Adaptive Management for Resilient Internet of Health Things Communication

Fernando Nakayama[1], **Michele Nogueira**[1,2]

[1]Center for Computational Security sCience (CCSC)
Universidade Federal do Paraná (UFPR)

[2]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)

fernandonakayama@ufpr.br, michele@dcc.ufmg.br

Abstract. *Nowadays, one of the primary goals of the healthcare sector is integrating multiple technologies to monitor and keep track of the distinct clinical parameters of patients. In this regard, the Internet of Health Things (IoHT) is one of the most relevant concepts. IoHT offers communication between healthcare devices and the Internet, the continuous sensing of personal and environmental data, remote care, and insights into symptoms and treatments. However, the heterogeneous nature of devices and technologies, data sensitivity, and privacy-related issues make security a priority in IoHT. Also, IoHT applications transmit critical data, demanding stringent requirements for communication performance. This thesis addresses the crucial security and performance issues in IoHT communication. The hypothesis investigated concerns adding adaptive management throughout IoHT communication levels to increase resilience and preserve the network performance required for healthcare applications. The results from experiments show that adaptive management increases communication resilience and performance when integrated into IoHT.*

1. Introduction

The intersection of healthcare and technology is witnessing remarkable advancements with the emergence of the Internet of Health Things (IoHT). This paradigm shift in healthcare delivery is exemplified by applications such as smart medicine, real-time monitoring of cancer treatments and glucose levels, automated insulin delivery systems, and ambient assisted living. IoHT, characterized by the interconnectedness of medical devices and systems, has garnered significant attention from both academia and industry. The imperative driving the adoption of IoHT is the evolving landscape of healthcare, marked notably by an aging population and the demand for decentralized, continuous care delivery. A substantial portion of Internet of Things (IoT) devices, approximately one-third, are dedicated to healthcare applications [IBM 2023], underscoring the growing significance of IoHT in modern healthcare ecosystems.

The reliance on IoHT requires a meticulous consideration of system resilience, particularly in ensuring continuous connectivity, achieving ultra-low latency, and supporting mobility, even in the presence of faults and security threats. Moreover, the proliferation of portable healthcare devices, such as fitness trackers and smartwatches, combined with advancements in high-speed communication technologies like 5G/6G, has opened up new frontiers for IoHT applications. These advancements pave the way for scenarios characterized by continuous health monitoring, culminating in the realization of ubiquitous smart medicine. IoHT represents a transformative force in healthcare, offering unprecedented opportunities for personalized, remote, and continuous care delivery. However, realizing the full potential of IoHT requires addressing challenges related to resilience, security, and interoperability, thereby ensuring its seamless integration into existing healthcare infrastructures.

Current IoHT devices are vulnerable to the exploitation of weak authentication, poor implementation of communication technologies, and outdated solutions. The outcome of attacks and failures includes information loss, inaccurate treatment for users, and the denial of IoHT services, among others. 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. Also, communication channels in IoHT are prone to attacks during pairing and data transmission, resulting in user authentication failures. 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].

The IoHT ecosystem comprises many heterogeneous devices, communication protocols, and processing mechanisms. Considering the dynamic characteristics of devices and mobile elements, the IoHT environment is constantly and drastically changing. Due to these dynamic characteristics, conventional detection and prevention security mechanisms can not protect it against threats that are becoming increasingly sophisticated. Health-related situations, such as those dealt with by IoHT, require fast and dynamic responses to the threats faced. Hence, adaptation is a fundamental property in the IoHT architecture [Muccini et al. 2018]. Adaptation is a system property that makes regulation and reconfiguration possible according to the faced challenges, 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. 2010].

2. Problem Statement

The complex characteristics of the IoHT environment 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 strict communication performance requirements once they deal with critical data (e.g., low delay, high throughput, and constant data transmission). Secondly, numerous threats jeopardize the IoHT environment regarding communication performance and security (e.g., poor authentication mechanisms, eavesdropping attacks, denial of service attacks, and privacy-related threats). The conventional preventive and reactive security controls employed in traditional networks are inadequate to protect the dynamic and constantly expanding IoHT environment. The existing countermeasures rely primarily on static information, delivering static responses. Thus, although there are solutions to face threats and communication performance issues for IoHT, they ignore the multiple configurations required for communication, making it challenging to anticipate issues concerning the performance and security tradeoff.

