IAES Journal of Electrical and Electronics Engineering
Vol. 7, No. 2, December 2020, pp. 21~24
ISSN: 2338-7432, DOI: 10.11591/jeee.v7i2.pp21-24

Microcontroller-based remote patient monitoring systems: a review of wireless body area networks, data security, system reliability, and patient safety

Lina Handayani[1], Watra Arsadiando[2], Anggit Pamungkas[2]
[1]Faculty of Public Health, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received Dec 3, 2018
Revised Aug 1, 2019
Accepted Dec 6, 2019

Keywords:

Data Security
Healthcare IoT
Microcontroller
Patient safety
Remote patient monitoring
System reliability
Wireless body area network

ABSTRACT

Remote patient monitoring has emerged as an important application of embedded systems and wireless communication in modern healthcare. Microcontroller-based monitoring devices enable physiological information to be collected from patients and transmitted to healthcare providers without requiring continuous physical attendance at medical facilities. This review examines the development of remote patient monitoring systems, focusing on wireless body area networks (WBANs), embedded system architecture, communication technologies, data security, and patient safety. The integration of physiological sensors, microcontrollers, wireless communication modules, and remote monitoring platforms is discussed in relation to healthcare applications. Particular attention is given to Bluetooth, Wi-Fi, and other short-range communication technologies, including their respective advantages and limitations. The review also investigates important system reliability issues, such as communication interruptions, inaccurate measurements, battery limitations, and unauthorized access to medical information. Furthermore, patient safety considerations are evaluated through the perspectives of data integrity, device dependability, alarm management, and monitoring continuity. The analysis indicates that reliable remote monitoring requires coordinated development of hardware, communication protocols, and security mechanisms. Future systems should prioritize interoperability, low-power operation, secure communication, and clinical evaluation to improve the effectiveness of remote healthcare services.

This is an open access article under the CC BY-SA license.



1. INTRODUCTION

The development of information and communication technologies has created new opportunities for delivering healthcare services through remote monitoring systems. Conventional patient monitoring generally requires patients to visit healthcare facilities or remain connected to medical monitoring equipment. Remote patient monitoring provides an alternative by allowing physiological information to be collected and transmitted through electronic devices and wireless communication networks.

Microcontrollers play an important role in these systems because they coordinate physiological data acquisition, local processing, and wireless communication. When integrated with biomedical sensors and communication modules, microcontrollers can support monitoring architectures that connect patients, smartphones, gateways, and healthcare providers. Wireless body area networks (WBANs) have consequently become an important technological foundation for wearable and remote healthcare applications [1].

This review examines microcontroller-based remote patient monitoring from a system engineering perspective. Unlike reviews primarily concerned with individual physiological sensors, this article emphasizes communication reliability, data protection, system dependability, and patient safety. These aspects are essential because the usefulness of remote monitoring depends not only on collecting physiological measurements but also on delivering trustworthy information to the appropriate healthcare personnel.

2. ARCHITECTURE OF REMOTE PATIENT MONITORING SYSTEMS

A remote patient monitoring system generally consists of four major components: physiological sensor nodes, a microcontroller-based processing unit, a wireless communication network, and a remote monitoring platform. Sensors collect physiological information, while the microcontroller processes the acquired measurements and prepares them for transmission. The receiving platform subsequently presents the information to healthcare providers or authorized users.

WBAN technology enables multiple sensor nodes to communicate within or around the human body. These networks can support continuous monitoring while reducing the need for conventional wired connections. The overall architecture must consider communication distance, network topology, energy consumption, and the different data requirements of individual physiological sensors [2].

As illustrated in Table 1, remote monitoring requires cooperation between hardware and software components. A failure in one component can affect the performance of the entire monitoring system. Therefore, system architecture should incorporate appropriate fault detection and recovery mechanisms rather than depending exclusively on successful sensor acquisition.

Table 1. Main components of microcontroller-based remote patient monitoring systems

System component	Main function	Example technologies	Important consideration
Physiological sensors	Collect patient health information	ECG, PPG, temperature, SpO2	Measurement accuracy
Microcontroller	Process sensor information and coordinate operations	Arduino, ESP32, ARM Cortex-M	Processing capability
Communication module	Transmit physiological measurements	Bluetooth, BLE, Wi-Fi, Zigbee	Reliability and energy consumption
Gateway device	Forward information to remote platforms	Smartphone, Raspberry Pi	Network connectivity
Monitoring platform	Display and store patient information	Web dashboard, mobile application	Data accessibility
Healthcare provider interface	Support clinical observation	Computer or mobile device	Data interpretation and usability

3. WIRELESS BODY AREA NETWORKS AND COMMUNICATION TECHNOLOGIES

Wireless communication is a fundamental requirement for remote patient monitoring because it connects wearable devices with external monitoring platforms. Several communication technologies can be implemented depending on the required transmission range, power consumption, data rate, and network infrastructure. Bluetooth Low Energy, Wi-Fi, and Zigbee represent commonly considered options for embedded healthcare applications. Bluetooth Low Energy is suitable for wearable devices because it supports communication with smartphones and other nearby receivers while offering low-power operating modes. Wi-Fi provides direct access to network infrastructure and can facilitate communication with cloud-based monitoring services. Zigbee offers low-power networking capabilities and can be considered for applications involving multiple interconnected sensor nodes. The selection of communication technology should reflect the operational requirements of the healthcare application. For example, a wearable device transmitting periodic heart rate measurements may not require the same bandwidth as a system transmitting continuous ECG waveforms. Research on WBAN technologies demonstrates that communication protocols must address energy efficiency, interference, mobility, and quality-of-service requirements [1], [2].

