

Performance Evaluation of IoT Protocols in Resource-Constraints Smart Home Networks

Habibu Abubakar Sifawa¹, Abubakar Bello Tambawal² and Shehu Malami S/Tudu³

¹Department of Computer Science, Faculty of Computing, Sokoto State University

²Department of Computer Science, College Of Science and Technology, Umaru Ali Shinkafi Polytechnic, Sokoto

³Department of Computer Science, Faculty of Computing, Sokoto State University

Corresponding Author's Email and Phone No.: habeabsifawa@gmail.com: +2347033155307

Received on: January, 2026

Revised and Accepted on: February, 2026

Published on: March, 2026

ABSTRACT

Smart home systems rely heavily on internet of things (IoT) communication protocols to support real-time monitoring, automation, and energy efficient operation. However, the heterogeneity of IoT devices and resource constraints such as limited bandwidth, processing capability, and battery power complicate protocol selection. This paper presents a technical performance evaluation of four widely used IoT application layer protocols which include constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Hypertext Transfer Protocol (HTTP). Using a unified simulation environment based on Omnet++6.2.0/Inet 4.5, the protocols were assessed under identical smart home network conditions. Key performance metrics include latency, throughput, packet delivery ratio (PDR), and energy consumption. The results demonstrate that CoAP achieves the lowest latency and energy consumption, making it suitable for delay sensitive and low power devices. MQTT and HTTP provide perfect packet delivery reliability due to their TCP based mechanisms, while HTTP offers the highest throughput at the expense of higher delay and energy cost. The findings highlight that protocol selection must be application specific, balancing performance requirements and resource limitations.

Keywords: IoT, Smart Home, Heterogeneity, Communication Protocols, Resource-Constraints.

1.0 INTRODUCTION

The adoption of Internet of Things (IoT) devices in smart home technologies has accelerated due to their ability to enhance convenience, security, and energy efficiency (Pettersson, 2021). Smart home devices such as smart bulbs, thermostats, fans, cameras, and air conditioners increasingly rely on iot communication protocols to provide seamless automation, user comfort, and energy optimization (Afoluwaso & Ajibola, 2024). Efficient communication is therefore essential to ensure smooth operation and reliable interaction between devices, gateways, and cloud services (bayilmiş et al., 2022). IoT devices in smart home technologies has accelerated due to their ability to enhance convenience, security, and energy efficiency (Afoluwaso & Ajibola, 2024; Caro et al., 2019; Shahinzadeh, 2024). Efficient communication is therefore essential ; Shafik et al., 2020). Prior researches on IoT protocols (Bayilmiş et al., 2022; Bhardwaj et al., 2021; Shahrokhi & Ahmadi, 2024; Shah et al., 2021; Sidna & Alami, 2020) have largely focused on how protocols perform in the unique context of smart home networks, where device density, inefficient communication risk, poor scalability, energy consumption, heterogeneous traffic and compromised security which make communication more challenging. Consequently, it becomes difficult for the developers to select the suitable protocols due to the smart home

devices resource constraints. Despite the aforementioned research efforts, a significant gap exists in resolving the challenges of IoT protocol faced by stakeholders due lack evidence-based clear guidance on protocol selection and optimization for smart home deployments. To bridge this literature gap, the present study proposed performance evaluations of IoT protocols in resource-constraints smart home network, particularly in terms of latency, throughput, packet delivery ratio and energy consumption. Several popular protocols at the application layer available today are geared towards the M2M communication role, namely message queue telemetry transport (MQTT) (Yalçinkaya et al., 2020). Constrained application protocol (CoAP) (Seoane et al., 2021). Advanced message queuing protocol (AMQP) (*comparing the efficiency of lwm2m and mqtt : hands-on test results of two technology clients on a typical iot device april 2020 table of contents*, 2020). Hypertext transfer protocol (HTTP) (Naik, 2023) the justification of this study is because smart homes increasingly rely on iot devices for automation (stolojescu-crisan et al., 2021), energy management, (Hadi, 2024; Prasad, 2025), security (Bouzidi et al., 2022; Mofawiz, 2022; Nur Issi, 2022), and these devices depend on communication protocols to operate effectively (Shahinzadeh, 2024; Yalçinkaya et al., 2020). However, smart home environments are limited by factors such as low bandwidth, unstable

wireless signals, energy constraints, and diverse device types (Naik, 2023; Sadikin et al., 2019; Tanishka and Prof. Shikha Gupta, 2020). These limitations often reduce network performance, especially in terms of latency, throughput, packet delivery and energy consumption (Divyashree & Sujatha, 2020; Gemirter, 2020). Although various studies have examined IoT protocols like MQTT, CoAP, AMQP, and HTTP, most of them were carried out under ideal conditions or focused on one protocol at a time, only a few of them have assessed how these protocols perform Side-by-Side within real smart home constraints (Lagervall, 2023; Seoane et al., 2021; Shahinzadeh, 2024; Ua et al., 2021). Consequently, engineers and other users of IoT systems lack clear evidence to guide protocol selection and optimization in practical smart home deployments (Amir Khanov, 2025). This study is therefore necessary, as it compares the performance of four major IoT protocols under the same constrained smart home conditions. By evaluating latency, throughput, packet delivery ratio and energy consumption. The research provides realistic insights that address existing gaps in the literature. The results will support better decision making among researchers and practitioners and contribute to improving the effectiveness and reliability of IoT based smart home systems.

1.1 Related Works

A considerable body of research has examined the comparative performance of IoT communication protocols, particularly with respect to their suitability for constrained networks. These studies, while diverse in focus and methodology, provide valuable insights into the tradeoffs associated with protocols such as MQTT, CoAP, AMQP, HTTP, and their derivatives. In (Sidna & Alami, 2020) conducted an empirical evaluation of MQTT, CoAP, and HTTP under constrained networking conditions. Their findings revealed that CoAP consistently achieved the lowest latency, a result attributed to its lightweight, UDP based design, whereas MQTT demonstrated stronger reliability, owing to its publish-subscribe architecture. Similarly, (Pettersson, 2021; Shahrokhi & Ahmadi, 2024) through simulations in contiki/cooja, emphasized the role of transport mechanisms in protocol efficiency. Their results showed that MQTT-SN and CoAP were more energy-efficient than MQTT operating over TCP, highlighting the importance of protocol transport layer alignment in resource-constrained environments. Other researchers have critically evaluated protocol overheads. For example, (Bayilmiş et al., 2022; Md. Milon, 2022) noted that http suffers from significant message overhead, which compromises its efficiency in constrained IoT deployments. Moreover, in (Khan et al., 2023), the

context of smart grid IoT applications, highlighted MQTT scalability advantage, though they also cautioned that its dependency on a centralized broker may introduce bottlenecks and single points of failure. More broadly, in (Bayilmiş et al., 2022), a comprehensive review of application layer IoT protocols, concluded that no single protocol offers universal optimality across all IoT scenarios, suggesting that protocol suitability is highly context-dependent.

