HBRP PUBLICATION

Journal of Network Security and Data Mining
Volume 6 Issue 1

A survey of Challenges and Solutions for Reliable Communication between Sensors and Network Devices in IoT

***Brinda Chanv*[1], *Jayraj Chanv*[2]**
[1]*Assistant Professor, Department of Computer Engineering, V.V.P. Engineering College, Rajkot, India*
[2]*Assistant Professor, Electrical Engineering Department, R. K. University, Rajkot, India*

***Corresponding Author**
***E-Mail Id:** - brinda.chanv.ce@vvpedulink.ac.in*

ABSTRACT
This review paper analyzes the challenges and solutions for reliable communication between sensors and network devices in IoT. It discusses factors affecting communication reliability, such as interference, congestion, and distance limitations. The paper also examines various protocols and technologies, including LPWANs and WSNs, and strategies like multi-path routing and adaptive power control to improve reliability. Additionally, it covers security challenges and solutions when transmitting data between sensors and network devices in IoT. This review paper provides an overview of reliable communication challenges in IoT and can guide researchers and developers in designing more robust and secure IoT networks.

Keywords: *IoT (Internet of Things), Sensors, Network devices, Reliable communication, Signal interference, Power constraints, Network bandwidth, Security, Privacy, Scalability, Signal amplification, Filtering, Low-power communication protocols, Data compression, Aggregation, Encryption, Authentication, Distributed processing, Edge computing.*

INTRODUCTION

The Internet of Things (IoT) is rapidly expanding, with an increasing number of devices and sensors being connected to the internet every day. However, communication between these devices can be challenging due to various factors such as limited bandwidth, low power, and connectivity issues. This review paper aims to provide a comprehensive analysis of the challenges that arise during communication between sensors and network devices in IoT and the solutions to address them [1].

Internet of Things (IoT) is a rapidly growing technology that connects various devices and objects to the internet, enabling them to communicate with each other and share data [2].IoT has the potential to revolutionize many industries, including healthcare, transportation, and agriculture. However, the reliable communication between sensors and network devices remains a significant challenge in IoT. In this review paper, we will explore the challenges and solutions for reliable communication between sensors and network devices in IoT.

The review begins by discussing the various factors that affect the reliability of communication in IoT networks, including interference, network congestion, and distance limitations. It then examines the different protocols and technologies that have been developed to address these challenges, such as Low-Power Wide-Area Networks (LPWANs), Wireless Sensor Networks (WSNs), and the MQTT protocol [3].

Furthermore, the review paper discusses several strategies for improving the

reliability of communication in IoT networks, such as multi-path routing, duty cycling, and adaptive transmission power control. Additionally, it also covers security challenges and solutions that can arise when transmitting data between sensors and network devices in IoT.

Overall, this review paper provides an overview of the challenges and solutions for reliable communication between sensors and network devices in IoT. The information presented in this review paper can be used to guide researchers and developers in the design and implementation of more robust and reliable IoT networks.

CHALLENGES

A. Network Connectivity

The primary challenge in IoT is establishing reliable connectivity between sensors and network devices. IoT devices use a range of communication technologies such as Wi-Fi, Bluetooth, Zigbee, and cellular networks. The challenge is to ensure that these devices can communicate with each other despite differences in communication protocols, signal strengths, and interference from other devices [4].

Network connectivity challenges can be caused by a variety of factors, including interference from other devices, physical obstacles such as walls or buildings, and limited bandwidth. These challenges can result in lost or delayed data, which can compromise the reliability of the entire IoT system.

To overcome network connectivity challenges, several strategies can be employed. One approach is to use multiple connectivity options, such as cellular, Wi-Fi, and satellite, to ensure that devices can connect to the network regardless of their location. Another approach is to deploy mesh networks, where devices can communicate with each other to relay data, reducing the reliance on a central network infrastructure.

Network redundancy is also important to ensure reliable communication. This involves having multiple paths for data to travel to its destination, so if one path is disrupted, data can still be transmitted through an alternate path.

Lastly, signal strength and quality must be optimized to ensure reliable communication. This can be achieved by deploying network equipment in strategic locations, using signal boosters or repeaters, and optimizing the placement and orientation of IoT devices [5].

B. Security

IoT devices are vulnerable to security threats due to their constant connection to the internet. Hackers can exploit vulnerabilities in IoT devices to gain access to sensitive information or take control of the devices. Ensuring the security of communication between sensors and network devices is essential to prevent these threats [6][9].

C. Interference

Interference from other devices can affect the reliability of communication between sensors and network devices in IoT. For example, Wi-Fi signals can interfere with Zigbee signals, causing communication failures.

D. Power Consumption

IoT devices often run on batteries, which have limited power. To conserve power, these devices need to use efficient communication protocols that consume less power. However, these protocols can affect the reliability of communication between sensors and network devices.

