International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-13 Issue-9, August 2024

Datadog with Zigbee Wireless Communication Network Protocol for an Internal Implementation in an Educational Institution

P. Swapna, Bandi. Aruna, G. Vinutha, Ch. Mary Pushpa

Abstract: ***Wireless Sensor Networks are the most powerful technique for monitoring Environmental factors. As the role of WSN relies entirely on the service life of the sensor nodes, it is necessary to have complete network monitoring. Energy efficiency has always been a key concern for Wireless sensor networks. This paper presents a detailed literature review that examines how an artificial intelligence networking tool(datalog)can be used with ZIGBee-based network protocol for continuous Real-time data quality monitoring to detect bad data quality issues in an educational organization It also Tracks and improves application speed by following requests from beginning to end and monitoring application performance. By utilising AI algorithms for routing decisions and optimisation methods, the study seeks to enhance network performance, energy efficiency, and system scalability. The analysis of various routing strategies with AI implementations will be covered, emphasising the potential advantages and challenges of this innovative approach within an organisation.***

Keywords*: Protocol, Routing, Dashboard.*

I. INTRODUCTION

Depending on the network architecture and application, several routing protocols are used in WSNs [1]. Used sensors can be widely deployed in areas with limited human access, such as disaster zones and battlefields, as they are small, affordable, intelligent, and disposable. Military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and factory automation, distributed robotics, environment monitoring, and building and structural monitoring are some of the current and future uses for WSNs. In the evolving landscape of [2] network management and monitoring, integrating advanced tools and technologies is essential to maintain robust, efficient, and secure communication systems.

One such powerful combination is Data Dog, a comprehensive monitoring and analytics platform that utilises networks employing the Zigbee routing protocol. This synergy offers enhanced visibility, proactive troubleshooting, and intelligent automation, ensuring optimal performance and reliability of Zigbee-based networks. This article provides a comprehensive review of wireless sensor networks and the ZigBee protocol, aiming to achieve these objectives.

To present a more realistic picture of how the Data Dog protocol performs and behaves in a real-world setting, this article will run various simulations. The dashboard in DataDog is used to visualise ZigBee power consumption data (heatmap, unusual power usage, time series graph which displays power usage for individual devices). The DataDog is an emulations AI tool that will be utilized for this purpose.

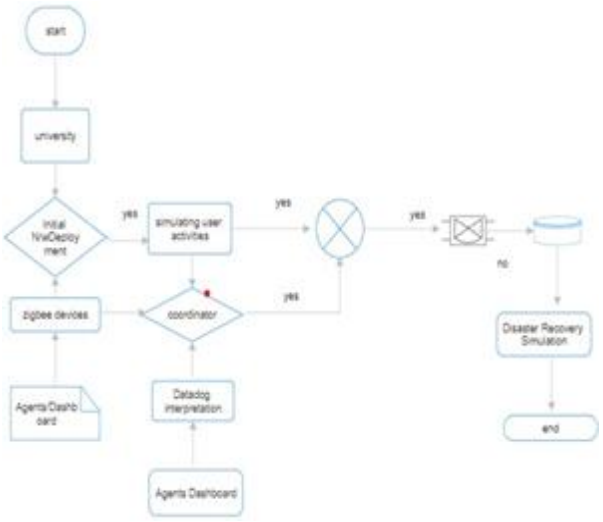

Figure 1: Simulation Model Diagram

II. NETWORK DESIGN AND LAYOUT

Fig (1) This simulation Model Diagram explains about network design and layout for an educational Institution integrating the DataDog platform with ZigBee Routing protocol to map the university's interconnected Network, deploying ZigBee devices (sensors) using coordinators and Routers. It displays agents and Dashboards, which include Monitoring Metrics, increasing the Number of Devices, and simulating security threats. Here, we are using these features. A Repeater Network is used to restore a damaged or weak signal. Despite all the above processing models, there is a practical possibility of Disaster Recoverability and User Activity Monitoring.

Manuscript received on 13 July 2024 | Revised Manuscript received on 22 July 2024 | Manuscript Accepted on 15 August 2024 | Manuscript published on 30 August 2024.

