	Electrical	Heart	Touching (different body sides)	N/A
(Wu et al., 2018)	PPG + Accelerometer	Optical + Mechanical	Heart	No action required	Bluetooth
(Zhou et al., 2017)	EEG	Electrical	Brain	Repetitive thinking	Bluetooth
(Mosenia et al., 2017)	BP + ECG + PPG	Electrical + Optical + Mechanical	Heart	No action required	Bluetooth
(Yamaba et al., 2017)	EMG	Electrical	Muscles	Hand gesture	Bluetooth
(Enamamu et al., 2017)	Temperature + GSR	Electrical	Skin	No action required	Bluetooth
(Chauhan et al., 2017)	Breathing pattern	Microphone	Lungs	Breathing (Sniff, normal, deep)	Wired
(Tomlinson et al., 2019)	ECG	Electrical	Heart	N/A	GC
(Yeh et al., 2018)	Plantar Biometric	Mechanical	Muscles	Walking	N/A
(Camara et al., 2015)	ECG + GSR	Electrical	Heart + Skin	No action required	Zigbee
(Lin et al., 2017)	ECG	Doppler	Heart	No action required	Wi-Fi
(Sitová et al., 2015)	Hand Movement + Gait	Electrical	Muscles	Walking, using smartphone	N/A
(Blasco and Peris-Lopez, 2018)	ECG + PPG + GSR	Electrical + Optical	Heart + Skin	Not implemented	Bluetooth
(Peng et al., 2016)	Hand Movement + Voice	Electrical	Muscles	Touching, Swiping, Talking	N/A
(Yadav et al., 2018)	Hand PPG	Optical	Heart	No action required	N/A

pressure of a footstep. Based on an occasional or repetitive movement (e.g., arm gesture, walking, leg movement), the system can identify a pattern employed to identify the user.

User authentication systems, such as the ones proposed by Mosenia et al. (2017) and Belgacem et al. (2015), employ electric biosensors to interpret the electrical activity of the body (e.g., muscle or heart activity) during a period to get biosignals, that will later act as a unique characteristic to identify each registered user. These biosensors require direct contact (or the use of electrodes) with the activity area to allow signal acquisition. The sensors may require or not conductive gel at the points of contact.

Optical sensors analyze the dilatation of blood vessels to calculate the user's heart rate, among other features. These sensors emit light against the user's skin and measure light reflection. Optical sensors can collect biosignals from the heart (PPG and heart rate) and lungs (Respiratory rates). For instance, PPG biosignal is the unique identifier for continuous authentication in the works proposed by Wu et al. (2018), Gu et al. (2003), and Spachos et al. (2011). PPG generates a pulse wave in which several features are estimated, analyzed, and extracted. Those features are exclusive for each human being, making it feasible to use them for authentication.

Few continuous user authentication systems rely on multisensory devices, i.e., devices carrying more than one sensor of different types. Multisensor devices have become popular, given their miniaturization and cheapness. Multiple sensors in the same device may offer multiple biosignals, improving efficiency through their combination. For instance, the authors in Mosenia et al. (2017), and Blasco and Peris-Lopez (2018) employed multisensors for user authentication.

4.1.2 Sources of Biosignals

This category tracks the continuous authentication systems from the perspective of the biosignal source. Identified works from the literature have commonly collected biosignals from the heart, brain, lungs, muscle movement, and skin. Each source of biosignals results in specific characteristics with advantages and disadvantages, as discussed next.

Biosignals from the heart are the most commonly used in continuous authentication systems. PPG, ECG, and blood pressure are biosignals offering information about heart rate variation. We rely on optical sensors to collect photoplethysmogram (PPG) signals and measure blood vessels' dilation and contraction to identify the HRV (Heart Rate Variation). Recently, PPG sensors have become popular in fitness trackers and smartwatches to acquire heart rate variation. ECG signals rely on electrical sensors, and blood pressure usually depends on mechanical sensors. Authentication systems based on heart-related biosignals are available in the literature, such as the works proposed by Belgacem et al. (2015), Wu et al. (2018), and Enamamu et al. (2017).

Brainwaves are biosignals that originate in the brain. Studies have shown their feasibility to authenticate users, such as the work proposed by Zhou et al. (2017), but it is required repetitive

thinking from the user to create a pattern (e.g., think about an action, a picture, a geometric shape, memorize a speech). EEG is the brain's most common biosignal; electrodes connected to sensors and placed on different spots on the head collect the signal. Less invasive methods are also available, like headsets and in-ear sensors.

Respiratory rate is a biosignal once it is possible to create a breathing pattern, having the biosignal collected through microphones or the level of oxygen saturation measured through a PPG signal. This rate is the most common type of biosignal observed from the lungs. Chauhan et al. (2017) presented an authentication system using the breathing pattern recorded from a microphone as a user identifier.

Upon contraction, muscles generate small electric signals. The signals are constantly measured and stored, aiding the extraction of a pattern that serves as a user identifier. The most common signal observed from muscles is the electromyogram (EMG). Muscles can trigger a mechanical sensor, press a button, or activate a foot pressure sensor for plantar biometric recognition. Yeh et al. (2018), Peng et al. (2016), and Yamaba et al. (2017) presented authentication systems based on muscle-related biosignals.

Lastly, different skin properties can be measured, and their values are considered biosignals. For instance, electrodermal activity (Galvanic skin response) reflects the variation of the electrical characteristics in the skin by mirroring its conductance. Sudden changes in the skin's electrical conductivity show stress, fear, and surprise, among other emotions. The galvanic skin response is unique for each user and has been employed to authenticate a user continuously. (Blasco and Peris-Lopez, 2018) evaluated the feasibility of using Galvanic skin response biosignal to authenticate a user.

4.1.3 Actions from Users

The development of continuous authentication mechanisms must comprise the authentication of a legitimate user throughout the entire session (Gupta et al., 2018). Existing systems collect biosignals with or without the necessity of specific action from the user. Recent continuous authentication systems seek to perform seamless authentication, i.e., with low user interaction with the system or no user interaction. However, achieving seamless authentication in this context is still a relevant challenge. In continuous authentication systems requiring no user action, the sensor collects biosignals with no specific action from the user (e.g., a smartwatch that collects a biosignal continuously) (Wu et al., 2018).

There are authentication systems that require interaction from the user within periods. Examples of interactions are touching the device to collect the biosignal, like in work proposed by Belgacem et al. (2015), a specific gesture like proposed by Yamaba et al. (2017), walking such as the proposal from Yeh et al. (2018), or thinking about a previously defined theme like the implementation proposed by Zhou et al. (2017). Touching is required in different systems, such as the works from Belgacem et al. (2015) and Singh and Singh (2012). For instance, ECG-capable smartwatches need signals from both sides of the body to authenticate a user. Hence, if the user wears the smartwatch on the right wrist, s/he will need to touch it with the left hand to generate the authentication signal. Similarly, gestures and thinking generate EMG and EEG signals, respectively. The first is collected through muscle contraction, whereas the second requires the user to think about something (e.g., shapes, colors, speeches, numbers) to generate a pattern and then employ it for authentication.

4.1.4 Communication Channels

Most biosignal-based authentication mechanisms use wireless radio frequency transmission as a communication channel. However, significant technologies such as Bluetooth, Zigbee, and NFC have presented security flaws (Celebucki et al., 2018; Lonzetta et al., 2018; Alaba et al., 2017). Galvanic Coupling (GC) method is a promising communication channel by the human body, having the skin and tissues as conductors. Recently, we have observed an increase in the number of works employing GC as a communication channel, such as the proposals from Tomlinson et al. (2019), Ito (2018), Alquaydheb et al. (2019), and Kumar et al. (2019). Using the human skin as a communication medium pursues a secure data transmission once signal interception is impossible without skin contact.

4.2 THE BEAT AUTHENTICATION SYSTEM

This section presents BEAT, a new biosignal-based and continuous user authentication system to attain seamless and secure authentication. BEAT authenticates a user based on PPG biosignals, collected continuously by wearable sensors and transmitted by GC from these sensors to a coordinator device, where the user needs access. BEAT acts within the s-health concept, considering a star network topology composed of a coordinator (e.g., a smartphone) as a central device and a wearable device. The network coordinator usually has higher computational resources (energy, memory, and processing power) than other wearable devices in or on the human body. Furthermore, GC can protect data transmission between a wearable device and the network coordinator.

BEAT follows three steps: (i) data collection and preprocessing, (ii) data transmission by GC, and (iii) the authentication procedure, as shown in Figure 4.2. Hence, Figure 4.2a illustrates the network coordinator as a smartphone, but it could be any device in direct contact with the user's skin and able to operate as a communication gateway between the wearable network and other networks (e.g., a wireless local area network (WLAN), the Internet). It is out of the scope of this work to handle the communication between the network coordinator and the Internet; or between the first and a WLAN.

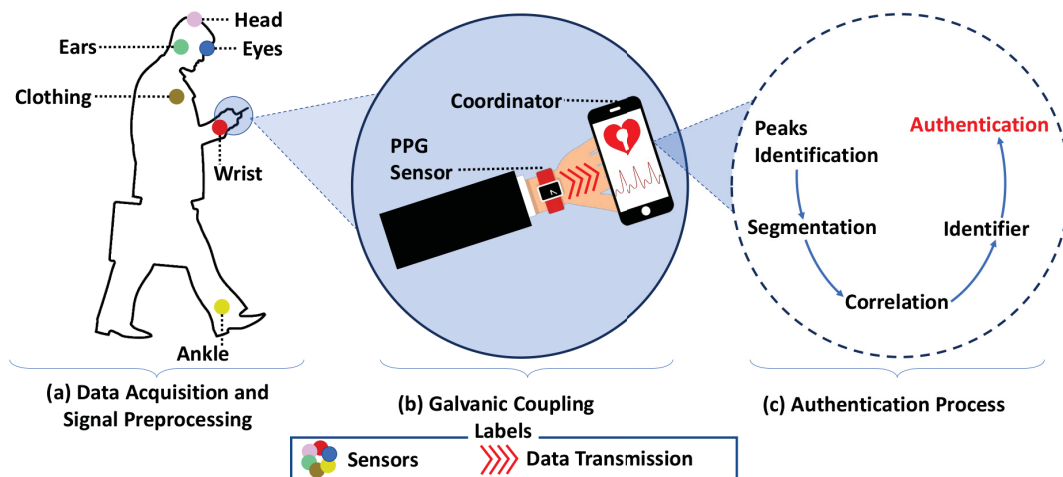


Figure 4.2: The steps of the BEAT authentication system

Figure 4.2 (a) also indicates multiple wearable devices positioned on different body parts, such as the head, eyes, ears, clothing, wrist, and ankle. A wearable device is an autonomous, non-invasive device performing a specific function related to the body, such as monitoring the

user's vital signs. Examples of wearable devices are smartphones, smartwatches, physical activity monitors, smart sneakers, and others. A generic architecture of a wearable device follows the modules: sensor, low-power processor, and communication. After data collection, wearable devices convert collected signals into raw data. Depending on the monitoring task, different types of sensors can be employed. BEAT is founded on optical sensors, such as those in smartwatches and physical activity monitors since this type of sensor benefits user convenience and usability.

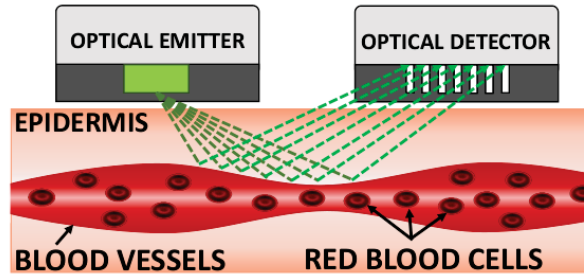


Figure 4.3: Optical Sensor

4.2.1 Data Acquisition and Signal Preprocessing

BEAT collects PPG signals, allowing the observation and extraction of unique user features, such as the number of peaks and valleys, peak shapes, wave amplitude, and the distance between peaks and valleys, as shown in Figure 4.4. BEAT uses a combination of these features, using the time-frequency domain, to correlate the entire set of collected data by wave segments and improve robustness for user authentication. Identifying peaks and valleys is crucial regardless of the extracted trait, as the threshold authentication limit relies on overlapping peaks.

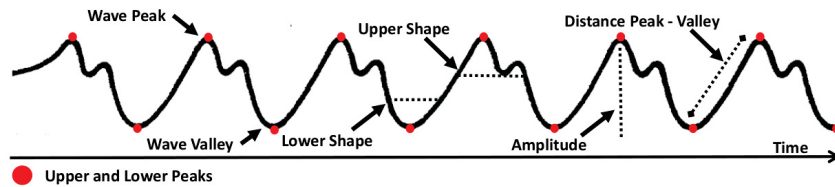


Figure 4.4: Main features in a PPG signal waveform

After data acquisition, BEAT filters the collected signals to reduce noise from electromagnetic interference, light excess, and sudden user movements. Hardware filters are efficient and fast for extracting specific data (e.g., data related to cardiac variation or breathing). However, they are limited in terms of flexibility because they collect data in a specific range of frequencies. Similarly to hardware filters, software filters limit the amplitude of the collected signal. Although these filters are slower than the hardware ones, they adjust the filtered frequency band flexibly.

Among the filtering techniques, the most common examples are frequency band segmentation, high-pass, low-pass, and band-pass filters. The choice for a given filter depends on the goals. Also, the filter choice should consider computational restrictions in wearable devices, and it is necessary to select filters with low computational complexity. Thus, high-pass, low-pass, and band-pass filters are preferable because they perform signal segmentation in several bands (multidimensional), and their configuration allows a cutoff frequency and a reduced number of operations, leading to efficient energy use.

4.2.2 Data Transmission by Galvanic Coupling

BEAT adopts GC to significantly reduce vulnerability to attacks compared to conventional communication technologies, such as Bluetooth, Zigbee, and others. In GC, data is encoded and transmitted by low-voltage electrical impulses sent through the human skin, thus being immune to attacks, such as eavesdropping and others. GC acts on intra-corporal communication, which is within the scope of the IEEE 802.15.6 standard. In an intra-corporal data transmission using GC, a differential electric signal is applied to two transmission electrodes on the skin. Most of the signals sent by the electrodes to the skin are dispersed. However, the skin and tissues conduct an amount of the signal, reaching the two contact electrodes in the receiver. The main feature of differential signal in GC comprises the model of sending data through the two electrodes. The biosignals are reversed proportionally at each electrode before transmission through the skin. The receiving device calculates the difference between the two received signals, getting the original signal. Figure 4.5 exemplifies the GC model.