Energy optimization approach was proposed to minimize energy consumption within the connected objects by utilizing MQTT with CoAP to check the quantity of the energy optimization. The approach has minimize energy consumption with integration CoAP protocol by using joulemeter to measure and estimate the energy consumption of computers and applications. The MQTT-CoAP achieved 1.2j while COAP attained 2.5j and MQTT score 3.7j which indicate 50% reduction in energy consumption (Haman et al., 2024). Also in (Ochoa et al., 2023) the real-time monitoring system was propose using NODEMCU module integrated with MQTT and HTTP with different QoS levels. The experimental result demonstrated that the MQTT with QoS 0 and 1 saved power between 6.03% and 8.33% compared with http. The MQTT has the potential to adapt as technological solution for the transport operations. The proposed methodological approach suitable for IoT communication protocol in real-time data transmission with stability and security by comparing MQTT over TCP, MQTT over websocket, and http protocols by utilizing Esp32 microcontroller and DHT22 sensor. The results revealed that MQTT over TCP achieves the lowest average latency at 290.5 ms while HTTP has higher average latency of 342.6 ms. The MQTT over TCP performed better with stability and security (Amir Khanov, 2025). According to (Khaleefah et al., 2025) proposed an extensive empirical study of the most prominent IoT standards namely MQTT, COAP, and HTTP by imitating real-world smart city using a raspberry pi based testbed. The proposed study evaluated based on latency, message overhead, delivery rate and energy consumption. The experimental results demonstrate that CoAP under QoS-1 reliability attained lower latency of 18 with delivery rate of 99.3 while MQTT attained latency of 22 with delivery rate of 99.7 outperforming HTTP latency and delivery rate. The findings has the potential to adapt and construct a secure, efficient and scalable communication protocols in urban IoT settings. However in (Moraes et al., 2019) investigate the performance evaluation of IoT communication protocols namely: AMQP, CoAP, and MQTT. The experimental results revealed that the AMQP protocol has the greatest mean value score of 93.34 kbps for

throughput while MQTT over TCP attained 58.81 kbps and coap attained lowest values of 37.75 kbps which has lowest impact on network bandwidth. To the best of our knowledge, this study is the only quantitative comparison including a wide set of iot protocols such as CoAP, MQTT, AMQP and HTTP protocols with four key metrics include latency, throughput, packet delivery ration(PDR) and energy consumption. The aim of this study is to evaluate and compare the performance of selected iot communication protocols in resource-constraints smart home networks.

2.0 MATERIALS AND METHOD

2.1 Materials

The evaluation was conducted using the Omnet++ 6.2.0 discrete-event network simulator integrated with the Inet 4.5 framework. The simulation environment models a smart home topology consisting of multiple IoT sensor nodes and a server or central broker. The Inet energy framework, including the StateBasedEpEnergyconsumer and IdealEpEnergystorage modules, was used to model device energy consumption.

2.1.1 Simulation Hardware and Operating Environment

All simulations were executed on a windows 10 (64-Bit) machine equipped with:

1. Processor: Intel Core I5 (2.8 Ghz, 4 Cores)
2. Memory: 8gb RAM
3. Storage: 250 SSD

This configuration provided adequate computational resources for running multiple simulations efficiently, ensuring stable results without performance degradation.

2.2 Methodology

A simulation based approach was adopted using the Omnet++ version 6.2.0/INET version 4.5 framework to ensure repeatability and fairness. A smart home network topology consisting of sensor nodes, and a central server/broker was modeled. All protocols were evaluated using identical parameters, including payload size, transmission interval, link characteristics, and simulation time.

2.2.1 Research Design

The experimental research design, which is appropriate for investigating the performance of Internet of Things (IoT) communication protocols (MQTT, COAP, AMQP, and HTTP) under controlled and reproducible conditions. The experimental design allows to systematically manipulate variables, observe their effects on network performance metrics, and draw empirical conclusions regarding protocol efficiency and suitability for smart home applications.

2.2.2 Protocol Configuration

Each protocol under test (MQTT, COAP, AMQP, and HTTP) is configured with its default operational behavior within the INET Framework.

- i. MQTT scenario: The MQTT protocol follows a publish/subscribe model, where each sensor acts as a publisher transmitting data to the broker (subscriber). Mqtt's lightweight nature and small header size make it suitable for constrained devices, and its quality of service (QoS) settings are tested at levels 0 (at most once) and 1 (at least once).
- ii. CoAP scenario: CoAP operates over UDP using a request/response model optimized for lightweight m2m communication. Each sensor sends confirmable messages to the broker, which responds with acknowledgments. Retransmission timers and message ids are used to manage packet loss.
- iii. AMQP scenario: AMQP is implemented over tcp, providing reliable message delivery and flexible routing. It supports queue-based communication and message acknowledgments, introducing additional overhead but offering robust reliability features.
- iv. HTTP scenario: The HTTP configuration employs a client-server model where each sensor node periodically sends http post requests to the broker. Although widely used, http's verbose headers and reliance on persistent tcp connections typically increase latency and bandwidth consumption in constrained environments.

2.2.3 Protocol Features

This section provides a summary of the main features for the IoT protocols MQTT, AMQP, HTTP under TCP and COAP, under custom user datagram protocol (UDP), which are compared in this paper.

A. CoAP stands for constrained application protocols is a stateless protocol developed by the IETF to replace http in resource-constrained devices. Being a user datagram protocol (UDP) based RESTFUL protocol, it uses a request/reply structure and has low overhead and a low degree of optional qos (Bayilmiş et al., 2022). In order to receive telemetry, a client must constantly request the server to send the information. CoAP primarily supports a peer-to-peer style of communication but can be expanded to support one-to many functions via the use of IP multicast (Seoane et al., 2021).

B. MQTT stand for message queuing telemetry protocol it is a lightweight publish-subscribe protocol under tcp base, developed by IBM and then open-sourced for

messaging applications. In publish-subscribe format, clients can either “publish” data on a specific topic to the server or subscribe to a topic where the server/broker will automatically send new data on the topic to the subscriber once registered (Yalçinkaya et al., 2020). MQTT combines the relatively high overhead and high QoS of TCP with the one-to-one, one-to-many, and many-to-one capabilities of publish-subscribe format. Additionally, this protocol also allows clients to specify which telemetry topics are of interest and receive only data published through those topics (Cui, 2017).

C. AMQP stand for advanced message queuing protocol is a more feature-rich messaging protocol initially developed for enterprise applications. Unlike MQTT, AMQP provides advanced functionalities such as message orientation, queuing, routing, and transaction management, making it suitable for complex distributed systems (*Comparing the efficiency of lwm2m and mqtt: hands-on test results of two technology clients on a typical iot device april 2020 table of contents*, 2020). In terms of strengths, AMQP offers high reliability and strong delivery guarantees, which are essential for applications requiring strict consistency in message exchange. It also provides robust interoperability across heterogeneous systems and supports persistent message storage, ensuring that no data is lost even if Nodes temporarily go offline (Seoane Et Al., 2021) (Cui, 2017).

D. HTTP stand for hypertext transfer protocol is the most widely used communication protocol on the internet and has also been extended into IoT applications due to its universality and compatibility with web-based systems (Naik, 2023) (Cui, 2017). HTTP enables smart home devices to interact seamlessly with cloud services and mobile applications, leveraging the well-established ecosystem of web technologies. Http’s strengths lie in its universal adoption, simplicity of implementation, and compatibility with restful web services. It also benefits from mature security frameworks through the use of transport layer security (TLS) and secure sockets layer (SSL), ensuring robust protection of transmitted data. However, HTTP is less efficient in resource-constrained environments. Its reliance on TCP introduces high connection overhead and latency, which are unsuitable for real-time communication in smart homes. The protocol’s heavy payload structure further exacerbates energy consumption, reducing device lifespan in battery-powered networks (D. Persson, P. Niklas, 2020). Consequently, while HTTP remains attractive for interoperability and integration with web platforms, it is generally less effective for applications requiring low latency, energy efficiency, and lightweight communication.