2.1. Hypothesis and Contributions

My thesis investigates the feasibility of adding adaptive management throughout the multiple IoHT services to enhance overall communication resilience and security and assist 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 to fully meet the objectives of management. The fundamental research question addressed was: *Can adaptive management increase communication resilience in complex environments like IoHT?* To consistently answer this question, it becomes necessary to divide it into subquestions that address specific aspects, 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. These subquestions are as follows: (RQ.1) *How can the techniques that improve communication performance incorporate adaptive management to increase resilience?* (RQ.2) *Which security approaches fit adaptive management, and how do they impact resilience versus performance balance?* (RQ.3) *Assuming the multiple communication topologies in IoHT, how can adaptive management converge with IoHT-based systems?*

The following are the primary contributions of this work:

- A resilience management architecture with performance management of multiple communication paths for IoHT-based portable assisted living systems.
- A biosignal continuous authentication mechanism with secure wireless intrabody communication to assist in the security management of IoHT sensing services.
- A novel resilience analysis approach for IoHT considering the communication topologies available, the adaptation management possibilities, and threats that influence network performance.

The fundamentals of adaptive management, how they relate to communication resilience, and the main contributions are as follows. The main contribution relates to building a portable assisted living system to provide health monitoring while users are on the move. Unlike traditional assisted living systems, the proposal in this work relies on the increasingly popular IoHT devices paired with fixed and mobile communication technologies to build a communication-efficient and resilient mobile health monitoring system. Such a system requires high security to collect and transfer sensitive data. Thus, the proposal involves a mechanism to increase security regarding IoHT devices and communication. Finally, to investigate communication resilience and performance regarding IoHT environments, the proposal includes recognizing and investigating the existing communication topologies and evaluating them when facing threats.

3. Adaptive Management and Communication Resilience in IoHT

Most strategies inspired by adaptive management focus on a Decision-Theoretic approach. 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, the main approach pursued is founded on the concepts of the

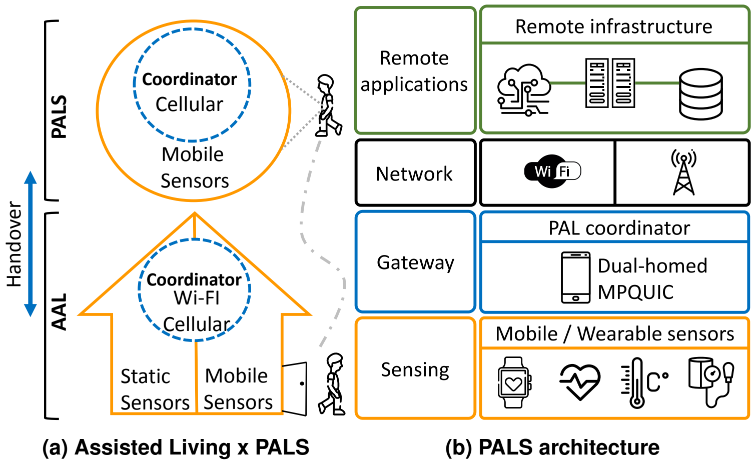
Resilience-Experimentalist process, investigating the relationship between the stakeholders of a system and envisioning the possible management actions considering the defined objectives and the autonomy regarding the reach of the systems and subsystems.

The essence of adaptive management is developing actions designed as much for learning as to meet predefined objectives. Thus, designing new experiments and treatments is one of the outcomes of evaluations. Implementing those experiments has been problematic and can be hindered for numerous reasons, including 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]. Adopting Adaptive management in this Thesis aims to integrate multiple 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 dependent services. The stakeholders represent IoHT components, communication represents the information from processes, and uncertainties represent threats to communication resilience. Additionally, experimentation aims to obtain the best conclusions that can, later, act as input for improving system behavior regarding communication performance and security.

3.1. Communication and Mobility Management

The applications in IoHT retrieve valuable information (e.g., user heartbeat rate and temperature), predict and identify falls, and provide locations for urgent care through environmental and body monitoring. Traditional assisted living supported by health devices has significant relevance given the aging of the world population. Modern medicine allows seniors to live longer, healthier, and more actively. Thus, it is necessary to modernize the concepts of assisted living systems to support their benefits without limiting users' activities. The idea of promoting additional freedom by integrating traditional assisted living and new IoHT devices and communication technologies is called Portable Assisted Living [Nakayama et al. 2021]. 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 opposite to traditional assisted living systems where users are in a controlled environment. Aside from reliability, communication in portable assisted living must offer adequate performance metrics, such as delay and throughput, according to the requirements of applications.

