International Journal of Current Engineering and Technology
©2021 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Resilient Communication Protocols for Industrial IoT: Securing Cyber-Physical-Systems at Scale

Gaurav Sarraf*

Independent researcher

Received 01 Nov 2021, Accepted 10 Dec 2021, Available online 13 Dec 2021, **Vol.11, No.6 (Nov/Dec 2021)**

Abstract

The Industrial Internet of Things (IIoT) and Cyber-Physical Systems (CPS) bring together computing, networking, and physical processes (PP) to automate, control and monitor industrial settings in real-time. By interconnecting sensors, actuators, controllers, and networks, IIoT and industrial CPS enhance efficiency, productivity, and operational resilience across manufacturing, energy, and transportation domains. This survey provides a comprehensive review of IIoT architectures, including communication protocols like LPWAN, WPAN, MQTT, CoAP, REST, XMPP, AMQP, WIFI, ZigBee, Bluetooth, Z-Wave, and Lora WAN, as well as associated security considerations. Key challenges such as standardization, interoperability, privacy, regulatory compliance, and cyber threats are analyzed. The survey further examines resilience mechanisms encompassing self-protecting, self-configuring, and self-healing strategies, supported by redundant nodes, traffic replication and splitting, and SDN/NFV-based virtual network management. Cross-layer approaches that leverage adaptive routing, quality of service, and fault-tolerant strategies are discussed to maintain reliable and secure operations in the face of failures or attacks. The insights presented aim to guide researchers and practitioners in designing robust, scalable, and resilient IIoT and CPS infrastructures.

Keywords: *Communication Protocols, Industrial Internet of Things (IIoT), Network Resilience, Security, SDN/NFV, Cyber-Physical Systems.*

Introduction

The IoT has revolutionised connectivity by enabling billions of devices to exchange data for automation, monitoring, and intelligent decision-making. IoT applications span various domains, including healthcare, transportation, smart cities, and agriculture, driving efficiency and innovation. However, as IoT networks grow in scale and complexity, they also face increasing challenges related to reliability, latency, and security. These concerns become even more critical in industrial environments, where disruptions in communication can cause significant safety, operational, and economic impacts [1]. The areas of machine-to-machine, or M2M, and industrial communication technologies, with a focus on automation applications, make up Industrial IoT (IIoT), a subset of the Internet of Things (IoT). My Industrial IoT Network With an emphasis on industrial automation and mission-critical systems, a subset of the Internet of Things (IoT) known as Industrial Internet of Things (IIoT) has developed. This subset mainly deals with automation-associated M2M and industrial communication technologies [2]. IIoT integrates sensors, actuators, controllers, and smart devices to optimise operations in manufacturing, energy, logistics, and healthcare. Unlike consumer IoT, IIoT demands stringent guarantees for low latency, fault tolerance, and high availability [3]. This industrial emphasis not only enhances productivity but also raises the importance of secure and resilient communication frameworks that can sustain large-scale, safety-critical operations.

At the heart of IIoT lies CPS, which tightly couple computational intelligence with PP [4]. CPS enables real-time feedback loops, where machines, networks, and control systems coordinate autonomously to ensure efficiency and safety. The integration of IIoT with CPS drives Industry 4.0, creating highly adaptive environments capable of autonomous decision-making, predictive maintenance, and process optimization. Yet, the reliance of CPS on seamless communication introduces vulnerabilities, where even minor cyber or network disruptions may cascade into large-scale physical failures.

The role of resilient communication protocols in IIoT which are designed to ensure secure, fault-tolerant, and adaptive information exchange. Such protocols employ techniques like lightweight cryptography, redundancy, and intelligent recovery to maintain reliability under diverse threat conditions,

*Corresponding authors' ORCID ID: 0000-0000-0000-0000

DOI: https://doi.org/10.14741/ijcet/v.11.6.14

including cyberattacks and hardware failures. In CPS-driven environments, where both safety and efficiency are non-negotiable, resilient protocols serve as a critical safeguard, ensuring operational continuity and trustworthiness [5][6]. Resilient communication protocols serve as the essential link between cyber infrastructures and physical processes, ensuring that industrial CPS maintain secure, continuous, and reliable functionality [7]. By enabling adaptability, fault tolerance, and robustness, these protocols reinforce the ability of IIoT-enabled CPS to operate dependably under dynamic and adverse conditions. Consequently, resilient communication protocols emerge as the foundation of trustworthy industrial systems, supporting both large-scale deployment and long-term sustainability.

Organisation of the Paper

This study is structured as follows: Section I introduces study. Section II discusses Industrial IoT and Cyber-Physical Systems. Section III explores Industrial IoT Communication Protocols, while Section IV examines Resilience in IIoT Communication Protocols. Section V shows a review of existing literature on Resilient Communication Protocols for Industrial IoT, and Section VI concludes study with key findings and outlines directions for future research.

Industrial Iot and Cyber-Physical Systems

Industrial IIoT and CPS signify integration of computational, communication, and physical processes through the combination of embedded devices, or smart sensors and actuators, that are interconnected often without wires to monitor, analyse, and control industrial processes in real-time. IIoT and CPS are expected to deliver considerable technical, economic, and societal benefits, improving performance, efficiency, and autonomy in various industrial applications, counting energy, manufacturing, and transportation [8]. The combination of IIoT and CPS drives significant opportunities for research and development in industrial networking, data analytics, control systems, and smart manufacturing systems.

