smart cities

MDPI

Review

Investigation of Data Quality Assurance across IoT Protocol Stack for V2I Interactions

Danladi Suleman [1], Rania Shibl [1,*] and Keyvan Ansari [2]

[1] School of Science, Technology and Engineering, University of the Sunshine Coast, UniSC Moreton Bay, Petrie, QLD 4502, Australia; danladi.suleman@research.usc.edu.au
[2] School of Information Technology, Murdoch University, Murdoch, WA 6150, Australia; keyvan.ansari@murdoch.edu.au
* Correspondence: rshibl@usc.edu.au

Abstract: Networking protocols have undergone significant developments and adaptations to cater for unique communication needs within the IoT paradigm. However, meeting these requirements in the context of vehicle-to-infrastructure (V2I) communications becomes a multidimensional problem due to factors like high mobility, intermittent connectivity, rapidly changing topologies, and an increased number of nodes. Thus, examining these protocols based on their characteristics and comparative analyses from the literature has shown that there is still room for improvement, particularly in ensuring efficiency in V2I interactions. This study aims to investigate the most viable network protocols for V2I communications, focusing on ensuring data quality (DQ) across the first three layers of the IoT protocol stack. This presents an improved understanding of the performance of network protocols in V2I communication. The findings of this paper showed that although each protocol offers unique strengths when evaluated against the identified dimensions of DQ, a cross-layer protocol fusion may be necessary to meet specific DQ dimensions. With the complexities and specific demands of V2I communications, it's clear that no single protocol from our tri-layered perspective can solely fulfil all IP-based communication requirements given that the V2I communication landscape is teeming with heterogeneity, where a mixture of protocols is required to address unique communication demands.

Keywords: data quality; IoT protocols; IP communication; V2I

Citation: Suleman, D.; Shibl, R.; Ansari, K. Investigation of Data Quality Assurance across IoT Protocol Stack for V2I Interactions. *Smart Cities* **2023**, *6*, 2680–2705. https://doi.org/10.3390/smartcities6050121

Academic Editor: Pierluigi Siano

Received: 12 August 2023
Revised: 25 September 2023
Accepted: 27 September 2023
Published: 6 October 2023

1. Introduction

Smart cities have continued to grow worldwide, giving rise to various innovations such as smart agriculture, smart buildings, smart health, and smart transportation. At the core of this growth is the Internet of Things (IoT) [1–3]. The shift to ubiquitous computing has led to the interconnection of smart and embedded devices, resulting in the generation of substantial amounts of data, aka "big data" [4]. The continuous increase in IoT-generated data underscores the critical importance of data quality (DQ) [5]. The success of this IoT paradigm shift relies heavily on DQ guarantees [6]. However, ensuring DQ under the current big data collection and transmission methods of IoT networks becomes a challenge for various applications. The multifaceted nature of big data, characterised by the five Vs, volume, velocity, variety, veracity, and value, are some of the constraints faced in ensuring data quality [7]. These complexities demand the adoption of meticulous data quality management methodologies encompassing comprehensive validation, cleaning, and integration techniques for big data applications in various smart city segments. DQ is essential across various domains of smart cities, including the cooperative intelligent transportation system (C-ITS), which is defined by its interactive components, facilitating various communications crucial for its operation. These components include communication between Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Pedestrian (V2P). The integration of communication technologies into

transportation has ushered in a transformative transference from autonomous systems to cooperative ones, which is an integral aspect of smart cities requiring high DQ for efficiency and effectiveness. Communications between these components of C-ITS are reliant on several protocols to transmit data between nodes, and hence, the need to ensure DQ within each of the protocols is paramount.

Over the past three decades, network protocols have defined and maintained principles of data communications and provided foundational protection for data transmission [8]. With the emergence of IoT, network protocols have experienced an evolution due to the dynamic and constrained nature of IoT devices and networks. Such characteristics pose a major challenge, as identified by Shang et al. [9], in integrating the existing Transmission Control Protocol/Internet Protocol (TCP/IP) [10] in IoT networks. Despite these challenges, IoT supports interoperability with the TCP/IP protocol stack, which, however, faces some drawbacks such as throughput, link delay, and energy consumption—are metrics that the current TCP/IP protocol stack struggles to meet in IoT applications. Furthermore, without optimisation, the TCP/IP protocol stack is inadequate for IoT communications within the cloud and distributed computing services [11]. To mitigate these challenges, suitable and lightweight IoT protocols have been revealed in the literature as fixable alternatives for constrained devices [12]. These advancements have led to the application of IoT in transportation to increase road safety and enhance cooperative driving and traffic management [13]. However, vehicular communications must be precise, which requires advanced embedded DQ measures to achieve efficiency, safety, and sustainability. Some protocols in the TCP/IP protocol stack do not meet specific criteria, such as ensuring the dimensions of DQ for vehicular communications. For example, certain protocols lack agility, while others are unreliable or vulnerable to cyber-attacks, which impedes the accurate flow of data in vehicular communications.

Vehicular communication networks are still an active area of research [14,15], although several technologies have emerged to support C-ITS. V2I, specifically, is an integral part of vehicular communication technologies that promises to optimise the efficiency of transportation systems. V2I communications span a wide range of applications, including safety and non-safety related. V2I safety applications include collision warning, emergency vehicle priority, driver assistance and road hazards warming, and speed and intersection warning messages, all aimed at preventing road crashes and enhancing mobility [16]. Meanwhile, non-safety applications focus on traffic efficiency and optimisation, remote vehicle diagnostics, air pollution monitoring and onboard infotainment [17]. These diverse arrays of applications stem from various components, technologies and data types involved in the interconnected V2I ecosystems. These applications are facilitated using Dedicated Short Range Communication (DSRC) [18] and Cellular-Vehicle-to-Everything C-V2X technologies [19]. The DSRC and C-V2X technologies establish a communication link between Onboard Units (OBU) and Roadside Units (RSU) [20]. An OBU, which is mounted on vehicles, allows communication with other OBUs and RUSs [21]. RSUs are part of the infrastructure which are strategically positioned along road networks to serve as communication nodes or access points for exchanging vital information with trusted authorities for traffic management [22]. Collectively, this ecosystem exchanges data for time-critical, urban planning, and infotainment use cases with the aim of revolutionising and redefining road transportation to improve road safety, comfort, and efficiency. Figure 1 shows the V2I communications landscape.

The success of the V2I communications ecosystem hinges heavily on the quality of data being exchanged and, hence, the importance of assuring DQ in V2I interactions. Vehicular communication has a plethora of use cases, and some of these use cases have a unique and customised protocol stack. Some use cases in V2I communications are time-sensitive or time-critical. Delayed or incomplete data can result in vehicles receiving inaccurate information, potentially leading to catastrophic outcomes. Therefore, ensuring DQ in V2I communication scenarios is of paramount importance. This research aims to investigate

the most viable IoT protocols for V2I communications, ensuring DQ across the application, transport, and Internet layers.

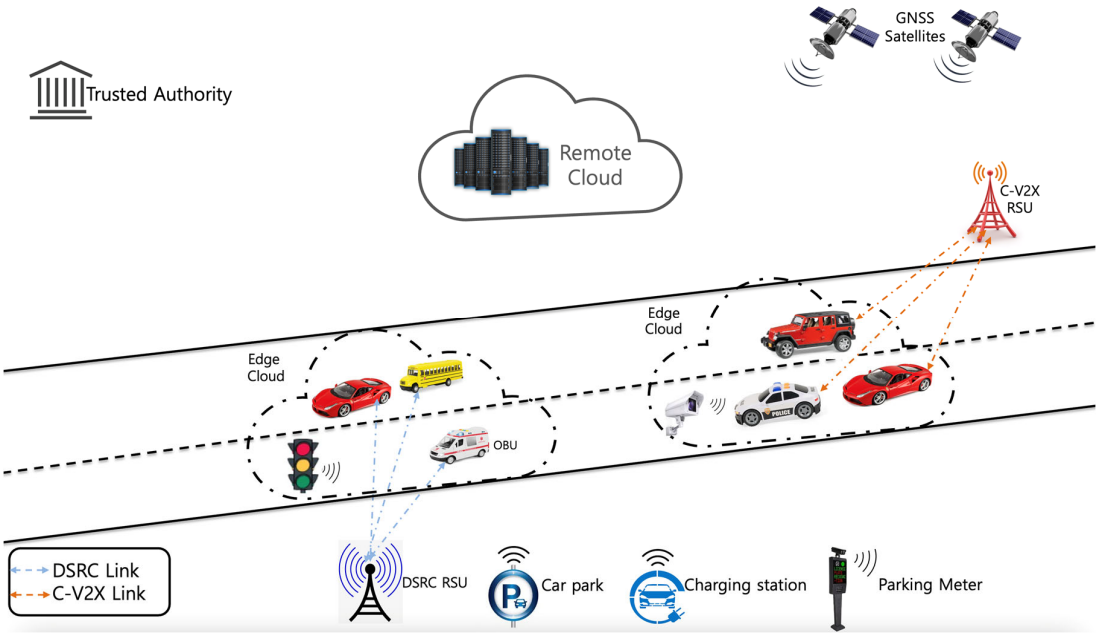


Figure 1. Heterogeneous V2I communications.

This research makes the following contributions:

- Presents an unconventional viewpoint on the IoT protocol stack, underscoring the drawbacks of depending solely on a single protocol/layered approach for ensuring reliable data transmission within IoT applications.
- Provides a support framework with a focus on DQ for identifying and selecting suitable IoT protocol stack for a specific use case requiring efficient data transmission within the V2I ecosystem and IoT applications in general.
- Presents a structured way of organising and customising the IoT protocol stack, making it easier to pinpoint areas for adaptation and optimisation.

The rest of the paper is structured as follows. Section 2 presents a summary of data quality and related dimensions. An overview of network protocols is presented in Section 3. Section 4 presents a survey of the IoT protocol stack. Section 5 presents the research methodology. Section 6 presents findings and discussion. The conclusion is presented in Section 7.

2. Data Quality and Related Dimensions

There is no universally established definition for DQ since the concept is subjective to the user, the domain, and the context of the use case [23]. Thus, providing DQ continues to pose a challenge for developing and deploying the various components of smart cities [24–26]. Due to constant changes in big data characteristics [7,27,28], the demand for DQ continues to change. In the context of C-ITS, we define DQ dimensions as data characteristics that assess the suitability of data for a specific use case.

2.1. Accuracy

We define accuracy as the precision and correctness of data while it is being transmitted from source to destination. The primary objective is to maintain the precision and integrity of data during transmission, preventing any loss, errors, or compromise. Localisation accuracy is an example of a use case to support automated driving systems [29]. Another use case example can be seen in a real-time map update using an MQTT network proposed by Szántó et al. [30] to accurately support trajectory planning.