Our main contribution involves developing a Portable Assisted Living System (PALS) to face communication resilience and performance issues in IoHT connectivity services. The main functionality of the system is to provide portable health assistance to users while they execute daily tasks. PALS allows users to use existing assisted living environments based on static sensors, and it extends its services to remote locations using applications that collect data from wearable devices. The data collected reaches the Internet through a coordinator device, such as a smartphone, capable of using multiple communication technologies simultaneously (e.g., WiFi and 5G). Figure 1, illustrates PALS integration with traditional ambient assisted living systems and its architecture. To achieve PALS goals, we propose a resilient management architecture for communication. The architecture assists in transferring data from IoHT devices that constantly collect data from users and transmit it to the Internet using the available communication technologies.



(a) Assisted Living x PALS (b) PALS architecture

Figure 1. PALS and Traditional Assisted Living Integration

The architecture evaluation comprised communication resilience and performance experiments, and the results demonstrate the architecture's capabilities to provide adequate network throughput and efficient use of redundant communication channels while promoting user mobility regarding IoHT scenarios and health-related applications. The experiments occur through simulations, and the characterization relies on real-life scenarios regarding fixed and mobile data transfer speeds and multiple worldwide regions. The experiments results were published in [Nakayama et al. 2021, Nakayama et al. 2022].

3.2. Security Management

Data privacy is a significant concern in IoHT mainly due to the vulnerabilities in wearable devices regarding data collection and communication technologies, such as wireless communication. In this context, user authentication is crucial to grant access to sensitive data and devices. Traditional authentication methods follow one-time events, demanding users to deliberately engage with the system, such as scanning a fingerprint or inserting a password. Additionally, data transmission in current authentication systems relies on traditional wireless technologies. These technologies are susceptible to eavesdropping, being necessary to design a distinct and secure communication channel. Hence, the significance and the challenges of IoHT applications have led to the exploration of new forms of human-computer interactions and communication technologies for designing continuous and seamless user authentication.

Aiming to tackle the issues regarding user authentication and data transmission in IoHT, we propose BEAT (Biosignal Enhanced Authenticator), an original continuous authentication system. BEAT relies on photoplethysmography (PPG) signals and data transmission through a secure intrabody Galvanic Coupling (GC) channel. The PPG biosignal is one of the easiest to collect. It allows for the inference of heart rate variation, becoming prevalent in commercial wearable devices like fitness trackers and smartwatches. BEAT adopts GC to significantly reduce vulnerability to attacks compared to conventional communication technologies, such as Bluetooth. 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.

In order to evaluate BEAT, we have built a prototype based on a PPG sensor and the Arduino open-source platform. We have created our datasets with the prototype and collected data from 30 healthy individuals. Based on the individuals' heart rate variation, we extracted the exclusive features from the biosignals and built a signature model for each user. Later, we employ the signature to validate the user. The GC evaluation comprised experiments involving data transmission through synthetic skin, mimicking human skin. We have tested the BEAT system considering the dataset built at NR2 Lab at Universidade Federal do Paraná and a popular publicly available PPG dataset. Figure 2 illustrates BEAT efficiency regarding both datasets. 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. The full results of this case study were published in [Nakayama et al. 2019a, Nakayama et al. 2019b].

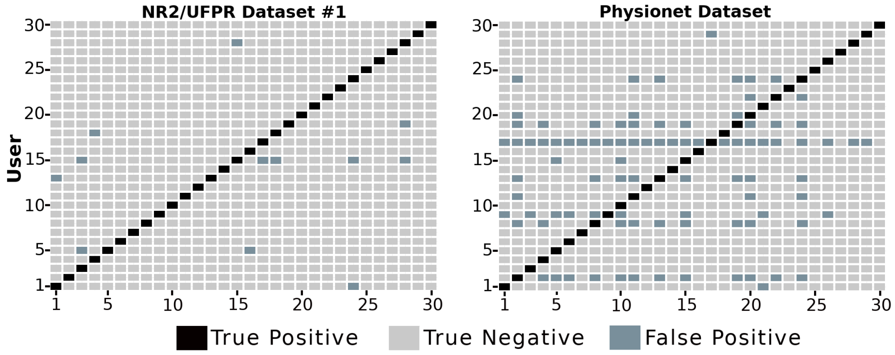


Figure 2. Selected Result - BEAT Evaluation.