P. Swapna, Department of Computer Science, St. Pious X Degree & PG College for Women, Nacharam, Hyderabad (Telangana), India. E-mail: Swapnapasham@stpiouscollege.org

Bandi. Aruna*, Department of Computer Science, St. Pious X Degree & PG College for Women, Nacharam, Hyderabad (Telangana), India. E-mail: bandiaruna@stpiouscollege.org, ORCID ID: 0009-0008-1401-2914

G. Vinutha, Department of Computer Science, St. Pious X Degree & PG College for Women, Nacharam, Hyderabad (Telangana), India. E-mail: vinuthag@stpiouscollege.org

Ch. Mary Pushpa, Department of Computer Science, St. Pious X Degree & PG College for Women, Nacharam, Hyderabad (Telangana), India. E-mail: marypushpa@stpiouscollege.org

A networking device called a repeater is used to create and magnify incoming signals. Repeaters function at the physical layer of the OSI model. A networking device called a repeater is used to create and magnify incoming signals. Repeaters function at the physical layer of the OSI model.

Networks (WANs) and Local Area Networks (LANs) are used to measure their performance. Using repeaters allows data to be sent to specific areas exclusively, reducing errors and data loss. The primary benefit of employing a repeater is that it enables data to be transmitted across vast distances with enhanced security in a reliable educational environment.

A. Network Deployment, Routine Monitoring, and Performance Assessment

The primary goal of employing a repeater is to extend the network. Zigbee is a low-power, low-data-rate wireless network protocol commonly used for home automation, industrial automation, and other IoT applications [5]. Depending on the network size, consider using Zigbee routers (also known as repeaters) to extend the network range and enhance reliability. Identifying the end devices (sensors, actuators, etc.) that will be part of the network. If needed, set up Zigbee-to-IP bridges to enable remote control and monitoring. Measure the Received Signal Strength Indicator (RSSI) for each device to ensure that signals are strong enough for reliable communication. One of the measures is the link quality indicator (LQI), which assesses the reliability of communication.

III. SCALABILITY TESTING, ANOMALY, AND SECURITY TESTING

Any data point or suspicious event that deviates from the baseline pattern is a data anomaly. Unexpected deviations from the established dataset can indicate system failures, security breaches, or newly discovered security gaps in advance. Any inconsistent or redundant data points—including incomplete data uploads, unexpected data deletions, or data insertion failures—in a database are included in the definition of anomalous data [4]. Data mining anomaly detection enables security teams to identify statistically significant deviations from standard operating patterns in imperceptible events or data points. To respond to data anomalies, prevent breaches, detect fraud, or assess system health, teams frequently require capabilities for real-time data monitoring. Teams can quickly locate the source of security issues by following the breadcrumbs left behind by malicious data points.

A. Wireless Connection Standards

As a component of the IEEE Computer Society's

802 Local and Metropolitan Area Network Standards Committee, IEEE forms the 802.15 working group [3] in active mode with specified results as of March 1999. 802.15.

The primary objective of the working group was to establish standards for Wireless Personal Area Networks (WPANs), also referred to as short-range wireless networks. Within the 802.15 working group, there are many target groups. Any Target group for instance (802.15.1) specifies the WPAN according to Bluetooth version 1.1's Physical (PHY) and Medium Access Control (MAC) levels [6] The next target group (802.15.2) establishes a paradigm for coexistence between WLAN (802.11) and WPAN (802.15). The leading target group's (802.15.3) goal is to create specifications for a WPAN data flow (20 Mbps and beyond).

B. DataDog Monitoring Service

In a rapidly evolving technological landscape, institutions such as universities, hospitals, and research facilities face increasing challenges in managing complex networks of interconnected devices. The proliferation of Internet of Things (IoT) devices has further complicated network management, necessitating advanced monitoring solutions to ensure reliability, security, and efficiency. One such solution is Datadog, which was designed to provide a cloud-based monitoring and analytics platform with comprehensive visibility into IT infrastructure and applications.