2.2. Availability

Availability refers to the continuous and uninterrupted data flow between systems or devices in real-time. It ensures that data remains readily available and immediately accessible after transmission, free of interruptions, delay, or loss. A typical use-case example within V2I is incident detection and reporting. As observed by Bhatti et al. [31], inefficient accident detection and reporting systems have resulted in an increase in the number of fatalities from auto crashes. The authors proposed an accident detection and reporting system (ADRS) using Wi-Fi or 3G/4G to transmit and report vehicle telemetry data from a crash site to an emergency response unit and a nearby hospital.

2.3. Completeness

Completeness refers to the extent to which all relevant and necessary data elements are included and conveyed in data exchange. It guarantees that no critical information is lost on transmission, enabling a comprehensive comprehension of the transmitted data for effective use. Completeness is an important characteristic of DQ and one of the essential DQ dimensions. For data to be considered complete, it must meet the requirements of its intended application. Completeness impacts other DQ dimensions, including accuracy, consistency, and timeliness [32]. Kaneyasu et al. [33] proposed a transmission control mechanism that considers data completeness of large Spatial-temporal data. (STD). In their scheme, each node keeps accounts of received packet statuses and dispatches the information only when all packets have been accounted for, thereby minimising2 unnecessary transmission and optimising wireless bandwidth. STD combines geographical locations and timestamps to provide insights. It is worth noting that there is a plethora of applications in V2I interactions, ranging from traffic management applications to location-based services.

2.4. Confidentiality

Confidentiality pertains to safeguarding privacy and preventing unauthorised access to sensitive data during transmission. It ensures that sensitive or private information remains protected and inaccessible to unauthorised entities. A secure and reliable routing approach for mobile networks was proposed by Bhalaji [34], using cryptography and the Euclidean Distance formula for confidentiality, reliability, and integrity in data transmission.

2.5. Consistency

Refers to preserving coherence and uniformity of data throughout the data circle. It involves maintaining data integrity, a consistent format, meaning, and structure during transmission between sending and receiving nodes. Consistency is crucial for accurate interpretation and reliable utilisation by intended recipients. A beneficial use-case example in V2I is a beacon message broadcasting where homogeneity in broadcast messages is essential to relay important/emergency communications. As observed by Liu et al. [35], spatial consistency is fundamental in supporting the targeting and effective distribution of beacon messages to vehicles within the proximity of infrastructure elements, ensuring seamless communication in V2I scenarios.

2.6. Data Integrity

Refers to the assurance that data remains unaltered, complete, and reliable throughout its transmission process. It ensures that data is not tampered with, modified, or corrupted during its exchange, maintaining its accuracy and trustworthiness. Integrity is measured using data conformity to defined protocols, information assurance principles, and standards [36]. Gopinath, Vinoth, and Jaya [37] proposed a protocol to support data integrity, using location integrity and multicasting to secure data transmission.

2.7. Reliability

Pertains to the dependability and consistency of data in transmission. It focuses on ensuring that data is delivered accurately and consistently without loss, errors, or disruptions. Ensuring packet delivery reliability depends on multiple factors. The utilisation of a retransmission-based recovery mechanism and packet loss awareness leads to congestion and routing failure awareness protocols to guarantee packet reception [38]. These reliability-centric initiatives in protocol communications are pivotal in achieving accurate and effective data transmission, contributing to overall performance and reliability in V2I interactions and communication networks in general.

2.8. Timeliness

Timeliness refers to the prompt and timely delivery of data within a specified time, ensuring its relevance and currency for the intended use. Timeliness underscores the significance of transmitting and receiving data within predefined time boundaries, catering to the demands of real-time or time-sensitive applications. Timeliness measures the currency of data. That is when data was generated and arrived at the destination [39]. The timeliness dimension has received a lot of attention in IoT protocol research and is one of the most important dimensions in V2I interactions to facilitate communications for various use cases, such as emergency warning messages, pedestrian safety messages and traffic signal pre-emption, which are safety-critical V2I communications.

2.9. Traceability

Traceability refers to accurately documenting and tracking the provenance of data from source to destination [40]. It involves capturing and maintaining a comprehensive audit that identifies data sources, including the entities that have accessed or modified the data and the timestamps of these activities. Integrating traceability in a system will offer better security management, safety management, better response to crises, and overall strengthen the performance and coordination of the system [41]. The traceability dimension will benefit V2I use case examples like Pseudonym resolution [42,43].

2.10. Validity

Validity refers to the quality and trustworthiness of transmitted data. It ensures that data is legitimate, accurate, and conforms to predefined criteria, standards, or specifications. Various methods determine data validity, including accuracy, timeliness, and usability [44]. In addition, validity assesses the fitness of data for the desired purpose.

3. Overview of Network Protocols

Technological advancements and evolution in various IoT applications have spurred the development of various lightweight protocols and adaptation of some of the existing TCP/IP protocol stack to improve communication in IoT networks [9]. Several studies have addressed shortcomings of the conventional TCP/IP protocol stack in fulfilling the fast-paced real-time data transmission requirements of vehicular communications [45,46]. In addition, the TCP/IP protocol stack was originally designed for best-effort delivery of packets across the internet and does not support a fine-grained Quality of Service (QoS) coveted in IoT networks. The TCP/IP protocol stack faces significant challenges in effectively interfacing with cloud computing and distributed computing services without adaptation [11], which is critical for managing the enormous amounts of data generated by vehicular networks. In contrast, IoT protocols have demonstrated exceptional performance in seamlessly integrating with cloud services and have demonstrated compatibility with heterogeneous protocols [47]. This section provides an overview of the existing structures of the TCP/IP protocol stack and the new IoT protocol stack, solely focusing on the application, transport, and Internet layers. The network access layer (Data Link and Physical layers) can operate efficiently irrespective of the underlying technologies deployed at the layers above [48]. Figure 2 Shows the IoT protocol stack.

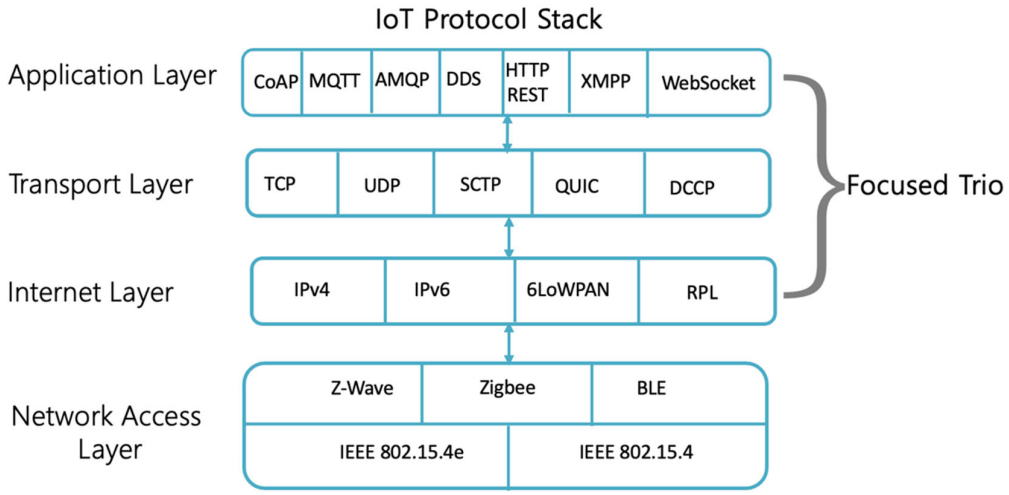


Figure 2. IoT Protocol Stack.

3.1. Application Layer

The application layer sits at the top of the communication protocol suite, irrespective of the prevailing network environment or conditions. It is an abstract layer that contains a combination of protocols to facilitate and define how applications communicate with others. In addition, these protocols specify how data is formatted, transmitted, and received. Hypertext transfer protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Domain Name Server (DNS) are some of the most popular TCP/IP application protocols. Most TCP/IP application protocols operate on a client-server model, in which a client device sends a request to the server, and the server acknowledges and responds with the required information [49]. This method works well with a typical client-server architecture. Meanwhile, the demands for real-time communication in the IoT domain require more efficient application protocols. Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Extensible Messaging, Presence Protocol (XMPP), Data Distribution Service (DDS), and WebSocket have been developed and upscaled to address these fast-paced communications in IoT applications by providing publish-subscribe or request-reply communication architecture which can reduce latency and provide communication improvements in IoT systems [50]. Some of these IoT protocols support different QoS, ensuring that communication in the IoT environment receives the necessary performance level to meet operational requirements, including interoperability and scalability.

3.1.1. Constrained Application Protocol

CoAP is a lightweight protocol apt for the ever-increasing Machine-to-Machine (M2M) communications in resource-constrained environments [51]. Supporting specific features suitable for V2I communication, this protocol implements a request-response architecture between application endpoints, which supports QoS that ensures reliable transmissions, simple congestion control, and flow control. In addition, CoAP underpins asynchronous message exchange and offers a built-in discovery of services and resources. Furthermore, the protocol implements an optional subscription mechanism for resource observation. The CoAP protocol operates a client-server model like TCP and relies on UDP as the underlying transport protocol, establishing a robust connection that ensures reliable communication even in dynamic and intermittent connected environments, such as those with high-speed connectivity and rapidly changing topologies. CoAP's compatibility with mobility management [52] further enhances its capability to handle high mobility-related and handover challenges. Refer to Figure 3 for CoAP architecture.

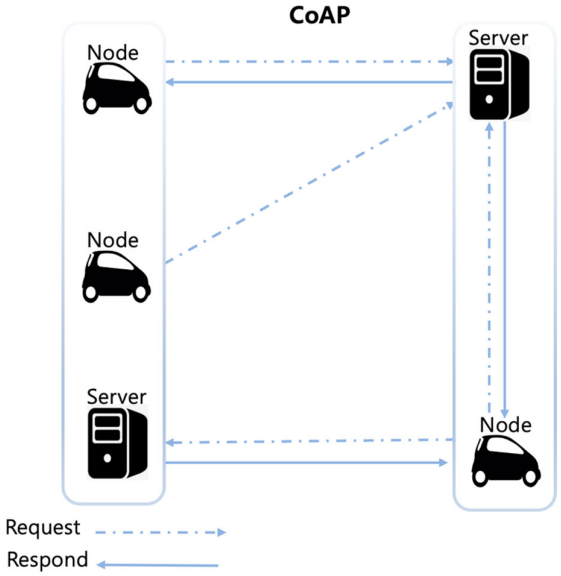


Figure 3. CoAP architecture.

