scientific reports

Check for updates

OPEN

# 5G-based SharkNet protocol adaptation and wireless communication links

Yanzhang Xie[1,2], Wenyi Liu[1]✉ & Qingping Yang[2]

**5G communication technology has become well established in daily life, but its use in industrial control remains in its early stages of development. Due to its low latency and high reliability, 5G URLLC holds substantial potential for development in industrial control. Meanwhile, although SharkNet offers high transmission speed and reliability, its dependence on wired connections limits its coverage and flexibility.To address these limitations, this paper proposes a novel wireless communication link adaptation scheme that integrates 5G URLLC and SharkNet. We first conduct an in-depth analysis of the data packet formats and communication timing characteristics of both SharkNet and 5G protocols. Based on this analysis, we design a protocol conversion scheme and prototype a wireless link system. To validate the adaptability and performance of this scheme, we conducted a number of experiments to evaluate its reliability and latency. The experimental results indicate that compared with a transparent transmission approach, the proposed adaptation scheme significantly reduces communication latency and enhances reliability.**

**Keywords** Protocol adaptation, 5G, SharkNet, End-to-end latency, Wireless communication link

With the steady advancement of Industry 4.0, industrial automation is accelerating towards digitization and intelligence[1]. As the foundation of smart industries, the Industrial Control Network (ICN) plays a crucial role in industrial control systems. ICNs must meet stringent requirements for real-time performance, good reliability, and low jitter in industrial automation[2]. Currently, ICNs can be categorized into three main types: fieldbus, industrial Ethernet, and industrial wireless networks (IWN).

In traditional industrial communication, fieldbus and industrial Ethernet protocols dominate due to their superior real-time performance and reliability. For instance, the PROFIBUS protocol has a maximum transmission rate of 12 Mbps with real-time performance around 10 ms. For protocols like EtherCAT and PROFINET, with transmission rates reaching 100 Mbps, the former achieves real-time performance under 10 µs, while the latter varies by application scenario from 31.25 µs to 100 ms[3]. However, China lags in high-end bus technology development, facing challenges from technical patents and bottlenecks that limit current system performance. To address these challenges, SharkNet emerged as an innovative industrial fieldbus solution[4]. SharkNet (SharkNet Real-time Automatic Reconfiguration Network), developed independently by the Shanxi Provincial Engineering Research Center for New Industrial Buses, is a masterless network employing a store-and-forward mechanism. It supports high dynamic automatic reconfiguration, multipath redundancy, and time synchronization, making it widely applicable in measurement and control, aerospace, and industrial automation fields[4].

Although ICN protocols perform well, they still face limitations such as complex wiring, limited flexibility, and high maintenance costs. To address these issues, Industrial Wireless Networks (IWN) emerged as a solution. The main IWN protocols include Wireless HART, WIA-PA, and ISA100.11a, which are primarily used in industrial process automation with transmission rates around 250 kbps[5]. The WIA-FA protocol, designed specifically for factory automation, achieves a transmission rate of 54 Mbps with end-to-end latency of less than 10 ms[2].

SharkNet delivers outstanding performance through automatic reconfiguration, high speed, high reliability, and strong real-time capabilities. By balancing high-reliability control functions with optimized scheduling for large data volumes, it has built a solid foundation for advancing intelligence in areas like instrumentation and industrial control. However, as a wired network, it faces limitations in supporting mobile nodes and flexible deployment, which presents certain challenges to the highly adaptable requirements of smart industries:

[1]Key Laboratory of Instrumentation Science & Dynamic Measurement, Ministry of Education, North University of China, Taiyuan 030051, China. [2]Department of Mechanical and Aerospace Engineering, Brunel University London, Uxbridge, UK. ✉email: liuwenyi418@126.com

(1) Limitations in flexibility and scalability: Wired networks rely on fixed cabling, making it challenging to quickly adjust equipment layouts or expand to include new devices. Complex and fixed wiring restricts the flexibility needed for agile production within factories.
(2) High installation and maintenance costs: The initial installation process is complex and expensive, and later maintenance can be challenging. Cables are prone to damage, with repairs and troubleshooting being time-consuming and labor-intensive, leading to production interruptions and increased operational costs.
(3) Constraints in long-distance and complex environmental communication: The cost of long-distance wiring is high, and signal attenuation is significant. In complex industrial environments, cables are susceptible to damage, affecting network reliability and stability.
(4) Inability to meet modern automation and industrial IoT (IIoT) requirements: Wired networks face bottlenecks in supporting large-scale, fast-connected IIoT applications. Their slow upgrade pace fails to meet the needs of modern industry for high-speed transmission, flexible configuration, and real-time responsiveness.
(5) Limitations in real-time performance and device mobility: Traditional wired protocols underperform in high real-time applications, and physical cabling restricts the mobility of devices, making it challenging to support the free movement of mobile robots and automated transport equipment.