Architecture

"Industry 4.0" is the new paradigm for manufacturing., utilising information and communication technologies to efficiency in manufacturing and enhance productivity and automation. Two key paradigms emerge: Industrial IoT and Industrial CPS. I-IoT enables interconnection and sensing of industrial devices using IoT technologies, while I-CPS extends traditional CPS to industrial settings, intertwining physical and cyber systems for control, command, automation, and security [9]. From a CPS viewpoint (Figure 1), control, networking, and computing systems integrate components and physical systems, performing monitoring and control to ensure efficient industrial operations.

Understanding the interconnections and distinctions across I-IoT, IoT, and I-CPS. The IoT is the network of interconnected computing, communication, and media devices which enable the monitoring and control of physical objects in a control-and-power-system (CPS), like a smart transportation or a smart grid system. This networking will eventually lead to a world where countless commonplace devices are linked [10]. In a similar vein, I-CPS is tailored to sustain industrial production and manufacturing, as opposed to CPS for consumer applications or critical infrastructures.

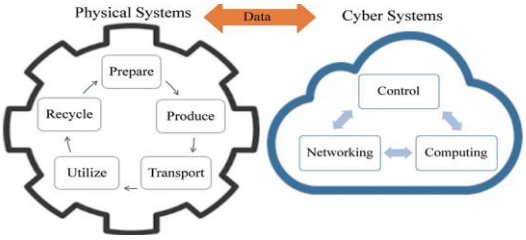

Fig.1 I-IoT from a CPS Perspective.

Components of Cyber-Physical Systems (CPS)

CPS integrate PP with computational and communication capabilities, enabling decision-making and intelligent control in industrial settings. The main components include:

Sensors: Devices that measure environmental and process parameters like vibration, temperature, chemical characteristics, and pressure. These instruments contain the unprocessed information required for monitoring and for analysis.

Actuators: Devices that carry out control instructions to create physical changes, such as open valves, modify motor speeds, or activating alarms.

Controllers: Embedded systems, microcontrollers, and PLCs that evaluate the data from sensors and issue the associated control signals. These components are the intelligent computing core of CPS decision-making.

Networks: The method of communication that connects devices together, enabling various opportunities for data-driven interactions and actions of coordination and remote monitoring in real-time [11]. Measurement technologies in a wired context include Ethernet and Modbus, while wireless measurement technologies encompass LoRa, Zigbee, and 5G, depending on the application's requirements.

Research Directions of Control, Networking and Computing for I-IoT

Following this, lay out theoretical underpinnings, models, and testbeds for I-IoT networking, control, and computing, along with areas that require further investigation in the future, like intelligent data and co-design management and analysis.

Networking, Co-design of Computing and Control: The IIoT depends on the merged integration of control, networking, and computing to achieve reliability, efficiency, and productivity [12]. It is not enough to design each of these domains independently; rather, their integrated co-design is crucial for the effective and scaled implementation of IIoT.

Intelligent Data Management & Analytics: IIoT applications are moving rapidly towards large, heterogeneous, and complex datasets, and there are major issues for the management of these datasets, and consequentially for the system performance of the elements of the system. Big data-enabled analytics and intelligent data management methods convert raw datasets into usable knowledge, enhancing application's performance like control, networking, and computing.

Theoretical Foundations, Models and Testbeds: Moving the IIoT forward requires strong theoretical models and simulation facilities to design, test, and evaluate suitable emerging techniques in both control, networking, and computing. Building these foundations, along with testbeds from industry, will enable researchers and practitioners to validate solutions, address interoperability judgements, and resolve the uncertainties associated with large-scale deployment.

Industrial Iot Communication Protocols

Industrial networking processes differ from those in enterprise and consumer settings due to their unique requirements and constraints. One of the fundamental differences is in the combination of IT and OT. Information-based computation processes must be integrated with physical industry processes. The design of IIoT communication protocols must consider several important requirements, including the transition from wired to wireless or vice versa, as well as mobility (for vehicles, equipment, robots, and personnel), and dynamic reconfiguration. IIoT protocols play a crucial role in applications like condition and energy monitoring, which collect real-time data from equipment during operational cycles.

Key Communication protocols in I-IOT

Communication protocols are essential in IIoT, enabling data exchange between devices and cloud systems while balancing range, latency, QoS, power, and security [13]. Traditional IP-based protocols often require high power and memory, making them less suitable for IoT. Low-power wireless protocols have emerged as the preferred choice, offering reliable, scalable, and energy-efficient communication, and are generally categorised into two main groups:

Low-Power Wide Area Networks (LPWAN)

LPWANs are a category of wireless communication protocols utilized to transmit data to and from devices in low-cost modes, low-power, and long-range of operation, particularly for IoT devices. Unlike cellular networks, which may require complex infrastructure such as antennas and amplifiers and be high-energy intensive, LPWANs enable low-power and resource-constrained small devices with minimal to no processing capability [14]. In general, LPWAN technologies are capable of transmitting data at distances greater than 10 km, depending on the environment, at data rates from 0.3-50 kbit/s (one channel). QoS and scaling issues are also important considerations when selecting LPWAN protocols for use in industrial IoT applications.