3.1.2. The Message Queuing Telemetry Transport

MQTT is a lightweight protocol designed and used in a plethora of IoT applications and M2M communications [53], utilising the publish/subscribe architecture, which is well-suitable for remote connections with limited network bandwidth and system resources. This model facilitates efficient data dissemination techniques. Its ability to process massive volumes of data concurrently while consuming little bandwidth becomes an asset in V2I communications, where real-time, widespread information sharing is critical. Furthermore, MQTT's QoS levels ensure message delivery, which is critical in the context of traffic safety and infrastructure coordination. The protocol supports scalability, which aligns well with the requirements of the V2I environment that necessitates efficient and dynamic connectivity between a multitude of clients and a central broker. The broker plays an integral role in the MQTT network, effectively managing a catalogue of topics, e.g., traffic information and weather conditions, that function akin to communication channels. These topics facilitate the publishing and subscription of messages, thereby orchestrating the flow of information within the V2I domain. Specifically, when a client publishes a message on a given topic, the broker ensures this message reaches all clients subscribed to that specific topic. The multi-topic subscription capability of MQTT [54] provides clients with the advantage of receiving messages from diverse sources, enhancing the scope and versatility of information dissemination within the context of V2I. Refer to Figure 4 for MQTT architecture.

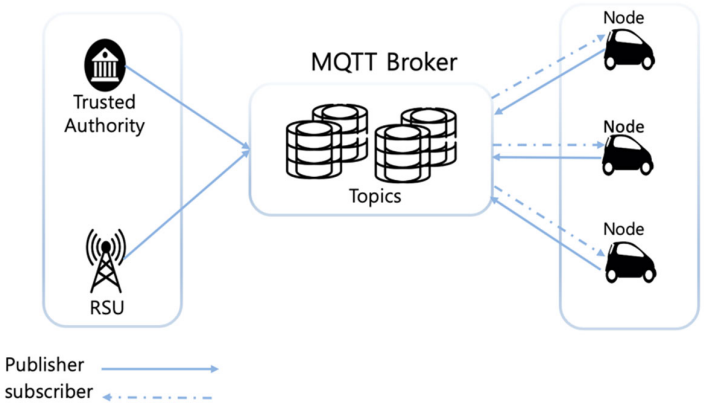


Figure 4. MQTT architecture.

3.1.3. Data Distribution Service

DDS protocol is a communication standard designed for messaging and data-centric exchange in distributed systems, and the protocol dynamically discovers a new node within a network architecture such as Vehicular Ad Hoc Network (VANET) and Mobile Ad Hoc Network (MANET) [55]. DDS uses the publish-subscribe architecture, allowing publishers to disseminate data to multiple subscribers asynchronously and in a decoupled manner. DDS is characterised by its support for real-time and high-performance communication, achieved using a decentralised architecture with a focus on data-centric principles. In the context of V2I applications, supporting high data rates and low latency requirements, enabling a single node to subscribe and receive information from multiple sources bi-directionally, facilitating effective communication. In addition, DDS is a highly functional middleware that is suitable for a multitude of V2I communication that supports efficient distributed communication. This protocol's inherent features, such as its reliable communication, scalability, interoperability, and flexible configuration of various QoS settings, make it a suitable option for V2I applications. Refer to Figure 5 for DDS architecture.

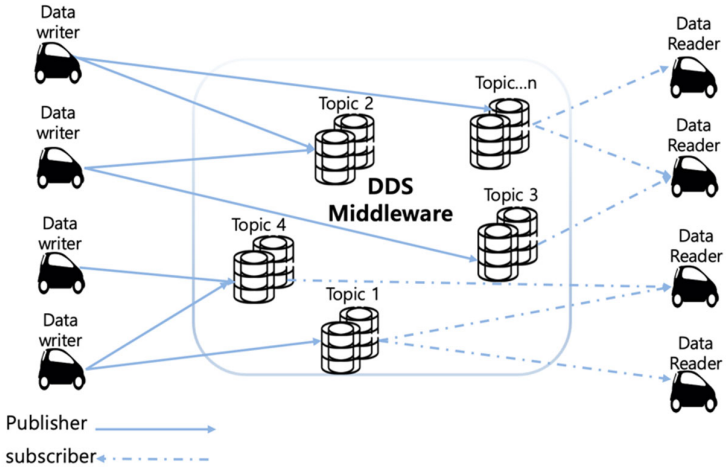


Figure 5. DDS architecture.

3.1.4. Extensible Messaging and Presence Protocol

XMPP is an XML-based protocol designed for real-time, extensible communications. Originally designed for communication on the internet with ample resources, XMPP has now found relevance in the field of IoT applications owing to its distinctive attributes [56]. The protocol's decentralised architecture promotes heterogeneous and federated communication by facilitating seamless communication between servers and clients. XMPP also support the publish-subscribe communication model, facilitating the simultaneous broadcasting of messages to multiple nodes [57]. The extensibility and decentralised characteristics present distinct advantages in V2I communication, enabling the management of diverse communication services, including real-time traffic monitoring, as noted by Hayes and Omar [58]. XMPP could enable immediate communication of safety alerts or evacuation instructions from central control units to all vehicles in a specific geographic location. The flexibility of XMPP also supports the potential for future expansions or adaptations as the requirements of the V2I communication system evolve. Refer to Figure 6 for XMPP architecture.

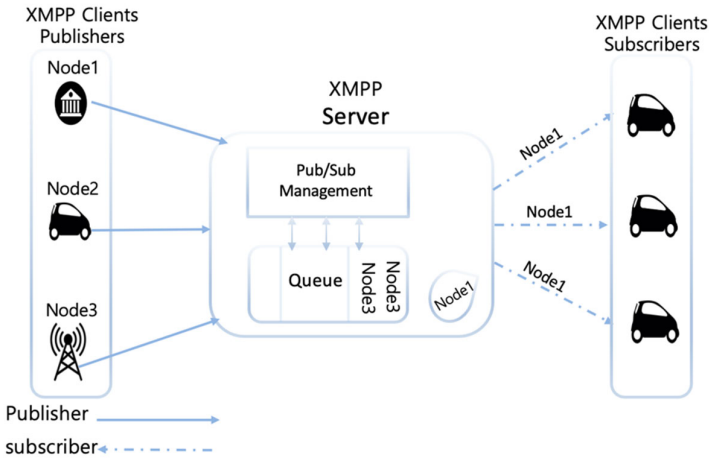


Figure 6. XMPP architecture.

3.1.5. Advanced Message Queuing Protocol

AMQP is an open-standard application layer protocol designed and tailored to support communication in a distributed environment [59]. AMQP supports various messaging models such as point-to-point, publish-and-subscribe, and request-reply, providing flexibility in designing distributed systems and enabling effective message-based communication. The core feature of AMQP is the guaranteed delivery of messages with its store-and-forward feature that ensures reliability [60]. This utilitarian feature is paramount in a V2I communication environment where real-time messages are important for the successful operation of the entire system. Refer to Figure 7 for AMQP architecture.

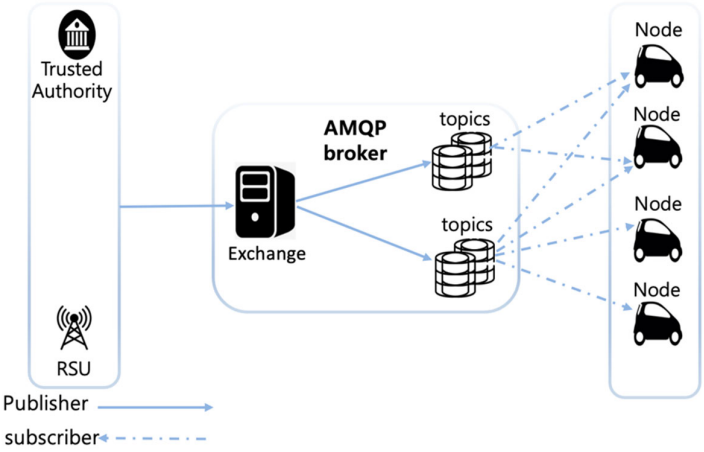


Figure 7. AMQP architecture.

3.1.6. HTTP REST

Representational State Transfer (REST), often referred to as HTTP REST, is an architectural-style protocol widely employed in web development [61]. It adheres to the principle of statelessness, where every HTTP request includes all the essential information needed to comprehend and handle the request. REST employs GET, POST, PUT, and DELETE methods for various operations. This protocol is well suited for scenarios where a vehicle node periodically requests information from a server or sends occasional updates. Hireche, Dennai, and Kadri [62] present a GET method to disseminate and visualise real-time traffic data over REST vehicle web service. This architecture is characterised using clear client-server segregation, with the client handling the user interface and experience and the server managing data [63]. Refer to Figure 8 HTTP REST Architecture.

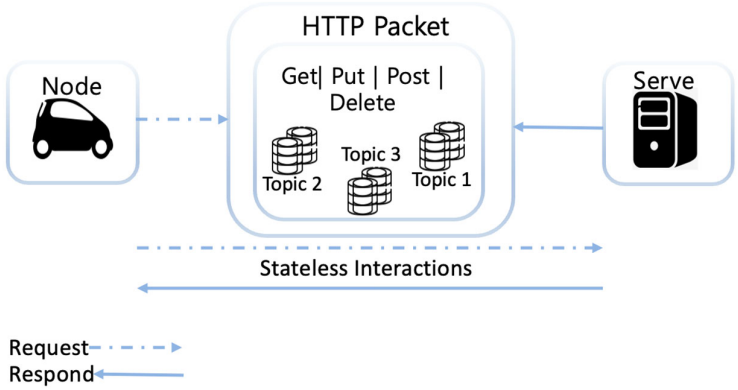
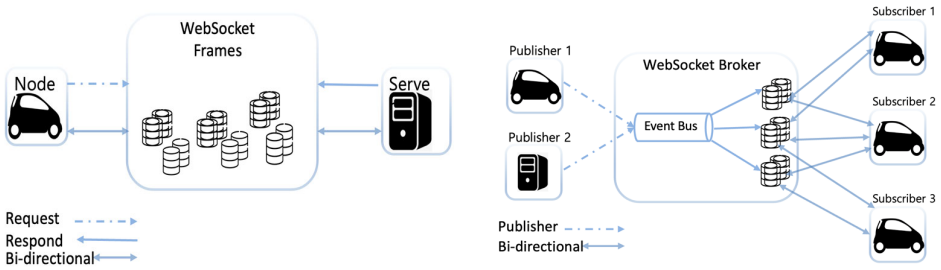


Figure 8. HTTP REST Architecture.

3.1.7. WebSocket

Established by the Internet Engineering Task Force (IETF) in 2011, WebSocket facilitates continued full-duplex communication over a single TCP connection. Initially designed for web servers and web browsers, WebSocket has gained increasing popularity in IoT applications [64,65]. Contrasting HTTP's request-response model, WebSocket supports both the request-respond and publish-subscribe model using real-time data transfer, thus enabling servers to provide continuous updates to clients via an ongoing WebSocket connection. This dynamic capability is particularly important in IoT applications and is integral for V2I applications requiring sustained data exchange for real-time analytics and decisions. The real-time data transfer capability of WebSocket is particularly valuable in V2I use cases requiring bi-directional communications and interaction between vehicles and infrastructural elements like roadside units or traffic control centres [66].