3.3. Evaluating Resilience Management In IoHT

Incorporating adaptive management in such a complex and interconnected environment as IoHT is challenging, particularly considering numerous configuration possibilities within the wide range of components. 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]. Therefore, we propose 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 topologies currently available. This approach is composed of three steps (i) the identification of possible network configurations in IoHT; (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 existing IoHT configurations, considering devices and communication technologies, were transposed into six topologies and later into graph representations. Each topology has at least one sensing device representing a wearable device, a coordinator device that manages the network of wearable devices, an access network gateway to the Internet, and a data endpoint representing a data storage and management facility. Those topologies also represent the most common and accessible communication configurations nowadays regarding IoHT devices and communication technologies. 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. It aims to identify the most relevant nodes within each topology and which topologies are intrinsically more resilient.

The communication performance and adaptation evaluation comprised the characterization of the graph representation of the IoHT topologies in terms of communication technologies and device capabilities. Since the review 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. The evaluation comprises the representation of failures at the crucial points of the topologies. The importance of each specific node has been previously identified through experiments regarding the existing resilience metrics. An increased workload at a particular failure point represents the threats. Figure 3 illustrates a scenario where a communication gateway faces a problem and manages to recover through adaptive management.

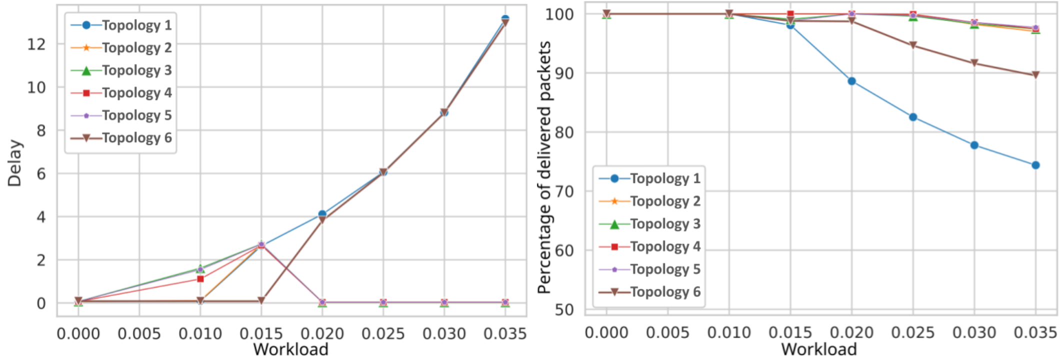


Figure 3. Selected Result - Resilience Evaluation of IoHT Topologies

4. Conclusion

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.

In order to promote seamless and ubiquitous mobile health monitoring for users, we propose PALS, a novel concept founded on portable assisted living systems. PALS promotes mobile health monitoring of users during their everyday routines. PALS leans on an original architecture to manage communication on multiple paths, allowing prime communication performance and resilience while increasing user mobility. However, systems like PALS require increased security for devices and data transfer since IoHT deals with critical and sensitive information. Thus, to promote security in IoHT environments, we propose a continuous biometric authentication mechanism for IoHT employing a secure data transmission communication channel. BEAT relies on users' biosignals and a safe intrabody communication technology to promote continuous user authentication and secure data transmissions. We have also investigated the feasibility of adding adaptive management regarding the existing IoHT communication topologies. Our exploration indicates that existing communication topologies can benefit from adaptive management, especially in the presence of threats that jeopardize communication performance.

Acknowledgment

We would like to acknowledge the support of the Brazilian research agency: CAPES, grant #88882.382204/2019-01, and FAPESP, grant #2022/14299-7.

References

Gunderson, L. (2015). Lessons from adaptive management: obstacles and outcomes. *Adaptive management of social-ecological systems*, pages 27–38.

IBM (2023 (Accessed December 11, 2023)). *Cost of a Data Breach Report.*

Junior, F. M. R. and Kamienski, C. A. (2021). A survey on trustworthiness for the internet of things. *IEEE Access*, 9:42493–42514.

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. (2019a). A continuous user authentication system based on galvanic coupling communication for s-health. *Wireless Communications and Mobile Computing*, 2019:1–11.

Nakayama, F., Lenz, P., Cremonezi, B., Banou, S., Rosário, D., Chowdhoury, K., Nogueira, M., Cerqueira, E., and Santos, A. (2019b). Autenticação contínua e segura baseada em sinais ppg e comunicação galvânica. In *Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 707–720. SBC.

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.

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265.