Wireless Personal Area Networks (WPANs)

WPANs operate using local mesh topologies, which enable interconnected devices or nodes to communicate directly with each other, transferring messages from one device to another until they are delivered to the intended recipient. The decentralised network topology improves robustness, as devices do not rely on a single point of failure, provides simpler sensor node deployment, and eliminates the need for infrastructure costs. Among the WPAN solutions, Zigbee is the most commonly deployed in IoT applications [15]. ZigBee is a short-range, low-energy consumption communication protocol that allows energy-efficient systems in areas where many devices communicate with each other.

Internet Protocol-Based Communication.

The following are five internet protocols: MQTT, REST, CoAP, AMQP, and XMPP. Also covered are inherent security characteristics and issues:

Message Queuing Telemetry Transport (MQTT)

Operating via TCP/IP or other protocols, the message queuing and transmission over TCP/IP protocol is known as the MQTT protocol which follows a basic client/server format. Its openness, lightweight nature, and ease of implementation make it well-suited to limited situations, such the Internet of Things (IoT). In order for MQTT implementations to be safe, authentication, authorisation, and encrypted communication must be met. Using MQTT and its suggested features, key infrastructures and apps that deal with sensitive data can get superior security services.

Constrained Application Protocol (CoAP)

In RFC 7252, the CoAP is described as a customised web transfer protocol. The moniker "lightweight" comes from the fact that this protocol is designed for usage with limited nodes and networks due to its low transmission rate and small size. Smart meters, which monitor energy usage, and supply chain management are two examples of machine-to-machine (M2M) applications that could benefit from the architecture. Integrating it with the Web is made easier by its excellent HTTP interface. DTLS is mechanism that ensures security; nevertheless, it is regrettably not widely utilised in the Internet of Things (IoT) [16].

Representational State Transfer (REST)

For hypermedia systems that are distributed, the RESTful approach is a hybrid architectural style. It contains guidelines for creating applications within certain limitations, outlining the software engineering principles that should be followed. The development of RESTful web services is its primary use. (a) The client-server constraint is part of REST; (b) the stateless constraint enhances network efficiency; (c) the cache constraint achieves visibility, dependability, and scalability; (d) a consistent interface between parts is guaranteed by a set of four restrictions; etc.

Extensible Messaging and Presence Protocol (XMPP)

The XMPP is a free and open-source XML protocol for instant messaging. Its primary functions are presence, collaboration, and instant messaging. When an entity is "present," it means it is prepared to receive messages. A real-time capability is guaranteed by messaging through the use of an efficient push mechanism. The expandable features and open design of XMPP make it a good fit for Internet of Things implementations. Recent updates to the NVD databases maintained by NIST have added a large number of CVE numbers pertaining to XMPP vulnerabilities that allow for a cascade of attacks.

Advanced Message Queuing Protocol (AMQP)

The AMQP is an attempt to standardise business messaging amongst asynchronously running apps on various platforms and inside various businesses, an open standard. Reliable corporate messaging is enabled by this wire-level protocol. At the most fundamental level, we have message transmission between processes; at the messaging layer, we provide the expected format for every messages' encoding.

Wireless Communication Protocols.

Here are the five network protocols presented: WiFi, Bluetooth, Z-Wave, LoRaWAN, and Zigbee. Security-related aspects and issues are also covered:

WiFi

A wireless communication standard known as 802.11 was created by the IEEE is the foundation of WiFi, the most popular and well-known form of wireless networking. It is compatible with more devices, has lower latency, and is constantly becoming better. The authentication, availability criteria, data privacy for safeguarding WIFI connections are met by enhancing security with each iteration of WiFi. Wireless connections allow devices to communicate with one another through the transmission of signals within a theoretically limited range of 100 m.

Blacktooth

Due to its low power consumption, an excellent choice for the IoT is the Blacktooth Low Energy (LE) radio. Its data-transfer capabilities across several channels provide the adaptability required for deployment in a wide variety of communication topologies, including mesh topologies, broadcast, and point-to-point, and networks of numerous wireless devices. It also provides very accurate device positioning services.

ZigBee

Similar to Bluetooth, ZigBee is a widely used technology in IoT networks. It has a communication range of up to 200 meters—double that of the related Bluetooth—, meets modern security requirements, uses little power, and has a limited data range. It allows the building of big IoT models with several nodes and is suitable for devices and sensors with several limitations.

Z-wave

A home automation protocol developed by Z-Wave is Z-Wave. It avoids interference by using its own radio frequency band. 4.5.5. LiDAR WAN For Internet of Things (IoT) deployments including battery-operated devices, LoRaWAN is a suitable networking protocol because to its Low Power, Wide Area (LPWA) capabilities. It satisfies important needs for end-to-end security and bidirectional communication.

Security Challenges in IIoT Communication

IoT devices interact through networks to provide users with the required information. But dealing with IoT deployments isn't a picnic, especially when security isn't the only obstacle; many other issues arise, and some of the key challenges are discussed below:

Standardisation

One key issue in IIoT is that there are still no globally accepted standards in place. Whenever IoT evolves rapidly without standard regulations, guidelines, and standardisation, there can be poor interoperability and various approaches to security across different sectors. IoT devices also work with unstructured data across different databases (e.g., NoSQL), which have distinct query framework logic, resulting in even more substantial compatibility challenges.