For instance, WebSocket is suitable for facilitating instantaneous relay of traffic light status to oncoming vehicles, enabling them to adjust their speed or plan alternate routes, thereby improving traffic efficiency and safety. Refer to Figure 9a for publish and subscribe architecture, Figure 9b for request and respond architecture, and Table 1 for the characteristics of application layer protocols.



(**a**) (**b**)

Figure 9. (**a**) WebSocket Req/Res Architecture, (**b**) WebSocket pub/Sub Architecture.

3.2. Transport Layer

The Transport Layer plays a crucial role in ensuring the successful delivery of data packets to the destination. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the two traditional transport protocols. TCP is a reliable, connection-oriented protocol that guarantees the delivery of data packets to the intended destination. It is a heavyweight protocol with high packet overhead. Conversely, UDP is a connectionless protocol that lacks reliability in data transmission. While UDP does not provide guaranteed packet delivery, it is known for its speed and is used for applications that can tolerate packet loss during transmission. With the introduction of innovative transport protocols like SCTP [67], DCCP [68], and QUIC [69], the transport layer has attracted significant research

interest. Additionally, there have been efforts focused on the performance optimisation of traditional transport protocols [70] as well as congestion and error control [71]. The development of new protocols and upscaling of the traditional transport layer protocols are crucial in enabling reliable and efficient communication in the rapidly evolving IoT paradigm.

Table 1. Characteristics of application layer protocols.

	CoAP	**MQTT**	**HTTP REST**	**AMQP**	**XMPP**	**WebSocket**	**DDS**
Transport	UDP	TCP	TCP	TCP	TCP	TCP	TCP/UDP
Security	DTLS	SSL	TLS	TLS	TLS	SSL/TLS	SSL/TLS
Model	Req-Rep	Pub-Sub	Req-Rep	Pub-Sub	Pub-Sub Req-Rep	Pub-Sub	Pub-Sub
QoS	Yes	Yes	No	Yes	No	No	Yes
Architecture Style	Client-Server	Broker	Client-Server	Broker	Client-Server	Client-Server	Distributed
Interoperability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Discovery	Yes	No	No	No	NA	No	Yes

3.2.1. Datagram Congestion Control Protocol

In 2006, DCCP [68] was standardised by IETF to support applications that require timely delivery of data packets, an inherent feature of UDP, also benefiting from the congestion control mechanisms of TCP. DCCP aims to reduce network congestion while enabling speedy data transfer between nodes. It achieves this by offering an unreliable flow of datagrams with congestion control mechanisms in place. DCCP is specifically designed to cater to applications like streaming media, online multiplayer games, and Voice over IP (VoIP) services. These applications can tolerate certain data loss but are sensitive to delays, making them suitable for application in IoT communication.

3.2.2. Steam Control Transmission Protocol

SCTP was initially designed for VoIP and telephony services and standardised in 2007; SCTP is a transport layer protocol developed to address limitations inherent in TCP and UDP [72]. It is distinguished by its multi-streaming and multi-homing capabilities, along with the capability to support multiple IP addresses per association. Consequently, these unique facets have propelled the expansion of SCTP into a wider array of applications, augmenting its significance and relevance in the IoT communication landscapes [73].

3.2.3. Quick UDP Internet Connection

The QUIC protocol was developed by Google in 2013 specifically to enhance the efficiency and effectiveness of web applications [74]. QUIC is a purpose-built protocol that prioritises low-latency and secure data transfer across a network. It achieves this objective by leveraging UDP as its underlying transport protocol and features similar techniques, such as connectionless communication and header compression. QUIC integrates various functionalities, including encryption, multiplexing, and connection migration, to enhance the efficiency, reliability, and security of data transfer. Its effectiveness in reducing latency and enhancing the overall user experience has garnered significant attention, especially in applications that necessitate real-time communication and low-latency transmission. In addition, QUIC boasts advanced congestion control mechanisms and rapid packet loss recovery techniques, contributing to optimised network performance [75]. These unique functionalities maintain and preserve connection continuity during hand-off, making the protocol particularly desirable in the V2I communication landscape.

3.3. Internet Layer

The Internet layer, often referred to as the network layer, plays a pivotal role in the TCP/IP protocol stack. The Internet Protocol (IP) holds paramount significance at this layer. The layer's fundamental role entails facilitating the transmission and reception of data packets across interconnected networks, encompassing tasks such as packet forwarding, logical addressing, routing and error handling. Unlike connection-oriented protocols, the IP protocol operates in a connectionless manner, foregoing the use of acknowledgements or connection establishment. These responsibilities are delegated to the protocols situated above and below its layer. Consequently, the IP protocol is sometimes perceived as lacking reliability on its own [48]. Nevertheless, the IP protocol remains indispensable in today's communication landscape, particularly considering the proliferation of networked devices.

The surge in Internet connectivity and IoT deployments has impacted the availability of Internet Protocol version 4 (IPv4) addressing schemes. As a result, IPv4 has exhausted its available addresses for internet nodes. To mitigate this issue, the IETF has introduced a new version, Internet Protocol Version 6 (IPv6) [76]. In addition to the introduction of IPv6 as a solution for addressing the shortage, several protocols have been developed to support efficient communication in constrained networks. IPv6 over Low-Power Wireless Personal Area Networks (6LowPAN), Routing Protocol for Low-Power, and Lossy Networks (RPL) are notable protocols in IoT's Internet layer to support efficient transmission and routing in a resource-constrained environment, respectively.

3.3.1. Low-Power Wireless Personal Area Networks

6LowPAN is an IETF standard facilitating the integration of low-power devices into the IoT communication paradigm by transmitting IPv6 packets over low-power wireless networks [77]. Providing support to address the challenges posed by resource-constrained devices by employing efficient packet and header compression techniques, effectively reducing overhead [78]. In addition, IPv6 incorporates adaptation and fragmentation mechanisms to handle packet loss and variable link quality in low-power nodes. By optimising data transmission and network efficiency, 6LowPAN facilitates the seamless integration of IoT devices with limited resources into the larger IPv6-based network infrastructures. 6LowPan is easily adaptable to an increase in the number of nodes in a network, making it a suitable, easy choice for V2I communications.

3.3.2. Routing Protocol for Low-Power and Lossy Networks

RPL is a distance-vector routing protocol designed specifically for low-power and lossy networks (LLNs) to support efficient packet routing and reliable paths from source to destination. It is one of the initiatives observed by the IETF to solve the unique communication needs of LLNs. These networks have a unique set of characteristics, including a limited power supply (often battery-powered), high loss rates, low data rates, and a large number of devices. [79,80]. LLNs are typically used in sensor networks, smart transportation, smart grid, home and building automation, industrial monitoring, and a host IoT application.

4. Survey of Network Protocols

The computing limitations of IoT devices have received extensive attention from academia and industry. These efforts have resulted in the development of several lightweight protocols to compensate for the constrained nature of IoT devices [81]. As a result, several application layer protocols have been developed to support communication in IoT networks, each with a unique and problem-specific communication solution. Various studies have employed a range of methodologies, including experiments [82,83], simulations [84], and testbed implementation [85], to compare the performance of various protocols. These evaluations used several performance metrics such as bandwidth consumption, efficiency, energy consumption, latency, reliability, Round Trip Time (RTT), upload and download time, average response time, and throughput. With these metrics, more emphasis has been placed on investigating timeliness in the IoT application layer.

Mijovic, Shehu, and Buratti [81] performed an experiment by comparing the performance of three application layer protocols, CoAP, WebSocket, and MQTT, using different Internet connections. Protocol efficiency and RTT were the measured metrics. Their experiment showed that CoAP achieved the highest protocol efficiency and the lowest average RTT, closely followed by WebSocket. The performance of MQTT depended on QoS profiles. QoS1 generally achieved better RTT. Another set of comparisons was conducted via an experiment by Tandale, Momin, and Seetharam [82]. They measured the performance metrics of CoAP, MQTT, and REST HTTP using time and bandwidth consumption on a 4G cellular network with a speed of 6 Mbps and an Internet broadband connection with a speed of 50 Mbps. Their results showed that CoAP is faster among the protocols when transmitting payloads less than 10 kb. MQTT and CoAP outperformed REST HTTP when sending smaller payloads. With larger payloads, REST HTTP became the faster protocol. Additionally, the experiment showed bandwidth consumption is equally reduced in CoAP and MQTT when transmitting smaller payloads. With an increase in Payloads, REST HTTP consumed less bandwidth. Assessing these protocols over a 4G cellular network is favourable for CoAP and MQTT in V2I communications use cases requiring the broadcast of smaller payloads. In Babovic, Protic, and Milutinovic [86], the transmission latency and throughput of various sensor data sizes and formats were studied using AMQP, DDS, MQTT, and XMPP over the web with MQTT outperforming the other protocols in latency. Another experiment was observed by Kayal and Perros [87]; their study measured and compared the RTT for different loads using CoAP, MQTT, XMPP and WebSocket. CoAP and MQTT showed better response times.

In another study, Ghotbou and Khansari [88] performed an analytical comparison between AMQP, CoAP, DDS, MQTT, MQTT-SN, XMPP, WebSocket, HTTP/1.1, HTTP/2.0, and RTP to investigate the most suitable IoT protocol for video transmission over LLN. Their comparative analysis showed that CoAP is the most appropriate protocol for video transmission due to its associated transport protocol (i.e., UDP), which supports best-effort packet delivery. A comparison between CoAP, MQTT, XMPP, and AMQP was observed by Sharma and Gondhi [12]; their study revealed that CoAP, AMQP, and XMPP ensure reliability by some built-in features. In addition, AMQP and XMPP both benefit from the reliability provided by their associated transport protocols, e.g., TCP. On the other hand, reliability is provided using the various QoS in MQTT. Their research further showed that CoAP, MQTT, and XMPP all support real-time communication, while AMQP does not. + A study by Chaudhary, Peddoju, and Kadarla [89] compared the performance of AMQP, MQTT, and CoAP and found that MQTT exhibited high packet overhead, especially in 3G networks due to QoS requirements. At high message volumes, MQTT delivered superior throughput, while CoAP and MQTT (QoS 1 and 2) maximised bandwidth usage. Furthermore, Gupta [90] conducted a comparative study of CoAP, MQTT, WebSocket, XMPP and AMQP to ascertain the most reliable protocol using better power usage and latency. CoAP and MQTT performed better when transmitting smaller messages, while AMQP and MQTT are in the pole position for QoS reliability, and XMPP and AMQP lead in security. Al-Qassab and Aal-Nouman [91] conducted a simulation study to compare the most power-efficient protocol for wireless sensor networks using CoAP and MQTT-SN. The results showed that CoAP consumed less power. Timeliness and reliability have also received much research attention at the application layer. While V2I will certainly benefit from this research, more effort is required to investigate other factors like security.