2.2.4 Simulation Workflow For IoT Protocol Performance Evaluation

The simulation workflow in figure 1 illustrates the systematic process used to evaluate the performance of IoT communication protocols in Omnet++ version 6.2.0 and Inet version 4.5. The procedure involves initializing experiment parameters, configuring network topologies and protocol settings, executing multiple simulation runs, and collecting .vec and .sca outputs. The results are post processed to obtain key performance metrics such as latency, throughput, and packet delivery ratio, which are then aggregated and visualized to enable comparative analysis across different protocols and scenarios.

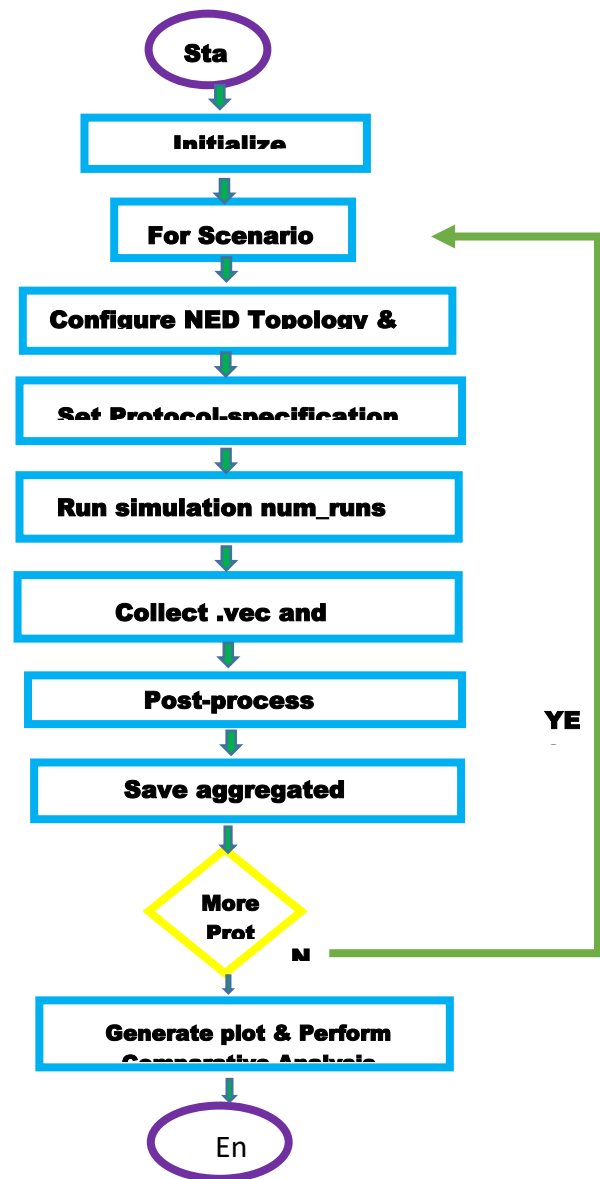


Figure 1: Simulation Workflow for IoT Protocol Performance Evaluation in Omnet++**a. Simulation Parameters**

To maintain uniformity across the experiments, key simulation parameters are carefully selected to approximate real-world Smart Home Environments, as summarized In Table 1

Table 1: Simulation Parameters

S/N	Parameter	Value / Description
1	Simulation Tool	Omnet++ 6.2.0 With Inet 4.5
2	Topology	Star Network (4 Sensors + 1 Broker)
3	Link Data Rate	250 Kbps
4	Propagation Delay	10 Ms
5	Packet Size	512 Bytes
6	Transmission Interval	2 Seconds (Per Sensor)
7	Simulation Duration	60 Seconds
8	Transport Layer	TCP (for HTTP, AMQP, MQTT) and UDP (for COAP)
9	Traffic Type	Periodic Sensor Data Updates
10	Metrics Evaluated	Latency, Throughput, PDR and Energy Consumptions
11	Energy Storage	Idealepenergystorage,10,000j Capacity

b. Performance Metrics And Measurement Method

Performance evaluation is an essential aspect of network experimentation, as it provides quantifiable insights into how efficiently communication protocols operate under constrained smart home conditions. This section presents the performance metrics used in the study, which include latency, throughput, packet delivery ratio (PDR) and energy consumption describes the corresponding measurement techniques and formulas adopted during the simulation. The selected metrics were chosen because they directly reflect the responsiveness, reliability, and efficiency of communication in IoT based smart home network environments. Each metric was extracted from simulation data generated by Omnet++ 6.2.0 using the inet 4.5 modules and subsequently analyzed to compare the behavior of MQTT, CoAP, AMQP, and HTTP protocols.

- I. Latency (end-to-end delay) milliseconds: The total time required for a data packet to travel from the sensor node to the broker. It reflects the responsiveness of the protocol. Lower latency

indicates faster communication and is crucial for time-sensitive applications (e.g., motion detection or alarms).

Relevance: in smart home systems, where time sensitive applications such as alarm triggers and environmental monitoring are common, low latency is critical for maintaining system responsiveness and reliability. It is presented in equation 3.1

$$D_{avg} = \frac{1}{N} \sum_{i=1}^n (t_{receive,i} - t_{sent,i}) \quad (3.1)$$

Where:

- a. D_{avg} = Average End-To-End Delay (Seconds)
- b. N = Total Number Of Successfully Received Packets
- c. $t_{sent,i}$ = Timestamp When Packet I Was Sent
- d. $t_{receive,i}$ = Timestamp When Packet I Was Received

Measurement method: Omnet++ version 6.2.0 records both packet send and receive times in the vector output files (.vec). These timestamps were extracted and processed using the Omnet++ version 6.2.1 to compute the average delay for each protocol. The computed latency values were then averaged across ten simulation repetitions to improve accuracy.

- ii. Throughput (kbps): the total volume of successfully delivered data (in bits per second) over the duration of the simulation. This metric indicates how efficiently the network handles data transmission under constrained bandwidth conditions. It is presented in equation 3.2

$$T = \frac{\sum_{i=1}^N P_{size,i}}{t_{end} - t_{start}} \quad (3.2)$$

Where:

- a. T = Throughput (Bits Per Second, Bps)
- b. $P_{size,i}$ = Size Of The I The Successfully Received Packet (Bits)
- c. t_{start} = Simulation Start Time
- d. t_{end} = Simulation End Time
- e. N = Total Number Of Packets Successfully Received

Measurement method: Omnet++ automatically tracks the total bytes received per node, which can be accessed from the .sca (scalar) output file. The total number of received bytes was divided by the simulation duration to compute the average throughput for each protocol configuration.