Integration and Interoperability

IoT device integration is severely impacted by absence of suitable standards in communication networks.

Because there are so many moving parts in Internet of Things (IoT) hardware development and so many different languages used, implementing communication interoperability is an even greater challenge than traditional communication interoperability, given the variety of technology at our disposal, is already challenging to accomplish. Because of this, it is already challenging for gadgets from different manufacturers to connect without any hitches.

Privacy

The proliferation of Internet-enabled devices throughout the globe has given hackers a plethora of new vectors to exploit vulnerabilities in computer systems. Put another way, the attack surface grows in direct proportion to number of IoT devices linked to a network. This is because an attacker now has a greater number of devices to target, which in turn makes the entire network more susceptible to hacking.

Regulatory and Legal Compliance

There are a lot of problems with consumers trying to figure out if anything is illegal in each jurisdiction since there is a lack of uniformity in the rules and regulations that govern IoT devices and the many ways in which IoT technology is being used. Data retention and deletion regulations, legal liability for IoT devices' accidental usage, and privacy lapses or security breaches are just a few of the legal problems that have surfaced in relation to IoT devices.

Cost Considerations

The aforementioned list of challenges is difficult to disentangle from the consideration of cost. Incompatibilities are minimised through standardisation, and network reliability is diminished due to a lack of device integration. Sophisticated security measures are necessary to protect personal information. Internet of Things (IoT) systems will be more trustworthy thanks to a worldwide legal framework. Energy depletion impacts functioning, and hardware diversity affects and decides cost in several ways. Cost evaluation is one of the obstacles that businesses with IoT infrastructures must overcome in order to make good judgements [17].

Threats and Vulnerabilities in Industrial Networks

IIoT networks are extremely susceptible to various cyberthreats:

Man-in-the-Middle (MitM) Attacks: In these types of attacks, an attacker will intercept and may even modify messages between two devices or systems. MitM attacks compromise data integrity and confidentiality, allowing attackers to manipulate an industrial process or steal sensitive information.

DoS Attacks: A DoS attack is an effort to disrupt normal functioning of networks within the IIoT ecosystem. DoS attacks can exhaust devices, servers, and communication channels, resulting in operational downtime, increased response times, and total failures of industrial processes.

Data Tampering and Injection Attacks: An attacker may inject false data or manipulate information going into legitimate data streams to confuse decision-making systems. Given that automation, monitoring, and control systems must be accurate in real-time, this creates a significant risk.

Resilience of IIoT Communication Networks

Resilience is a crucial characteristic of IIoT communication networks, representing their ability to continue operating despite internal failures and external disturbances. Resilience in communication networks encompasses operations during natural disasters, weather-related disturbances, technological failures, or malicious activities, while continuing to allocate resources effectively and efficiently [18]. A resilient IIoT network should support services, and fault-tolerant and adaptive recovery, enabling it to absorb repeated disturbances while protecting essential industrial infrastructures and processing.

Resilience in Iiot Communication Protocols

Resilience is of critical importance in IIoT communication protocols, facilitating in a continuous, reliable, and secure passage of data while coping with failures, attacks or unexpected conditions in the environment. Resilience will enable industrial networks to maintain operational efficiency, provide critical services, and minimise costly downtime [19].

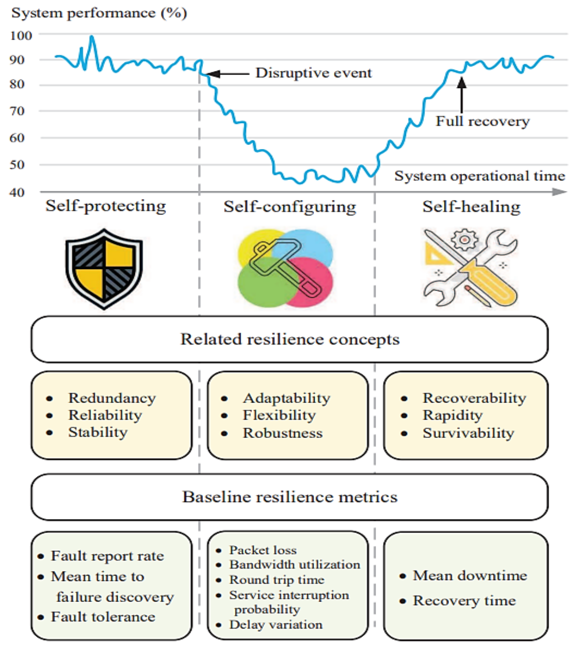

Fig.2 Resilience-Related Concepts

Resilience in IIoT communication networks encompasses numerous related concepts, and for the purposes of this thesis, can be classified into self-protecting, self-configuring, and self-healing mechanisms [20]. Under normal or acceptable conditions, self-protecting mechanisms will provide for system stability through encryption, authentication, and basic fault tolerance If the disruptive events exceed the capabilities offered by self-protecting mechanisms, then a self-configuring mechanism provides a degree of functionality via mechanisms such as adaptive routing and service load balancing, and/or, if required, a self-healing restored normalcy by adding an additional layer of redundancy via mechanisms such as traffic replication or embedded services (as illustrated in Figure 2) .Although some resilience concepts may not fit neatly into one category or another, this classification provides an operational framework for resilient protocol design, enabling continuous, secure, and reliable operations during adverse conditions.