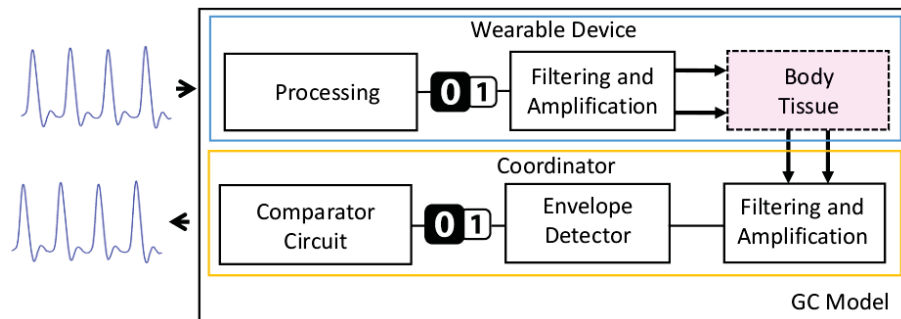


Figure 4.5: Galvanic coupling model

Signal power is strongly influenced by the body tissues' dielectric (insulating) properties. The body is the medium for sending (Tx) and receiving (Rx) data, being the modulation and power of the signal-relevant issues. Modulation reflects the characteristics of the GC circuit, emphasizing robustness and simplicity. BEAT follows the Pulse Width Modulation (PWM) for consuming less energy and conforming to the On-Off nature of digital devices. PWM represents the digital data through variations in amplitude and period in a carrier envelope. It estimates data through the presence or absence of an undercut and its percentage of duration in each state On-Off. The existence of a wave for a specific period means binary 1, while its absence for a period means binary 0.

4.2.3 Authentication Procedure

The authentication procedure (Figure 4.2c) happens in the network coordinator. When the coordinator receives the preprocessed PPG signal, it assigns a function to extract features from the PPG waveform. The authentication procedure handles the waveform in four tasks: peak identification, segmentation, correlation, and user identifier calculation. The first is identifying peaks along the entire length of the collected and preprocessed biosignal. This task is fundamental to defining reference points for the segmentation phase. To identify peaks, BEAT employs specific algorithms based on moving averages or features (e.g., peak and minimum height) for threshold calculation (Shin et al., 2009).

The second task segments the collected biosignal in cycles related to the wavelength. Thus, each cycle is identified, and all detected cycles are overlapped and aligned, taking as reference the center of the previously detected peaks. This allows us to correlate (the third task) all segments and calculate their average. This average is called a user identifier, the fourth

calculation task. Thus, BEAT authenticates the user when the user identifier matches an existing reference model in the system. Otherwise, it denies the user access to services and data.

The authentication procedure relies on the previous registration of the users. The registration procedure takes place offline, and its tasks are similar to the authentication ones, but registration demands a higher amount of data, considering different user positions and physical states. User registration begins with data collection, following feature extraction and signal segmentation. Segmented cycles are aligned, taking peaks as reference. This allows the correlation among all segments and their average calculation. Correlation defines an authentication threshold (user reference model), calculated by the minimum average value for a user to be authenticated. On an authentication attempt, the reference model is compared to the generated user identifier following authentication, as previously described.

Figure 4.6 summarizes the registration and authentication procedures. The registration procedure occurs before the authentication procedure and requires a more significant amount of time for capture when compared to the authentication process. This is due to the need for more data to build the reference model. The authentication process occurs online, i.e., when the user needs to access the system or service.

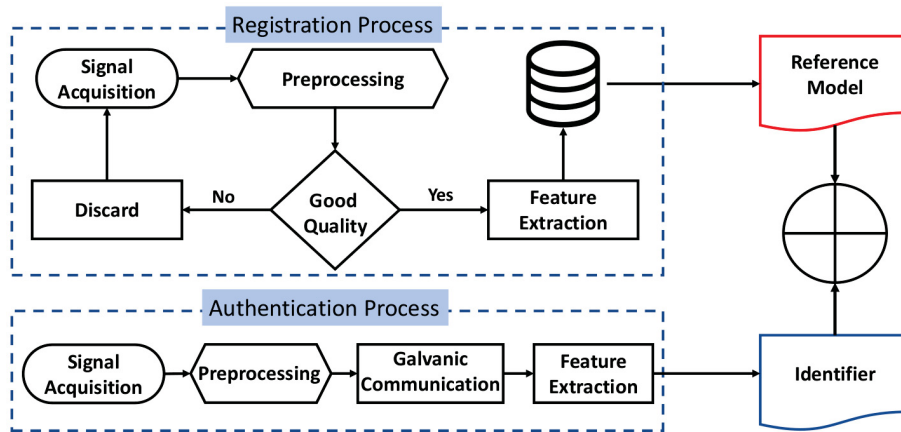


Figure 4.6: Register and authentication for the BEAT system

4.3 EXPERIMENTAL DESIGN AND ANALYSIS

This section details a real implementation of BEAT and its performance analysis. Evaluations have followed two approaches: (i) an experimental environment within the context of the NSF/RNP U.S.-Brazil HealthSense project; and (ii) based on a dataset available in the Physionet online repository. These two approaches aim at comparing their results.

4.3.1 Implementation of BEAT in an Experimental Environment

This implementation of BEAT employs the PPG Gravity Heart Rate Monitor Sensor from DfRobot, whose spectral response peak is 570 nm. It has been integrated to an open Arduino platform version R3, with a 16 MHz ATmega328 microcontroller, the same in several wearable devices. Figure 4.7(a) shows a picture from the data collection.

The galvanic coupling implementation and analysis employ two 72 MHz 32-bit Teensys 3.2 development boards acting as signal transmitter (TX) and receiver (RX), powered by different sources and with no shared ground. The PPG signal is amplified, binary encoded, and injected into a synthetic skin tissue through jump wires that emulate contact skin electrodes. For evaluation

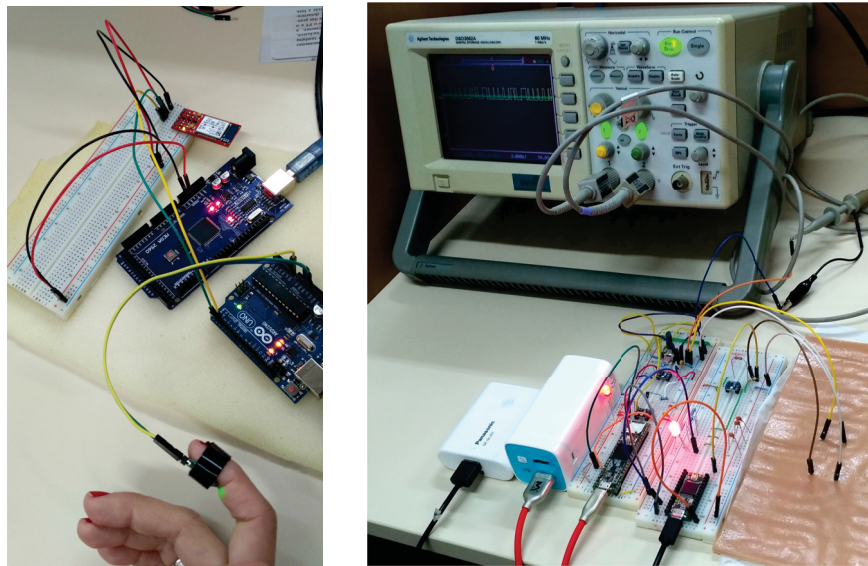


Figure 4.7: Testbeds

purposes, we transfer a sample of real PPG signal from the emitter to the receiver through the synthetic skin using a distance of 8 centimeters. At the receiver, the signal is amplified once again, as the synthetic tissue has insulating properties, and then it is restored to the original form. We evaluate the data integrity of the signal by the transmitted sample to create an identifier model. This model is latter compared to the reference model to perform user authentication, assuring the correctness and compatibility of the signal. Figure 4.7(b) shows a picture of the GC testbed.

The user registration procedure is accomplished in a controlled environment, restricted from electromagnetic interference and without direct incidence of light. PPG signal collections contain both time of capture and the numerical values of signal for each individual. The outcomes of the registration procedure are two datasets (NR2/UFPR#1 and #2), comprising data from 30 healthy individuals from 23 to 53 years old and with no record of cardiac issues. Each individual had their PPG signal collected and recorded in two positions: standing and sitting. The NR2/UFPR#1 dataset contains data from the seated individuals, whereas the NR2/UFPR#2 dataset contains data from standing individuals. User registrations were made at different time as would occur in a real situation. Datasets hold three-minute sample per individual. Figure 4.8 shows for a real sample the original PPG signal (as captured by the sensor); the filtered signal; and the filtered signal with detected peaks.

Using the R software, the testbed employs the eighth-order Chebyshev II low-pass filter over the collected signal. This filter fits wearable devices which have low computational power microcontrollers. Feature extraction from the PPG signal uses the frequency band from 0.5 to 5.0 Hz. Earlier, peaks are detected, and segments are overlapped. Hence the R Cross-Correlation Function (CCF) computes the correlation among all overlapping segments. CCF establishes the correlation between two different series and their respective confidence intervals. Hence, BEAT calculates the user reference model (authentication threshold), as seen in Figure 4.10.

The authentication procedure has as input one-minute real-time collected data per user in each position. The evaluated metrics are true and false positive, true and false negative, total of inferences, and accuracy. Figure 4.11(a) compares the reference model recorded for a given user (red wave) and the identifier for the same user (blue wave) calculated on the authentication procedure. Although such waves are not entirely identical, they are within the established

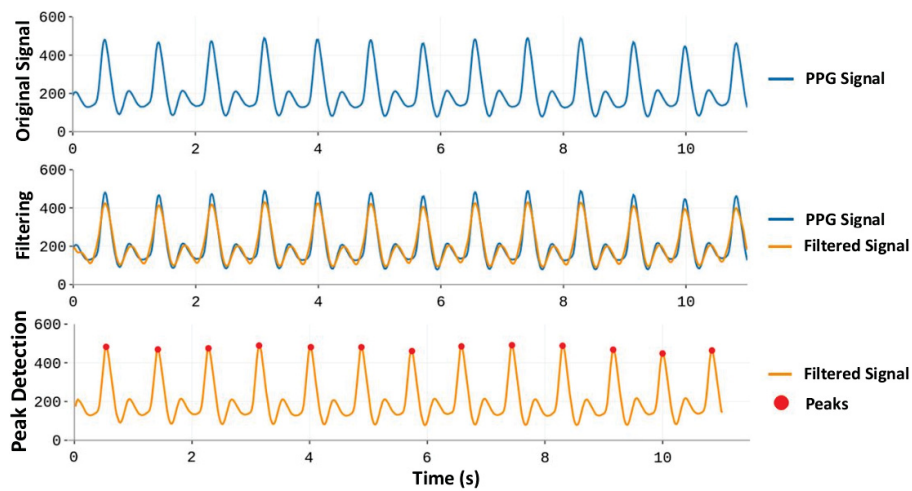


Figure 4.8: Signals and preprocessing

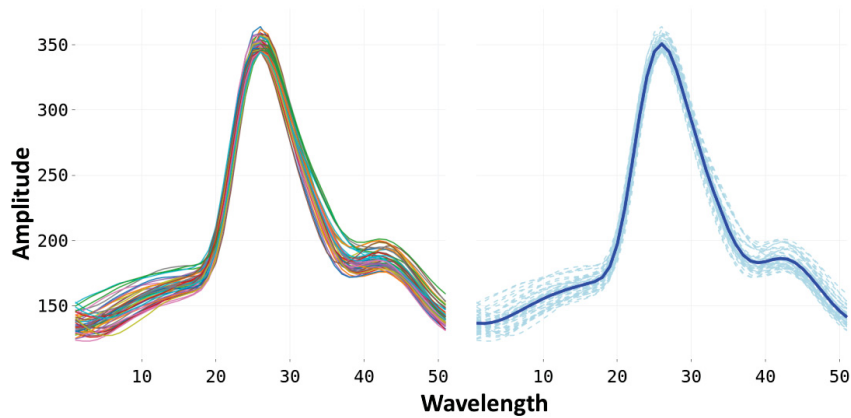


Figure 4.9: Overlapping waves and mean

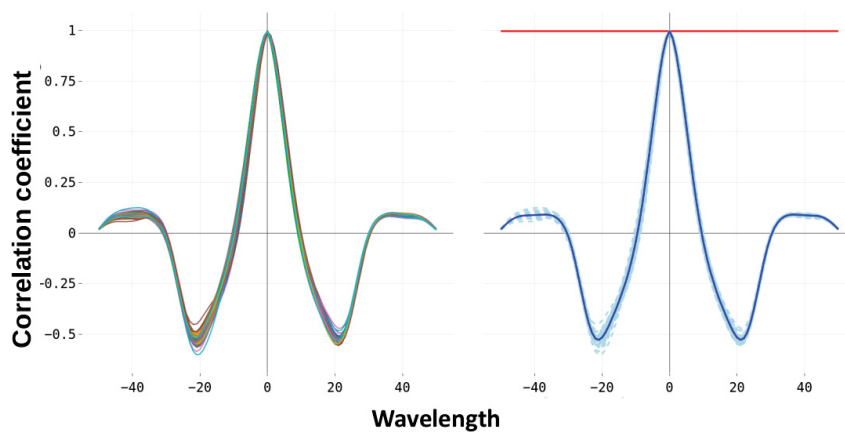


Figure 4.10: Authentication threshold

threshold, showing enough similarity to allow user authentication. Figure 4.11(b) compares a reference model and the identifier from different users; in this case, the access was denied.