- iii. Packet delivery ratio (PDR)

Packet delivery ratio (PDR): the ratio of successfully received packets at the broker to the total number of packets sent by sensors. A higher pdr implies better reliability and robustness of the communication protocol against packet loss and transmission errors. Each metric is computed using built-in Omnet++ statistical modules and validated across multiple simulation runs to ensure accuracy and repeatability. Relevance: in IoT smart homes, high PDR ensures reliability and consistency in communication between sensors, controllers, and the central broker. It is presented in equation 3.3

$$\text{PDR}(\%) = \left(\frac{N_{\text{received}}}{N_{\text{sent}}} \right) \times 100 \quad (3.3)$$

Where:

- a. N_{Received} = Total Number Of Packets Received By The Broker
- b. N_{Sent} = Total Number Of Packets Transmitted By Sensors

Measurement method: The number of packets transmitted and received was extracted from Omnet++ simulation logs. These values were aggregated across all sensor nodes to determine the overall network PDR for each protocol.

Energy consumption: energy consumption refers to the total amount of electrical energy expended by each smart home iot device during the 60s simulation period, measured in joules (j). Energy consumption is computed based on the duration that each device spends in different operational states namely transmission (tx), reception (rx), idle and sleep combined with the corresponding power consumption values defined in the energy model. The inet StatebasedEpenErgyconsumer module records these state transitions and calculates energy using it is presented in equation 3.4

$$E = P_{tx}t_{tx} + P_{rx}t_{rx} + P_{idle}t_{idle} + P_{sleep}t_{sleep} + P_{off}t_{off} \quad 3.4$$

Where :

Tx: Sending Packets

Rx: Receiving Packets

Idle: NIC online but not communicating

Sleep: Low-Power Mode

Off: No Operation

P_i = Power Consumption (W) In State I

t_i = Time spent in the State

State $I \in$ (Tx, Rx, Idle, Sleep, Off)

Energy Is Measured In Joules, Since: Joules = Watts \times Seconds

c. Evaluation Method

The evaluation process involved the following systematic steps:

- i. Simulation execution: each protocol configuration (MQTT, COAP, AMQP, HTTP) was executed independently for 60 seconds of simulation time and repeated ten times to obtain statistically stable results.
- ii. Data extraction: key parameters (latency, throughput, PDR and energy consumption) were obtained from .vec and .sca files using Omnet++'s result analysis utility.
- iii. Computation and averaging: the raw data from multiple simulation runs were averaged using Microsoft excel to eliminate random variations.
- iv. Visualization: graphical plots were generated to compare performance metrics across all protocols. Typical representations included:
 - a. Average latency (ms) vs protocol
 - b. Throughput (kbps) vs protocol
 - c. Packet delivery ratio (%) vs protocol
 - d. Energy consumption (j) vs protocol
- v. Comparative analysis: results were analyzed to identify the most balanced protocol based on all three metrics. Performance tradeoffs were discussed in relation to protocol design characteristics.

d. Experimental Procedure

- i. Initialization: the simulation environment is initialized with all devices configured using the ipv4networkconfigurator module to ensure consistent addressing.
- ii. Protocol selection: one communication protocol (MQTT, CoAP, AMQP, OR HTTP) is activated for each simulation run.
- iii. Traffic generation: sensors begin transmitting data periodically to the broker using their respective application-layer protocol configurations.
- iv. Performance monitoring: Omnet++ collects real-time statistics on packet delay, throughput, and delivery success.
- v. Result logging and analysis: the collected data is stored in output vector files (.vec) and scalar files (.sca) for post-simulation analysis using the Omnet++ ide or external tools (e.g., matlab or excel).
- vi. Comparison and interpretation: results from all four scenarios are compared quantitatively to identify performance trade-offs and determine the most balanced protocol for constrained smart home networks.

e. Simulation Configuration And Execution Settings

Figure 3 presents the omnet++ simulation configuration interface, which specifies the operational parameters controlling the execution of the smart home network model. The configuration was managed through the omnetpp.ini file, serving as the primary control file for defining simulation scenarios, runtime limits, and output management.

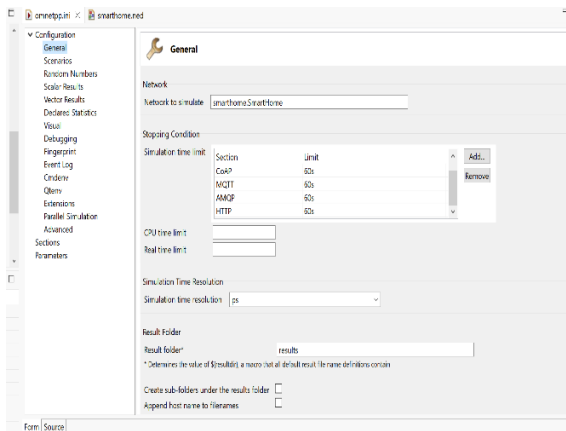


Figure 2: Simulation configuration interface showing protocol time limits and result folder setup.

f. Simulation Configuration Interface

Figure 4 illustrates the Omnet++ configuration setup interface, which appears before the commencement of a simulation run. This interface allows the researcher to select a specific experimental configuration as defined in the omnetpp.ini file. Each configuration corresponds to a distinct IoT communication protocol scenario CoAP, MQTT, AMQP, OR HTTP representing the different communication paradigms evaluated in this study.

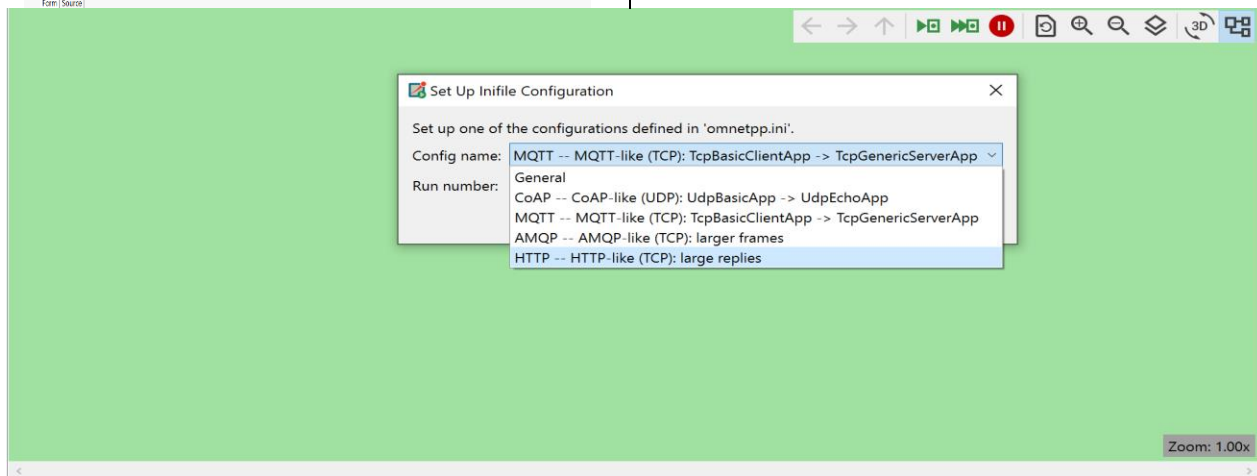


Figure 3: Simulation configuration setup window showing protocol selection options (COAP, MQTT, AMQP, and HTTP)

g. Simulation Execution and Runtime Visualization

Figure 4, illustrates the Omnet++ simulation runtime environment, representing the dynamic communication process within the smart home network topology. The simulation consists of four iot sensor nodes (sensor[0]–sensor[3]), a central broker node, and a network configurator responsible for automatic ip address assignment and routing configuration and figure 3.7: showing iot sensors and the broker in the smart home network are connected