Resilient Service Embedding In IoT Networks

Application reliability in face of node, link, or traffic failures is guaranteed by service embedding in IoT networks. Introducing resilience to service embedding enables networks, such as those in smart buildings, to maintain acceptable fault tolerance and recover from failures while optimising performance metrics, including energy consumption and end-to-end delay [21]. The following approaches represent progressively stronger levels of resilience:

Node Coexistence Constraint

The fundamental resilience approach provides a single route from destination node and source node. Lost packets may be re-sent until they are acknowledged. This provides a mechanism to address temporary failures (such as a collision or a lost packet). While basic, this method produces bursty transmissions at times, which results in an additional overhead, and may contribute to network congestion.

Sensor–Actuator Node Redundancy

Redundant sensor and actuator nodes enhance resilience against service failures and attacks [22]. This approach ensures data fidelity and accuracy while improving fault tolerance, allowing critical sensing and actuation functions to continue during node failures.

All-Node Redundancy

For services with high resilience requirements e.g., fire protection or security systems redundant components are allocated to all nodes, enabling multipath routing and end-to-end fault tolerance. This approach prioritizes reliability over cost.

Traffic Redundancy and Replication

Redundant traffic creates several paths between source nodes and destination nodes. The main path will be used to transfer traffic under normal operating conditions, with backup paths serving as alternative paths. In the case of a failure, the network can reroute traffic based on a keep-alive signalling method, ensuring traffic is not lost and faces no interruption. Replication involves transmitting multiple replicas of every data packet over an intended selected path. Since the receiver can retrieve lost packets from the replicated streams, this guarantees that messages will arrive with minimal latency and a high packet delivery ratio. The trade-off is increased energy consumed for both the additional traffic and processing mechanisms.

Traffic Splitting

Traffic splitting manipulates the actual transfer of data in sending it over two or more paths (e.g. 50% of the traffic over this path and 50% of the traffic over another path). If one of the paths becomes unavailable for an extended period, the undelivered portion of traffic can be resent over the alternative path. Traffic splitting maximizes energy usage and minimizes delivery time.

Resilient Virtual Network Layer For IIoT.

The combination of NFV and SDN provides a solid foundation for increasing resiliency at the virtual network layer in IIoT scenarios. This allows for the centralized management of virtualized infrastructure installed on commercial off-the-shelf (COTS) hardware, enabling dynamic control and monitoring of industrial networks such as smart grids [23]. With SDN/NFV, it is feasible to observe network performance in real-time and dynamically calculate the relevant key QoS metrics, like packet loss, latency, and throughput [24]. SDN controllers allow for the rapid reconfiguration of virtual networks to address the impacts of faulty switches, automate data delivery, reproduction of service level attributes, and to ensure that a consistent quality of service is delivered. Time-stamping and packet synchronisation ensure the coordinated operation of networked devices across nodes.

The resilience workflow for IIoT data in smart grids based on SDN is shown in Figure 3. The workflow begins when a data forwarding request triggers an update to the database and a QoS assessment. A set of optimal paths is then selected through local monitoring. The end-to-end path will also be continuously monitored for network failures and potential congestion. When either of these two scenarios occurs, the SDN controller automatically updates the switches, informing them of when to reroute traffic and creating a reliable and resilient communication infrastructure within the network.

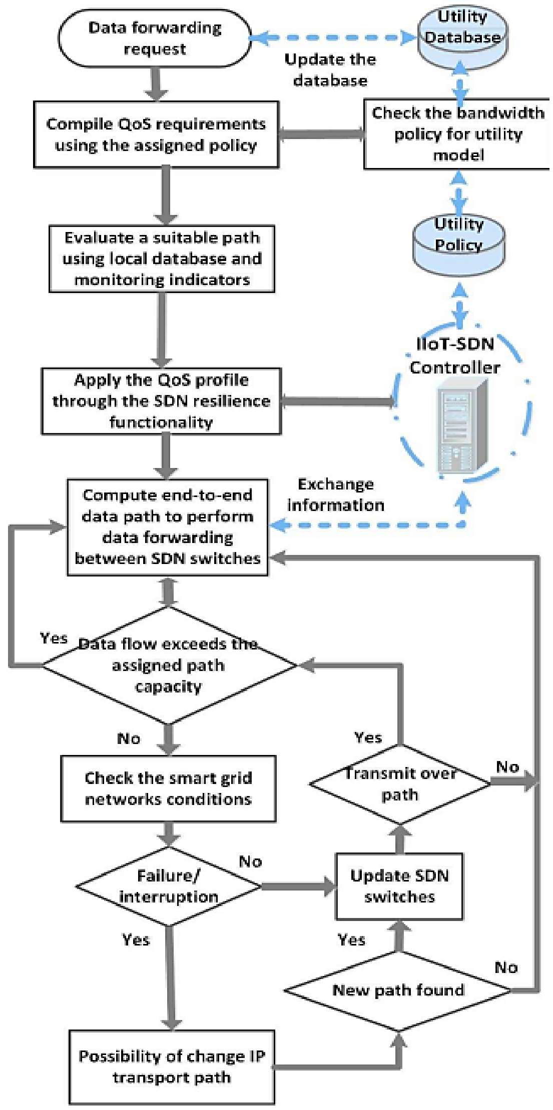
Data forwarding request
Utility Database
Update the database
Compile QoS requirements using the assigned policy
Check the bandwidth policy for utility model
Utility Policy
Evaluate a suitable path using local database and monitoring indicators
IIoT-SDN Controller
Apply the QoS profile through the SDN resilience functionality
Exchange information
Compute end-to-end data path to perform data forwarding between SDN switches
Yes
Data flow exceeds the assigned path capacity
No
Yes
Check the smart grid networks conditions
Transmit over path
No
Failure/ interruption
No
Update SDN switches
Yes
Yes
No
New path found
Possibility of change IP transport path