While wireless technologies such as IEEE 802.11ac/ax (Wi-Fi 5/6) have the potential to address some of these limitations, in the long run they will not be able to meet the requirements of fieldbuses such as SharkNet to cope with the demands of Industry 4.0 such as high flexibility. While IEEE 802.11ac/ax has high transmission rates[6] and is easy to deploy, there are several factors that make it unsuitable for the wireless expansion of SharkNet. First, both technologies are based on the CSMA/CA channel access mechanism, which does not guarantee deterministic latency of the transmission link[7], which would create a greater potential for disrupting the strong real-time performance of SharkNet. Second, they operate in unlicensed frequency bands which makes the transmission process more susceptible to interference, especially in industrial environments with strong electromagnetic interference[8]. Thirdly, their performance degrades significantly as the number of connected devices increases[9], thus neutering SharkNet's ability to support large-scale deployments of more than 50,000 end-devices and, in the long term, making it difficult to meet the requirements of future large-scale device support.

In contrast, the unique benefits of 5G technology, such as its ultra-reliable, low-latency communications (URLLC) capabilities, are a perfect fit for many of SharkNet's features. The 99.999% reliability and deterministic millisecond latency communication (URLLC)[10] that the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP) are committed to providing for industrial control applications can be a greater fit and maintain SharkNet's high performance characteristics. Licensed spectrum operation ensures robust interference immunity in industrial environments[11]. In addition, 5G's network slicing capabilities provide end-to-end quality of service guarantees[12], while its massive machine-based communication (mMTC) capabilities support the connectivity density required for large-scale deployments of SharkNet.

In this context, we will explore the wireless communication integration technology of SharkNet network based on 5G technology, aiming to break through the limitations of SharkNet wired network architecture in terms of flexibility and dynamic adaptability, and try to break through the existing 'pyramid' structure of hierarchical heterogeneous industrial control system and realise network flattening through the exploration of compatibility and adaptation between the two protocols. It also tries to break through the existing 'pyramid' structure of hierarchical heterogeneous industrial control systems and realise network flattening by exploring the compatibility between the two protocols. However, the application of 5G in the field of smart industry is still limited and immature. Therefore, this study proposes a novel SharkNet-5G wireless communication link adaptation scheme based on 5G URLLC technology and SharkNet network protocol. Specifically, we first analyse the frame structure features of SharkNet and 5G, and design an adaptive protocol scheme based on these features to achieve protocol parsing and conversion between SharkNet and 5G. Subsequently, we implement this adaptation scheme and construct a prototype wireless link system based on 5G and SharkNet.

To assess the feasibility of the protocol adaptation scheme and verify the prototype system's performance, we conducted a series of experiments. The results demonstrate that the proposed wireless link system not only overcomes many limitations of wired fieldbus networks but also, compared to transparent transmission, effectively reduces latency without a significant drop in reliability.

The main contributions of this paper are as follows:

(1) Focusing on the emerging industrial bus SharkNet, we propose an adaptation scheme for protocol parsing and conversion between the SharkNet network and 5G protocols, and experimentally compare this adaptation scheme with the transparent transmission method.
(2) We developed a 5G-based SharkNet wireless link prototype system, achieving end-to-end transmission, network address translation, and automatic protocol adaptation.
(3) Through extensive experimentation, we evaluated the effectiveness and reliability of the proposed scheme and prototype system, demonstrating its advantages over traditional wired networks.

The remainder of this paper is organized as follows: Section "Related work" provides a brief overview of related work on multi-protocol integration and the integration of industrial control protocols with 5G and wireless technologies. Section "Protocol analysis on SharkNet and 5G" analyzes the frame structures of the SharkNet and 5G protocols. Section "Protocol adaption of SharkNet and 5G" details the adaptation scheme for SharkNet and 5G protocols. Section "Experimental evaluation" outlines the development process of the SharkNet wireless link system prototype based on commercial 5G. Section "Conclusions" presents the experimental evaluation

of the protocol adaptation wireless link based on SharkNet and 5G versus transparent transmission. Section 7 concludes the paper and discusses future research directions.

## Related work

With the arrival of Industry 4.0, the industrial sector demands higher levels of intelligence and scalability. However, existing traditional industrial network protocols are diverse and lack compatibility, making it challenging to meet these new requirements. To address this limitation, substantial research has explored potential solutions. For instance, Wei et al. proposed an architecture to connect WIA-PA and WirelessHART to the IPv6 Internet[13]. Gil et al. integrated HTTP, MQTT, LoRaWAN, and OPC UA into an IoT platform for smart power applications, addressing multi-scenario issues[14]. Kulik et al. proposed a software architecture for data format conversion between different industrial protocols[15]. Shi et al. implemented an industrial IoT system based on MQTT and OPC UA[16]. Silva et al. designed an IoT gateway prototype to bridge traditional Modbus RTU devices to the MQTT network[17]. While these studies have effectively extended traditional industrial networks to support industrial IoT, most of them rely on low-rate network protocols, limiting their ability to meet the demands for higher speed, low latency, and high reliability in today's industrial sector.

Additionally, some research has attempted to combine fieldbus and industrial Ethernet protocols with wireless technologies to improve communication quality. Botero et al. proposed a PROFIBUS industrial wireless gateway based on ZigBee technology[18]. Zhou and Yuan designed an FPGA-based embedded gateway that combines 4G technology with the PROFIBUS-DP industrial protocol[19]. Wu and Xie investigated interoperability between the EtherCAT protocol and IEEE 802.11/802.15.4 wireless standards[20]. Morato et al. proposed implementing the EtherCAT-based Fail-Safe over EtherCAT (FSoE) protocol over IEEE 802.11 WLAN[21]. Furthermore, Wu and Xie explored the feasibility of interconnecting PROFINET with wireless standards like IEEE 802.11 via bridging or gateways[22]. Trancă et al. designed an innovative industrial communication system based on ZigBee that aggregates data from multiple Modbus slaves[23]. Although these studies successfully integrated industrial Ethernet with IWN, they frequently lack thorough testing and validation of performance metrics within industrial control applications.