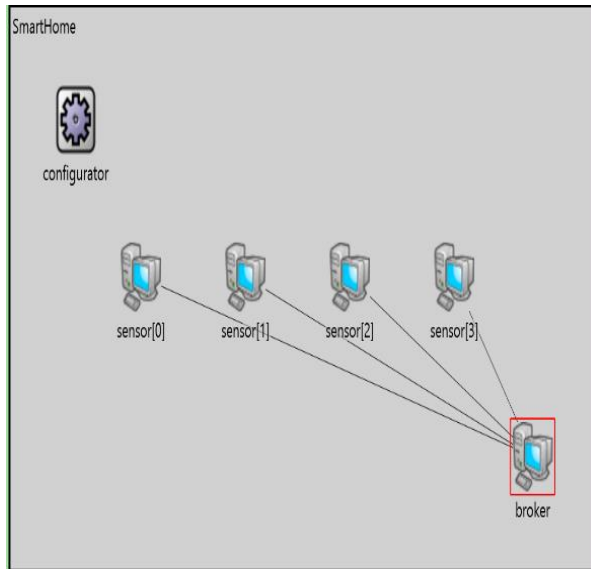


Figure 4: Showing IoT sensors and the broker in the smart home network are connected

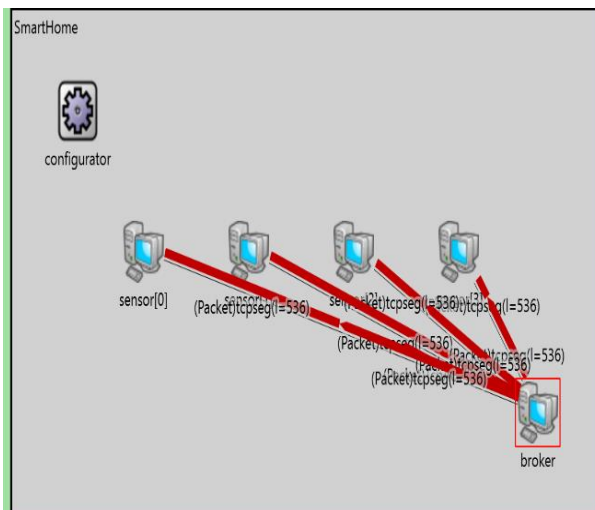


Figure 5: Simulation runtime visualization showing packet transmission between IoT sensors and the broker in the Smart Home Network

h. Data Collection and Analysis

During simulation, Omnet++ collected data using the inet framework's statistical modules. Key performance data (latency, throughput, PDR) were exported in csv format for post-processing.

Data analysis followed three steps:

- i. Aggregation: raw statistics were aggregated across multiple simulation runs.
- ii. Visualization: python plotting libraries were used to generate graphs, enabling visual comparisons among the protocols.

- iii. Comparative analysis: results were compared against each other to determine relative performance strengths and weaknesses.

3.0 RESULTS AND DISCUSSION

The results of the simulation experiments conducted to evaluate the performance of four IoT communication protocols MQTT, COAP, AMQP, and HTTP in resource-constraints smart home network. The evaluation focuses on four key performance metrics: latency, throughput, packet delivery ratio (PDR) and energy consumptions. The results are presented using tables and graphs, followed by an in-depth discussion of the findings.

3.1 Latency

Latency refers to the average time taken for a packet to travel from an iot device to the gateway or server. In smart home applications, low latency is critical for time sensitive services such as motion detection alerts, fire alarms, and access control.

The latency evaluation shows that COAP achieved the lowest delay (30 ms), making it the fastest protocol in the experiment. MQTT followed with a moderate latency of 45 ms, indicating reasonably quick message delivery suitable for most smart-home applications. AMQP recorded a higher latency of 55 ms, reflecting additional processing overhead. Http produced the highest latency (110 ms), showing that it is significantly slower than the other protocols and less suitable for delay sensitive IoT tasks.

Table 2: Average Latency of Protocols

S/N	Protocols	Latency(Ms)
1	COAP	30
2	MQTT	45
3	AMQP	55
4	HTTP	110

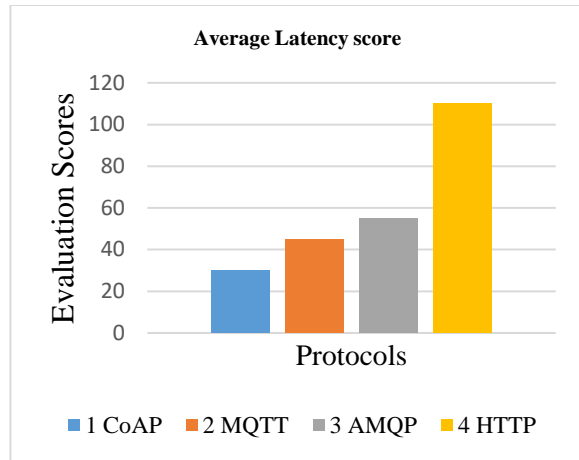


Figure 5: Average Latency Of Protocols

3.2 Throughput

Throughput measures the rate at which data is successfully delivered over the network. High throughput is desirable in smart homes where multiple devices operate simultaneously, generating diverse data streams.

The throughput evaluation presented in table 3, reveals significant variation in the data handling capacity of the four IoT communication protocols. Http recorded the highest throughput at 152.8 kbps, which is expected due to its verbose message structure and connection-oriented operation that enables larger payload transfer. AMQP followed with a moderate throughput of 19.4 kbps, benefiting from its message queuing and routing capabilities that support higher data exchange rates. In contrast, MQTT 7.8kbps and COAP 4.10kbps delivered substantially lower throughput, reflecting their lightweight architectures designed primarily for low-power, constrained environments. These findings indicate that while http and amqp support higher data rates, MQTT and CoAP prioritize efficiency and minimal overhead, making them more suitable for scenarios where bandwidth and energy conservation are critical.

S/N	Protocols	Throughput (Kbps)
1	COAP	4.10
2	MQTT	7.8
3	AMQP	19.4
4	HTTP	152.8

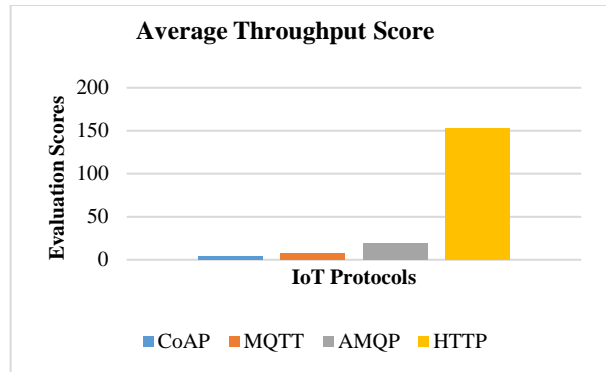


Figure 6: Average Throughput of Protocols

3.3 Packet Delivery Ratio (PDR)

PDR represents the percentage of successfully delivered packets compared to the total transmitted packets. High PDR indicates reliable communication, which is essential for smart home safety and automation.