Fig.3 SDN-Based Network Configuration

Cross-Layer Approaches for Reliability

Cross-layer resilience leverages coordination among different network layers to optimise overall reliability and performance:

Quality of Service (QoS): The evaluation of a service's entire performance to gauge user satisfaction is known as QoS. These metrics, packet loss, latency, bandwidth, and network end-to-end delay, are utilized to assess its performance. Specifically, the type of application determines the QoS level in IoT low-power networks. For instance, some IoT applications, like smart metering, can withstand delays, but others, like forest fire detection, cannot. Therefore, it is crucial to take the QoS requirement into account when constructing the network to prevent poor network performance.

Adaptive Routing Strategies: AI- or context-aware routing algorithms dynamically adapt routes based on conditions such as congestion, energy consumption, or risk of threats, leading to improved resilience in the long run. For example, RPL includes extensions for dynamic routing for constrained IIoT networks.

Fault Tolerance: Strategies based on adaptive error correction, retransmissions, and load balancing can help ensure continued communication even under high interference or partial network failures. For example, DDS includes fault-tolerant publish–subscribe protocols.

Literature Review

This review highlights key trends, findings, and comparative insights from existing studies on resilient communication protocols in Industrial IoT, providing guidance for designing reliable, secure, and energy-efficient IIoT networks and informing future research and practical implementations in industrial automation and cyber-physical systems.

Sidna et al. (2020) this study offers an analysis of well-known protocols for Internet of Things applications, including HTTP, DDS, MQTT, AMQP, XMPP, and CoAP. To start, it introduces the various communication protocols by providing a general comparison of them. Then, it determines their relative merits and shortcomings by conducting an exhaustive and thorough examination of the associated procedure. Users can then utilise this comprehensive review to choose the best Internet of Things (IoT) application for their needs, taking efficiency and suitability into account. Data transmission in IoT applications relies heavily on the communication protocols [25].

Rashid, Pecorella and Chiti (2020) propose a new architecture for WSNs that moves required functions from unstable to stable and dependable domains in order to overcome these difficulties. Our work primarily contributes by addressing the fundamental network needs of IoT devices and by outlining several recommendations for the development of common virtualised protocols and features. Furthermore, we bring attention to a few significant unanswered questions and present a new design that strengthens IoT systems by making them more resilient and durable. Research into the Internet of Things (IoT) has recently taken centre stage, with specifications that aid network managers in designing and guaranteeing the capabilities and resources of every device [26].

Babiceanu and Seker (2019) proposes a unified modelling environment that can handle SDN application resilience and cybersecurity concerns related to virtual manufacturing systems. The research suggests a software-defined networking (SDN) manufacturing testbed and an ontology that documents the requirements of the VMS design phases in terms of cybersecurity and resilience. Afterwards, Cybersecurity resilience protection strategies for virtual manufacturing applications are described in the article that are based on software-defined networking (SDN). It ends with the planned research that will be necessary to put this structure into action. For a long time, industrial systems have been built to prioritise not only quality and productivity but also safety and reliability [27].

Jaloudi (2019) the goal of this research is to create an open and interoperable IIoT environment by studying protocols that rely on polling and those that rely on events. After much research and evaluation, the event-based, MQTT, the publish-subscribe protocol, has been chosen as the protocol for the Internet of Things (IoT). The research demonstrates that MODBUS specifies an optimised application layer message structure tailored to industrial applications. More than that, it proves that MODBUS TCP is not a replacement for event-oriented IoT protocols but rather that they supplement them. As a result, two plans for the IIoT infrastructure are put up. Data acquisition and Connected control systems, online monitoring, and industrial control systems can all benefit from the environment's openness and interoperability [28].

Lavric and Petrariu (2018) the Doppler effect, interference, and multi-path propagation fading; LoRa modulation employs chirp spread spectrum (CSS) technology to overcome these barriers. This method also provides excellent performance at low power consumption and a large budget for communication links. The fundamental contribution of this research is investigation of LoRa technology's sustainability and performance evaluation. In order to address the diverse requirements of IoT applications, Low-Power Wide-Area (LPWA) wireless networks have been developed to augment more conventional and shorter-range wireless communication methods [29].

Tao, Cheng and Qi (2018) proposed IIHub for IIOT is made up of three parts: an A-Hub, a CA-Module, and an LSP, or local service pool. Connecting diverse physical manufacturing resources is made possible by a series of configurable CA-Modules. Furthermore, the IIHub enables rapid design and deployment for smart connectivity and supports online development of manufacturing services using service encapsulation templates. To demonstrate the features and smart interconnection capabilities of the planned IIHub, a prototype is displayed. Smart analysis and accurate management that is interconnected are also within reach. The adoption of smart manufacturing practices is quickly becoming a shared objective among different national plans [30].