A low-pass filter removes the harmonics from the collected PPG signal, preserving the central band ($FC = 100\text{kHz}$). Next, data is sent through the communication channel within the frame's payload, which comprises a preamble (13-bit Barker code) for synchronization, a data

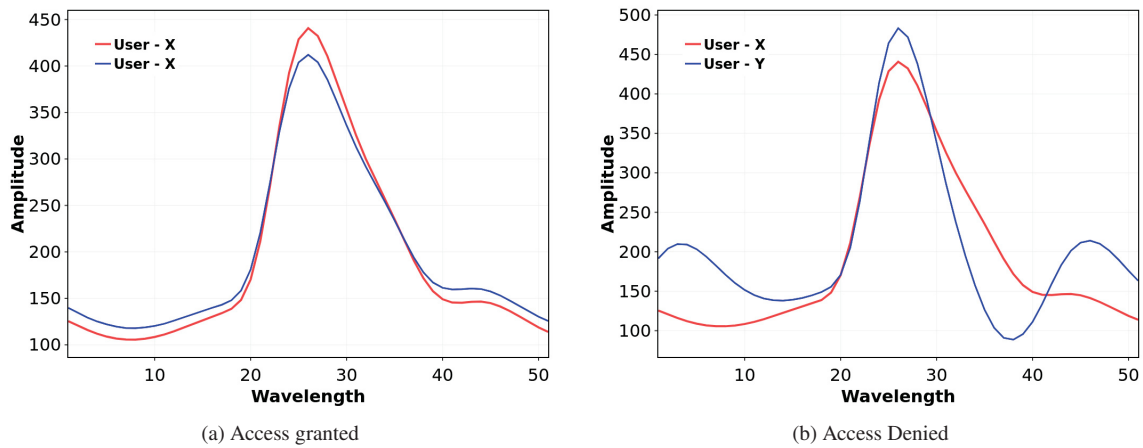


Figure 4.11: Authentication process

length field, a payload (64 bits), and an 8-bit CRC. As the signal propagates through the synthetic skin, an analog receiver hardware uses a high-pass filter to remove any low-frequency noise from interference. An amplifier (MAX4488 from Maxim Integrated TM) neutralizes the channel attenuation, and the high-frequency filter raises the signal level to meet the activation voltage required for the diode. An envelope detector circuit converts the signal back to the baseband and removes any possible carrier wave oscillations before delivering the signal to the comparator.

Aside from the tests performed in the described experimental environment, the Beth Israel Deaconess Medical Center dataset from the Physionet repository (Goldberger et al., 2000) has been the basis for comparative analysis. This dataset contains PPG signals collected from 30 individuals at the 125 Hz frequency by the Israeli center. The individuals suffer from some critical health condition (e.g., heart, respiratory), and when the data was collected, the individuals were resting in the hospital bed. It is worth mentioning that there was no control over this last dataset creation (i.e., there was no management of the conditions of the environment in which data was collected or about the PPG sensor quality). Signal segments have resulted in handling three minutes of information from this dataset to create the user reference model (user registration); and one minute to calculate the user identifier employed for user authentication.

Table 4.2 summarizes the results for the analyzed metrics over the three evaluated datasets. BEAT has shown the best results for the NR2/UFPR#1 dataset, presenting an accuracy of 98.66%, 12 false positives, and no false negatives. The Physionet dataset has obtained an accuracy of 89.88% and no false negatives but reached 91 false positives in 900 inferences. The NR2/UFPR#2 dataset has presented 26 valid users (peaks satisfactorily identified) of the initial 30 users and 676 inferences. For valid users, BEAT has achieved an accuracy of 92.15%, three false negatives, and 50 false positives for the NR2/UFPR#2 dataset.

Table 4.2: Comparing results from the NR2/UFPR and Physionet datasets

	TP	FP	TN	FN	IT	Accuracy
NR2/UFPR Dataset #1	30	12	858	0	900	98.66%
NR2/UFPR Dataset #2	23	50	600	3	676	92.15%
Physionet Dataset	30	91	779	0	900	89.88%

Even with the application of filters to remove signal noise, some factors, such as excessive movement during collection, electromagnetic interference, and other environmental issues, could not be circumvented. The best outcome of the NR2/UFPR#1 dataset is due to the

stability offered by the sitting position, which allows the user's arm to be at rest position, which generates less movement and a stable PPG waveform.

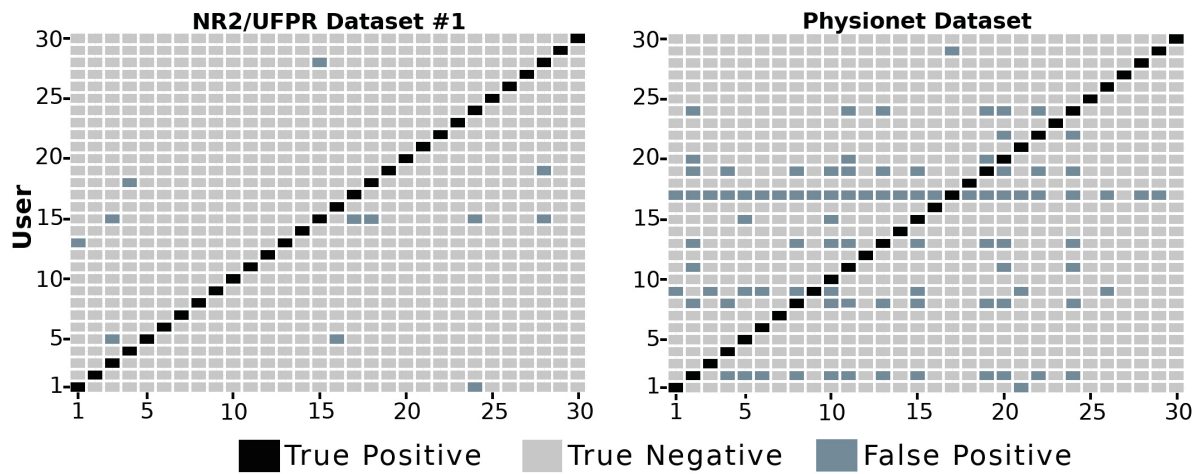


Figure 4.12: Authentication map

Figure 4.12 shows the validation results for all individuals of the NR2/UFPR#1 dataset. The false positive values in the authentication map indicate that the collected data are stable, making it possible to extract several features from the waveforms. Even with the signal collected from users with critical health conditions, the system achieved an accuracy close to 90% for the Physionet dataset. We suspect the high number of false positives is due to the low-quality PPG signal since four users from the dataset account for 60.4% of all false positives. Evaluating the two authentication maps, we observe that none of them got false negatives, showing that it was successful in every situation in which a legitimate user tried to authenticate. Authentication accuracy yielded by BEAT is equivalent to other PPG authentication systems such as (Zhao et al., 2018; Yadav et al., 2018). However, BEAT employs GC to provide a secure communication channel, making it difficult to perform a complete comparison. To the best of our knowledge, no other system jointly applies PPG biosignal and GC to user authentication.

4.4 CHAPTER SUMMARY

Smart healthcare (s-health) is a relevant topic that has led to considerable research mainly concerned with the security of data continuously collected from users by devices integrated into their clothing or worn on the body. In order to provide security, user authentication systems play a crucial role. However, it is imperative to redesign them considering the limitations of wearable devices, in which human-computer interaction varies from the traditional perspective. For instance, one can expect no longer using long-alphabetic passwords in wearable devices (mainly implanted ones) to grant access to systems once passwords lack convenience and require users' regular attention.

Based on the literature overview, this chapter presented BEAT, a new authentication system that uses PPG signals and Galvanic Coupling (GC) as a communication channel to authenticate users in a wearable network. BEAT aims to achieve high user transparency in the authentication process and security. The acquisition of the PPG signal is non-intrusive, and data is transmitted by GC, keeping the user always connected. Results from real experimentation have shown high accuracy, high true positives, and low false positives, being the incidence of false positives directly related to the quality of the PPG signal. The results of the experiments with the

system indicate the feasibility of the PPG signal as a biometric authenticator. Furthermore, using the galvanic coupling communication to transfer data raises security to a new level.

This chapter also presented an organization for state-of-the-art biosignal-based user authentication. The organization follows four important categories considering the type of sensors; the employed biosignal and its source of the collection; the necessity of specific user actions; and the communication channel. This chapter highlighted each category and associated them with the main existing works from the literature.

Despite prominent advances, there are still challenges and opportunities for researches in this relevant topic. First, techniques to extract features and patterns from biosignals require improvements in efficiency (accuracy and low false positive rates) to work on real-time over short time windows of collected data. Second, designing resilient biosignal-based authentication systems is paramount to dealing with low-quality collected signals. A path in this direction should consider using multisensory with different biosignals or redundancy for collecting the same signal. Third, designing user authentication systems that require no actions from users, i.e., seamless authentication to users, is urgent, given the rapid advances in nanotechnology that allow wearing devices in the body. Fourth, it is necessary to advance in efficient communication interfacing body-implanted devices and network coordinators in the search for seamless authentication.

5 A RESILIENCE ANALYSIS APPROACH FOR IOHT

IoHT interconnects wearable healthcare devices and the Internet through access networks, offering continuous sensing of personal data and remote monitoring of users health. However, IoHT is a relatively new concept, and its particularities regarding infrastructure and performance requirements demand approaches to assess its resilience when facing uncertainties. Incorporating adaptive management in such a complex and interconnected environment is challenging, particularly considering numerous configuration possibilities within the wide range of components. Thus, aside from proposing adaptive solutions, it is crucial to verify whether the existing configurations can handle them. Threats that degrade communication performance in IoHT are increasingly frequent and endanger the lives of individuals. Hazards in IoHT include legitimate faults and malicious attacks that degrade communication performance by increasing end-to-end delay or decreasing the number of delivered packets (Junior and Kamienski, 2021).

Emerging wireless and mobile networks also face environmental challenges due to the open nature of their communication channels. Furthermore, the co-existence of multiple communication technologies in IoHT generates diverse topologies and increases the surface of possible failures. The need for resilience in computer networks is a recurring topic and draws the attention of many authors with multiple perspectives. While many proposals suggest methods for increasing or evaluating communication resilience considering a single and complete system, the works rarely attempt to estimate the resilience regarding the possible network configurations within the IoHT spectrum when facing specific failures.

Few works in the literature address communication resilience encompassing various types of networks within a broad spatial scope. In general, the works focus on a specific network segment, disregarding problems that occur outside the scope of this network. Threat identification and evaluation also happen separately, reducing the possibility of analyzing the impact of specific failures or the proposed solutions on the overall behavior of the network. Graph-based proposals usually consider massive networks with multiple end devices and communications links with the same characteristics, contrasting with the fewer nodes and heterogeneous communication technologies in IoHT. Therefore, an approach is needed in which it is possible to assess the resilience of multiple possible network configurations in the IoHT when they face challenges.

Estimating IoHT resilience considering multiple possible network configurations and diverse threats is challenging, but necessary. Therefore, the study presented in this chapter proposes an approach to analyzing resilience in the IoHT that assesses the multiple achievable network configurations regarding the devices and communication technologies available and the challenges imposed by threats. This approach assists in determining the feasibility of embracing adaptive solutions in IoHT, given the most typical communication configurations currently available. This approach is composed of three steps (*i*) the identification of possible network configurations in the IoHT considering the communication technologies and devices distribution; (*ii*) the identification of the most relevant and vulnerable nodes and data links and (*iii*) the identification of the main threats regarding IoHT communication. The main contributions of this work include a novel perspective for configuring and designing IoHT networks founded on resilience. This work also contributes to identifying the main threats to the IoHT environment, considering each stage of the spatial scope.

5.1 BACKGROUND

The resilience analysis of a network assuming multiple topologies and components is one of the most important and widely studied approaches. Those studies usually evaluate intricate networks employing numerous nodes, links, and topological features. Despite drifting from the restricted characteristics regarding the number of devices, communication links, and possibilities of configurations available in the IoHT, those works contribute to identifying the advantages of including multiple configurations for communication. Still, the resilience analysis of the IoHT environment must consider the infrastructural-specific particularities to provide insights regarding the most critical or vulnerable elements.

Network survivability is a system capability that allows systems to survive, limit damage, heal, and operate robustly, particularly in the face of attacks and intrusions (Ellison et al., 1997). Usually, survivability evaluation is done by removing important nodes and connections in a graph representation, leading to partial or complete network segmentation and communication failure. The nodes and connections on a graph represent the devices and communication channels on a network. Graph analysis is one of the most employed methods of measuring resilience and related disciplines. The authors in (Fu and Yang, 2021) proposed a model to evaluate the propagation of failures considering three distinct service levels: sensing, retransmission, and aggregation. The work also includes a new metric to characterize the load distribution across the components of an IoT network. The work differentiates itself from articles that only evaluate the survivability of devices or the complete topology of the network; however, it still considers the possibility of numerous devices and communication channels as a basis for the IoT environment. That assumption is valid for some IoT-based systems but is unsuitable for the IoHT environment.

Another metric employed to analyze resilience is network robustness based on edges and node connectivity. In the context of resilience, robustness describes the quantifiable reliability of a system when facing threats (Sterbenz et al., 2010b). The authors in (Ratnayake et al., 2021) proposed quantifying the robustness of complex networks composed of heterogeneous nodes. Node heterogeneity is a characteristic of IoHT environments and one of the main challenges when evaluating resilience. The authors propose a new robustness metric that aims to capture the heterogeneity of nodes using the fitness-incorporated average network efficiency. Subsequently, they adopted the proposed metric in several experiments with different topologies. The results from the experiments show that the suggested approach efficiently captures the diversities of nodes and communication links when evaluating the robustness of complex networks. However, the randomly generated topologies encompass numerous nodes and communication channels. Although the diversity is similar to the characteristics found in IoHT, the abundance of devices and communication channels deviate from the scarce network configuration possibilities in IoHT.

Aside from assessing the resilience of networks, some works relate network resilience and communication performance. That is particularly difficult once the unique characterization of multiple devices and communication technologies is complex. Additionally, network segmentation, considering its diverse topologies, is challenging to capture through models. The authors in (Althoubi et al., 2021) proposed the performance evaluation of an IoT sensor network in terms of delay and also considering the robustness of the network. In order to carry out the experiments, the authors assumed some premises to represent the model. The devices were characterized according to their processing power and delay, while communication channels were characterized considering bandwidth and delay. However, due to the complexity of depicting the scope of the network, the authors assume that the interconnections of the different topologies occur through simple associations, disregarding the different network services funded on short and long-range

communication. Despite those assumptions, the authors offer an essential understanding of resilience in IoT networks and its association with network performance and delay.

5.2 A NOVEL APPROACH ON IOHT RESILIENCE ANALYSIS

The particularities existing in the IoHT environment make evaluations in terms of communication resilience difficult. In other types of network configurations, such as wireless sensor networks and further concepts derived from IoT, a wide range of devices, communication channels, access networks, storage media, and support structures strengthen redundancy, one of the pillars of resilience. The small number of sensing sources, the few concurrent communication channels, and the limited offer of access networks make adapting existing evaluation methods challenging and designing communication resilience arduous. Thus, we propose a novel hybrid method of evaluating communication resilience that assesses the most vulnerable points regarding the possible communication topologies in IoHT and evaluates the communication performance when the vulnerable points face threats.