In the transport layer, TCP and UDP are the most prevalent protocols; their limitation in the IoT paradigm has brought about the introduction of QUIC, SCTP, and DCCP as promising alternatives. These protocols offer improvements in ACK, connection management, and cryptographic integration. QUIC shows potential with flexible deployment and promising performance [92]. AL-Dhief et al. [93] conducted a study comparing the performance of TCP and UDP under varying conditions using simulations to analyse two scenarios: varying bandwidth with a fixed packet size and varying packet size with a fixed bandwidth. The key metrics used for performance evaluation included end-to-end delay,

throughput, packet delivery ratio, and packet loss ratio. Their findings indicated that TCP consistently outperforms UDP across all metrics in both scenarios, thereby demonstrating its greater reliability.

Similarly, Wheeb [94] conducted an in-depth comparative study of the performance of transport protocols, including UDP, DCCP, SCTP, and TFRC (TCP-Friendly rate control), within a wired network environment. Their findings indicated that SCTP generally outperformed its counterparts in terms of throughput. However, for video streaming, TFRC demonstrated superior performance. This edge is attributed to its association with the UDP transport, which provides a TCP-style congestion control solution suitable for multimedia and interactive applications that demand low-latency and consistent data delivery. Furthermore, DCCP was found to have the least end-to-end delay in data traffic transmissions, whereas UDP exhibited better performance in video streaming scenarios. The evidence from this study suggested that for high throughput and reliable transport requirements, SCTP and TFRC could be the optimal choices. In another study, Sahraoui et al. [95] conducted a simulation to compare the performance of TCP and UDP for video streaming in VANET, examining metrics like throughput, packet delivery ratio, end-to-end delay, and Peak Signal-to-Noise Ratio (PSNR). Their results showed that UDP offers superior throughput and lower end-to-end delay in comparison to TCP due to the absence of congestion control, making it potentially beneficial for real-time video streaming despite its relative unreliability. However, TCP's retransmission technique results in a slightly better packet delivery ratio.

Park and Koh [96] compared the performance of SCTP and TCP using throughput, traffic competition, and multi-homing. Their results showed that TCP outperforms SCTP with small data sizes, but SCTP surpasses TCP with larger sizes. Both protocols compete fairly in traffic handling, and SCTP's multi-homing offers faster data transmission and better throughput compared to its single-homing. Performance comparison of modified QUIC (ModQUIC), QUIC, and TCP was carried out by Kharat and Kulkarni [97], and ModQUIC produced superior performance both in throughput, delay, and loss rate, demonstrating better network performance overall, particularly with maximised bandwidth utilisation. In addition, ModQUIC and QUIC outperformed TCP in packet loss rate, even in lossy links.

Patel, Chatbar, and Shah [98] highlighted the performance factors of IPv4 and IPv6. Address space, throughput, security, and jitter values were examined, highlighting the advantages of IPv6 over IPv4, including efficient routing, simplified configuration, built-in IPsec security, and support for new services and mobility. In another study, Sandur and Giri [99] compared the performance of 6LoWPAN-CoAP and RPL-CoAP, evaluating average latency and Packet Delivery Ratio (PDR). Both protocols saw improved PDR, but RPL-CoAP outperformed 6LoWPAN-CoAP in latency. In a similar study, Mahmud et al. [100] investigated the pairing of RPL-CoAP and 6LoWPAN-CoAP protocols. Their study showed that RPL-CoAP surpassed the 6LoWPAN-CoAP combination in received packets, suggesting that the former is a superior option for efficient IoT communication. Table 2 shows a comparative analysis of IoT protocol from the application, transport, and Internet layer in the literature, highlighting performance metrics and the best-performing protocols from the analysis.

Table 2. Performance evaluation of network protocol.

	Authors	**Year**	**Network Protocol Analysed**	**Experiment Setup and Testbed Environment**	**Performance Metrics**	**Best-Performing Protocol**
APPLICATION LAYER	Mijovic et al. [82]	2016	CoAP, MQTT, and WebSocket	STM32F411RE, ESP8266, Wi-Fi, and ARM-Mbed	Protocol efficiency and RTT	CoAP
	Babovic et al. [85]	2016	AMQP, DDS, MQTT, and XMPP	Wi-Fi, Adobe Flash, HTML5, and Microsoft Silver	Latency and Throughput Server Utilisation	MQTT
	Tandale et al. [83]	2017	CoAP, MQTT, and HTTP REST	4G and Broadband Raspberry Pi Aiocoap, Django & Mosquitto.	Bandwidth Consumption and Upload and Download time	CoAP
	Kayal and Perros [87]	2017	CoAP, MQTT, XMPP, and WebSocket	Eclipse Mosquitto, Hivemq, Openfire Server, Paho Python Client, and Smack Client	Average response Time Server Utilisation	CoAP
	Chaudhary et al. [89]	2017	CoAP, MQTT, and AMQP	Raspberry Pi, Wi-Fi, and Wireless RabbitMQ, Mosquitto broker, Libcoap server, Wireshark. Python and C	Packet Overhead, Message throughput, and Bandwidth Utilization	MQTT and CoAP
	Sharma and Gondhi [12]	2018	AMQP, CoAP, MQTT, and XMPP	Secondary data	Reliability Real-Time communication	CoAP
	Ghotbou and Khansari [88]	2021	AMQP, CoAP, DDS, MQTT, MQTT-SN, XMPP, WebSocket, HTTP/1.1/2.0, and RTP	Secondary Data	Video Streaming	CoAP
	Bansal and Priya [84]	2021	MQTT and CoAP	Cooja simulator, NS-3, and OMNeT++	IoHT environment	
	Al-Qassab, and Aal-Nouman [91]	2022	CoAP and MQTT-SN	Wireless Sensor Networks, Contiki-O, and Cooja	Power consumption	CoAP

Table 2. *Cont.*

	Authors	Year	Network Protocol Analysed	Experiment Setup and Testbed Environment	Performance Metrics	Best-Performing Protocol
TRANSPORT LAYER	Park and Koh [96]	2008	SCTP and TCP	Linus	Throughput, Multi-homing.	TCP
	Wheeb [94]	2017	UDP, DCCP, SCTP, and TFRC	Wired Network and NS 2	Throughput, End-to-End Video Streaming	SCTP DCCP UDP
	Sahraoui et al. [95]	2018	TCP and UDP	VANET, NS 2, and SUMO	Throughput, Packet Delivery Ratio, End-to-End Delay, and PSNR.	UDP
	AL-Dhief et al. [93]	2018	TCP and UDP	NS-2	Bandwidth, End-to-End Delay, Throughput, Packet Delivery Ratio, Packet Size, and Packet Loss Ratio.	TCP
	Kharat, and Kulkarni [97]	2019	QUIC, Mod QUIC, and TCP	Wi-Fi and Client-server model	Throughput, delay, and loss rates.	ModQUIC
INTERNET LAYER	Patel et al. [98]	2014	IPv4 and Ipv6	Secondary data	Address space, Throughput, Security, and Jitter value	Ipv6
	Mahmud et al. [100]	2019	6LoWPAN-CoAP and RPL-CoAP	Cooja and Ubuntu OS	Received packets, simulation time, and communication range.	RPL-CoAP
	Sandur and Giri [99]	2022	6LoWPAN-CoAP and RPL-CoAP	Ubuntu OS and Cooja	Average Latency and Packet Delivery Ratio	RPL-CoAP

5. Methodology

Significant advancements have been made in the field of IoT networking concepts due to the extensive array of applications and use cases; IoT networking protocols have evolved into a vibrant research area influenced by their diverse characteristics [101]. Consequently, considerable studies have been dedicated to evaluating and comparing the effectiveness of various IoT and related protocols. This study has adopted a simple but effective methodology by conducting a literature survey to carefully select publications related to networking protocols for constrained devices. To gather pertinent literature within this study domain, our literature screening and selection were focused on protocols at the application, transport, and Internet layers of the IoT protocol suite. The selection process prioritised publications that directly compared the performance of different protocols, as these studies provide valuable insights into the strengths and weaknesses of each protocol. Additionally, publications that examined the fundamental functions and design purposes of the protocols were included in the survey.

DQ is integral to the success and broad adoption of the IoT paradigm [6]. Recognising this paramount importance, the second phase of this study focuses on identifying the protocols capable of satisfying our study-specific DQ dimensions. This was achieved by performing an exhaustive evaluation and analysis of the performances of each of the selected protocols [102]. In following this course, we hoped to distil the sets of protocols that not only meet but optimally satisfy our study-specific DQ dimensions for V2I applications and use cases. To achieve this, we conducted a mapping exercise, linking each of the protocols' design objectives, performance evaluations and inherent characteristics to our study-specific DQ dimensions. This crucial step was carried out to assess the strengths, suitability, and limitations of the protocols and to establish a clear correlation between the capabilities of each protocol and their potential to fulfil the communication requirements in IP-based V2I interactions, thereby laying the groundwork for a use-case -driving approach in V2I.

6. Findings and Discussion

6.1. Mapping

Each protocol within the protocol suite plays a specific and pivotal role in the overall network performance, with combined responsibilities ranging from formatting, managing, routing, forwarding, and receiving data packets between nodes. Ensuring communication efficiency in a multifaceted V2I communication landscape requires each protocol to perform optimally to ensure reliable data transmission across diverse use cases, e.g., beacon message broadcasting [103]. It's imperative to understand the most suitable protocols for V2I communications within the context of DQ. In achieving this, mapping the protocols to our identified DQ dimensions is essential in identifying: 1. The most suitable protocols to deploy in specific use cases. 2. Providing a structured way to effectively manage the layered suite to achieve efficiency in data transmission, and 3. Making it easier to pinpoint areas for optimisation which leads to an operational improvement in the overall performance of the network.

This mapping can act as a blueprint to support network engineers and managers working on V2I systems in deploying IoT devices within traffic infrastructures, providing a useful guide in selecting the most suitable protocols based on their identified DQ requirements inherent in their specific V2I use-case, such as traffic light managements requiring XMPP protocol to communicate traffic light information to upcoming traffic simultaneously, the application of MQTT to timely update the availability of parking space in a smart parking scenario, the use WebSocket to continually communicate real-time traffic information and the use of SCTP to support vehicle infotainments by reliable streaming multimedia data. In addition, software developers can also leverage this mapping when designing IoT applications, as observed in [104], providing them with a detailed understanding of how different protocols may impact their application's performance. Another useful application is that this research can provide a support framework for policy formation and standardisation when setting guidelines for IoT

protocol development and deployments, ensuring that protocols are optimised for the IoT paradigm's diverse and evolving communication demands.

In a broader sense, this research can stimulate networking communication innovations to support V2I communication ecosystems by providing a clear understanding of the strengths and weaknesses of various IoT protocols, which could lead to more robust and efficient V2I systems, enhancing safety, improving traffic management, and ultimately paving the way for fully autonomous driving systems. Refer to Table 3 for the mapping of DQ dimensions against the various protocols.