With the rapid advancement of 5G technology, some studies have deeply integrated Time-Sensitive Networking (TSN) with 5G to explore the possibilities of achieving low latency and high reliability for the Industrial Internet. Yang et al. proposed a new uplink transmission method to provide TSN services for a 5G-based industrial IoT prototype system[24]. Nikhileswar et al. constructed a TSN over 5G testbed based on 3GPP Release 15 hardware, discussing the measurement methods and key performance indicators to meet the timing requirements of industrial control applications[25]. Satka et al. introduced a traffic conversion technique between 5G and TSN, evaluating it through industrial case studies[26]. These studies demonstrate some progress in fulfilling the time precision and data transmission demands of industrial automation environments through the combination of 5G and TSN, although practical applications in the industrial sector remain challenging.

Although various studies have explored the application of 5G in the industrial domain (as shown in[27–29]), protocol adaptation schemes for 5G with industrial fieldbuses are still at an early stage of exploration. Khoshnevisan et al. evaluated a 5G prototype system in an industrial setting using the PROFINET protocol[27]. Ghassemian et al. provided a comprehensive overview of the 5G-VINNI facilities in the UK, including the development of 5G test infrastructure encompassing backhaul, edge computing, slicing, interoperability, and validation[28]. Ansari et al. evaluated 5G wireless performance in a real industrial production environment[29].

In summary, existing research highlights a shortage of systematic studies on protocol adaptation, prototype development, and experimental evaluation, which underscores the need for this study.

## Protocol analysis on SharkNet and 5G

Compared with existing fieldbuses, SharkNet offers significant improvements in architecture, protocol design, transmission speed, reliability, and real-time performance. This section provides a detailed overview of the main characteristics and protocol structure of SharkNet and discusses its adaptation scheme with the 5G protocol.

### Main features of SharkNet

SharkNet is composed of switches and terminal devices. The switches are responsible for core network data forwarding and routing, supporting up to 31 full-duplex ports and expanding the network through six-level cascading. Each switch is identified by a 16-bit address and contains a data exchange center that stores routing tables and processes data packets. Terminal devices connect to the SharkNet network via control and status interfaces, supporting parallel, UART, and SPI data transmission modes. SharkNet can connect over 50,000 terminal devices, with redundancy in the terminal interface module's uplink ports to ensure high reliability and flexibility, meeting diverse application requirements.

Additionally, SharkNet combines the strengths of international industrial buses with advanced communication technologies. It operates independently of existing network protocols, utilizing an entirely new network architecture that addresses Ethernet's shortcomings in industrial applications. SharkNet's main features include:

(1) Fully autonomous innovation: SharkNet adopts a completely self-developed network architecture, data structures, and protocol system. It is independently designed and developed at the code level, with full intellectual property rights, incorporating multiple underlying technologies for controlled technical details.
(2) Wide-speed support for heterogeneous media: Unlike traditional buses such as 1553B and Ethernet-based systems, which have limited adaptability in speed and media, SharkNet supports transmission speeds from 1 Kbps to 4 Gbps, accommodating various media like fiber optics, LVDS, and RS422, thus overcoming these limitations.

(3) High reliability in connectivity: SharkNet supports point-to-point, ring, tree, and mesh hybrid topologies. Its mesh redundancy topology provides over 4,000 physical redundant paths, ensuring high reliability at a low cost. It also supports multi-network redundancy, with options for single-network dual redundancy and dual-network quadruple redundancy transmission, using a first-come-first-served merge algorithm.
(4) High-precision automatic time synchronization and strong real-time determinism: SharkNet incorporates an enhanced IEEE 1588 PTP time synchronization protocol that runs automatically without configuration, achieving nanosecond-level precision. Unlike Ethernet-based buses, SharkNet supports prioritized message transmission, ensuring high real-time performance. Its 80-bit parallel processing core matches the data packet width, with checksum and error correction handled without additional time, ensuring precise clock forwarding and controllable data transmission time to meet strict real-time application requirements.
(5) High-dynamic network auto-reconfiguration and optimal path routing: SharkNet features a unique auto-reconfiguration capability that is completely transparent to users, requiring no configuration. Switches automatically detect port changes, dynamically update the network, and isolate faults, always selecting the optimal path. When a link fault occurs, SharkNet automatically restores the optimal route as long as a physical path exists. The system maintains network consistency and completeness, eliminating coordination costs between users and lowering the barrier to entry.
(6) Support for high-dynamic network decomposition and fusion: In highly dynamic applications, traditional buses struggle to meet demands. As a masterless, peer-to-peer network, SharkNet can autonomously manage network decomposition and fusion in high-dynamic topologies without a central control node. When a local network is disconnected, subnetworks reconfigure as independent networks. When reconnected, SharkNet automatically detects and triggers fusion, without user intervention.
(7) Guaranteed network scalability: Its network architecture is specially designed to cope with the growth in device size. Each switch supports free connection of up to 32 peer ports, which can cover more than 50,000 end devices through six levels of cascade expansion. When the number of connected devices increases, SharkNet employs a multi-dimensional strategy to safeguard network performance. At the network structure level, it dynamically adjusts the communication range through network packet management (up to 16 packets can be set) to effectively control network broadcast storms. At the data transmission level, it supports up to 1024 virtual links (VLs) and assigns independent traffic parameters to each VL through a traffic control mechanism to ensure rational allocation of bandwidth resources and avoid over-occupation of network resources by individual nodes. Especially when the network scale expands, SharkNet's automatic reconfiguration mechanism can quickly respond to topology changes and ensure the network's self-recovery capability through periodic network reconfiguration (with adjustable period), while continuously optimising communication paths based on multi-level routing algorithms to reduce network congestion. In addition, SharkNet adopts a layered service scheduling strategy: Time Trigger (TT) to reserve a deterministic time window for critical services, Traffic Profile (TP) to ensure that bandwidth is reasonably allocated according to priority, and Best Effort (BE) for non-critical services to maintain network quality of service despite the increase in the number of devices and the amount of traffic.
(8) Multi-level security assurance: SharkNet implements a multi-level security protection mechanism. At the port access control level, a 32-bit dynamic security password is set through the port access password check (PPC) mechanism, so that only devices that have passed the password verification can access the network. At the data transmission level, data integrity is ensured by Cyclic Redundancy Check (CRC) and Error Correcting Coding at Subset Distance (ECCSD), where the ECCSD technique corrects the packet mode field without adding additional error correction bits. At the system control level, register write protection prevents misoperation and supports packet management to limit the communication range between different groups. Together, these mechanisms form SharkNet's basic security protection system at the protocol level. In addition, higher-level security mechanisms such as data encryption and access control can be further implemented in the application layer according to specific needs.