IoHT relies on the operation of its essential services. Thus, each device and data link in the systems that support the essential services must fully operate for IoHT to function accurately. Any threat affecting a device or data link will impact the conditional and adjacent services. In that regard, the first step in creating a graph-based model for resilience analysis is to assemble an abstract representation of the IoT environment. This task is particularly complex because the level of generalization must be sufficient to suit the various communication configurations in the IoHT but should also capture the environment's unique characteristics. A proper scientific model will be abstract enough to provide an overview of the IoHT environment but also recognize the implications of technological heterogeneity and their interactions. Figure 5.1 illustrates the architecture and overview of IoT and its services. Each essential service in IoHT is supported and depends on various devices and communication technologies; this variety allows the construction of different topologies.

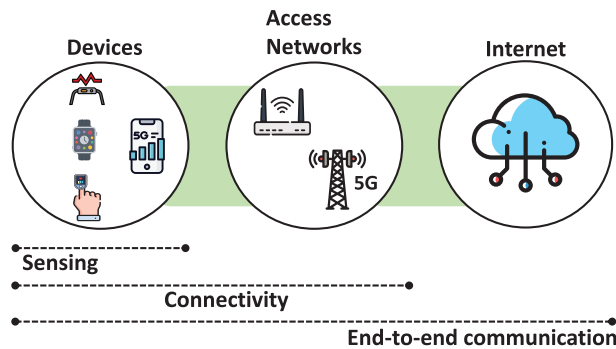


Figure 5.1: Essential services in IoHT

Regarding the Sensing essential service, the basic configuration relies on a smartphone as a coordinator for wearable devices. However, the ongoing evolution of IoHT devices offers new possibilities, especially regarding communication technologies and mobility. New and more capable devices promote variations in communication configurations, and each topology might offer a different level of resiliency. The communication technologies considering the connectivity essential service do not offer the same diversity for resilience as the sensing essential service. The reason is that enhancements usually happen regarding the existing technologies instead of developing new ones. Nonetheless, the existing communication technologies can offer redundancy possibilities bolstered by devices with multiple communication technologies and multipath communication protocols.

Communication performance evaluations rely primarily on end-to-end evaluations once they comprise aspects from sensing and connectivity essential services. However, evaluating communication performance by focusing only on topologies endpoints makes it challenging to identify the specific essential service related to a threat. In this case, it is possible to identify an anomalous behavior regarding the IoHT system but unattainable to identify its origin or how it affects each essential service separately. We aim to identify and assess the main configuration possibilities for IoHT, considering the most available communication technologies and devices. By assessing each configuration individually, we propose a graph-oriented representation and apply resilience metrics to define the most significant nodes in each representation. Hence, we identify the most vulnerable nodes regarding IoHT topologies. Afterward, we conduct the communication performance analysis, which consists of inserting induced failures in the main vulnerable points to identify the outcomes regarding the communication performance for each proposed configuration.

5.3 GRAPH-THEORETIC REPRESENTATION AND ANALYSIS

The analysis regarding the IoHT communication configurations employs a formal graph representation. We apply different graph analysis metrics to study each topology's properties. The employed metrics encompass resilience and centrality metrics. Resilience is fundamentally a network property once; usually, it is achieved through redundant paths and devices. Centrality evaluations assess a node's structural properties and provide an overall understanding of its importance for each configuration. The communication configurations represent a possible IoHT topology with links and nodes depicting communication and devices. Here, we aim to study the logical representation of technologies employed in IoHT without being unnecessarily constrained by the details of a particular network and its associated components.

5.3.1 Analysis Regarding IoHT Network Configurations

The evolution of IoHT devices happens quickly. The latest products on the market reflect the efforts of academia and industry in researching innovations that promote lighter, more efficient, connected, powerful, and cheaper devices. The evolution of devices and their integration into existing environments supports the development of new communication configurations concerning devices and data dissemination to the Internet. Thus, it becomes necessary to specify the main existing communication configurations in IoHT, including device and communication redundancy, and consider the available possibilities of transmitting data to the Internet.

The existing IoHT configurations, considering devices and communication technologies, were transposed into six topologies. Each topology has at least one sensing device that represents a wearable device, a coordinator device that manages the network of wearable devices, an access network gateway to the Internet, and a data endpoint that represents a data storage and management facility. The topologies also mimic the connections between wearable devices and coordinators, coordinator devices and access networks, and access networks and the Internet, given its possibilities in terms of devices and communication links. Fig. 5.2 illustrates the proposed topologies, and a detailed description is presented next.

- **Topology 1** represents a basic configuration commonly used in IoT where a sensing device represented by *Node A* communicates with a coordinating device represented by *Node B* using short-distance communication technology. *Node B* communicates with the gateway to an access network represented by *Node C*. Finally, *Node C* transmits the data to a storage and management facility on the Internet, represented by *Node D*.

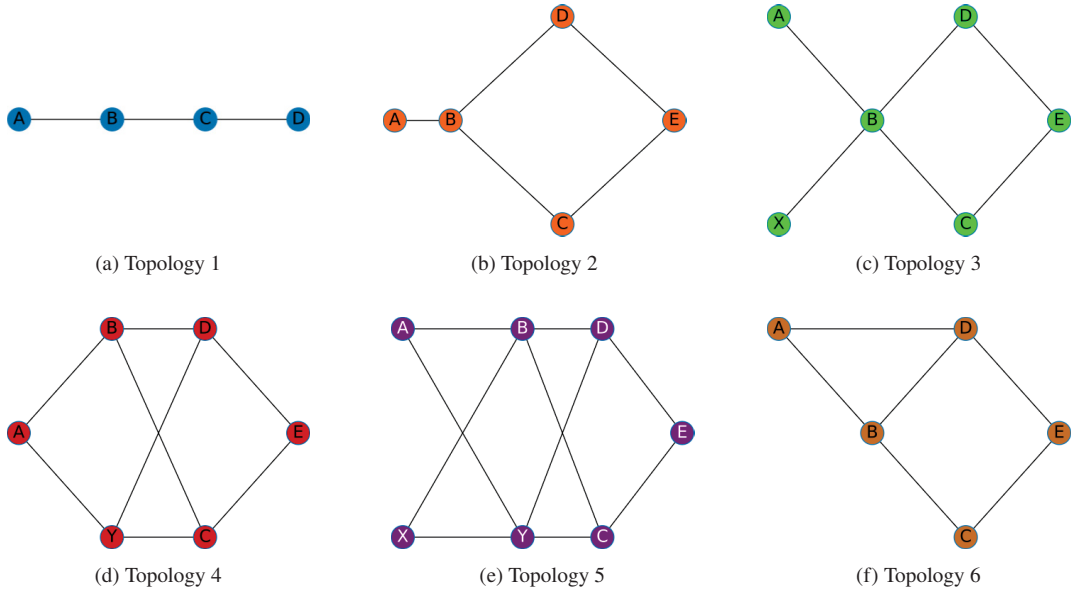


Figure 5.2: Possible communication configurations for IoHT

- **Topology 2** is similar to the first Topology, with the only difference being that there is redundancy for the communication gateways to the access networks. This configuration represents a scenario studied in previous works (Nakayama et al., 2021, 2022), where the coordinator device represented by *Node B* can access two access networks simultaneously represented by the access gateways *Node C* and *Node D*.
- **Topology 3** is a variation of **Topology 2** with added redundancy for the sensing devices. In this scenario, two wearable devices are represented by *Node A* and *Node X*. With this configuration, sensing devices can still collect user data and forward it to the coordinator, even when one of the devices is compromised.
- **Topology 4** is also a variation of **Topology 2**. However, instead of duplicating sensing devices, we have redundancy for the coordinator devices, represented by *Node B* and *Node Y*. This scenario deviates slightly from traditional IoHT configurations since it requires two coordinator devices and two distinct access networks. However, if a coordinating device is compromised, this configuration promotes a greater variety of paths for transmitting information and for continued operation.
- **Topology 5** represents the highest redundancy capacity possible among all topologies. In this configuration, there is a redundancy of sensing devices represented by *Node A* and *Node X*. Redundancy of coordinator devices represented by *Node B* and *Node Y*. And redundancy in access gateways represented by *Node C* and *Node D*. This configuration is quite atypical. However, it was considered, given the possibility of its implementation and due to the diversity of devices and paths offered.
- **Topology 6** provides innovative features regarding sensing devices that have been incorporated into the topology. The sensing device represented by *Node A* can connect both to the coordinator represented by *Node B* and to an access gateway represented by *Node D*. This represents a new generation of existing wearable devices with short and long-distance communication capabilities.

5.3.2 Centrality and Resilience Metrics

In order to analyze the graph-represented topologies, we calculate various analysis metrics. This assessment relies on extensively studied metrics regarding centrality and resilience in graph-based network topologies (Platt, 2019). This evaluation aims to identify the most relevant nodes within each topology and which topologies are intrinsically more resilient. Given the objectives regarding this evaluation, even though the topologies comprise multiple stages or services, as stated previously, we evaluate the topologies as a single functional network. This initial analysis will support further experiments, following the topologies characterization according to the particularities of the devices and communication technologies in IoHT.

The topologies' design and metric evaluations employ the NetworkX software (Hagberg et al., 2008). The metrics are built into the software and applied to each topology individually. The first evaluation comprises the Density metric. Density is one of the most straightforward measures of resilience and represents a ratio between the number of nodes and the number of links for each topology (Petrenko, 2022). A higher value implies a more dense and connected environment, indicating a more resilient topology. Entropy and Eigenvector Centrality indicate how centralized each topology is. Increased values for these metrics reveal higher dependence in one or a few nodes. The previous metrics are directly associated with the resilience of a network regarding service preservation scenarios (Alenazi and Sterbenz, 2015).

Some additional centrality-related metrics support the resilience evaluation, even though they are not explicitly designed for this purpose. Edge betweenness is an edge centrality metric that provides the shortest path between every pair of nodes that passes over a particular edge. Node betweenness centrality measures the fraction of the number of shortest paths between every two nodes that lie on a particular node (Modarresi and Symons, 2019). Usually, the center of the configuration that represents each topology has the maximum closeness centrality value. Higher values regarding closeness centrality indicate topologies with better chances of disseminating information. Degree centrality in communication networks is a measure of the importance of a node concerning how well-connected it is. Node connectivity indicates the resilience to network segmentation for each topology, showing how many nodes can be removed from the topology before being divided into separate and disconnected parts (Platt, 2019).

The evaluation considering centrality and resilience metrics reflects the simplicity of the topologies. Many of the considerations reached could be accepted by just observing the topologies. However, evaluating the results without assuming the type of communication technology represented in the connections and the importance of each node to the topology can lead to dubious deductions. Figure 5.1 summarizes the results for centrality and resilience metrics. As expected, none of the configurations are particularly prone to communication resilience due to the low number of nodes and communication channels. Density and entropy results corroborate this statement. The values for Eigenvector centrality also indicate that the topologies are highly dependent on a few nodes; this is common for all topologies but particularly for Topology 1, which represents the most traditional configuration for IoHT environments.

Betweenness and Closeness metrics provide essential information regarding the most active and vital nodes on each topology. Based on those metrics, defining the main spots where the induced failures will happen is possible. The complementary Degree centrality and Node connectivity metrics will identify if more connected nodes represent higher data dissemination levels for the topologies. That is especially important since adding nodes to the topologies represents an extra device for the user or adding a communication gateway for the configuration. By employing centrality and resilience metrics results to identify the most vulnerable zones, we will characterize the topologies accordingly to the communication technologies and devices in IoHT and evaluate the topologies through emulated experiments.

Table 5.1: Topologies evaluation regarding centrality and resilience metrics

		Topology					
Metric		1	2	3	4	5	6
Density	overall	0.5	0.5	0.4	0.5	0.4	0.6
Entropy	overall	1.959	2.283	2.524	2.571	2.778	2.299
Eigenvector centrality	min	0.372	0.557	0.602	0.444	0.261	0.529
	mean	0.487	0.437	0.392	0.404	0.371	0.444
	max	0.602	0.261	0.263	0.325	0.465	0.357
Node betweenness	min	0	0	0	0.3	0.25	0
	max	2	3.5	7.5	1.8	3.833	1.5
Edge betweenness	min	3	2.5	5	2.833	3.25	2
	max	4	4	3	2.916	3.583	3
Closeness	min	0.5	0.5	0.5	0.555	0.5	0.666
	max	0.7	0.8	0.833	0.714	0.75	0.8
Degree centrality	max	0.666	0.75	0.8	0.6	0.666	0.75
Node connectivity	average	1	1.6	1.4	2.4	2.333	2.1

5.3.3 Communication Performance Evaluation of IoHT Topologies

As described previously, IoHT has limited configurations considering communication devices and technologies. The communication performance analysis aims to identify the impact of a legitimate failure or an attack on a fundamental point. By inducing threats at a critical point individually while we measure the delay from collecting data from a sensor and delivering it to the cloud, for instance, it is possible to analyze the impacts on communication performance. The experimental evaluation relies on simulations regarding the proposed topologies in IoHT. We simulate data traffic on each topology, any-to-any, mimicking the IoHT network dynamics.

The network simulation is an adaptation based on the ANX Python package proposed by (Likic and Shafi, 2018). It is developed in Python 3, mainly using the SimPy (Matloff, 2008) and NetworkX (Hagberg et al., 2008) libraries for discrete event simulation and definition of the network topology. Network nodes create packets destined for other nodes. Such packets travel from source to destination, employing the shortest paths. The packet generation follows a Poisson process. Nodes have an internal structure and implement packet queue, packet sink, and packet forwarding, among other features. Nodes and links properties at the simulator are summarised in Table 5.2. Nodes are named 'n0', 'n1', 'n2', ... according to the number of nodes on the topology. Links are defined by connecting node types: 'ni-nj', $i, j = 'n0-n1', 'n1-n2, 'n0-n2', \dots$ accordingly to the available links on the topology. Table 5.3 illustrates the values applied regarding the characterization of experiments.