Table I summarizes recent studies on Resilient Communication Protocols for Industrial IoT, highlighting their approaches, key findings, challenges, and implications for SMEs in leveraging these platforms for business growth

Table 1 Literature Summary on Resilient Communication Protocols for Industrial IoT

Reference	Focus Area	Approach	Findings/Insights	Limitations / Open Issues	Key Performance Metrics
Sidna et al. (2020)	Evaluation of IoT communication protocols (MQTT, HTTP, XMPP, DDS, CoAP, AMQP)	Comparative analysis of characteristics, strengths, and limitations of IoT protocols	Provides guidelines for selecting appropriate communication protocols based on efficiency, suitability, and application needs	Lack of experimental deployment validation	Protocol efficiency, reliability, latency, scalability
Rashid, et.al. (2020)	Wireless Sensor Networks (WSNs) & IoT resilience	Proposed novel architecture shifting functionalities to stable domains; guidelines for virtualized protocols	Enhances resilience and robustness of IoT systems; identifies open research issues in IoT networking	Implementation challenges, scalability concerns	Network resilience, fault tolerance, virtualization overhead
Babiceanu et.al. (2019)	Cybersecurity & resilience in virtual manufacturing	SDN-based testbed; cybersecurity-resilience ontology; framework for secure virtual manufacturing	Integrated approach enhances reliability, productivity, and safety of manufacturing systems	Prototype stage, real-time testing missing	Security enforcement, reliability, productivity optimization
Jaloudi, et.al. (2019)	Protocols for IIoT interoperability	Comparison of polling-based & event-based protocols; MQTT chosen for publish-subscribe; MODBUS TCP used for industry	Event-oriented IoT protocols complement but do not replace MODBUS; two scenarios for IIoT integration proposed	Limited to specific industrial scenarios	Interoperability, SCADA integration, real-time responsiveness
Lavric et.al. (2018)	LoRa performance in LPWA networks	Performance evaluation using CSS modulation	LoRa offers interference resilience, low-power operation, and strong communication link budget	Bandwidth limitations, scalability issues	Energy efficiency, long-range coverage, interference resilience
Tao, et.al. (2018)	Industrial IoT hub for smart manufacturing	Proposed IIHub architecture with CA-Module, A-Hub, and LSP for interconnection	Facilitates heterogeneous device connection, smart service generation, and efficient management	Deployment complexity, integration with legacy systems	Service encapsulation, interoperability, configuration flexibility

Conclusion and Future Work

IIoT and CPS are transforming industrial operations by integrating networking, computation, and physical processes to enable real-time monitoring, automation, and intelligent control. This survey reviewed the architectures of IIoT and industrial CPS, highlighting the roles of sensors, actuators, controllers, and communication networks in facilitating autonomous and adaptive industrial processes. Key communication protocols, including LPWAN, WPAN, MQTT, CoAP, REST, XMPP, AMQP, WiFi, ZigBee, Bluetooth, Z-Wave, and LoRaWAN, were analysed in terms of performance, scalability, and security. The paper also discussed security challenges, such as standardization, interoperability, privacy, regulatory compliance, and cyber threats, and examined resilience mechanisms including self-protecting, self-configuring, and self-healing strategies, supported by SDN/NFV-based network virtualization, traffic redundancy, and cross-layer reliability approaches. Overall, IIoT and CPS technologies present opportunities to enhance productivity, efficiency, and reliability in industrial environment.

Future research directions include the development of unified standards for IIoT interoperability and security, energy-efficient and scalable communication protocols, and advanced resilience techniques leveraging AI-driven adaptive routing and predictive fault management. Integrating edge and fog computing with IIoT can further reduce latency and improve real-time analytics. Moreover, AI-enabled security frameworks for threat detection, mitigation, and self-healing mechanisms are essential for ensuring reliable industrial operations. Large-scale experimental testbeds and real-world deployments are also necessary to validate the performance, scalability, and robustness of emerging IIoT and CPS solutions

References

[1] P. Pathak, A. Shrivastava, and S. Gupta, "A Survey on Various Security Issues in Delay Tolerant Networks," J. Adv. Shell Program., vol. 2, no. 2, pp. 12–18, 2015.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," IEEE Trans. Ind. Informatics, vol. 14, no. 11, pp. 4724–4734, 2018, doi: 10.1109/TII.2018.2852491.

[3] A. Karmakar, N. Dey, T. Baral, M. Chowdhury, and M. Rehan, "Industrial Internet of Things: A Review," in 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), IEEE, Mar. 2019, pp. 1–6. doi: 10.1109/OPTRONIX.2019.8862436.

[4] X. Koutsoukos, "Systems Science of Secure and Resilient Cyberphysical Systems," Computer (Long. Beach. Calif)., vol. 53, no. 3, pp. 57–61, 2020, doi: 10.1109/MC.2020.2966109.

[5] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber Physical Systems and Internet of Things in Industry," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, Oct. 2018, pp. 2839–2840. doi: 10.1109/IECON.2018.8591610.

[6] A. Pereira, N. Rodrigues, J. Barbosa, and P. Leitão, "Trust and risk management towards resilient large-scale Cyber-Physical Systems," in 2013 IEEE International Symposium on Industrial Electronics, 2013, pp. 1–6. doi: 10.1109/ISIE.2013.6563837.