DataDog offers a unified approach to monitoring by collecting and analysing data from various sources in real-time, enabling institutions to gain critical insights into the performance and health of their systems. The powerful analytics and visualisation tools allow the identification of patterns, detection of anomalies, and proactive resolution of issues, thereby minimising downtime and enhancing operational efficiency. By exploring the implementation of Datadog within an institutional context, with a focus on its integration with Zigbee Networks, we can gain valuable insights. It is the most widely adopted wireless communication protocol for IoT devices. By

leveraging Datadog's capabilities, institutions can effectively monitor and manage their Zigbee-connected devices, ensuring seamless operation and optimal performance. The integration of Datadog with Zigbee networks in institutions offers numerous benefits. Benefits include improved resource utilization, enhanced security and better support for critical applications. This introduction sets the stage for a detailed examination of how Datadog can address the unique challenges that are faced by institutions in managing their IoT infrastructure, ultimately contributing to their broader goals of innovation, efficiency, and reliability.

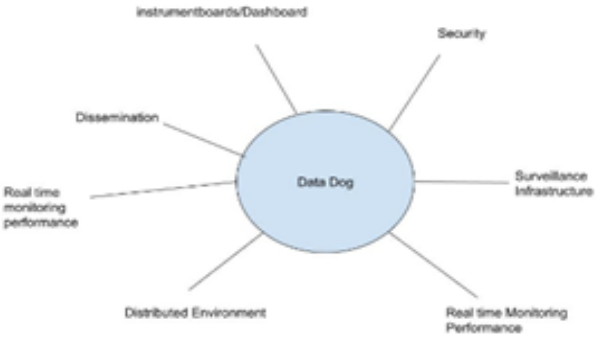

Figure 1: Architecture of Data Dog

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This architecture enables comprehensive monitoring and observability for modern cloud environments, facilitating the proactive detection and resolution of issues. It features several key aspects, including security, Latency Time, continuous Application performance Monitoring, compatibility with distributed systems, and Dashboard Measurements.

DataDog is a cloud-scale application monitoring solution that uses a SaaS-based data analytics platform to monitor servers, databases, tools, and services. Dashboards: Datadog allows you to construct two different kinds of dashboards.

An event graph generates a new timeline for correlation and troubleshooting, utilising time-synchronised metrics. With the use of time boards, you can simultaneously identify metrics and services, as well as resolve problems.

A disorganized dashboard list page might impede the discovery of relevant content and contaminate a search query with superfluous or unrelated results. You can delete unneeded dashboards in bulk and undo any inadvertent removals by combining bulk delete with Recently Deleted dashboards. This manual comprises: Overarching guidelines for recognising inactive dashboards for scheduled deletion. The best ways to keep your list page manageable

IV. USER ACTIVITY MONITORING

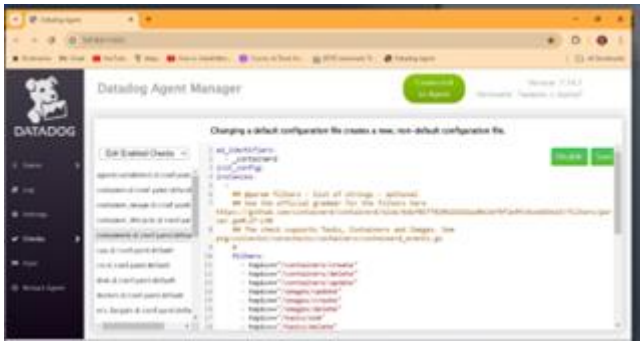

Figure: 2(a)

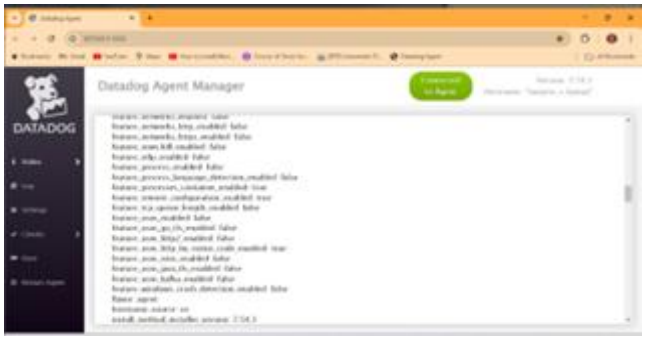

Figure: 2(b)