Table 5.2: Elements and properties of the network simulator

Node n_i : definition	Link $n_i - n_j$: definition
$n_i : \{$ node_pkt_rate node_proc_delay node_queue_check node_queue_cutoff $\}$	$n_i - n_j : \{$ link_transm_delay link_capacity $\}$

Each topology has been characterized according to the communication technologies and devices' capabilities. Since this evaluation aims to analyze the impact of threats on communication performance, we propose an assessment based on the premise that communication happens directly among devices, access networks, and the Internet, even though end-to-end communication

Table 5.3: Characterization of experiments

Experiments characterization	
Communication flow	Link speed
Wearable - Gateway	300
Wearable - Gateway 2	300
Gateway - Access network	2000
Gateway - Access network 2	10000
Gateway 2 - Access network	2000
Gateway 2 - Access network 2	10000
Access network - Cloud	1000
Access network 2 - Cloud	5000

comprises multiple network segments. The first experiment aims at building a baseline regarding communication performance in IoHT. In order to create the baseline experiment, each topology has been characterized and evaluated separately.

For the baseline experiment, we employed the default values of the network simulator ANX presented in (Likic and Shafi, 2018). Each network node was assumed to generate network packets as a simple Poisson process events with the average packet rate set to 20/time unit. Each node held a queue of packets with a cut-off value of 128. Any packet arriving while the queue is full is dropped. Each simulation has a runtime of 1000 time units and was repeated 30 times. All nodes send packets at the same rate, the only difference being the link capacities between the nodes. The link capacity for communication between a sensing device and a coordinator is 300 packets/time unit; between a coordinator and an access gateway is 2000 packets/time unit; and between an access gateway and a delivery point on the Internet is 4000 packets/time unit. Given the simulator time unit configuration, those values represent an adaptation regarding short-range and long-range communication.

The baseline evaluation provided the expected results since it comprised a near-perfect environment free of perturbations or threats. All experiments regarding the IoHT topologies occurred with the expected incidence of delay and no packet loss. Figure 5.3 illustrates the results of the experiments. Figure 5.3 (a) and (b) shows the delay for the IoHT topologies. Once there are no threats to the environment, the delay stands stable for all topologies. Topologies 1, 4, and 6 have a marginally inferior delay. However, considering the fraction of the simulation time, all topologies are fit for delay-sensitive applications in perfect network conditions. It is worth mentioning that configurations represented by Topologies 2, 3, and 5 are more resilient than those illustrated by topology 1, as observed in centrality and resilience metrics evaluation. However, the resilience provided by redundant nodes and paths has low benefits regarding the delay and considering the absence of threats.

The next part of the evaluation comprises the insertion of threats at the crucial points of the topologies, represented by an increased workload. The workload increase represents a threat that can induce each critical point to increase the delay when performing its functions. The most relevant nodes represent the sensing device, the coordinator device, and the access gateways, as identified in the centrality and resilience evaluations of the topologies. The experiments comprise four scenarios (*i*) threats on the sensing device, (*ii*) threats on the coordinator device, (*iii*) threats on an access gateway, and (*iv*) threats on an access gateway with recovery. For each scenario, the experiments comprise six workloads on the crucial points, representing any threat that can increase the delay at that specific point with values raised at 0.005-time units per workload.

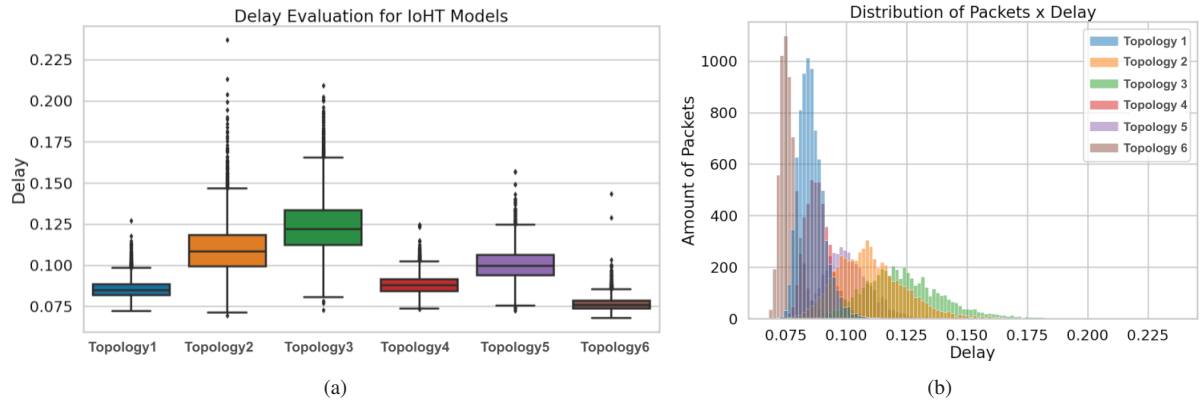


Figure 5.3: Communication performance baseline evaluation

Additionally, we continuously measure the delay regarding the endpoints of each topology (the sensing device and the storage infrastructure on the Internet) and the overall packet loss.

An important concept regarding those experiments is that most threats on IoHT environments can harm communication performance, as seen in Section 2.2.3. These experiments aim to identify how a delay-inducing threat on a crucial IoHT point impacts end-to-end communication regarding communication delay and packet loss. For the experiments, we assume that nodes connected through multiple links are capable of using redundant paths. We also assume that the nodes on each topology are unaware of the increased workload on the crucial points. The additional configurations, such as the transmitting rate of the nodes, the queue values, and the processing delay, are the same employed in the baseline experiments.

The first scenario focuses on threats affecting the sensing device, such as a smartwatch or a fitness tracker. Figure 5.4 (a) shows the results regarding the IoHT topologies when the sensing device is under a menace that affects communication performance, represented by the increasing workloads. Once the sensing device is on the extreme edge of the described configuration, the threats have a low impact on the other areas of the topology and, consequently, low interference with the overall delay. Most of the added end-to-end delay originates from the induced workload values themselves. Similarly, packet loss values are low, representing a 2% loss in the worst case. Figure 5.4 (b) illustrates the percentage of delivered packets for each topology and workload.

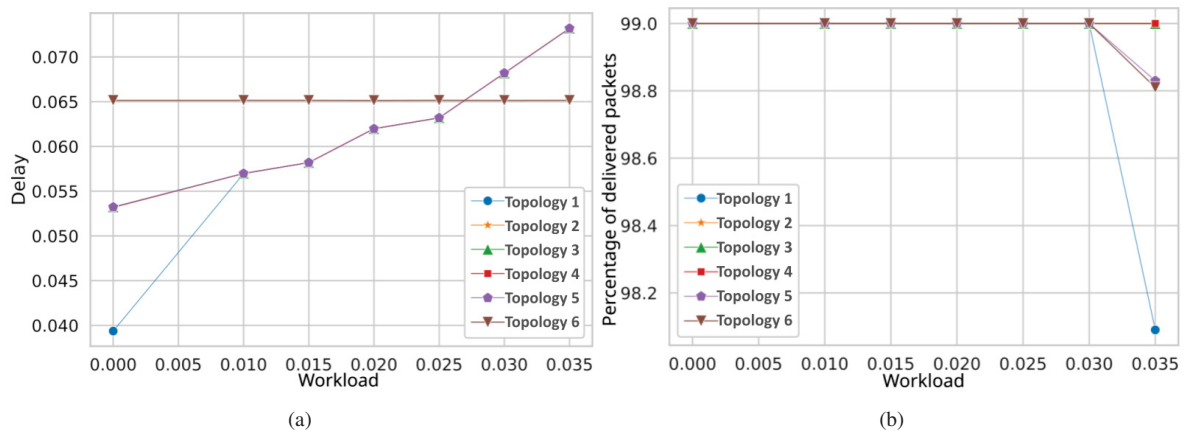


Figure 5.4: Communication evaluation - threats regarding the sensing device

The second scenario introduces threats on the coordinator device of an IoHT environment. The coordinator device is crucial for IoHT communication configurations since it plays the role of a portable gateway connecting the sensing devices and the Internet. The coordinator device is

also the most centralized on IoHT configurations, offering access to sensing and connectivity services. Figure 5.5 (a) illustrates the topologies performance in terms of delay considering different workloads on the coordinator device. The delay increases dramatically for the topologies, exception made of Topology 6, which represents a configuration that employs sensing devices with short and long communication technologies. Currently, this type of configuration is not very common; however, it is one of the most probable combinations for future devices. Figure 5.5 (b) shows the results of the packet delivery experiment. Packet drop is also an issue when the workload increases, ranging from 20% to 50% approximately. The linear Topology 1 still offers better performance in terms of packet drop than more resilient topologies. The reason is that more resilient topologies comprise more nodes transferring data, saturating the coordinator device, and increasing the chances of losing packets, given the workload growth.

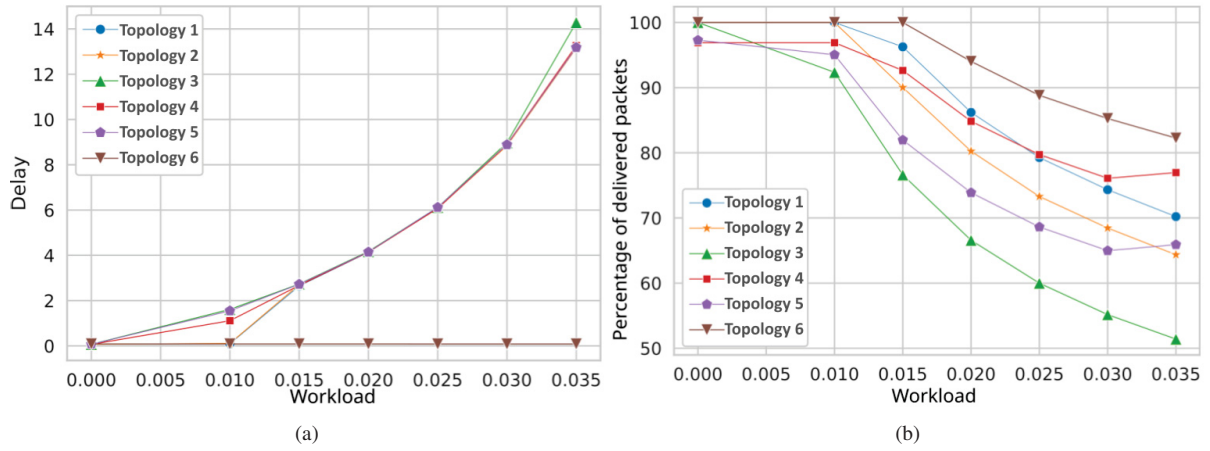


Figure 5.5: Communication evaluation - threats regarding the coordinator device

The third scenario comprises threats on an access network. Increasing the workload on the access network causes a growth in delay considering all evaluated topologies, as shown in Figure 5.6 (a). However, the topology components are unaware of a threat afflicting the access network and maintain an unaltered behavior in terms of packet exchange. Figure 5.6 (b) shows the percentage of received packets considering the increased workload on an access network. The packed delivery exceeds 80%, except for Topology 1, which includes only one access network.

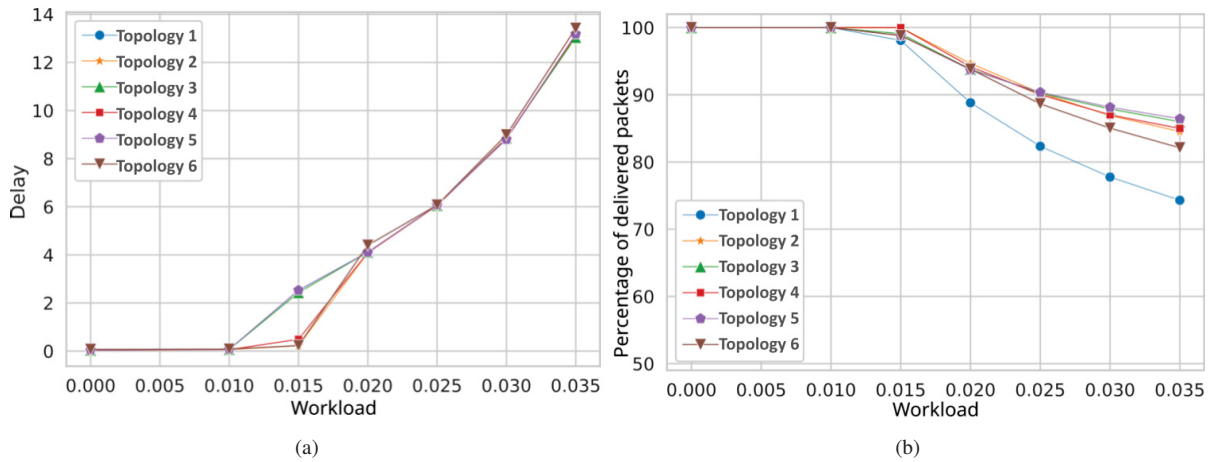


Figure 5.6: Communication evaluation - threats regarding the access gateway

The last scenario represents a situation where the participant nodes become aware of a problem regarding an access network. This experiment infers the possible gains in terms of

network performance in providing redundant configurations for communication regarding access networks. Noticeably the topologies with access network redundancy perform better than the linear one, except for Topology 6, as shown in Figure 5.7 (a). Even though Topology 6 initially provides redundant paths for access networks, it becomes a linear topology once the access network becomes unavailable, making its results pair with Topology 1. Figure 5.7 (b) illustrates the percentage of received packets regarding the experiment.