## SharkNet protocol frame structure

All information in the SharkNet bus is processed and transmitted using a unified 10-byte frame, referred to as the basic packet, which differs from the Ethernet frame length (64 to 1518 bytes). The data operation units within network devices are also based on 10-byte segments. Commands, status information, and data transmissions utilize different packet types, mainly classified into message packets and data packets.

Message packets are used for transmitting commands, status updates, and response information, having the highest priority, and usually only requiring a single basic packet. Message packets are further divided into internal, external, and user-defined message packets. Internal message packets are for network device interactions, helping maintain network consistency and enabling built-in functions such as port probing, auto-reconfiguration, and time synchronization; these are inaccessible to users. External message packets allow users to invoke network functions, such as reading device addresses, register read/write operations, and command broadcasts. User-defined message packets enable users to define message formats according to specific application needs.

Message packets follow a standard 80-bit format (as shown in Fig. 1), with each field defining a different function. The mode field specifies the packet type and priority, while the source and destination address fields identify the source and destination terminal devices, respectively. These addresses are embedded into the message packet during transmission, and the network forwards the packet to the correct terminal device based on the destination address. In the SharkNet network, all devices are uniformly addressed, with unique addresses assigned to each device. Values from $0\times0001$ to $0\times1FFF$ indicate switch devices, while values from $0\times2000$ to 0xFFFF indicate terminal devices. Parameter fields 1 and 2 set packet attributes and are transferred to the destination terminal device; these contents come from the upper-layer Application Data Unit (ADU, shown in the figure as PDU) and form the Protocol Data Unit (PDU, shown in the figure as ADU) needed for the lower-

| Modes Domain | Source Address Domain | Target Address Domain | Parameter Domain 1 | Parameter Domain 2 | Control Domain | Check Domain |
|---|---|---|---|---|---|---|
| 79...72 | 71...56 | 55...40 | 39...32 | 31...16 | 15...8 | 7...0 |
| Message Packet | Source Terminal Device Address | Destination Device Address | Parameter 1 | Parameter 2 | Control Info | CRC |
| 1 Byte | 2 Bytes | 2 Bytes | 1 Byte | 2 Bytes | 1 Byte | 1 Byte |

PDU

ADU

**Fig. 1**. Frame structure of the message packet.

| Modes Domain | Source Address Domain | Target Address Domain | Parameter Domain 1 | Parameter Domain 2 | Control Domain | Check Domain |
|---|---|---|---|---|---|---|
| 79...72 | 71...56 | 55...40 | 39...32 | 31...16 | 15...8 | 7...0 |
| 09-Data Starter Packages | Source Terminal Device Address | Destination Device Address | Parameter 1 | Parameter 2 | Control Info | CRC |
| 1E-Data Access Packages | 9 Bytes Data | | | | | |
| 09 - End of Data Packages | 9 Bytes Data or User-defined Information | | | | | |
| 1 Byte | 2 Bytes | 2 Bytes | 1 Byte | 2 Bytes | 1 Byte | 1 Byte |

PDU

ADU

**Fig. 2**. Frame structure of the data packet.

layer frame structure. Additionally, each switch port stores three dynamically reconfigurable optimal paths, with the control field used to select the appropriate transmission path. The checksum field, located in the last byte, uses CRC for verification.