[7] M. Elattar, V. Wendt, and J. Jasperneite, "Communications for Cyber-Physical Systems," in Industrial Internet of Things: Cybermanufacturing Systems, 2017, pp. 347–372. doi: 10.1007/978-3-319-42559-7_13.

[8] F. Xia, X. Kong, and Z. Xu, "Cyber-Physical Control Over Wireless Sensor and Actuator Networks with Packet Loss," in Wireless Networking Based Control, 2011, pp. 85–102. doi: 10.1007/978-1-4419-7393-1_4.

[9] I. Jawhar, N. Mohamed, and J. Al-Jaroodi, "Networking architectures and protocols for smart city systems," J. Internet Serv. Appl., vol. 9, no. 1, p. 26, Dec. 2018, doi: 10.1186/s13174-018-0097-0.

[10] H. Chen, "Applications of Cyber-Physical System: A Literature Review," J. Ind. Integr. Manag., vol. 02, no. 03, p. 1750012, Sep. 2017, doi: 10.1142/S2424862217500129.

[11] S. Gupta and A. Mathur, "Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad Hoc Networks," in 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, IEEE, Jan. 2014, pp. 316–321. doi: 10.1109/ICESC.2014.60.

[12] D. Z. Lou, J. Holler, C. Whitehead, S. Germanos, M. Hilgner, and W. Qiu, "Industrial Networking Enabling IIoT Communication," 2018 Ind. Internet Consort., pp. 1–16, 2015.

[13] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[14] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," IEEE Commun. Surv. Tutorials, vol. 19, no. 2, pp. 855–873, 2017, doi: 10.1109/COMST.2017.2652320.

[15] S. Deshpande and R. M. Jogdand, "A Survey on Internet of Things (IoT), Industrial IoT (IIoT) and Industry 4.0," Int. J. Comput. Appl., vol. 175, no. 27, pp. 20–27, Oct. 2020, doi: 10.5120/ijca2020920790.

[16] S. Gupta, N. Agrawal, and S. Gupta, "A Review on Search Engine Optimization: Basics," Int. J. Hybrid Inf. Technol., vol. 9, no. 5, pp. 381–390, May 2016, doi: 10.14257/ijhit.2016.9.5.32.

[17] A. Balasubramanian, "Ai-Enabled Demand Response: A Framework For Smarter Energy Management," Int. J. Core Eng. Manag., vol. 5, no. 6, pp. 96–110, 2018.

[18] A. Mauthe et al., "Disaster-resilient communication networks: Principles and best practices," in 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), IEEE, Sep. 2016, pp. 1–10. doi: 10.1109/RNDM.2016.7608262.

[19] G. Punzo et al., "Engineering Resilient Complex Systems: The Necessary Shift Toward Complexity Science," IEEE Syst. J., vol. 14, no. 3, pp. 3865–3874, Sep. 2020, doi: 10.1109/JSYST.2019.2958829.

[20] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," Comput. Secur., vol. 97, p. 101996, Oct. 2020, doi: 10.1016/j.cose.2020.101996.

[21] H. Q. Al-Shammari, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Resilient Service Embedding in IoT Networks," IEEE Access, vol. 8, pp. 123571–123584, 2020, doi: 10.1109/ACCESS.2020.3005936.

[22] S. Pahune, "sensor data collection and performance evaluation using a TK1 board," Univ. Memphis Digit. Commons, 2019.

[23] U. A. Korat and A. Alimohammad, "A Reconfigurable Hardware Architecture for Principal Component Analysis," Circuits, Syst. Signal Process., vol. 38, no. 5, pp. 2097–2113, May 2019, doi: 10.1007/s00034-018-0953-y.

[24] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency," IEEE Internet Things J., vol. 6, no. 1, pp. 267–277, Feb. 2019, doi: 10.1109/JIOT.2017.2734903.

[25] J. Sidna, B. Amine, N. Abdallah, and H. El Alami, "Analysis and evaluation of communication Protocols for IoT Applications," in Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications, 2020, pp. 1–6. doi: 10.1145/3419604.3419754.

[26] A. Rashid, T. Pecorella, and F. Chiti, "Toward Resilient Wireless Sensor Networks: A Virtualized Perspective," Sensors, vol. 20, no. 14, p. 3902, Jul. 2020, doi: 10.3390/s20143902.

[27] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," Comput. Ind., vol. 104, pp. 47–58, Jan. 2019, doi: 10.1016/j.compind.2018.10.004.

[28] S. Jaloudi, "Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study," Futur. Internet, vol. 11, no. 3, p. 66, Mar. 2019, doi: 10.3390/fi11030066.

[29] A. Lavric and A. I. Petrariu, "LoRaWAN communication protocol: The new era of IoT," in 2018 International Conference on Development and Application Systems (DAS), IEEE, May 2018, pp. 74–77. doi: 10.1109/DAAS.2018.8396074.

[30] F. Tao, J. Cheng, and Q. Qi, "IIHub: An Industrial Internet-of-Things Hub Toward Smart Manufacturing Based on Cyber-Physical System," IEEE Trans. Ind. Informatics, vol. 14, no. 5, pp. 2271–2280, May 2018, doi: 10.1109/TII.2017.2759178.