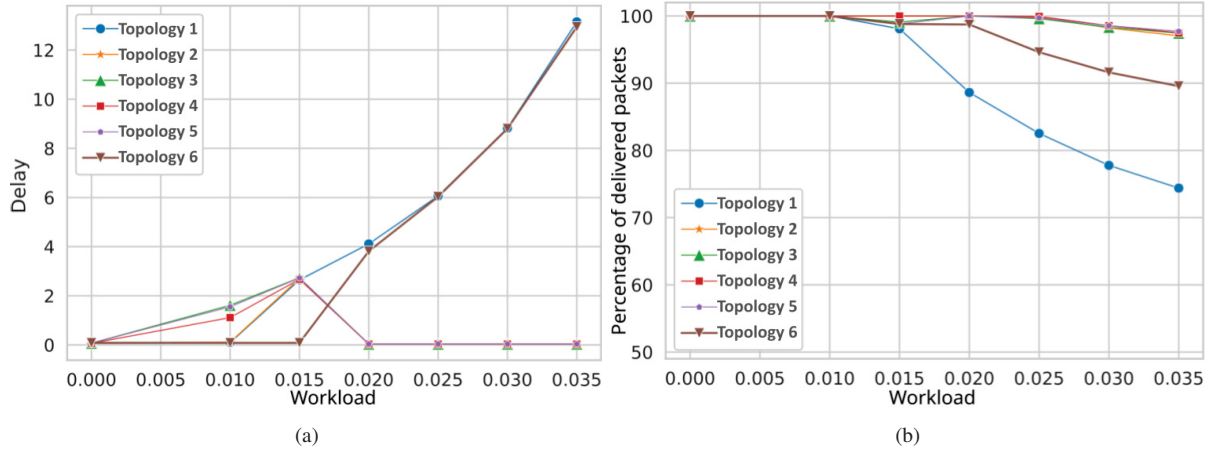


Figure 5.7: Communication evaluation - access gateway recovery

5.3.4 Discussion

Communication resilience in computational systems is a frequently debated topic. However, new communication technologies offer different environmental configuration possibilities, especially considering IoT-based systems. Formerly, communication resilience relied mainly on the redundancy of devices and communication channels. However, this is not always possible in IoHT. Furthermore, adding a small assortment of components does not significantly affect resiliency in these environments. Some significant issues surfaced during the experiments regarding the evaluations on IoHT communication resilience. The following paragraphs provide a discussion regarding those issues.

The first topic of discussion is the devices' capabilities to use the provided communication paths. As seen in Chapter 3, currently, there are a few protocols capable of adding multipath capabilities to IoHT devices. Theoretically, even less capable devices in terms of processing and memory can benefit from those protocols. However, there are some issues regarding protocol deployment and energy efficiency. Therefore, efforts are needed to ensure that the devices supporting the essential IoHT services can benefit from communication redundancy. In the experiments conducted, the communication performance degradation considering delay and packet loss was small for low workloads, indicating that the performance is acceptable in the absence of problems or when facing minor disturbances.

Another discussion topic is the simulation limitations. Translating all the communication technologies and device particularities into the simulations is challenging. Modeling the access networks and the Internet regarding the uncontrollable variables is particularly demanding. We have chosen abstract topologies to evaluate the impact of threats on communication performance; however, many granularities regarding communication details are missing in that approach. Still, regarding the experiments, it is possible to identify the most vulnerable points of an IoHT infrastructure and how threats aiming at those points impact communication performance. Experiments on an entire physical infrastructure could offer a more comprehensive view. However,

the end-to-end communication services in IoHT comprise multiple segmented topologies, making it difficult to monitor and manage the whole environment.

Regarding adaptation, the existing IoHT environment can encompass adaptive management solutions. However, adaption should consider interconnected points that can efficiently manage the existing redundant assets. If the uncertainties arising from threats are beyond the possibility of control, when they target a point on the Internet, for example, they should be overlooked for adaptive management. The coordinator device is currently the most noticeable management point for the existing IoHT configurations. However, as sensing devices become more capable regarding processing, memory, and assortment in communication technologies, the edge devices in IoHT might grow in importance and perform management tasks themselves. Additionally, including communication technologies in a device or adding devices to an existing configuration is a simplistic adaptation. Nevertheless, given the limited manageable devices in IoHT environments, more sophisticated techniques, such as self-adaptation, become unfeasible.

5.4 CHAPTER SUMMARY

This chapter introduced a resilience analysis approach for IoHT. The purpose of the analysis is to evaluate how resilient the IoHT communication configurations are, its most vulnerable points, and the impact of threats upon those weak points in terms of communication performance. This chapter provides a background on works that evaluate communication resilience in IoT-based configurations and the main security threats in those environments. This chapter also analyzes the possible IoHT communication configurations and comprehensively evaluates the topologies based on the configurations. Finally, this chapter proposes a discussion on communication resilience in IoHT considering the proposed experiments and presents the open issues concerning assessing communication resilience and IoHT-based configurations.

6 CONCLUSIONS

This chapter synthesizes the thesis conclusions, presents the open research issues, and offers future directions. The objective is to reinforce the contributions achieved and present directions that contribute to proceeding with the research. Hence, we will present the main contributions of this thesis in Section 6.1. Next, in Section 6.2, we summarize the limitations and future directions for continuing the research on adaptive management to increase communication resilience in IoT environments. Finally, in Section 6.3, we present the list of publications resulting from this thesis.

6.1 MAIN CONTRIBUTIONS

The complex characteristics of the IoHT environment have supported the development of new and crucial applications for smart health. At the same time, those characteristics make communication resilience challenging to achieve. This work presents a new approach for increasing the communication resilience of IoHT environments employing adaptive management. The main goal consists of enhancing overall resilience and security regarding IoHT communication while preserving the minimal required network performance. Our approach is inspired by adaptive management principles initially proposed for resource managers to integrate scientific understanding with managing natural resources. Adaptive management integrates scientific understanding, resolving and managing inherent uncertainties, and questioning assumptions, boundaries, and policies. Additionally, possible adjustments recognize that managed resources will always change, that surprises are inevitable, and that uncertainties will emerge. Our contributions tackle the main problems regarding IoHT communication, such as the communication requirements regarding communication performance and health-related applications, the security and performance tradeoff, and the feasibility of integrating adaptive management into the current IoHT topologies.

We explored the feasibility of adaptive management considering three fundamental elements regarding communication resilience in IoHT (*i*) security, (*ii*) performance, and (*iii*) adaptation. Figure 6.1 illustrates the elements and their major topics.

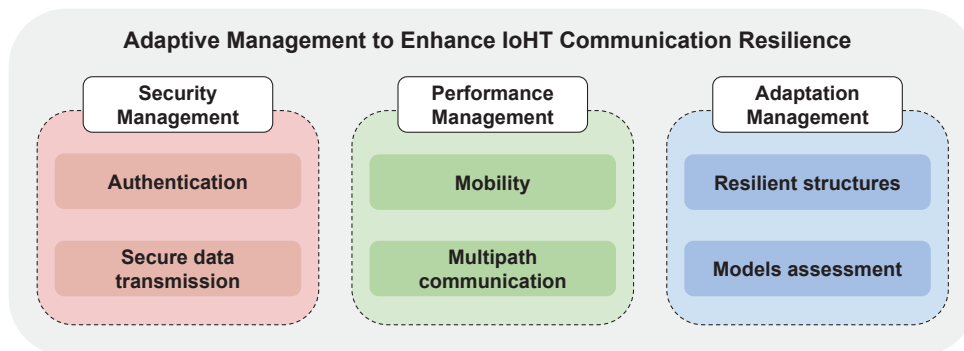


Figure 6.1: Main contributions

Considering security management, we proposed a continuous biometric authentication mechanism for IoHT employing a secure data transmission communication channel. In order to develop the mechanism, we researched the literature to identify the state-of-the-art regarding using biosignals to promote continuous authentication. The state-of-the-art survey allowed identifying a type of biosignal (PPG) rarely employed in continuous authentication mechanisms. In addition to the authentication mechanism, the evaluation comprised secure data transmission. We employed

an intrabody wireless communication channel using galvanic coupling technology. In complement to being secure, the additional channel promotes communication redundancy, if necessary. The evaluation of the mechanism showed that using a biosignal to identify a user is achievable and that it is possible to transmit authentication data through a secure communication channel using galvanic coupling communication. Assessments related to the security management element answer the second research question about which security approaches fit adaptive management and how they affect the balance of resiliency and performance. Regarding the compromise between resilience and performance, the main concern is that authentication delays sending data, no matter how efficient the mechanism is. Consequently, there is an explicit tradeoff between security level and communication performance in IoHT, especially regarding delay.

Regarding the performance management element, we proposed a resilience management architecture to increase user mobility and enhance communication performance. Two works compose the performance management element. The works following the performance management element answer the first research question: How do techniques that improve communication performance incorporate adaptive management to increase resilience? Regarding the works, we have promoted a novel concept of a portable living system that manages multiple communication technologies. First, we researched and classified works in the literature using multipath protocols to improve resilience and mobility for IoHT communication. Next, we proposed a resilience management architecture for communication in portable assisted living. The architecture is structured in congruence with the communication technologies, devices, and applications in IoHT. It employs multipath protocols in a portable coordinator device, promoting the mobility of a user within the coverage area of the communication technologies involved. Additionally, managing multipath protocols add resilience to communication failures and enhances communication performance for IoHT applications. The results concerning both experiments reveal benefits for communication performance and user mobility. The proposed architecture promotes low communication delay and steady data transfer rates in multiple scenarios with and without communication failures.

The adaptation management element comprises research and evaluations on IoHT communication configurations and their resilience to threats. This element contributes to identifying the main threats on IoHT environments, establishing the most crucial and vulnerable points on IoHT communication configurations, and evaluating those configurations when facing threats. Initially, we have identified and categorized the main threats to communication in IoHT environments. Then, we proposed a novel approach to IoHT resilience analysis by identifying the possible communication configurations for IoHT and modeling them into graph-based models. The graph evaluations encompass centrality and resilience metrics and contribute to identifying the most important nodes and paths for IoHT communication configurations. Later, we characterized the models mimicking the real-life IoHT network configurations and dynamics. We evaluated the models using simulations, which allowed us to identify the most resilient IoHT configurations and the impact of threats on the crucial communication points in terms of delay and packet loss. Adaptation is challenging in IoHT since a device linked to an essential service has few management options over devices linked to a different essential service. However, we evaluated a scenario assuming adaptive actions, which showed managed delay and packet loss results for most models. The research and experiments for this element tackle the third research question, which inquires if the current IoHT environment regarding communication can deal with the proposed adaptive management solutions.

6.2 LIMITATIONS AND FUTURE WORK

Some limitations can be identified in the current state of the research. Adaptive management is a promising approach to address communication issues in IoHT toward a more resilient environment. This work offers an initial approach for applying some of the existing concepts in adaptive management and verifies that its deployment is possible and brings several benefits. However, a more structured approach is required to provide consistent deployment over multiple scenarios. A possible strategy would be to structure adaptive management as a set of guidelines for implementation in IoT-based systems. One of the problems with this approach would be the different applications and characteristics of the systems regarding communication technologies and devices. Another direction would be developing a structured implementation guideline specifically for IoHT.

Regarding experimentation on IoHT environments, the main limitation is modeling the environment while maintaining all its specific communication technologies and device characteristics. It is possible to model and characterize each essential service separately through simulations. However, connecting the essential services to provide a comprehensive view is challenging. Real-life experiments are also complex once it is difficult to identify the specific segments causing delay and packet loss. Experiments regarding security, such as the authentication of devices, follow the same principle. It is possible to measure the delay for a specific type of authentication, but it is difficult to measure the impact of the delay considering the entire IoHT environment. Finally, IoHT devices constantly evolve, encompassing multiple communication technologies and additional processing power. New features highly impact communication resilience in IoHT since they enable unexplored communication configurations and the inclusion of communication protocols.

6.3 PUBLICATIONS

This section presents the list of publications resulted from this thesis.

- Nakayama, F., Lenz, P., Cremonezi, B., Banou, S., Rosário, D., Chowdhoury, K., Santos, A. (2019). **Autenticação contínua e segura baseada em sinais ppg e comunicação galvânica**. Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (pp. 707-720). SBC.
- Nakayama, F., Lenz, P., Banou, S., Nogueira, M., Santos, A., Chowdhury, K. R. (2019). **A continuous user authentication system based on galvanic coupling communication for s-health**. Wireless Communications and Mobile Computing, p. 1-11, 2019.
- Nakayama, F., Lenz, P., LeFloch, A., Beylot, A. L., Santos, A., Nogueira, M. (2021). **Performance management on multiple communication paths for portable assisted living**. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 340-348). IEEE.
- Nogueira, M., Borges, L. F., Nakayama, F. (2021). **Das Redes Vestíveis aos Sistemas Ciber-Humanos: Uma Perspectiva na Comunicação e Privacidade dos Dados**. Sociedade Brasileira de Computação.
- Nakayama, F., Lenz, P., Nogueira, M. (2022). **A resilience management architecture for communication on portable assisted living**. IEEE Transactions on Network and Service Management, 19(3), 2536-2548.

- Ribeiro, A. V., Nakayama, F., Nogueira, M., Sampaio, L. N. (2023). **Um Panorama dos Serviços de Saúde Avançados: Conectividade e Segurança em Sistemas de Vida Assistida**. Sociedade Brasileira de Computação.

The following manuscript is in preparation for submission.

- Nakayama, F. , Nogueira, M. **A Resilience Analysis Approach for IoHT**. Manuscript in preparation to be submitted for a journal, 2024.
- Nakayama, F. , França, T. N. , Nogueira, M. **A Low-overhead AML-based Obfuscation Method Against Traffic Classification Models**. Manuscript in preparation to be submitted for the IEEE Communications Letters Journal, 2024.