The data packet format, shown in Fig. 2, has a lower priority than message packets. Data packet transmission requires a data packet header (start packet) and a data packet trailer (end packet) to form a complete data structure. The mode field for the data start packet is $0 \times 09$, which transmits the source device address, target device address, parameters 1 and 2, control information, and CRC. The data continuation packet has a mode field of $0 \times 1E$, carrying 8 bytes of data and allowing for additional byte transfer. The data end packet has a mode field of $0 \times 07$ and transmits the source device address, target device address, parameters 3 and 4, control information, and CRC. Within the frame structure, data continuation packets beginning with $0 \times 1E$ form the upper-layer ADU (PDU as shown in the figure), and the entire frame structure constitutes the lower-layer protocol data unit PDU (ADU as shown in the figure).

For bulk data transfer, multiple basic packets are combined to form a composite packet. The data start and end packets include CRC checksum information and define the overall size of the data packet. Although SharkNet does not impose strict limits on packet length, to ensure real-time performance and channel sharing, the number of continuation packets in each data packet is typically limited to 256. The data start and end packets pass attributes through packet parameters, enabling the receiver to anticipate or verify the data. Data continuation packets transmit only data without additional field overhead, reducing transmission time and improving bandwidth efficiency.

## 5G protocol frame structure

5G data is transmitted through wireless channels, with its ADU divided into multiple fields according to the levels of the protocol stack. The 5G New Radio (NR) protocol stack is separated into the control plane and the user plane protocol stack[30]. During data transmission, terminal data is transmitted via the TCP/IP protocol to

the SDAP (Service Data Adaptation Protocol) sublayer within the user plane protocol stack. As shown in Fig. 3, the uplink frame structure in the user plane includes several fields:

- The lower-layer PDU section (shown as ADU in the figure) includes: a 1-bit PDU type identifier, a 1-bit reserved identifier, a 6-bit QoS flow identifier, and the actual IP data packet being transmitted.
- The upper-layer ADU section (shown as PDU in the figure) is the IP data packet along with its associated upper-layer protocol data, encapsulated in the PDU for transmission.

These fields are used for data encapsulation and transmission at the link layer. The data then passes sequentially through the PDCP (Packet Data Convergence Protocol) sublayer, the RLC (Radio Link Control) sublayer, and the MAC (Medium Access Control) sublayer before ultimately reaching the physical layer (PHY). Each protocol layer adds the necessary control information to the data packet to ensure accurate data transmission.

Traditional wireless communication technologies typically use a fixed physical layer frame structure, as early application scenarios had low demands for frame structure flexibility. However, with the growing demand for 5G technology across various services, researchers have redefined the physical layer frame structure of 5G NR. By combining fixed subframes with variable timeslots, this new frame structure can accommodate complex dynamic service requirements and significantly enhance network utilization[31]. The design of the PDU field and the QoS flow ID within the frame structure assists the link layer in dynamically managing data transmission quality, ensuring prioritized handling for different services.

## 5G URLLC features for industrial applications

This section details the technical characteristics of the 5G URLLC used in the SharkNet wireless link. This study explores the possibility of expanding the SharkNet fieldbus network wirelessly by designing the link based on the basic communication capabilities provided by the 5G network, so that SharkNet can better meet the requirements of high dynamics and high flexibility proposed by Industry 4.0.

*Physical layer transmission*

5G technology adopts Adaptive Modulation and Coding (AMC). Depending on the channel quality, the system can dynamically select different modulation methods such as QPSK, 16QAM or 64QAM to achieve high-speed data transmission while ensuring transmission reliability. In terms of coding technology, the control channel adopts Polar Code coding, while the data channel uses Low Density Parity Check (LDPC), which significantly improves the coding gain and strengthens the anti-interference capability[32]. In addition, the system further enhances signal quality and transmission reliability through multi-antenna MIMO technology and beam fouling[33].

*Transmission delay control*

5G URLLC reduces the transmission time interval (TTI) to 0.125 ms by adopting the mini-slot transmission mechanism, while its flexible frame structure design allows for multiple frame transmissions within a single time slot, which ensures timely transmission of important frames such as control frames[34]. For SharkNet's periodic control data, the network can take advantage of 5G's Semi-Persistent Scheduling (SPS) scheme[35], which reduces latency by pre-allocating a fixed number of transmission resources and avoiding the additional delay caused by frequent resource requests. In addition, 5G technology controls transmission jitter at multiple levels in order to deal with delay fluctuations that can be caused by network congestion and interference in wireless transmissions. At the physical layer, the technology reduces the transmission BER by dynamically adapting the modulation coding scheme (MCS) to channel variations, while precoding and interference coordination techniques are used at the MAC layer[36]. The synergy of these techniques ensures end-to-end transmission delay stability.

*Reliability assurance*

5G URLLC implements a multi-layered protection mechanism. At the data transmission level, the technology's hybrid automatic retransmission request (HARQ) mechanism quickly detects and retransmits erroneous packets[37]. For particularly important control frames, the system can use packet replication transmission to ensure 99.999% transmission reliability by sending the same packet over multiple paths simultaneously[38]. Combined with SharkNet's own CRC checksum retransmission mechanism, a double protection system is formed, providing a reliable data transmission guarantee for industrial control applications.