6.2. Data Quality Acting as a Complement of Quality of Service

It is worth noting that this mapping has shown an overlap between DQ and QoS with a shared objective of enhancing the performance of networked applications and services. These two concepts have shared attributes such as accuracy, availability, completeness, reliability, and timeliness [105]. QoS focuses on managing network traffic efficiency, resource allocation, and error handling to satisfy expected performance for various applications and use cases. Most Application layer protocols investigated in this study support QoS with the exception of HTTP REST, XMPP, and WebSocket, while at the Transport layer, TCP and SCTP support QoS, and the Internet layer supports QoS mechanism by default with the help of Ipv6. However, while QoS levels supported at these layers may be sufficient for specific IoT applications and use cases, the existing QoS levels and specific configurations need further investigation to satisfy the communication standards required in some V2I use cases.

The focal point of DQ, on the other hand, is "content suitability", which encompasses the assurance that data transmitted via various protocols aligns with the expected standards necessary for reliable decision-making processes and applications. Within the context of data transmission in IP-based communication using the IoT protocol stack, the intersection of QoS and DQ is evident, as mentioned earlier. QoS mechanisms available in various layers of the IoT protocol stack, depending on the type of protocol deployed, play a pivotal role in maintaining and managing the data flow and ensuring end-to-end delivery while supporting various DQ dimensions. For instance, prioritisation mechanisms [106,107] enable the delivery of time-critical data with high accuracy, meeting accuracy and timeliness dimensions, while retransmission mechanisms ensure reliability. The interfacing of these two concepts will collectively bolster efficiency and reliability in IP-based V2I communications.

6.3. Discussion

CoAP and MQTT protocols notably distinguish themselves within this multifaceted landscape, largely owing to their broad research base and wide deployments. From our in-depth analysis, both protocols satisfactorily address five of our specified ten dimensions, including Availability, Completeness, Consistency, Data Integrity, and Reliability. The successful adherence to these critical DQ dimensions has effectively positioned CoAP and MQTT as the predominant protocols in the application layer for V2I communication scenarios. However, their prevalence is not a testament that they are the ultimate solution. Rather, it indicates the efficacy of these protocols at their domiciled layer. They possess a unique characteristic that is beneficial to V2I systems. Nonetheless, acknowledging that they can fulfil only five of the ten dimensions effectively either due to their design, leveraging the capabilities of their associated transport protocol, or other mechanisms infer the importance of employing a variety of other methodologies, e.g., cross-layer approach [108,109] to compensate for other dimensions. For example, the reliability of data is one of the most coveted dimensions in IoT communications and is predominantly supported by layers underneath the application layer, the path layers (network and transport layer), and the link layers (data link and physical layer) [110]. Protocols such as MQTT and CoAP effectively support reliability due to mechanisms present in the protocols [111]. This is a testament to the heterogeneous and complex nature of V2I communication, which necessitates a versatile mix of protocols for optimal performance.

Table 3. Dimensions of DQ against IoT protocols.

	Application Layer								**Transport Layer**				**Internet Layer**		
DQ Dimensions	**AMQP**	**CoAP**	**DDS**	**MQTT**	**XMPP**	**HTTP REST**	**WebSocket**	**TCP**	**UDP**	**QUICK**	**DCCP**	**SCTP**	**Ipv6**	**RPL**	**6LoWPAN**
Availability	√	√		√			√		√	√	√		√	√	√
Data Accuracy						√		√		√	√	√			
Completeness	√	√		√		√		√				√			
Confidentiality										√			√	√	√
Consistency		√	√	√	√	√	√	√				√			
Data Integrity	√	√	√	√		√		√		√		√	√		
Reliability	√	√	√	√		√	√	√		√		√		√	√
Timeliness		√		√	√				√	√	√	√			
Traceability															
Validity															

In the transport layer, TCP has always been a dominant force. The inherent characteristics of reliability, guaranteed packet delivery, and error-checking ensure relevance, which has earned the trust of numerous developers. UDP, on the other hand, offers an effortless 'fire and forget' transmission model which excels in availability due to its connectionless nature and timeliness, making it a suitable choice for use cases like Emergency Vehicle Pre-emption [85] where low overhead and latency are prioritised. In addition, DCCP mirrors UDP's connectionless architecture but further augments it with a built-in congestion control mechanism, making it a promising candidate for streaming media feeds. Paralleling the features of UDP, the QUIC protocol offers superior performance under various metrics TCP is known for [112], making it a viable choice for a plethora of V2I applications. Leveraging the strengths of both TCP and UDP, SCTP uniquely combines these traditional protocols to create a distinctive transport layer solution. The efficacy of SCTP among its peers in addressing five of our DQ dimensions is largely attributed to its inherent multipath, multi-homing, and multi-streaming capabilities [113], which can significantly enhance the reliability, efficiency, and robustness of V2I communications.

The multipath capabilities ensure uninterrupted data flow between V2I nodes, even under challenging network conditions. This feature is particularly important for real-time traffic management, enabling smooth data transmission. The multi-homing feature allows vehicles to maintain a sustained connection with multiple infrastructures simultaneously, increasing reliability. This is especially beneficial for safety-critical applications like collision detection and avoidance. Finally, the multi-streaming capability can enable the transfer of diverse data types in separate streams, enhancing data delivery efficiency. This capability can significantly improve the performance of use cases that involve the exchange of a variety of data, such as traffic information, vehicle telemetry, and multimedia data. V2I communications necessitate high availability and timely and reliable packet delivery, even under challenging network conditions. These are key characteristics the transport layer protocols should effectively support that are beneficial to the numerous use cases and are particularly beneficial to smart traffic signal coordination [114,115]. Finally, as earlier discussed in Section 3, 6LoWPAN is specifically designed to enable IPv6 packets to be transmitted while RPL provides routing functionalities for IPv6 packets over constrained networks. These protocols underscore their critical role in maintaining robust V2I communication by satisfying three critical DQ dimensions: availability, confidentiality and reliability.

7. Conclusions

Despite the unique capabilities of the various protocols within our tri-layered study, there exists a gap in the traceability and validity dimensions. Addressing these gaps would involve incorporating additional methodologies, such as logging and monitoring systems, data validation rules and implementing anomaly detection techniques. Furthermore, adopting a cross-layer fusion approach by leveraging the synergy between protocols and layers, such as network conditions from the Internet layer, can enhance validity checks in the application layer. While all these approaches can potentially improve DQ across all layers, they could also lead to potential violations of the existing layered architecture principles. Thus, these strategies might introduce trade-offs, such as increased computational overhead or system complexity. Hence, achieving an optimal balance between DQ, security, system performance and efficiency in a protocol fusion approach is a compelling future research direction.

Author Contributions: Conceptualisation, D.S. and K.A.; methodology, D.S.; validation, D.S., K.A., and R.S.; formal analysis, D.S.; investigation, D.S.; resources, D.S.; data curation, D.S.; writing—original draft preparation, D.S.; writing—review and editing, D.S., K.A., and R.S.; supervision, R.S. and K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: All authors have declared no conflict of interest.

Abbreviations

3G	Third Generation
4G	Fourth Generation
6LowPAN	Pv6 over Low-Power Wireless Personal Area Networks
ACK	Acknowledgement
AMQP	Advanced Message Queuing Protocol
C-ITS	Cooperative Intelligent Transportation System
C-V2X	Cellular Vehicle-to-Everything
CoAP	Constrained Application Protocol
DCCP	Datagram Congestion Control Protocol
DDS	Data Distribution Service
DNS	Domain Name Server
DQ	Data Quality
DSRC	Dedicated Short-range Communication
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System.
HTTP	Hypertext transfer protocol
IETF	Internet Engineering Task Force
IoT	Internet of things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LLNs	Low-Power and Lossy Networks
M2M	Machine-to-Machine
MANET	Mobile Ad Hoc Network
ModQUIC	Modified Quick UDP Internet Connections
MQTT	Message Queuing Telemetry Transport
MQTT-SN	Message Queuing Telemetry Transport-Sensor Network
PDR	Packet Delivery Ratio
PSNR	Peak Signal-to-Noise Ratio
QoS	Quality of services
QUIC	Quick UDP Internet Connections
REST	Representational State Transfer
REST	Representational State Transfer
RPL	Routing Protocol for Low-Power and Lossy Networks
RTT	Round Trip Time
SCTP	Stream Control Transmission Protocol
SMTP	Simple Mail Transfer Protocol
STD	Spatial-Temporal Data
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFRC	TCP-Friendly Rate Control
UDP	User Datagram Protocol
V2I	Vehicle-to-Infrastructure
V2V	Vehicles-to-Vehicles
V2X	Vehicle-to-Everything
VANET	Vehicular Ad Hoc Network
XMPP	Extensible Messaging and Presence Protocol

References

1. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
2. Li, S.; Xu, L.D.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]
3. Sunyaev, A. The internet of things. In *Internet Computing*; Springer: Cham, Switzerland, 2020; pp. 301–337.