The packet delivery ratio (PDR) results in table 4 show that MQTT and HTTP achieved the highest reliability with a perfect delivery rate of 100%, indicating that all transmitted packets successfully reached their destination. AMQP also demonstrated strong reliability with a pdr of 97%, while CoAP recorded a slightly lower PDR of 96%, reflecting minor packet losses likely attributed to its UDP-based operation. Overall, the results indicate that all four protocols exhibit high delivery performance, with MQTT and HTTP offering the most consistent packet reliability under the simulated conditions.

S/N	Protocols	DPR%
1	COAP	96
2	MQTT	100
3	AMQP	97
4	HTTP	100

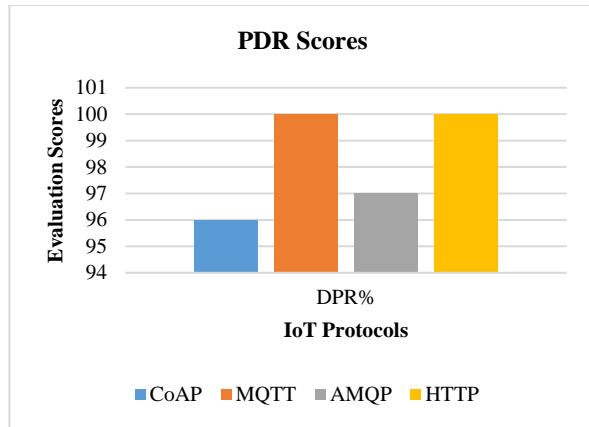


Figure 7: Packet Delivery Ratio of Protocols

3.4 Energy Consumption

Energy consumption refers to the total electrical energy expended by smart home IoT devices during communication, processing, sensing, and idle operations. It quantifies the amount of power required for devices to reliably exchange data and maintain network connectivity. Lower energy consumption improves battery lifetime, reduces operational cost, and enhances sustainability within smart home networks.

The energy consumption results in table 5 indicate substantial differences in the power efficiency of the evaluated IoT protocols. CoAP demonstrated the lowest energy usage at 1.9 j per sensor, highlighting its suitability for highly constrained, battery-powered smart-home devices. MQTT followed with a moderate consumption of 2.8 j, reflecting its lightweight design balanced with tcp-based reliability. AMQP consumed 3.4 j, indicating higher processing and communication overhead due to its message-oriented architecture. Http recorded the highest energy consumption at 4.9 j, confirming its poor suitability for low-power IoT environments. Overall, the results show that CoAP and MQTT are the most energy-efficient protocols, whereas http is the least optimal for energy-constrained applications.

Table 5: Energy Consumption of Iot Protocols

S/N	Protocols	Energy Per Sensor (J)
1	COAP	1.9
2	MQTT	2.8
3	AMQP	3.4
4	HTTP	4.9

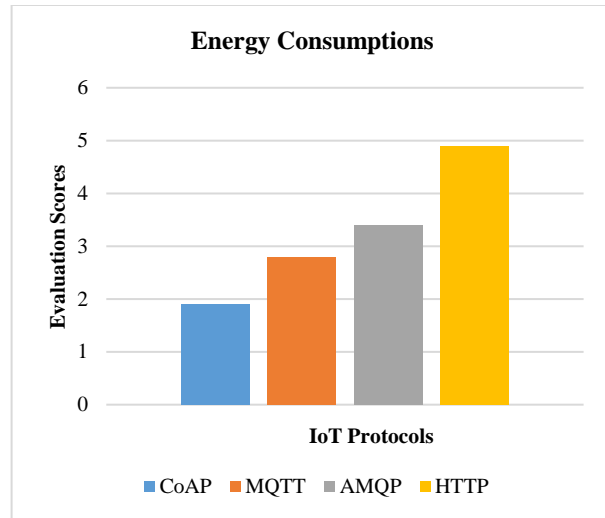


Figure 7: Energy Consumption

4.0 DISCUSSION OF RESULTS

i. Latency

Latency differences across protocols clearly reflect their underlying transport mechanisms. CoAP, which operates over UDP, achieves the lowest latency 30ms. The outcome a UDP eliminates connection establishment overhead and supports minimal packet headers, enabling rapid message exchanges. The performance advantage positions CoAP as a strong candidate for time sensitive applications, such as real-time sensor alerts or actuator commands.

In comparison, with TCP based protocols MQTT, AMQP, and HTTP demonstrate progressively higher latency, with http recording the highest delay at 110ms. The increase is attributed to TCP reliability mechanisms, including retransmissions, congestion control, and session establishment, which introduce additional processing time. HTTP request response architecture and larger payload structures further contribute to delay increments. Consequently, while these protocols ensure delivery reliability, their increased latency may limit applicability in real-time smart home operations.

ii. Throughput

Throughput, which measures the rate of successful data delivery over the network in bits per second (bps), provides insight into the bandwidth utilization and data-handling efficiency of each protocol. Throughput results further DISTINGUISH protocol capabilities. Http achieves the highest throughput 152.8kbps, a direct

result of its larger message size and extensive header structure. However, high throughput does not necessarily equate to efficiency in IoT environments rather, it reflects the protocols use of heavier data exchanges.

AMQP 19.4kbps and MQTT 7.8kbps display moderate throughput levels, benefiting from TCP reliability while maintaining smaller frame sizes than http. CoAP records the lowest throughput 7.8kbps, consistent with its lightweight architecture and compact message format. In the context of smart homes, where data transmissions typically consist of short sensor updates, high throughput is often less important than efficiency, scalability, and power savings. Thus, throughput advantages for http and AMQP may be beneficial for multimedia or bulk data applications, but unnecessary for simple telemetry traffic.

iii. Packet Delivery Ratio (PDR)

The packet delivery ratio (PDR), defined as the ratio of successfully delivered packets to the total number of packets transmitted, serves as a measure of communication reliability. PDR results reflect the reliability guarantees inherent in each protocol. MQTT and http achieve perfect delivery rates 100% supported by TCP built-in acknowledgment and retransmission mechanisms. These results validate their suitability in scenarios requiring high delivery assurance, including mission critical monitoring systems or event logging applications.

Amqp maintains a high PDR 97%, indicating strong reliability with minor packet loss. The slightly reduced delivery rate may stem from higher protocol overhead or queue handling delays in the simulated environment. CoAP, with a PDR of 96%, records the lowest reliability among the protocols due to Udp's lack of guaranteed delivery. Nonetheless, the performance remains acceptable for applications where occasional packet loss does not compromise system functionality, such as periodic sensing in smart thermostats or environmental monitoring.

iv. Energy Consumption

Energy consumption is a critical factor in smart home networks, particularly for battery-powered sensors. The results show that CoAP consumes the least energy 1.9j, aligning with its lightweight, connectionless nature. The minimal overhead reduces transmission time, ultimately conserving

power. This reinforces coap's suitability for long-lived, low-power devices.

MQTT 2.8j demonstrates moderate energy consumption, balancing reliability and power efficiency. Its publish-subscribe model reduces redundant traffic, contributing to its favorable energy profile relative to AMQP and HTTP. AMQP 3.4j requires more energy due to its complex message-queuing operations and larger protocol headers. Http exhibits the highest energy consumption 4.9j, a reflection of its verbose header format, larger data payloads, and persistent TCP sessions. For energy-constrained IoT deployments, HTTP is therefore the least appropriate choice, despite its widespread adoption in traditional web services.