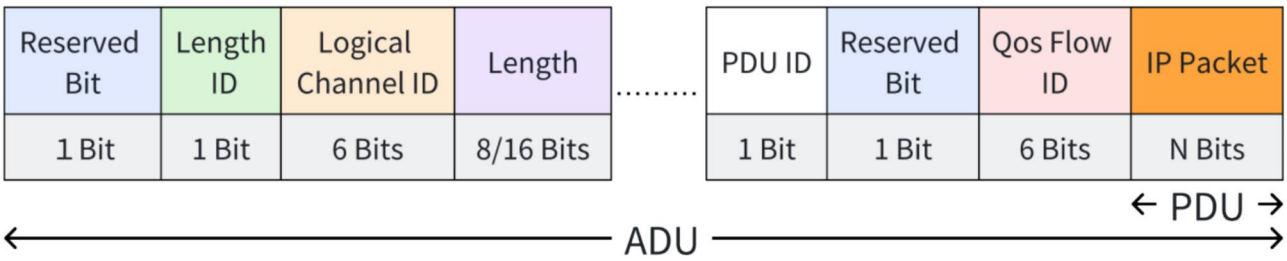


**Fig. 3**. Data link layer user plane uplink frame structure.

*Multi-terminal access management*
5G network provides reliable device authentication and access mechanism. Through network slicing technology, the system can provide differentiated quality of service assurance for different types of services[39]. SharkNet can assign a unique identification to each terminal based on this technology, and handle the data transmission demand of multiple terminals through resource scheduling mechanism to ensure the communication quality of each terminal. Compared with traditional industrial wireless technologies such as WirelessHART and WIA-FA[5], the system can achieve higher transmission rates (1Gbps uplink, 2Gbps downlink) and lower end-to-end latency.

*Scalability support*
5G technology provides robust support through massive machine class communication (mMTC) features. Base stations can support dense connectivity of 1 million terminal devices per square kilometer, meeting the demand for large-scale terminal deployment in industrial scenarios[40]. Meanwhile, through flexible subcarrier spacing (SCS) configuration and dynamic spectrum allocation, the system can dynamically adjust wireless resources according to the number of access devices[41]. At the resource scheduling level, a combination of centralised and distributed scheduling is used to ensure resource utilisation efficiency under large-scale access scenarios as well as service quality[42]. In addition, based on network function virtualisation (NFV) and software-defined network (SDN) technology, the system can flexibly expand network capacity according to the scale of access devices[43].

It is worth noting that since the current research is based on commercial 5G networks, the configuration rights of some advanced functions are in the hands of operators. In the future, if the industrial private network can be deployed or more network configuration rights can be obtained, the system performance will have more room for improvement. For example, the real-time performance and reliability of the system can be further improved by means of refined QoS parameter configuration and network slicing resource optimisation[44,45]. Based on the above 5G technology features, our SharkNet wireless link system will achieve relatively stable and reliable wireless communication.

## Protocol adaption of SharkNet and 5G

### Network architecture of SharkNet with 5G protocol adaptation

Although SharkNet boasts high reliability and redundancy design for industrial applications, the latency fluctuations caused by its wired transmission medium in complex, dynamic environments limit its real-time performance, especially under high loads or with frequent node changes. Leveraging the sub-millisecond low latency of 5G URLLC can significantly enhance the real-time performance and reliability of SharkNet, particularly in industrial control scenarios. Additionally, while SharkNet supports up to 50,000 terminal devices through cascading, the complexity and high maintenance costs of wired connections constrain scalability, especially in applications requiring rapid deployment or mobile terminal access. 5G wireless connectivity can improve flexibility and scalability by reducing cabling requirements, facilitating the rapid deployment of terminal devices over large areas, and expanding system coverage.

As shown in Fig. 4, the SharkNet network supports various adaptable interfaces and protocols, including RS-485, LVDS, and Ethernet, and achieves high reliability and flexibility through tree, ring, and mesh hybrid topologies. Switches, as the core components of SharkNet, are responsible for routing and forwarding data packets and connect to terminal devices via multiple adaptable interfaces. However, as industrial systems scale up and demand for flexibility increases, the limitations of SharkNet's wired architecture have become more apparent, particularly in large-scale distributed systems where cabling complexity and maintenance costs grow significantly. Therefore, we aim to organically integrate 5G technology with SharkNet to provide greater possibilities for industrial control networks, enhancing their convenience and scalability.

### Wireless link with protocol adaptation module

To enhance SharkNet's flexibility and scalability in industrial applications, we designed a 5G-based protocol adaptation module. The architecture of the SharkNet wireless communication link with this module is shown in Fig. 5. This module connects SharkNet with terminal devices and switches via a 5G wireless link, supporting multiple protocol conversions to ensure seamless communication across different transmission media. The wireless communication link comprises a switch module, a protocol adaptation module, and a terminal system module. The switch is responsible for sending and receiving SharkNet messages, the protocol adaptation module performs protocol conversions between 5G and SharkNet, and the terminal system module connects various terminal devices. The protocol adaptation module, through an interface adapter, is compatible with multiple communication media such as RS-485, LVDS, and Ethernet, ensuring seamless data switching between different transmission media.

Figure 6 further illustrates the specific implementation of this design. The protocol adaptation module consists of a 5G module and a Linux-based control system. The 5G module includes the RF unit and the 5G processing module, while the Linux control system consists mainly of the storage unit and the Ethernet interface. On one side, the switch connects to the protocol adaptation module through interfaces like RS-485 (or alternatively Ethernet, LVDS, etc.), and on the other side, it connects to the terminal system using the same interfaces. The protocol adaptation module transmits SharkNet data to a Raspberry Pi 4B for read, write, and temporary storage through interface adaptation. This data is then encapsulated and decapsulated by the 5G module, which ultimately communicates wirelessly with the 5G base station via the RF unit, enabling remote data transmission.