4. Sagiroglu, S.; Sinanc, D. Big data: A review. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20–24 May 2013; pp. 42–47.
5. Liu, C.; Nitschke, P.; Williams, S.P.; Zowghi, D. Data quality and the Internet of Things. *Computing* **2020**, *102*, 573–599. [CrossRef]
6. Karkouch, A.; Mousannif, H.; Al Moatassime, H.; Noel, T. Data quality in internet of things: A state-of-the-art survey. *J. Netw. Comput. Appl.* **2016**, *73*, 57–81. [CrossRef]
7. Chauhan, S.; Agarwal, N.; Kar, A.K. Addressing big data challenges in smart cities: A systematic literature review. *Info* **2016**, *18*, 73–90. [CrossRef]
8. Tanenbaum, A.S. Network protocols. *ACM Comput. Surv.* **1981**, *13*, 453–489. [CrossRef]
9. Shang, W.; Yu, Y.; Droms, R.; Zhang, L. Challenges in IoT Networking via TCP/IP Architecture. NDN Project. 2016. Available online: https://named-data.net/wp-content/uploads/2016/02/ndn-0038-1-challenges-iot.pdf (accessed on 14 April 2023).
10. Forouzan, B.A. *TCP/IP Protocol Suite*; McGraw-Hill Higher Education: Chicago, IL, USA, 2002.
11. Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient adaptive resource management for real-time vehicular cloud services. *IEEE Trans. Cloud Comput.* **2016**, *7*, 196–209. [CrossRef]
12. Sharma, C.; Gondhi, N.K. Communication protocol stack for constrained IoT systems. In Proceedings of the 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–6.
13. Chand, H.V.; Karthikeyan, J. Survey on the role of IoT in intelligent transportation system. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *11*, 936–941. [CrossRef]
14. Arena, F.; Pau, G. An overview of vehicular communications. *Future Internet* **2019**, *11*, 27. [CrossRef]
15. Peng, H.; Liang, L.; Shen, X.; Li, G.Y. Vehicular communications: A network layer perspective. *IEEE Trans. Veh. Technol.* **2018**, *68*, 1064–1078. [CrossRef]
16. Malik, R.Q.; Ramli, K.N.; Kareem, Z.H.; Habelalmatee, M.I.; Abbas, H. A Review on Vehicle-to-Infrastructure Communication System: Requirement and Applications. In Proceedings of the 2020 3rd International Conference on Engineering Technology and Its Applications (IICETA), Najaf, Iraq, 6–7 September 2020; pp. 159–163.
17. Ndashimye, E.; Ray, S.K.; Sarkar, N.I.; Gutiérrez, J.A. Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey. *Comput. Netw.* **2017**, *112*, 144–166. [CrossRef]
18. Li, Y. An overview of the DSRC/WAVE technology. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks, Proceedings of the 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010, and Dedicated Short Range Communications Workshop, DSRC 2010, Houston, TX, USA, 17–19 November 2010*; Revised Selected Papers 7; Springer: Berlin/Heidelberg, Germany, 2012; pp. 544–558.
19. Wang, X.; Mao, S.; Gong, M.X. An overview of 3GPP cellular vehicle-to-everything standards. *GetMobile: Mob. Comput. Commun.* **2017**, *21*, 19–25. [CrossRef]
20. Ansari, K. Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band. *IET Intell. Transp. Syst.* **2021**, *15*, 213–224. [CrossRef]
21. Wagh, T.; Bagrecha, R.; Salunke, S.; Shedge, S.; Lomte, V. A survey on vehicle to vehicle communication. In *Computational Methods and Data Engineering: Proceedings of ICMDE 2020*; Springer: Singapore, 2020; Volume 2, pp. 163–175.
22. Ganeshkumar, N.; Kumar, S. Obu (on-board unit) wireless devices in vanet (s) for effective communication—A review. In *Computational Methods and Data Engineering: Proceedings of ICMDE*; Springer: Singapore, 2020; Volume 2, pp. 191–202.
23. Wang, R.Y.; Strong, D.M. Beyond accuracy: What data quality means to data consumers. *J. Manag. Inf. Syst.* **1996**, *12*, 5–33. [CrossRef]
24. Shih, C.S.; Chou, J.J.; Reijers, N.; Kuo, T.W. Designing CPS/IoT applications for smart buildings and cities. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 3–12. [CrossRef]
25. Perez-Castillo, R.; Carretero, A.G.; Rodriguez, M.; Caballero, I.; Piattini, M.; Mate, A.; Kim, S.; Lee, D. Data quality best practices in IoT environments. In Proceedings of the 2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC), Coimbra, Portugal, 4–7 September 2018; pp. 272–275.
26. Alwan, A.A.; Ciupala, M.A.; Brimicombe, A.J.; Ghorashi, S.A.; Baravalle, A.; Falcarin, P. Data quality challenges in large-scale cyber-physical systems: A systematic review. *Inf. Syst.* **2022**, *105*, 101951. [CrossRef]
27. Kapil, G.; Agrawal, A.; Khan, R.A. A study of big data characteristics. In Proceedings of the 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 21–22 October 2016; pp. 1–4.
28. Sun, Z.; Strang, K.; Li, R. Big data with ten big characteristics. In Proceedings of the 2nd International Conference on Big Data Research, Weihai, China, 27–29 October 2018; pp. 56–61.
29. Rehrl, K.; Gröchenig, S. Evaluating localization accuracy of automated driving systems. *Sensors* **2021**, *21*, 5855. [CrossRef] [PubMed]
30. Szántó, M.; Hidalgo, C.; González, L.; Pérez, J.; Asua, E.; Vajta, L. Trajectory Planning of Automated Vehicles Using Real-Time Map Updates. *IEEE Access* **2023**, *11*, 67468–67481. [CrossRef]
31. Bhatti, F.; Shah, M.A.; Maple, C.; Islam, S.U. A novel internet of things-enabled accident detection and reporting system for smart city environments. *Sensors* **2019**, *19*, 2071. [CrossRef]
32. Issa, S.; Adekunle, O.; Hamdi, F.; Cherfi, S.S.S.; Dumontier, M.; Zaveri, A. Knowledge graph completeness: A systematic literature review. *IEEE Access* **2021**, *9*, 31322–31339. [CrossRef]

33. Kaneyasu, H.; Nobayashi, D.; Tsukamoto, K.; Ikenaga, T.; Lee, M. Data completeness-aware transmission control for large spatio-temporal data retention. In Proceedings of the 2022 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–9 January 2022; pp. 1–5.
34. Bhalaji, D.N. Reliable data transmission with heightened confidentiality and integrity in IOT empowered mobile networks. *J. IoT Soc. Mob. Anal. Cloud* **2020**, *2*, 106–117.
35. Liu, M.; Wang, Y.; Li, H.; Jing, Y.; Zhang, G.; He, W. Analyzing V2I Channel and Spatial Consistency through Simulation. In Proceedings of the 2021 7th International Conference on Computer and Communications (ICCC), Chengdu, China, 10–13 December 2021; pp. 453–458.
36. Zadorozhny, V.; Krishnamurthy, P.; Abdelhakim, M.; Pelechrinis, K.; Xu, J. Data credence in iot: Vision and challenges. In *Open Journal of Internet of Things (OJIOT), v. 3, N. 1, 114-126, 2017. Special Issue: Proceedings of the International Workshop on Very Large Internet of Things (VLIoT 2017) in Conjunction with the VLDB 2017 Conference*; Research online Publishing: Lübeck, Germany, 2017; Volume 3, pp. 114–126.
37. Gopinath, S.; Vinoth Kumar, K.; Jaya Sankar, T. Secure location aware routing protocol with authentication for data integrity. *Cluster Comput.* **2019**, *22* (Suppl. 6), 13609–13618. [CrossRef]
38. Kafi, M.A.; Othman, J.B.; Badache, N. A survey on reliability protocols in wireless sensor networks. *ACM Comput. Surv.* **2017**, *50*, 1–47. [CrossRef]
39. Franco, A.; Landfeldt, B.; Körner, U.; Nyberg, C. Statistical guarantee of timeliness in networks of IoT devices. *Telecommun. Syst.* **2022**, *80*, 487–496. [CrossRef]
40. Lomotey, R.K.; Pry, J.C.; Chai, C. Traceability and visual analytics for the Internet-of-Things (IoT) architecture. *World Wide Web* **2018**, *21*, 7–32. [CrossRef]
41. Corallo, A.; Paiano, R.; Guido, A.L.; Pandurino, A.; Latino, M.E.; Menegoli, M. Intelligent monitoring Internet of Things based system for agri-food value chain traceability and transparency: A framework proposed. In Proceedings of the 2018 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS), Salerno, Italy, 21–22 June 2018; pp. 1–6.
42. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726. [CrossRef]
43. Qi, J.; Gao, T. A privacy-preserving authentication and pseudonym revocation scheme for VANETs. *IEEE Access* **2020**, *8*, 177693–177707. [CrossRef]
44. Pandey, R.D.; Snigdh, I. Validity as a Measure of Data Quality in Internet of Things Systems. *Wirel. Pers. Commun.* **2022**, *126*, 933–948. [CrossRef]
45. Hussain, R.; Bouk, S.H.; Javaid, N.; Khan, A.M.; Lee, J. Realization of VANET-based cloud services through named data networking. *IEEE Commun. Mag.* **2018**, *56*, 168–175. [CrossRef]
46. Al-Omaisi, H.; Sundararajan, E.A.; Alsaqour, R.; Abdullah, N.F.; Abdelhaq, M. A survey of data dissemination schemes in vehicular named data networking. *Veh. Commun.* **2021**, *30*, 100353. [CrossRef]
47. Priyadarshi, D.; Behura, A. Analysis of different iot protocols for heterogeneous devices and cloud platform. In Proceedings of the 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 3–5 April 2018; pp. 0868–0872.
48. Alani, M.M. Tcp/ip model. In *Guide to OSI and TCP/IP Models*; Springer: Cham, Switzerland, 2014; pp. 19–50.
49. Kumar, S. A Review on Client-Server based applications and research opportunity. *Int. J. Recent Sci. Res.* **2019**, *10*, 33857–33862.
50. Dizdarević, J.; Carpio, F.; Jukan, A.; Masip-Bruin, X. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Comput. Surv.* **2019**, *51*, 1–29. [CrossRef]
51. Shelby, Z.; Hartke, K.; Bormann, C. The constrained application protocol (CoAP) (No. rfc7252). 2014. Available online: https://www.rfc-editor.org/rfc/rfc7252 (accessed on 29 April 2023).
52. Chun, S.M.; Park, J.T. Mobile CoAP for IoT mobility management. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; pp. 283–289.
53. Mishra, B.; Kertesz, A. The use of MQTT in M2M and IoT systems: A survey. *IEEE Access* **2020**, *8*, 201071–201086. [CrossRef]
54. Hussein, M.; Galal, A.I.; Abd-Elrahman, E.; Zorkany, M. Internet of things (IoT) platform for multi-topic messaging. *Energies* **2020**, *13*, 3346. [CrossRef]
55. Kaushik, S.; Poonia, R.C.; Khatri, S.K. Comparative study of various protocols of DDS. *J. Stat. Manag. Syst.* **2017**, *20*, 647–658. [CrossRef]
56. Bendel, S.; Springer, T.; Schuster, D.; Schill, A.; Ackermann, R.; Ameling, M. A service infrastructure for the Internet of Things based on XMPP. In Proceedings of the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), San Diego, CA, USA, 18–22 March 2013; pp. 385–388.
57. Wang, H.; Xiong, D.; Wang, P.; Liu, Y. A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices. *IEEE Access* **2017**, *5*, 16393–16405. [CrossRef]
58. Hayes, M.; Omar, T. End to end vanet/iot communications a 5g smart cities case study approach. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; pp. 1–5.
59. Kramer, J. Advanced message queuing protocol (AMQP). *Linux J.* **2009**, *2009*, 3.
60. Bhimani, P.; Panchal, G. Message delivery guarantee and status update of clients based on IOT-AMQP. In *Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development*; IoT4TD 2017; Springer: Singapore, 2018; pp. 15–22.