REFERENCES

- Abdellatif, A. A., Mohamed, A., Chiasserini, C. F., Tlili, M., and Erbad, A. (2019). Edge computing for smart health: Context-aware approaches, opportunities, and challenges. *IEEE Network*, 33(3):196–203.
- Abdelwahed, S., Bai, J., Su, R., and Kandasamy, N. (2009). On the application of predictive control techniques for adaptive performance management of computing systems. *IEEE Transactions on Network and Service Management*, 6(4):212–225.
- Abtoy, A., Touhafi, A., Tahiri, A., et al. (2020). Ambient assisted living system’s models and architectures: A survey of the state of the art. *Journal of King Saud University-Computer and Information Sciences*, 32(1):1–10.
- Aceto, G., Persico, V., and Pescapé, A. (2018). The role of information and communication technologies in healthcare: taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications*, 107:125–154.
- Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28.
- Alenazi, M. J. and Sterbenz, J. P. (2015). Comprehensive comparison and accuracy of graph metrics in predicting network resilience. In *2015 11th international conference on the design of reliable communication networks (DRCN)*, pages 157–164. IEEE.
- Alhaj, T. A., Abdulla, S. M., Iderss, M. A. E., Ali, A. A. A., Elhaj, F. A., Remli, M. A., and Gabralla, L. A. (2022). A survey: To govern, protect, and detect security principles on internet of medical things (iomt). *IEEE Access*, 10:124777–124791.
- Ali, S., Hafeez, Y., Jhanjhi, N., Humayun, M., Imran, M., Nayyar, A., Singh, S., and Ra, I.-H. (2020). Towards pattern-based change verification framework for cloud-enabled healthcare component-based. *IEEE Access*, 8:148007–148020.
- Allen, C. R., Fontaine, J. J., Pope, K. L., and Garmestani, A. S. (2011). Adaptive management for a turbulent future. *Journal of environmental management*, 92(5):1339–1345.
- Alquaydheb, I. N., Khorshid, A. E., and Eltawil, A. M. (2019). Analysis and estimation of intra-body communications path loss for galvanic coupling. In *Advances in Body Area Networks I*, pages 267–277. Springer.
- Althoubi, A., Alshahrani, R., and Peyravi, H. (2021). Delay analysis in iot sensor networks. *Sensors*, 21(11):3876.
- Angelucci, A., Kuller, D., and Aliverti, A. (2020). A home telemedicine system for continuous respiratory monitoring. *IEEE Journal of Biomedical and Health Informatics*, 25(4):1247–1256.
- Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

- Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33.
- Azghiou, K., El Mouhib, M., Koulali, M.-A., and Benali, A. (2020). An end-to-end reliability framework of the internet of things. *Sensors*, 20(9):2439.
- Azimi, I., Anzanpour, A., Rahmani, A. M., Pahikkala, T., Levorato, M., Liljeberg, P., and Dutt, N. (2017). Hich: Hierarchical fog-assisted computing architecture for healthcare iot. *ACM Transactions on Embedded Computing Systems*, 16(5s):1–20.
- Belgacem, N., Fournier, R., Nait-Ali, A., and Bereksi-Reguig, F. (2015). A novel biometric authentication approach using ECG and EMG signals. *Journal of Medical Engineering & Technology*, 39(4):226–238.
- Ben Arbia, D., Alam, M. M., Kadri, A., Ben Hamida, E., and Attia, R. (2017). Enhanced iot-based end-to-end emergency and disaster relief system. *Journal of Sensor and Actuator Networks*, 6(3):19.
- Benkhelifa, E., Welsh, T., and Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for IoT : Toward universal and resilient systems. *IEEE Communications Surveys & Tutorials*, 20(4):3496–3509.
- Blasco, J., Chen, T. M., Patil, H. K., and Wolff, D. (2019). Wearables security and privacy. In *Mission-Oriented Sensor Networks and Systems: Art and Science*, pages 351–380. Springer.
- Blasco, J. and Peris-Lopez, P. (2018). On the feasibility of low-cost wearable sensors for multi-modal biometric verification. *Sensors*, 18(9):2782–2802.
- Butun, I., Morgera, S. D., and Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1):266–282.
- Camara, C., Peris-Lopez, P., Tapiador, J. E., and Suarez-Tangil, G. (2015). Non-invasive multi-modal human identification system combining ecg, gsr, and airflow biosignals. *Journal of Medical and Biological Engineering*, 35(6):735–748.
- Cao, S., Zhang, G., Liu, P., Zhang, X., and Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences*, 485:427–440.
- Celebucki, D., Lin, M. A., and Graham, S. (2018). A security evaluation of popular internet of things protocols for manufacturers. In *International Conference on Consumer Electronics (ICCE)*, pages 1–6. IEEE.
- Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):1–58.
- Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., and Lee, Y. (2017). Breathprint: Breathing acoustics-based user authentication. In *International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 278–291. ACM.
- Chavez, E., Sifuentes, B., Vidal, R., Grados, J., Rubiños, S., and Cuzcano, A. (2020). Remote monitoring applying iot to improve control of medication adherence in geriatric patients with a complex treatment regimen, lima-peru. In *Proceedings of the 2020 3rd International Conference on Electronics and Electrical Engineering Technology*, pages 49–54.

- Cicioğlu, M. and Çalhan, A. (2019). Performance analysis of iee 802.15. 6 for underground disaster cases. *Computer Standards & Interfaces*, 66:364–374.
- Cipriano, M., Costagliola, G., De Rosa, M., Fuccella, V., and Shevchenko, S. (2021). Recent advancements on smartwatches and smartbands in healthcare. In *Innovation in Medicine and Healthcare*, pages 117–127. Springer.
- Cisotto, G., Casarin, E., and Tomasin, S. (2020). Requirements and enablers of advanced healthcare services over future cellular systems. *IEEE Communications Magazine*, 58(3):76–81.
- Classen, J., Wegemer, D., Patras, P., Spink, T., and Hollick, M. (2018). Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(1):5.
- Coelho, K., Damião, D., Noubir, G., Borges, A., Nogueira, M., and Nacif, J. (2019). Cryptographic algorithms in wearable communications: An empirical analysis. *IEEE Communications Letters*, 23(11):1931–1934.
- Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., and Linkov, I. (2017). Features of resilience. *Environment systems and decisions*, 37:46–50.
- Cui, P., Zhu, P., Wang, K., Xun, P., and Xia, Z. (2018). Enhancing robustness of interdependent network by adding connectivity and dependence links. *Physica A: Statistical Mechanics and its Applications*, 497:185–197.
- CynergisTek, R. (2017). Breach report 2016: Protected health information (phi).
- Dar, B. K., Shah, M. A., Islam, S. U., Maple, C., Mussadiq, S., and Khan, S. (2019). Delay-aware accident detection and response system using fog computing. *Ieee Access*, 7:70975–70985.
- De Coninck, Q. and Bonaventure, O. (2017). Multipath quic: Design and evaluation. In *International Conference on Emerging Networking EXperiments and Technologies, CoNEXT '17*, page 160–166. ACM.
- De Coninck, Q. and Bonaventure, O. (2019). Multipathtester: Comparing mptcp and mpquic in mobile environments. In *Network Traffic Measurement and Analysis Conference (TMA)*, pages 221–226. IEEE.
- De Lemos, R., Giese, H., Müller, H. A., Shaw, M., Andersson, J., Litoiu, M., Schmerl, B., Tamura, G., Villegas, N. M., Vogel, T., et al. (2013). Software engineering for self-adaptive systems: A second research roadmap. In *Software Engineering for Self-Adaptive Systems II*, pages 1–32. Springer.
- Deebak, B. D. and Al-Turjman, F. (2020). Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications*, 39(2):346–360.
- Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on software engineering*, SE-13(2):222–232.
- Dong, P., Ning, Z., Obaidat, M. S., Jiang, X., Guo, Y., Hu, X., Hu, B., and Sadoun, B. (2020). Edge computing based healthcare systems: Enabling decentralized health monitoring in internet of medical things. *IEEE Network*, 34(5):254–261.

- Ekiz, D., Can, Y. S., Dardagan, Y. C., and Ersoy, C. (2020). Can a smartband be used for continuous implicit authentication in real life. *IEEE Access*, 8:59402–59411.
- Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Longstaff, T., and Mead, N. R. (1997). Survivable network systems: An emerging discipline. Technical report, Carnegie Mellon University. Software Engineering Institute (SEI), Pittsburgh, PA (United States).
- Elsts, A., Fafoutis, X., Woznowski, P., Tonkin, E., Oikonomou, G., Piechocki, R., and Craddock, I. (2018). Enabling healthcare in smart homes: The sphere iot network infrastructure. *IEEE Communications Magazine*, 56(12):164–170.
- Enamamu, T. S., Clarke, N., Haskell-Dowland, P., and Li, F. (2017). Smart watch based body-temperature authentication. In *International Conference on Computing Networking and Informatics (ICCNI)*, pages 1–7. IEEE.
- Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37.
- Falcone, Y., Mounier, L., Fernandez, J.-C., and Richier, J.-L. (2011). Runtime enforcement monitors: composition, synthesis, and enforcement abilities. *Formal Methods in System Design*, 38(3):223–262.
- FBI (2015 (Accessed January 10, 2020)). *Internet of Things Poses Opportunities for Cyber Crime*.
- FDA (2018). Digital health innovation action plan. Technical report, U.S. Department of Health and Human Services Food and Drug Administration. Accessed: Jul/2019.
- Ford, A., Raiciu, C., Handley, M. J., and Bonaventure, O. (2013). TCP Extensions for Multipath Operation with Multiple Addresses. RFC 6824.
- Fu, X. and Yang, Y. (2021). Modeling and analyzing cascading failures for internet of things. *Information Sciences*, 545:753–770.
- Gaddam, A., Wilkin, T., Angelova, M., and Gaddam, J. (2020). Detecting sensor faults, anomalies and outliers in the internet of things: A survey on the challenges and solutions. *Electronics*, 9(3):511.
- Ghosh, S., Mukherjee, A., Ghosh, S. K., and Buyya, R. (2019). Mobi-iost: mobility-aware cloud-fog-edge-iot collaborative framework for time-critical applications. *IEEE Transactions on Network Science and Engineering*, 7(4):2271–2285.
- Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., and Zorzi, M. (2020). Toward 6g networks: Use cases and technologies. *IEEE Communications Magazine*, 58(3):55–61.
- Gmach, D., Krompass, S., Scholz, A., Wimmer, M., and Kemper, A. (2008). Adaptive quality of service management for enterprise services. *ACM Transactions on the Web (TWEB)*, 2(1):1–46.
- Goldberger, A. L., Amaral, L. A. N., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., and Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation*, 101(23):215–220.

- Gomes, B., Muniz, L., e Silva, F. J. d. S., Ríos, L. E. T., and Endler, M. (2015). A comprehensive cloud-based iot software infrastructure for ambient assisted living. In *International Conference on Cloud Technologies and Applications (CloudTech)*, pages 1–8. IEEE.
- Gu, Y., Zhang, Y., and Zhang, Y. (2003). A novel biometric approach in human verification by photoplethysmographic signals. In *International Special Topic Conference on Information Technology Applications in Biomedicine (EMBS)*, pages 13–14. IEEE.
- Gunderson, L. (2015). Lessons from adaptive management: obstacles and outcomes. *Adaptive management of social-ecological systems*, pages 27–38.
- Gupta, S., Buriro, A., and Crispo, B. (2018). Demystifying authentication concepts in smartphones: Ways and types to secure access. *Hindawi - Mobile Information Systems*, 2018:1–16.
- Hady, A. A., Ghubaish, A., Salman, T., Unal, D., and Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, 8:106576–106584.
- Hagberg, A., Swart, P., and S Chult, D. (2008). Exploring network structure, dynamics, and function using networkx. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States).
- Handigol, N., Heller, B., Jeyakumar, V., Lantz, B., and McKeown, N. (2012). Reproducible network experiments using container-based emulation. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, pages 253–264.
- Hassen, H. B., Ayari, N., and Hamdi, B. (2020). A home hospitalization system based on the internet of things, fog computing and cloud computing. *Informatics in Medicine Unlocked*, 20:100368.
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on iot security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743.
- Hemminger, S. et al. (2005). Network emulation with netem. In *Linux conf au*, pages 18–23.
- Holling, C. (1978). Adaptive environmental assessment and management.
- Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems*, 4:390–405.
- Holling, C. S. and Meffe, G. K. (1996). Command and control and the pathology of natural resource management. *Conservation biology*, 10(2):328–337.
- Hsu, C.-H. and Kremer, U. (1998). Iperf: A framework for automatic construction of performance prediction models. In *Workshop on Profile and Feedback-Directed Compilation, Paris, France*. Citeseer.
- IBM (2023 (Accessed December 11, 2023)). *Cost of a Data Breach Report*.
- Isa, I. S. M., Musa, M. O., El-Gorashi, T. E., and Elmirghani, J. M. (2019). Energy efficient and resilient infrastructure for fog computing health monitoring applications. In *International Conference on Transparent Optical Networks*, pages 1–5. IEEE.

- Islam, J., Kumar, T., Kovacevic, I., and Harjula, E. (2021). Resource-aware dynamic service deployment for local iot edge computing: Healthcare use case. *IEEE Access*, 9:115868–115884.
- Isravel, D. P., Silas, S., and Rajsingh, E. B. (2020). Sdn-based traffic management for personalized ambient assisted living healthcare system. In *Intelligence in Big Data Technologies—Beyond the Hype*, pages 379–388. Springer.
- Isravel, D. P., Silas, S., and Rajsingh, E. B. (2021). Sdn-based traffic management for personalized ambient assisted living healthcare system. In *Intelligence in Big Data Technologies—Beyond the Hype*, pages 379–388. Springer.
- Ito, K. (2018). Performance evaluation and improvement of PER and throughput in galvanic-coupling intra-body communication systems. In *International Conference of Engineering in Medicine and Biology Conference (EMBC)*, pages 3742–3745. IEEE.
- Jeong, Y.-S., Kim, H.-W., and Park, J. H. (2014). Visual scheme monitoring of sensors for fault tolerance on wireless body area networks with cloud service infrastructure. *International Journal of Distributed Sensor Networks*, 10(4):1–7.
- Jung, J., Krishnamurthy, B., and Rabinovich, M. (2002). Flash crowds and denial of service attacks: Characterization and implications for cdns and web sites. In *Proceedings of the 11th international conference on World Wide Web*, pages 293–304.
- Junior, F. M. R. and Kamienski, C. A. (2021). A survey on trustworthiness for the internet of things. *IEEE Access*, 9:42493–42514.
- Kamišalić, A., Fister, I., Turkanović, M., and Karakatič, S. (2018). Sensors and functionalities of non-invasive wrist-wearable devices: A review. *Sensors*, 18(6):1714.
- Kay, M., Santos, J., and Takane, M. (2011). mhealth: New horizons for health through mobile technologies. *World Health Organization*, 64(7):66–71.
- Kephart, J. O. (2005). Research challenges of autonomic computing. In *Proceedings of the 27th international conference on Software engineering*, pages 15–22.
- Khan, J. Y. and Yuce, M. R. (2010). Wireless body area network (WBAN) for medical applications. In Campolo, D., editor, *New Developments in Biomedical Engineering*, chapter 31. IntechOpen, Rijeka.
- Knight, J. C. (2002). Safety critical systems: challenges and directions. In *International conference on software engineering*, pages 547–550.
- Kounev, S., Lewis, P., Bellman, K. L., Bencomo, N., Camara, J., Diaconescu, A., Esterle, L., Geihs, K., Giese, H., Götz, S., et al. (2017). The notion of self-aware computing. In *Self-Aware Computing Systems*, pages 3–16. Springer.
- Kumar, G. S., Akshara, B., Dhivya, M., Anubama, S., and Kanimozhi, B. (2019). Intra-body communications in biomedical applications. *Engineering Reports*, 2(1):103–107.
- Laine, T. H., Lee, C., and Suk, H. (2014). Mobile gateway for ubiquitous health care system using zigbee and bluetooth. In *IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pages 139–145. IEEE.