With this design, we expect the wireless communication link to not only reduce SharkNet's wiring complexity but also significantly enhance its scalability and flexibility in high-load, complex environments. This improvement is anticipated to make SharkNet more adaptable to a wide range of industrial application requirements.

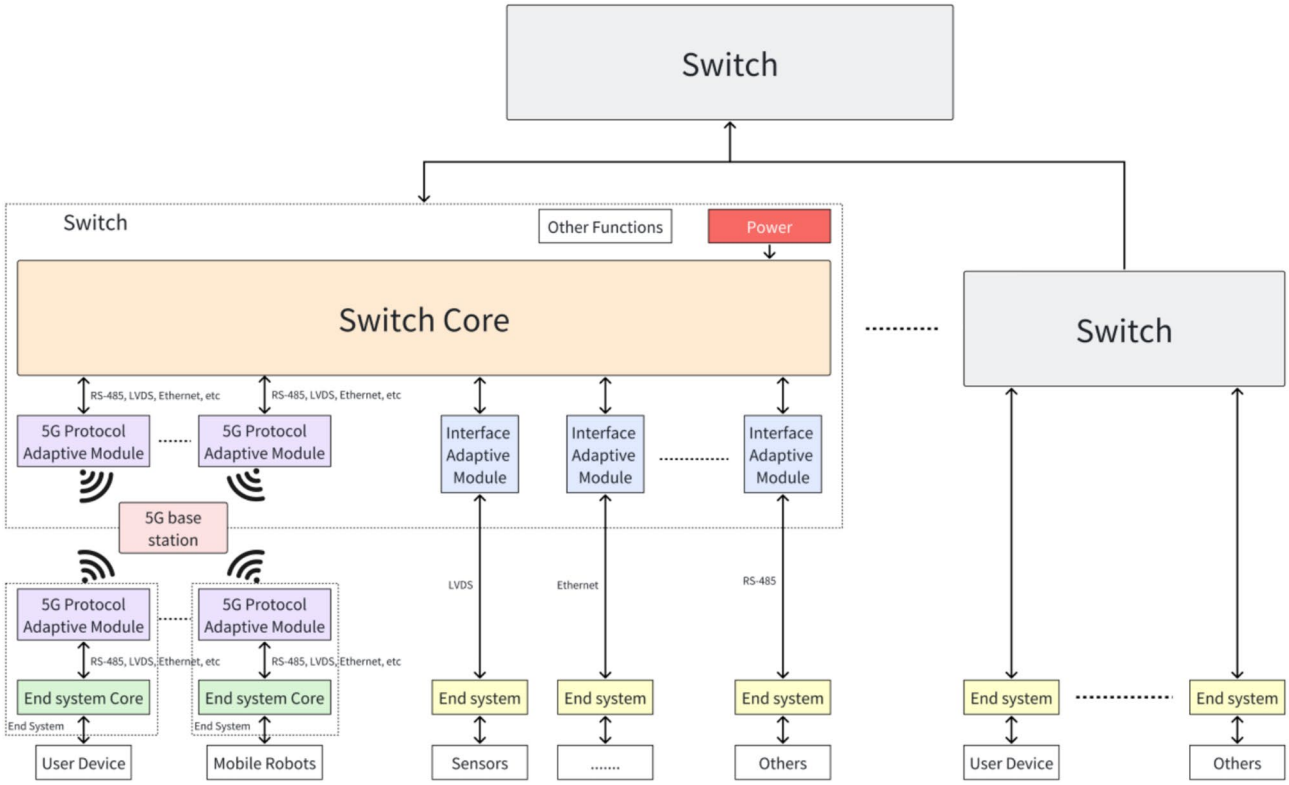


**Fig. 4**. Partial architecture of SharkNet hybrid network with 5G protocol adaptation.

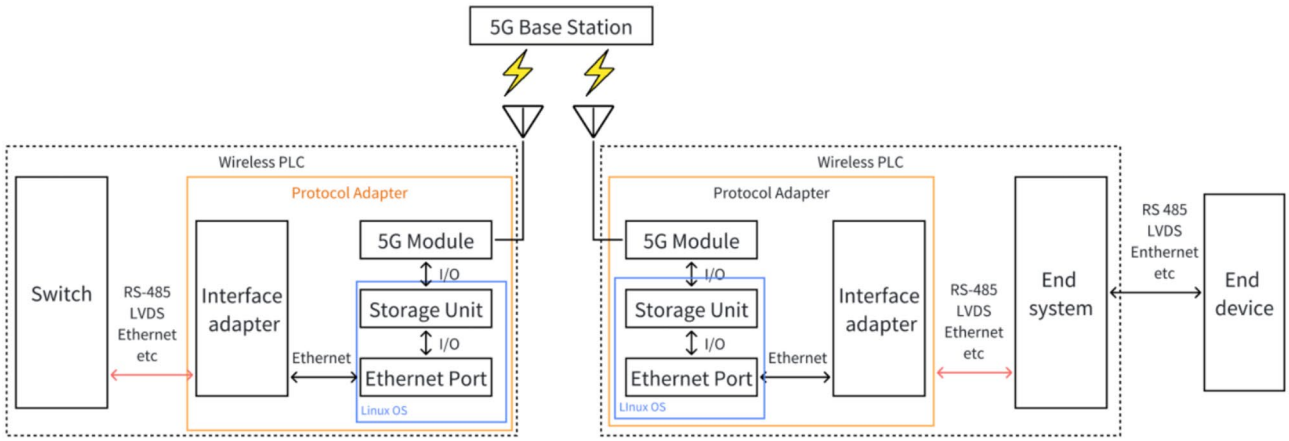


**Fig. 5**. SharkNet wireless communication link prototype.

In the actual implementation, the protocol adaptation module connects the switch and terminal system via Ethernet, while the 5G module carries data streams based on the TCP/IP protocol. To achieve this, we employed a socket-based approach to handle data reception, parsing, storage, conversion, and transmission. This method not only ensures efficient communication but also preserves the integrity of critical data within the SharkNet frame structure during parsing, maintaining data consistency and completeness.

In order to meet the requirements of establishing a network with multi-device grouping or multiple concurrent link connections, the transmission link (based on this architecture) adopts a multi-threaded management architecture for the cloud server part, in addition to technologies such as traffic