E. Data Volume

IoT devices generate vast amounts of data, which can overwhelm the network and lead to latency and network congestion. Moreover, transmitting large data volumes requires significant bandwidth, which can be costly and challenging to manage [7].

F. Interoperability

IoT devices use various protocols and standards, which can hinder interoperability between devices from different manufacturers. Interoperability challenges can lead to communication failures and limit the scalability of IoT systems.

G. Limited Bandwidth

Another challenge of reliable communication in IoT is the limited bandwidth available for data transmission. IoT devices generate large amounts of data, and the bandwidth available for data transmission is limited, which can result in packet loss, delay, and congestion.

SOLUTIONS

To address the challenges of reliable communication between sensors and network devices in IoT, various solutions have been proposed, including:

Standardization: Standardization of communication protocols can ensure that different IoT devices can communicate with each other reliably. The development of standards such as MQTT, CoAP, and DDS has enabled interoperability between different IoT devices [4].

Security measures: Implementing security measures such as encryption, authentication, and access control can prevent unauthorized access to IoT devices. Manufacturers should also ensure that their devices are regularly updated with security patches to prevent the exploitation of vulnerabilities [8].

Secure communication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) can provide end-to-end encryption and authentication to ensure that communication between sensors and network devices is secure and protected from unauthorized access and data tampering [9].

Channel separation: Separating communication channels between different types of devices can prevent interference and improve reliability. For example, using different communication protocols for Wi-Fi and Zigbee devices can reduce interference and improve communication reliability [4].

FHSS is a technique that allows devices to hop between different frequency channels to avoid interference from other wireless devices. FHSS can improve the reliability and performance of the system by reducing packet loss and delay [7].

Low-power communication protocols: Low-power communication protocols such as Bluetooth Low Energy (BLE) and Zigbee can help conserve power while ensuring reliable communication between sensors and network devices [10].
LoWPANs can extend the battery life of IoT devices and reduce the risk of network downtime [10].

Network Optimization: Network optimization techniques can improve network connectivity and reduce network congestion. These techniques include network load balancing, network virtualization, and quality of service (QoS) management. Network optimization can also enhance security by identifying and isolating malicious traffic.

Data Compression: Data compression techniques can reduce the data volume generated by IoT devices, enabling faster and more efficient data transmission.

These techniques include lossless compression, which reduces data size without compromising data integrity, and lossy compression, which reduces data size by discarding non-essential data.

Quality of Service (QoS): QoS is a mechanism that prioritizes different types of data based on their importance and ensures that high-priority data is transmitted with minimum delay and packet loss. QoS can improve the reliability and performance of the system by ensuring that critical data is transmitted without delay or loss.

CONCLUSION

Reliable communication between sensors and network devices is crucial for the success of IoT. The challenges of connectivity, security, interference, and power consumption need to be addressed to ensure that IoT devices can communicate with each other efficiently and reliably. The solutions of standardization, security measures, channel separation, and low-power communication protocols can improve the reliability of communication between sensors and network devices in IoT.

Reliable communication between sensors and network devices is critical for the performance, reliability, and security of IoT systems. Interference, limited bandwidth, power consumption, and security are the main challenges of reliable communication in IoT. FHSS, QoS, LoWPANs, and secure communication protocols are some of the solutions that can improve the reliability and performance of the system. The success of IoT depends on the ability to overcome these challenges and provide reliable and secure communication between sensors and network devices.

REFERENCES

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
2. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.
3. Jia, Z., Zhang, Y., & Zhou, Y. (2016). A review on the communication security of IoT. Journal of Network and Computer Applications, 75, 99-115.
4. Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, assumptions, problem statement, and goals. RFC 4919.
5. Morshed, S. B., Hussain, M., Azeem, M. I., Shahid, S., & Alam, S. (2018). Quality of service (QoS) in internet of things (IoT): A review. Journal of Network and Computer Applications, 121, 28-44.
6. Park, J., Lee, J. H., & Kim, J. (2016). A review on IoT security technologies and their potential applications. Journal of Communications and Networks, 18(6), 737-750.
7. Shariatmadari, M., & Kantarci, B. (2018). A survey of communication protocols for Internet of Things. IEEE Communications Surveys & Tutorials, 20(3), 2149-2171.
8. Wang, Y., & Zhang, Y. (2016). A survey on the security of the Internet of Things. Security and Communication Networks, 9(15), 2584-2611.
9. Yan, Y., Zhang, Y., Vasilakos, A. V., & Chen, H. (2014). A survey

on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120-134.

10. Yang, J., & Zhang, Y. (2018). A review on low power wireless communication protocols of internet of things for smart city applications. Journal of Network and Computer Applications, 103, 97-114.