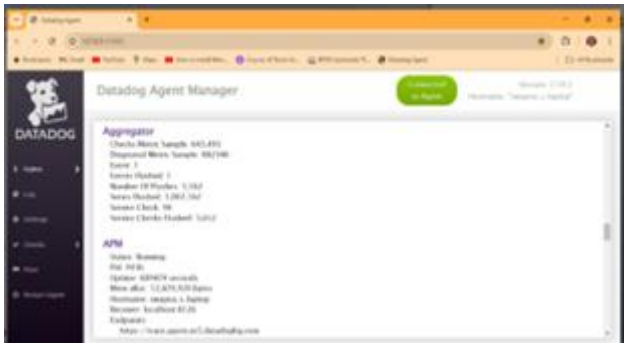

Figure: 2(c)

The above figures show that the Data Dog manager examines the dashboard, which monitors proxy settings with addresses, detects remote configurations, and serves as an aggregator that specifies the hostname and receiver local host.

V. SIMULATION SCENARIOS

The simulation displays the anticipated actions of the system under various circumstances using its simulation model. Therefore, this simulation model's goal is to ascertain the precise model and forecast the actual system's behavior. The DataDog AI tool manages the monitoring proxy settings, providing a comprehensive development environment to facilitate modelling of distributed systems and communication networks. It plays a significant role in detecting remote configurations with all the present details, including the host name and the receiver's local host address.

VI. CONCLUSION

The deployment of Datadog for monitoring Zigbee networks within an institutional environment offers a significant advancement in managing and optimizing IoT infrastructure. Datadog's comprehensive monitoring capabilities, coupled with Zigbee's robust wireless communication protocol, provide a powerful combination for ensuring the reliability and efficiency of networked devices and systems. For institutions such as universities, colleges, and research facilities, the ability to monitor and analyse real-time data from Zigbee-connected devices through Datadog can lead to enhanced operational efficiency and reduced downtime. This integration allows for proactive identification of issues, informed decision-making, and streamlined maintenance processes. The resulting improvements in network performance and device management can lead to enhanced resource utilisation and cost savings. In summary, integrating Datadog with Zigbee networks within an institutional context not only strengthens monitoring and management capabilities but also supports the institution's broader goals of innovation, efficiency, and reliability. This approach represents a strategic investment in the institution's technological infrastructure, paving the way for future advancements and scalability.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.

Retrieval Number: 100.1/ijitee.I995113090824
DOI: 10.35940/ijitee.I9951.13090824
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. "21 ideas for the 21st century," Business Week, pp. 78–167, Aug. 30, 1999.
2. Chong, C. and Kumar, P. "Sensor Networks: Evolution, Opportunities, and Challenges", *Proceedings of the IEEE*, vol.91, No.8, August 2003.
3. Bluetooth SIG, "Bluetooth Specification v1.1," 2001, http://www.bluetooth.org/spec/, Last accessed on 15 July 2011.
4. García-Hernández, C. F., Ibargüengoytia-González, P. H., García-Hernández, J. and Perez Diaz, J. A. "Wireless Sensor Networks and Applications: a Survey", International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.
5. Rehana, J. "Security of Wireless Sensor Networks", *Seminar on Internetworking*, April 27, 2009.
6. Devineni, A. "Performance evaluation of body area network using ZigBee protocol", *Faculty of San Diego State University,* spring, 2011.

AUTHORS PROFILE

Mrs P. Swapna is a Computer Science Lecturer presently working at St. Pious X Degree & PG College. Her Qualification is (M.C.A, MTech (CSE)) from Osmania University with 20 Years of Teaching Experience, specialising in Machine Learning, AI, and Data Analytics.

Mrs. Bandi. Aruna received a BSc. Computer Science Degree from St. Theresa's Women's College, Eluru, A.P., in 1997. Received M.C.A. Degree from Madras University, Chennai in the year 2006 and M.Phil from Anna University in 2008. She has been in the field of teaching for 24 Years. Her Areas of interest include cybersecurity and networks.

Mrs. G. Vinutha completed my master's degree in MCA from Osmania University in the year 2007, working as an assistant professor for the past 13 years, having immense knowledge in research on Data Structures, User Interface applications and developed a User Interface application

Ch. Mary Pushpa completed her M.Tech at JNTU and has 11 years of teaching experience. Her areas of interest include AI, Data mining, and Networks. Years of having immense knowledge in research on Data Structures, User Interface applications