Table 2 highlights the different characteristics of wireless technologies used in remote healthcare applications. No communication technology can be considered universally superior because each option has different operational requirements. Hybrid communication architectures may provide greater flexibility by combining short-range wearable communication with longer-range network connectivity.

Table 2. Comparison of wireless communication technologies for remote healthcare monitoring

Communication technology	Main advantage	Main limitation	Potential application
Bluetooth low energy	Low power consumption and smartphone compatibility	Relatively short communication range	Wearable patient monitoring
Wi-Fi	Direct network and internet connectivity	Higher energy requirements	Remote monitoring dashboards
Zigbee	Low-power multi-node communication	Requires compatible gateway infrastructure	Multi-sensor healthcare networks
Cellular Communication	Wide-area connectivity	Network availability and operating cost	Remote patient monitoring
NFC	Simple short-range communication	Very limited communication distance	Patient identification and device pairing

4. SYSTEM RELIABILITY AND PATIENT SAFETY

System reliability is one of the most important requirements in remote patient monitoring because inaccurate or missing information may affect healthcare decisions. Sensor malfunction, unstable electrical connections, wireless interference, and unexpected software behavior can interrupt the monitoring process. Consequently, reliable systems should incorporate error detection, sensor status monitoring, and appropriate notification mechanisms.

Patient safety also depends on the integrity and availability of transmitted physiological information. A monitoring platform should distinguish between valid measurements, incomplete data, communication failures, and abnormal physiological readings. In addition, alarm thresholds must be configured carefully because inappropriate notifications may create unnecessary concern or contribute to alarm fatigue.

The implementation of dependable WBAN systems requires attention to communication quality and network performance. Factors such as packet loss, transmission delay, interference, and temporary disconnection can influence the availability of patient information [3]. Therefore, systems should provide local data buffering and communication recovery where feasible, particularly when continuous monitoring is required.

Another important safety consideration is the limitation of automated monitoring devices. Microcontroller-based systems can assist healthcare professionals by collecting and presenting physiological information, but they should not automatically be regarded as replacements for validated clinical instruments. Medical interpretation and treatment decisions should remain under appropriate professional supervision.

5. DATA SECURITY AND PATIENT PRIVACY

Remote healthcare systems transmit sensitive physiological and personal information through wireless networks and connected devices. Unauthorized access, data interception, manipulation, and information disclosure can compromise patient privacy and the trustworthiness of monitoring services. Therefore, security must be considered during the initial design of the embedded system rather than added only after implementation.

Encryption can help protect physiological information during wireless transmission and storage. Authentication mechanisms are also necessary to ensure that only authorized devices and users can access monitoring information. Furthermore, access control and secure device pairing can reduce the possibility of unauthorized communication between sensor nodes and receiving platforms.

Previous research has identified security and privacy as major challenges in WBAN-based healthcare applications [4]. These challenges include limited processing resources, constrained battery capacity, and the difficulty of implementing strong security mechanisms on small embedded devices. A separate review of WBAN security also emphasizes the importance of protecting patient information throughout the communication and data-sharing process [5].

6. IMPLEMENTATION CHALLENGES AND FUTURE DIRECTIONS

Although remote patient monitoring offers substantial potential, several challenges remain before these systems can be widely adopted in clinical environments. Interoperability is an important issue because different microcontrollers, sensors, communication protocols, and software platforms may use incompatible data formats. Standardized communication interfaces and data structures can improve compatibility between monitoring devices and healthcare information systems.

Energy consumption is another significant implementation challenge. Continuous sensing, wireless transmission, and embedded processing can increase battery requirements, particularly in wearable devices. Low-power microcontrollers, efficient communication schedules, and appropriate battery management techniques can help extend device operating time.

Future development should also emphasize system validation and dependable alarm mechanisms. Remote monitoring devices should be evaluated against appropriate reference instruments under different operating conditions before their measurements are used to support clinical decisions. In addition, the integration of secure communication, reliable data storage, and fault-tolerant processing can improve the overall dependability of microcontroller-based healthcare systems.

7. CONCLUSION

Microcontroller-based remote patient monitoring systems provide an important technological approach for connecting physiological sensors with remote healthcare services. Their effectiveness depends on the integration of reliable embedded hardware, suitable wireless communication technologies, secure information transmission, and dependable monitoring platforms. Nevertheless, communication interruptions,

battery limitations, cybersecurity threats, and measurement inaccuracies remain important challenges. Future research should prioritize interoperability, data protection, fault detection, and clinical validation to improve patient safety. With appropriate engineering design and clinical evaluation, these systems can contribute to more accessible and continuous healthcare monitoring.

REFERENCES

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014, doi: 10.1109/SURV.2013.121313.00064.

[2] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1635–1657, 2014, doi: 10.1109/SURV.2014.012214.00007.

[3] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam, "A comprehensive review of wireless body area network," *Journal of Network and Computer Applications*, vol. 143, pp. 178–198, Oct. 2019, doi: 10.1016/j.jnca.2019.06.016.

[4] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113–122, Jul. 2017, doi: 10.1016/j.eij.2016.11.001.

[5] V. Shrivastava and M. Namdev, "A review on security and privacy issues in wireless body area networks for healthcare applications," *Smart Moves Journal Ijoscience*, vol. 5, no. 11, pp. 22–28, Nov. 2019, doi: 10.24113/ijoscience.v5i11.246.