61. Tilkov, S. A brief introduction to REST. *InfoQ*, December 2007, 10. Available online: https://www.espinosa-oviedo.com/web-programming/files/readings/A-Brief-Introduction-to-REST.pdf (accessed on 31 April 2023).
62. Hireche, S.; Dennai, A.; Kadri, B. Toward a Novel RESTFUL Big Data-Based Urban Traffic Incident Data Web Service for Connected Vehicles. *Comput. J.* **2023**. [CrossRef]
63. Bayılmış, C.; Ebleme, M.A.; Çavuşoğlu, Ü.; Küçük, K.; Sevin, A. A survey on communication protocols and performance evaluations for Internet of Things. *Digit. Commun. Netw.* **2022**, *8*, 1094–1104. [CrossRef]
64. Soewito, B.; Gunawan, F.E.; Kusuma, I.G.P. Websocket to support real time smart home applications. *Procedia Comput. Sci.* **2019**, *157*, 560–566. [CrossRef]
65. Mitrović, N.; Đorđević, M.; Veljković, S.; Danković, D. Implementation of WebSockets in ESP32 based IoT Systems. In Proceedings of the 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Nis, Serbia, 20–22 October 2021; pp. 261–264.
66. Rahman, M.R.; Akhter, S. Real time bi-directional traffic management support system with gps and websocket. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015; pp. 959–964.
67. Ong, L.; Yoakum, J. An Introduction to the Stream Control Transmission Protocol (SCTP) (No. rfc3286). 2002. Available online: https://www.rfc-editor.org/rfc/rfc3286.html (accessed on 31 April 2023).
68. Kohler, E.; Handley, M.; Floyd, S. Datagram Congestion Control Protocol (DCCP) (No. rfc4340). 2006. Available online: https://www.rfc-editor.org/rfc/rfc4340.html (accessed on 31 April 2023).
69. Iyengar, J.; Thomson, M. QUIC: A UDP-based multiplexed and secure transport. In *RFC 9000*; IETF 2021. Available online: https://datatracker.ietf.org/doc/html/rfc9000 (accessed on 31 April 2023).
70. Abdelsalam, A.; Luglio, M.; Roseti, C.; Zampognaro, F. TCP wave: A new reliable transport approach for future internet. *Comput. Netw.* **2017**, *112*, 122–143. [CrossRef]
71. Al-Saadi, R.; Armitage, G.; But, J.; Branch, P. A survey of delay-based and hybrid TCP congestion control algorithms. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3609–3638. [CrossRef]
72. Stewart, R.; Metz, C. SCTP: New transport protocol for TCP/IP. *IEEE Internet Comput.* **2001**, *5*, 64–69. [CrossRef]
73. Eklund, J. Latency Reduction for Soft Real-Time Traffic Using SCTP Multihoming. Ph.D. Thesis, Karlstad University Press, Karlstad, Sweden, 2016.
74. Langley, A.; Riddoch, A.; Wilk, A.; Vicente, A.; Krasic, C.; Zhang, D.; Yang, F.; Kouranov, F.; Swett, I.; Iyengar, J.; et al. The quic transport protocol: Design and internet-scale deployment. In Proceedings of the Conference of the ACM Special Interest Group on Data Communication, Los Angeles, CA, USA, 21–25 August 2017; pp. 183–196.
75. Megyesi, P.; Krämer, Z.; Molnár, S. How quick is QUIC? In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
76. Babatunde, O.; Al-Debagy, O. A comparative review of internet protocol version 4 (ipv4) and internet protocol version 6 (ipv6). *arXiv* **2014**, arXiv:1407.2717.
77. Olsson, J. 6LoWPAN demystified. *Tex. Instrum.* **2014**, *13*, 1–13.
78. Tömösközi, M.; Reisslein, M.; Fitzek, F.H. Packet header compression: A principle-based survey of standards and recent research studies. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 698–740. [CrossRef]
79. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks (No. rfc6550). 2012. Available online: https://www.rfc-editor.org/rfc/rfc6550.html (accessed on 5 May 2023).
80. Almusaylim, Z.A.; Alhumam, A.; Jhanjhi, N.Z. Proposing a secure RPL based internet of things routing protocol: A review. *Ad Hoc Netw.* **2020**, *101*, 102096. [CrossRef]
81. Al-Masri, E.; Kalyanam, K.R.; Batts, J.; Kim, J.; Singh, S.; Vo, T.; Yan, C. Investigating messaging protocols for the Internet of Things (IoT). *IEEE Access* **2020**, *8*, 94880–94911. [CrossRef]
82. Mijovic, S.; Shehu, E.; Buratti, C. Comparing application layer protocols for the Internet of Things via experimentation. In Proceedings of the 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI), Bologna, Italy, 7–9 September 2016; pp. 1–5.
83. Tandale, U.; Momin, B.; Seetharam, D.P. An empirical study of application layer protocols for IoT. In Proceedings of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 2447–2451.
84. Bansal, M. Performance Comparison of MQTT and CoAP Protocols in Different Simulation Environments. *Inven. Commun. Comput. Technol.* **2021**, *2017*, 549–560.
85. Safaei, B.; Monazzah, A.M.H.; Bafroei, M.B.; Ejlali, A. Reliability side-effects in Internet of Things application layer protocols. In Proceedings of the 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 20–22 December 2017; pp. 207–212.
86. Babovic, Z.B.; Protic, J.; Milutinovic, V. Web performance evaluation for internet of things applications. *IEEE Access* **2016**, *4*, 6974–6992. [CrossRef]

87. Kayal, P.; Perros, H. A comparison of IoT application layer protocols through a smart parking implementation. In Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 7–9 March 2017; pp. 331–336.
88. Ghotbou, A.; Khansari, M. Comparing application layer protocols for video transmission in IoT low power lossy networks: An analytic comparison. *Wirel. Netw.* **2021**, *27*, 269–283. [CrossRef]
89. Chaudhary, A.; Peddoju, S.K.; Kadarla, K. Study of internet-of-things messaging protocols used for exchanging data with external sources. In Proceedings of the 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Orlando, FL, USA, 22–25 October 2017; pp. 666–671.
90. Gupta, P. A Survey of Application Layer Protocols for Internet of Things. In Proceedings of the 2021 International Conference on Communication information and Computing Technology (ICCICT), Mumbai, India, 25–27 June 2021; pp. 1–6.
91. Al-Qassab, R.A.; Aal-Nouman, M.I. Performance Evaluation of CoAP and MQTT_SN Protocols. In *Proceedings of the International Conference on Emerging Technology Trends in Internet of Things and Computing, Erbil, Iraq, 6–8 June 2021*; Springer International Publishing: Cham, Switzerland, 2021; pp. 223–236.
92. Polese, M.; Chiariotti, F.; Bonetto, E.; Rigotto, F.; Zanella, A.; Zorzi, M. A survey on recent advances in transport layer protocols. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3584–3608. [CrossRef]
93. AL-Dhief, F.T.; Sabri, N.; Latiff, N.A.; Malik, N.N.N.A.; Abbas, M.; Albader, A.; Mohammed, M.A.; AL-Haddad, R.N.; Salman, Y.D.; Khanapi, M.; et al. Performance comparison between TCP and UDP protocols in different simulation scenarios. *Int. J. Eng. Technol.* **2018**, *7*, 172–176.
94. Wheeb, A.H. Performance evaluation of UDP, DCCP, SCTP and TFRC for different traffic flow in wired networks. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 3552. [CrossRef]
95. Sahraoui, Y.; Ghanam, A.; Zaidi, S.; Bitam, S.; Mellouk, A. Performance evaluation of TCP and UDP-based video streaming in vehicular ad-hoc networks. In Proceedings of the 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT), El Oued, Algeria, 27–31 October 2018; pp. 67–72.
96. Park, J.S.; Koh, S.J. Performance Comparison of SCTP and TCP over Linux Platform. *J. Korean Inst. Commun. Inf. Sci.* **2008**, *33*, 699–706.
97. Kharat, P.; Kulkarni, M. Modified QUIC protocol for improved network performance and comparison with QUIC and TCP. *Int. J. Internet Protoc. Technol.* **2019**, *12*, 35–43. [CrossRef]
98. Patel, U.; Chhatbar, J.; Shah, V. Comparitive study on ipv4 and ipv6 internet protocol. *Int. J. Adv. Eng. Res. Dev.* **2014**, *1*, 58–62.
99. Sandur, A.; Giri, A. Performance Analysis of the merged 6L0WPAN-CoAP and RPL-CoAP with different combination of MAC and RDC layer protocols. In Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; pp. 1–6.
100. Mahmud, A.; Hossain, F.; Juhin, F.; Choity, T.A. Merging the communication protocols 6LoWPAN-CoAP and RPL-CoAP: Simulation and performance analysis using Cooja simulator. In Proceedings of the 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 3–5 May 2019; pp. 1–6.
101. Sobin, C.C. A survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
102. Pohl, M.; Kubela, J.; Bosse, S.; Turowski, K. Performance evaluation of application layer protocols for the internet-of-things. In Proceedings of the 2018 Sixth International Conference on Enterprise Systems (ES), Limassol, Cyprus, 1–2 October 2018; pp. 180–187.
103. Bilal, M.; Munir, E.U.; Ullah, A. BEMD: Beacon-oriented Emergency Message Dissemination scheme for highways. *Ad Hoc Netw.* **2023**, *142*, 103095. [CrossRef]
104. Callebaut, G.; Leenders, G.; Van Mulders, J.; Ottoy, G.; De Strycker, L.; Van der Perre, L. The art of designing remote iot devices—Technologies and strategies for a long battery life. *Sensors* **2021**, *21*, 913. [CrossRef]
105. Resner, D.; de Araujo, G.M.; Fröhlich, A.A. Design and implementation of a cross-layer IoT protocol. *Sci. Comput. Program.* **2018**, *165*, 24–37. [CrossRef]
106. Singh, M.; Baranwal, G. Quality of service (qos) in internet of things. In Proceedings of the 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–6.
107. Beshley, M.; Kryvinska, N.; Seliuchenko, M.; Beshley, H.; Shakshuki, E.M.; Yasar, A.U.H. End-to-End QoS "smart queue" management algorithms and traffic prioritization mechanisms for narrow-band internet of things services in 4G/5G networks. *Sensors* **2020**, *20*, 2324. [CrossRef]
108. Jung, C. Prioritized Data Transmission Mechanism for IoT. *KSII Trans. Internet Inf. Syst.* **2020**, *14*, 1–21.
109. Tandon, A.; Srivastava, P. Location based secure energy efficient cross layer routing protocols for IOT enabling technologies. *Int. J. Innov. Technol. Explor. Eng. (IJITEE)* **2019**, *8*, 368–374.
110. Jiang, S. On reliable data transfer in underwater acoustic networks: A survey from networking perspective. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1036–1055. [CrossRef]
111. Kamble, S.J.; Kounte, M.R. A Survey on Emergency Vehicle Preemption Methods Based on Routing and Scheduling. *Int. J. Comput. Netw. Appl.* **2022**, *9*, 60–71. [CrossRef]
112. Dey, N.; Neha, N.; Hariprasad, M.; Sandhya, S.; Moharir, M.; Akram, M. A Detail Survey on QUIC and its Impact on Network Data Transmission. In Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 28–30 April 2022; pp. 378–385.

113. Eklund, J.; Grinnemo, K.J.; Brunstrom, A. Using multiple paths in SCTP to reduce latency for signaling traffic. *Compute. Commun.* **2018**, *129*, 184–196. [CrossRef]
114. Guo, Q.; Li, L.; Ban, X.J. Urban traffic signal control with connected and automated vehicles: A survey. *Transp. Res. Part C Emerg. Technol.* **2019**, *101*, 313–334. [CrossRef]
115. Lee, W.H.; Chiu, C.Y. Design and implementation of a smart traffic signal control system for smart city applications. *Sensors* **2020**, *20*, 508. [CrossRef]