4.2 Comparative analysis with the existing literature

A comparative analysis of the proposed performance evaluation results was conducted with the existing results obtained from the literature in order to prove the efficiency and reliability of the proposed technique. The results in table 6, are comprehensively reporting the performance of each protocols based on latency, throughput, packet delivery ratio, and energy consumption.

Table 6. Average performance evaluation results for IoT Protocols

S/N	Protocols	Latency (Ms)	Throughput (Kbps)	PDR (%)	Energy Consumption (J)
1	COAP	30	7.8	96	1.9
2	MQTT	45	3.62	100	2.8
3	AMQP	55	9.4	97	3.4
4	HTTP	110	152.8	100	4.9

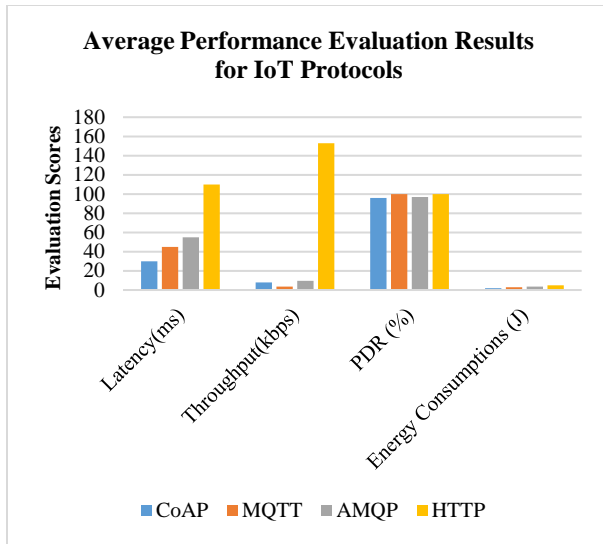


Figure 8: Average Performance Evaluation Results For Iot Protocols

The latency results in table 6 show that CoAP achieves the lowest latency 30ms, followed by MQTT 45ms, AMQP 55ms, and http 110ms. These findings strongly align with existing literature, which consistently reports that coap's lightweight, UDP based architecture enables faster request response cycles compared to MQTT and HTTP. For instance, prior empirical studies demonstrate that CoAP outperforms both MQTT and HTTP in constrained networks because it eliminates TCP session establishment delays and reduces protocol overheads. This is consistent with the literature in (sidna & alami, 2020), which found that CoAP delivered the lowest latency among tested protocols due to its minimal header size and direct messaging structure. Similarly, studies such as (bouzidi et al., 2022) reaffirm that protocols based on TCP, like http and MQTT, experience higher latency because of connection setup, acknowledgements, and larger payloads. Therefore, table 6 reinforces the widely accepted position that CoAP offers superior latency performance, particularly in resource-constrained iot environments.

Table 6 shows a contrasting trend in terms of throughput http produces the highest throughput 152.8 kbps, while AMQP 9.4kbps, CoAP 7.8kbps, and especially MQTT 3.62kbps achieve significantly lower throughput values. These results correspond with the literature emphasizing that HTTP, although heavy, can transmit large volumes of data because of its high overhead and connection persistence. As highlighted in (Shahinzadeh, 2024)(Md. Milton, 2022), HTTP suffers inefficiency in constrained networks, but its higher throughput reflects its ability to push more data rather than its suitability. Conversely, the

literature in (Toskov et al., 2021) shows that AMQP typically attains higher throughput than MQTT and CoAP, which aligns with the table results AMQP's structured messaging and broker-centric architecture enable it to achieve more consistent high-volume message delivery. CoAP's and MQTT's comparatively lower throughput in table 6, also mirror findings in (Shahrokhi & Ahmadi, 2024), where protocols optimized for lightweight operations naturally sacrifice throughput for reduced energy usage and lower overheads. Hence, the observed throughput trends match the documented trade-offs between protocol design and performance.

in table 6, MQTT and HTTP achieve a perfect packet delivery rate 100%, while AMQP 97% and COAP 96% follow closely. This distribution is consistent with literature that emphasizes MQTT strong reliability due to its publish-subscribe model and built-in qos levels. Studies such as (Bayilmiş et al., 2022) and (Chakraborty et al., 2023) report delivery rates of 99% and above for MQTT, demonstrating its robustness even under fluctuating network conditions. Http's 100% delivery rate in the table also aligns with findings that its tcp-based mechanism ensures guaranteed delivery through retransmissions and connection persistence, albeit at the cost of higher latency. COAP's slightly lower delivery rate is also consistent with empirical evidence: although COAP can achieve high reliability, its UDP foundation and optional confirmable messages mean it may drop some packets under congestion unless reliability extensions are activated. AMQP's moderately high delivery rate corresponds with its design for enterprise-grade messaging, where guaranteed delivery is a priority, but higher overhead can cause minor reductions in constrained IoT scenarios. Overall, the table supports the literature's consensus that protocols prioritizing reliability over speed (MQTT, HTTP, AMQP) tend to deliver higher packet success ratios.

The energy consumption outcomes in table 6, reveal that CoAP is the most energy-efficient protocol 1.9j, followed by MQTT 2.8j, AMQP 3.4j, and http 4.9j. These results align closely with multiple studies emphasizing that CoAP small message size, stateless interactions, and UDP transport significantly reduce energy requirements. Literature such as (Shahrokhi & Ahmadi, 2024) and (Ua et al., 2021) consistently demonstrates that COAP consumes substantially less power than MQTT and HTTP, with some studies showing up to a 50% reduction when COAP is integrated into an optimized configuration. MQTT, while slightly more energy-intensive due to TCP dependencies, still performs relatively efficiently compared to http, a trend supported by (Amirkhanov, 2025), where MQTT saved between

6.03% and 8.33% power relative to http. The higher consumption shown for AMQP and http in table 6, mirrors broader findings that both protocols involve heavier message structures and more complex connection handling. Therefore, the simulated outcomes align with the established literature emphasizing the energy-saving advantages of lightweight IoT protocols.

5.0 CONCLUSION

The study concludes that no single IoT communication protocol is universally optimal for all smart home applications. CoAP emerges as the most suitable protocol for smart home networks where low latency and energy efficiency are critical, owing to its lightweight UDP-based communication model. MQTT and HTTP offer the highest reliability due to their underlying TCP mechanisms, although this comes with trade-offs in delay and energy consumption. HTTP, despite being resource intensive, demonstrates the highest throughput capacity, making it applicable in smart home applications that require larger data transfers but are not constrained by energy or latency. AMQP maintains a balance between throughput and reliability but exhibits higher latency and energy usage, making it less optimal for highly constrained devices. The results confirm that selecting appropriate protocols based on application requirements significantly enhances network performance, reliability, and responsiveness in smart home IoT systems.