- Laprie, J.-C. (2008). From dependability to resilience. In *IEEE/IFIP Int. Conf. On Dependable Systems and Networks*, pages 1–2.
- Leucker, M. and Schallhart, C. (2009). A brief account of runtime verification. *The Journal of Logic and Algebraic Programming*, 78(5):293–303.
- Likic, V. and Shafi, K. (2018). Battlespace mobile/ad hoc communication networks: Performance, vulnerability and resilience. In *Data and Decision Sciences in Action: Proceedings of the Australian Society for Operations Research Conference 2016*, pages 303–314. Springer.
- Lin, F., Song, C., Zhuang, Y., Xu, W., Li, C., and Ren, K. (2017). Cardiac scan: A non-contact and continuous heart-based user authentication system. In *International Conference on Mobile Computing and Networking (MobiCom)*, pages 315–328, New York, NY, USA. ACM.
- Liu, J., Shen, H., Chi, H., Narman, H. S., Yang, Y., Cheng, L., and Chung, W. (2021). A low-cost multi-failure resilient replication scheme for high-data availability in cloud storage. *IEEE/ACM Transactions on Networking*, 29(4):1436–1451.
- Lonzetta, A., Cope, P., Campbell, J., Mohd, B., and Hayajneh, T. (2018). Security vulnerabilities in bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks*, 7(3):28–56.
- Marques, G., Pires, I. M., Miranda, N., and Pitarma, R. (2019). Air quality monitoring using assistive robots for ambient assisted living and enhanced living environments through internet of things. *Electronics*, 8(12):1375.
- Matloff, N. (2008). Introduction to discrete-event simulation and the simpy language. Davis, CA. Dept of Computer Science. University of California at Davis. Retrieved on August, 2(2009):1–33.
- McFadden, J. E., Hiller, T. L., and Tyre, A. J. (2011). Evaluating the efficacy of adaptive management approaches: is there a formula for success? *Journal of environmental management*, 92(5):1354–1359.
- McTear, M. F. (1993). User modelling for adaptive computer systems: a survey of recent developments. *Artificial intelligence review*, 7:157–184.
- Mendez, D. M., Papapanagiotou, I., and Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*.
- Modarresi, A. and Symons, J. (2019). Modeling and graph analysis for enhancing resilience in smart homes. *Procedia Computer Science*, 160:197–205.
- Mogensen, R. S., Markmoller, C., Madsen, T. K., Kolding, T., Pocovi, G., and Lauridsen, M. (2019). Selective redundant mp-quick for 5g mission critical wireless applications. In *IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–5. IEEE.
- Mosenia, A., Sur-Kolay, S., Raghunathan, A., and Jha, N. K. (2017). Caba: Continuous authentication based on bioaura. *IEEE Transactions on Computers*, 66(5):759–772.
- Muccini, H., Spalazzese, R., Moghaddam, M. T., and Sharaf, M. (2018). Self-adaptive iot architectures: An emergency handling case study. In *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*, pages 1–6.

- Nakayama, F., Lenz, P., Banou, S., Nogueira, M., Santos, A., and Chowdhury, K. R. (2019). A continuous user authentication system based on galvanic coupling communication for s-health. *Wirel. Commun. Mob. Comput.*, 2019:9361017:1–9361017:11.
- Nakayama, F., Lenz, P., LeFloch, A., Beylot, A.-L., Santos, A., and Nogueira, M. (2021). Performance management on multiple communication paths for portable assisted living. In *International Symposium on Integrated Network Management (IM)*, pages 340–348. IEEE.
- Nakayama, F., Lenz, P., and Nogueira, M. (2022). A resilience management architecture for communication on portable assisted living. *IEEE Transactions on Network and Service Management*, pages 1–1.
- Nikoloudakis, Y., Panagiotakis, S., Markakis, E., Pallis, E., Mastorakis, G., Mavromoustakis, C. X., and Dobre, C. (2016). A fog-based emergency system for smart enhanced living environments. *IEEE Cloud Computing*, 3(6):54–62.
- OECD (2019). *Health at a Glance*. OECD Publishing.
- Onesimu, J. A., Karthikeyan, J., Eunice, J., Pomplun, M., and Dang, H. (2022). Privacy preserving attribute-focused anonymization scheme for healthcare data publishing. *IEEE Access*, 10:86979–86997.
- Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., and Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (iomt). *Transactions on Emerging Telecommunications Technologies*, 33(6):e4049.
- Papp, Z. and Exarchakos, G. (2016). *Runtime Reconfiguration in Networked Embedded Systems: Design and Testing Practices*. Springer.
- Park, S.-T., Li, G., and Hong, J.-C. (2020). A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. *Journal of Ambient Intelligence and Humanized Computing*, 11(4):1405–1412.
- Paulos, A., Dasgupta, S., Beal, J., Mo, Y., Hoang, K., Bryan, L. J., Pal, P., Schantz, R., Schewe, J., Sitaraman, R., et al. (2019). A framework for self-adaptive dispersal of computing services. In *2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, pages 98–103. IEEE.
- Peng, G., Zhou, G., Nguyen, D. T., Qi, X., Yang, Q., and Wang, S. (2016). Continuous authentication with touch behavioral biometrics and voice on wearable glasses. *IEEE Transactions on Human-Machine Systems*, 47(3):404–416.
- Peng, Y., Wang, X., Guo, L., Wang, Y., and Deng, Q. (2017). An efficient network coding-based fault-tolerant mechanism in wban for smart healthcare monitoring systems. *Applied Sciences*, 7(8):817.
- Petrenko, S. (2022). *Cyber resilience*. CRC Press.
- Platt, E. L. (2019). *Network science with Python and NetworkX quick start guide: explore and visualize network data effectively*. Packt Publishing Ltd.

- Polese, M., Chiariotti, F., Bonetto, E., Rigotto, F., Zanella, A., and Zorzi, M. (2019). A survey on recent advances in transport layer protocols. *IEEE Comm. Surveys & Tutorials*, 21(4):3584–3608.
- Pollreisz, D. and Nejad, N. T. (2020). Reliable respiratory rate extraction using ppg. In *Latin American Symposium on Circuits & Systems*, pages 1–4. IEEE.
- Psaier, H. and Dustdar, S. (2011). A survey on self-healing systems: approaches and systems. *Computing*, 91(1):43–73.
- Rahouma, K. H., Aly, R. H. M., and Hamed, H. F. (2020). Challenges and solutions of using the social internet of things in healthcare and medical solutions—a survey. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, pages 13–30. Springer.
- Ratasich, D., Khalid, F., Geissler, F., Grosu, R., Shafique, M., and Bartocci, E. (2019). A roadmap toward the resilient internet of things for cyber-physical systems. *IEEE Access*, 7:13260–13283.
- Ratnayake, P., Weragoda, S., Wansapura, J., Kasthurirathna, D., and Piraveenan, M. (2021). Quantifying the robustness of complex networks with heterogeneous nodes. *Mathematics*, 9(21):2769.
- Russell, L., Goubran, R., Kwamena, F., and Knoefel, F. (2018). Agile iot for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach. *IEEE Internet of Things Journal*, 5(6):4454–4465.
- Safaei, M., Ismail, A. S., Chizari, H., Driss, M., Boulila, W., Asadi, S., and Safaei, M. (2020). Standalone noise and anomaly detection in wireless sensor networks: A novel time-series and adaptive bayesian-network-based approach. *Software: Practice and Experience*, 50(4):428–446.
- Sagar, A. K., Singh, S., and Kumar, A. (2020). Energy-aware wban for health monitoring using critical data routing (cdr). *Wireless Personal Communications*, pages 1–30.
- Salayma, M., Al-Dubai, A., Romdhani, I., and Nasser, Y. (2018). Reliability and energy efficiency enhancement for emergency-aware wireless body area networks (wbans). *IEEE Transactions on Green Communications and Networking*, 2(3):804–816.
- Sancho, J., Alesanco, Á., and García, J. (2018). Biometric authentication using the PPG: A long-term feasibility study. *Sensors*, 18(5):1525–1538.
- Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48.
- Sethuraman, S. C., Vijayakumar, V., and Walczak, S. (2020). Cyber attacks on healthcare devices using unmanned aerial vehicles. *Journal of medical systems*, 44(1):1–10.
- Shah, Y. and Sengupta, S. (2020). A survey on classification of cyber-attacks on iot and iiot devices. In *Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, pages 0406–0413. IEEE.

- Shahbazi, Z. and Byun, Y.-C. (2020). Towards a secure thermal-energy aware routing protocol in wireless body area network based on blockchain technology. *Sensors*, 20(12):3604.
- Shandilya, S. K., Upadhyay, S., Kumar, A., and Nagar, A. K. (2022). Ai-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis. *Future Generation Computer Systems*, 127:297–308.
- Shao, C., Park, H., Roh, H., Lee, W., and Kim, H. (2020). Polarscout: Wi-fi interference-resilient zigbee communication via shell-shaping. *IEEE/ACM Transactions on Networking*, pages 1–14.
- Sharma, G. and Kalra, S. (2019). A lightweight user authentication scheme for Cloud-IoT based healthcare services. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 43(1):619–636.
- Shin, H. S., Lee, C., and Lee, M. (2009). Adaptive threshold method for the peak detection of photoplethysmographic waveform. *Computers in Biology and Medicine*, 39(12):1145–1152.
- Siddiqui, M. N., Malik, K. R., and Malik, T. S. (2021). Performance analysis of blackhole and wormhole attack in manet based iot. In *2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, pages 1–8. IEEE.
- Singh, Y. N. and Singh, S. K. (2012). Evaluation of electrocardiogram for biometric authentication. *Journal on Information Security*, 3(1):39–48.
- Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., and Balagani, K. S. (2015). Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, 11(5):877–892.
- Spachos, P., Gao, J., and Hatzinakos, D. (2011). Feasibility study of photoplethysmographic signals for biometric identification. In *17th International Conference on Digital Signal Processing (DSP)*, pages 1–5. IEEE.
- SPEEDTEST, B. O. (2019). Speedtest global index. Technical report, citirano 2020-1-30, dostupno na: <https://www.speedtest.net/global-index>
- Standard, A. (2007). Atis telecom glossary.
- Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. (2010a). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265.
- Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. (2010b). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer networks*, 54(8):1245–1265.
- Strielkina, A., Uzun, D., Kharchenko, V., and Tetskyi, A. (2018). Modeling and availability assessment of mobile healthcare iot using tree analysis and queueing theory. *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*, pages 105–126.
- Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., and Abd El-Latif, A. A. (2022). Edge enabled iot system model for secure healthcare. *Measurement*, 191:110792.

- Tomlinson, W. J., Banou, S., Yu, C., Nogueira, M., and Chowdhury, K. R. (2019). Secure on-skin biometric signal transmission using galvanic coupling. In *International Conference on Computer Communications (INFOCOM)*, pages 1135–1143. IEEE.
- Tompkins, E. L. and Adger, W. N. (2004). Does adaptive management of natural resources enhance resilience to climate change? *Ecology and society*, 9(2).
- Tsigkanos, C., Nastic, S., and Dustdar, S. (2019). Towards resilient internet of things: Vision, challenges, and research roadmap. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 1754–1764. IEEE.
- Ullah, I., Youn, J., and Han, Y.-H. (2021). Multisensor data fusion based on modified belief entropy in dempster–shafer theory for smart environment. *IEEE Access*, 9:37813–37822.
- Viernickel, T., Froemmgen, A., Rizk, A., Koldehofe, B., and Steinmetz, R. (2018). Multipath quic: A deployable multipath transport protocol. In *International Conference on Communications (ICC)*, pages 1–7. IEEE.
- Walters, C. (1997). Challenges in adaptive management of riparian and coastal ecosystems. *Conservation ecology*, 1(2).
- Walters, C. J. (1986). *Adaptive management of renewable resources*. Macmillan Publishers Ltd.
- Wolf, M. and Serpanos, D. (2017). Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, 106(1):9–20.
- Wood, D., Apthorpe, N., and Feamster, N. (2017). Cleartext data transmissions in consumer iot medical devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pages 7–12. ACM.
- Wu, G., Wang, J., Zhang, Y., and Jiang, S. (2018). A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors*, 18(1):179–199.
- Yadav, U., Abbas, S. N., and Hatzinakos, D. (2018). Evaluation of PPG biometrics for authentication in different states. In *International Conference on Biometrics (ICB)*, pages 277–282. IEEE.
- Yamaba, H., Kurogi, A., Kubota, S.-I., Katayama, T., Park, M., and Okazaki, N. (2017). Evaluation of feature values of surface electromyograms for user authentication on mobile devices. *Artificial Life and Robotics*, 22(1):108–112.
- Yang, X., Li, Z., Geng, Z., and Zhang, H. (2012). A multi-layer security model for internet of things. In *Internet of things*, pages 388–393. Springer.
- Yeh, K.-H., Su, C., Chiu, W., and Zhou, L. (2018). I walk, therefore i am: Continuous user authentication with plantar biometrics. *IEEE Communications Magazine*, 56(2):150–157.
- Zaman, U., Mehmood, F., Iqbal, N., Kim, J., and Ibrahim, M. (2022). Towards secure and intelligent internet of health things: A survey of enabling technologies and applications. *Electronics*, 11(12):1893.
- Zamanifar, A. (2020). Social iot healthcare. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, pages 1–11. Springer.

- Zhao, K. and Ge, L. (2013). A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*, pages 663–667. IEEE.
- Zhao, T., Wang, Y., Liu, J., and Chen, Y. (2018). Your heart won't lie: PPG-based continuous authentication on wrist-worn wearable devices. In *International Conference on Mobile Computing and Networking (MobiCom)*, pages 783–785. ACM.
- Zhou, L., Su, C., Chiu, W., and Yeh, K.-H. (2017). You think, therefore you are: Transparent authentication system with brainwave-oriented bio-features for iot networks. *IEEE Transactions on Emerging Topics in Computing*.
- Zinner, T., Geissler, S., Helmschrott, F., Spinsante, S., and Braeken, A. (2017a). An aal-oriented measurement-based evaluation of different http-based data transport protocols. In *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 1162–1167. IEEE.
- Zinner, T., Wamser, F., Leopold, H., Dobre, C., Mavromoustakis, C. X., and Garcia, N. M. (2017b). Matching requirements for ambient assisted living and enhanced living environments with networking technologies. In *Ambient assisted living and enhanced living environments*, pages 91–121. Elsevier.