REFERENCES

- Afoluwaso Giwa, T., & Ajibola, A. (2024). A Secure Smart Home Automation System With Mobile Platform. *Article In Journal Of Computer Science And Information Technology*, 18(1), 8–21. <https://www.researchgate.net/publication/385717656>
- Amirkhanov, B. (2025). Evaluating Http , Mqtt Over Tcp And Mqtt Over Websocket For Digital Twin Applications : A Comparative Analysis On Latency , Stability , And Integration. 8(1), 679–694. <https://doi.org/10.53894/ijirss>.
- Bayılmış, C., Ebleme, M. A., Çavuşoğlu, Ü., Küçük, K., & Sevin, A. (2022). A Survey On Communication Protocols And Performance Evaluations For Internet Of Things. *Digital Communications And Networks*, 8(6), 1094–1104. <https://doi.org/10.1016/j.dcan.2022.03.013>
- Bhardwaj, T., Jain, A., Tembhekar, V., & Garg, M. (2021). Smart Homes Technologies, Connectivity Standards And Challenges. *Academia.Edu*, 11(2), 28–36. <https://doi.org/10.9790/9622-1102062836>
- Bouzidi, M., Gupta, N., Cheikh, F. A., Shalaginov, A., & Derawi, M. (2022). A Novel Architectural Framework On Iot Ecosystem, Security Aspects And Mechanisms: A Comprehensive Survey. *Ieee Access*, 10(September), 101362–101384. <https://doi.org/10.1109/Access.2022.3207472>
- Caro, N. De, Colitti, W., & Steenhaut, K. (2019). Comparison Of Two Lightweight Protocols For Smartphone-Based Sensing. January 2013.
- Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., & Hasan, M. (2023). Smart Home System: A Comprehensive Review. *Journal Of Electrical And Computer Engineering*, 2023. <https://doi.org/10.1155/2023/7616683>
- Comparing The Efficiency Of Lwm2m And Mqtt : Hands-On Test Results Of Two Technology Clients On A Typical Iot Device April 2020 Table Of Contents. (2020). April.
- Cui, P. (2017). Comparison Of Iot Application Layer Protocols. April, 63.
- D. Persson, P. Niklas, C. (2020). Performance Comparison Of Messaging Protocols And Serialization Formats For Digital Twins In Iov. December, 1785–1789.
- Divyashree, D. A., & Sujatha, B. R. (2020). Energy Management System For Office / Home Automation. 8(14), 20–24.
- Gemirter, C. B. (2020). A Comparative Evaluation Of Amqp , Mqtt And Http Protocols Using Real-Time Smart Home. 23(December), 1–6.
- Hadi, T. H. (2024). Eai Endorsed Transactions Iot Protocols : Connecting Devices In Smart Environments. 11(6), 1–12. <https://doi.org/10.4108/Eetsis.5665>
- Haman, S., Temoa, D., Michel, E., & Djomadji, D. (2024). Proposal For Energy Consumption Reduction Between Connected Objects In A Network Running On Mqtt Protocol. 177–188. <https://doi.org/10.4236/jcc.2024.1210012>
- Khaleefah, R. M., Abed, A. A., & Al-Shareeda, M. A. (2025). Empirical Evaluation Of Mqtt , Coap And Http For Smart City Iot Applications. 1(2), 74–81.
- Khan, A., Shirazi, S. H., Adeel, M., Assam, M., Ghadi, Y. Y., Mohamed, H. G., & Xie, Y. (2023). A Qos-Aware Data Aggregation Strategy For Resource Constrained Iot-Enabled Ami Network In Smart Grid. *Ieee Access*, 11(August), 98988–99004. <https://doi.org/10.1109/Access.2023.3312552>
- Lagervall, M. (2023). *Smart Home Protocols Architecture*. Book.
- Md. Milon, I. S. N. (2022). Internet Of Things Device Capabilities, Architectures, Protocols, And Smart Applications In Healthcare Domain: A Review. 9(June).
- Mofawiz, A. K. (2022). Iot Future Security Challenges And Recent Solutions. *Journal Of Information Technology Management*, 14(2), 1–14.

- Moraes, T., Nogueira, B., Lira, V., & Tavares, E. (2019). Performance Comparison Of Iot Communication Protocols. 2019 Ieee International Conference On Systems, Man And Cybernetics (Smc), 3249–3254.
- Naik, N. (2023). Choice Of Effective Messaging Protocols For Iot Systems: Mqtt,Coap, Amqp And Http. 9(November).
- Nur Issi, H. (2022). A Systematic Study Of Data Security Issues In Smart Home Iot Devices. University Of Alabama At Birmingham. <https://Digitalcommons.Library.Uab.Edu/Etd-Collection/579>
- Ochoa, H. J. J., Peña, R., Mezquita, Y. L., Gonzalez, E., & Camacho-Leon, S. (2023). Comparative Analysis Of Power Consumption Between Mqtt And Http Protocols In An Iot Platform Designed And Cold Chain Transport Operations.
- Pettersson, W. (2021). An Evaluation Of Iot Protocol Efficiency And Suitability. 1–52.
- Prasad, M. S. (2025). Efficient Power Management In Iot Communication Protocols. 7(3). <https://Doi.Org/10.21590/Ijhit.07.03.02>
- Sadikin, N., Sari, M., & Sanjaya, B. (2019). Smarthome Using Android Smartphone, Arduino Uno Microcontroller And Relay Module. Journal Of Physics: Conference Series, 1361(1). <https://Doi.Org/10.1088/1742-6596/1361/1/012035>
- Seoane, V., Garcia-Rubio, C., Almenares, F., & Campo, C. (2021). Performance Evaluation Of Coap And Mqtt With Security Support For Iot Environments. 197(June).
- Shafik, W., Matinkhah, S. M., Asadi, M., Ahmadi, Z., & Hadiyan, Z. (2020). A Study On Internet Of Things Performance Evaluation. April.
- Shah, A. G., Gaurav, A., Anand, A., & Shah, G. K. (2021). Home Automation System. 04, 1785–1789.
- Shahinzadeh, H. (2024). Smart Home Connectivity: Identifying The Best Iot Application Layer Protocols. March 2025. <https://Doi.Org/10.1109/Iccke65377.2024.10874634>
- Shahrokhi, A., & Ahmadi, M. (2024). Power Evaluation Of Iot Application Layer Protocols.
- Sidna, J., & Alami, H. E. L. (2020). Analysis And Evaluation Of Communication Protocols For Iot Applications. 3–8.
- Stolajescu-Crisan, C., Crisan, C., & Butunoi, B. (2021). Sensors-21-03784-V2.Pdf. 1–23.
- Tanishka And Prof. Shikha Gupta. (2020). Designing Smart Home (Iot) Using Cisco Packet Tracer 7.2 Simulator. International Journal For Modern Trends In Science And Technology, 6(12), 208–216. <https://Doi.Org/10.46501/Ijmtst061240>
- Toskov, B., Toskova, A., Bogdanov, S., & Spasova, N. (2021). Intelligent Management Of Iot Devices With Limited Connectivity. International Conference Automatics And Informatics, Icai 2021 Proceedings, September, 354–357. <https://Doi.Org/10.1109/Icai52893.2021.9639653>
- Ua, O. P. C., Silva, D., Carvalho, L. I., & Soares, J. (2021). Ppalied Sciences A Performance Analysis Of Internet Of Things Networking.
- Yahya, A., & Almihyawi, T. (2025). A Secure Smart Monitoring Network For Hybrid Energy Systems Using. Discover Computing. <https://Doi.Org/10.1007/S10791-025-09506-4>
- Yalçinkaya, F., Aydilek, H., Erten, M. Y., & İnanç, N. (2020). Iot Based Smart Home Testbed Using Mqtt Communication Protocol. Uluslararası Muhendislik Arastirma Ve Gelistirme Dergisi, 317. <https://Doi.Org/10.29137/Umagd.654056>