control based on the SharkNet protocol and network slicing and QoS management based on the 5G protocol. The main thread is dedicated to monitoring the client connection status to ensure that the wireless link system can respond to new connection requests in a timely manner, while the sub-threads are responsible for handling routing table updates, broadcasting and data transmission operations. This multi-threaded structure greatly improves the system's concurrent processing capability and data transmission efficiency. In addition, the cloud server

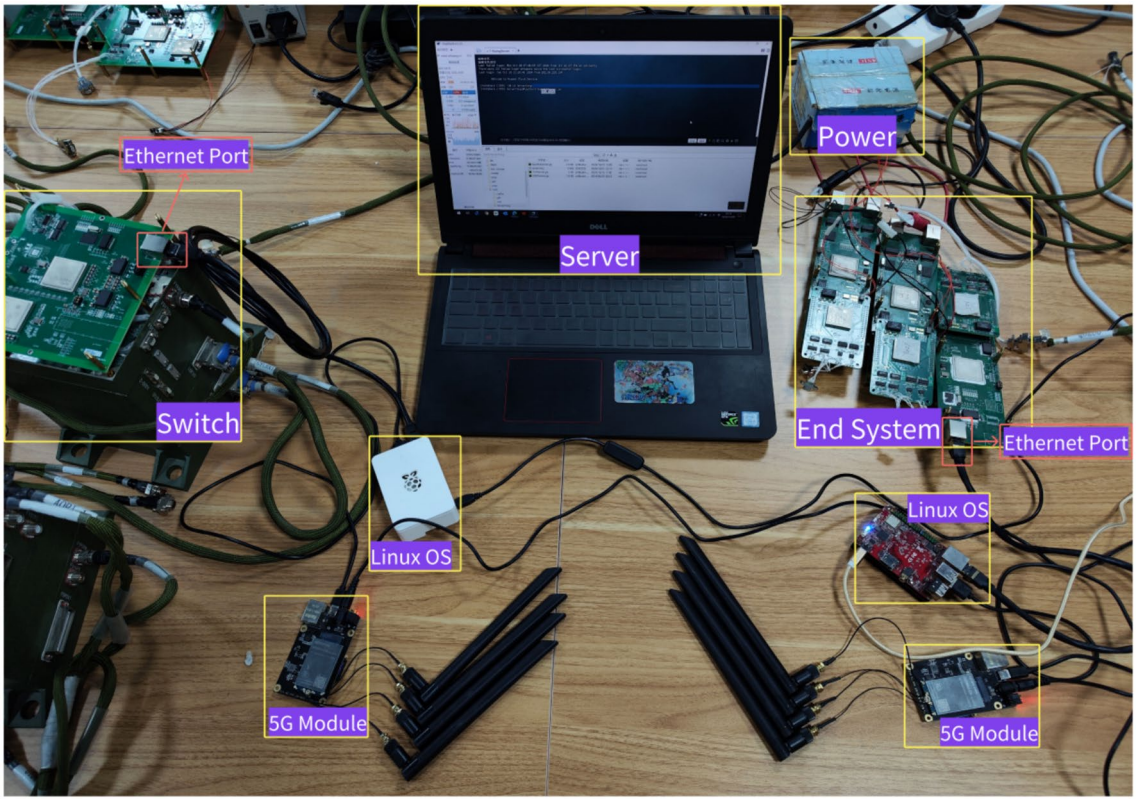


**Fig. 6**. Implementation of SharkNet wireless communication system.

optimises thread resource management through thread pooling, which reduces system overhead and further improves performance and response time.

## SharkNet and 5G protocol adaptation

In Section "Protocol analysis on SharkNet and 5G", we analyse the SharkNet and 5G frame structures in detail. Specifically, we first gain a comprehensive understanding of the frame structures of SharkNet and 5G to prepare for how each structure is unpacked and repacked in this protocol adaptation section. Based on Section "Protocol analysis on SharkNet and 5G", we propose the protocol adaptation scheme shown in Fig. 5 to establish an end-to-end wireless communication link between SharkNet and 5G. The core of this scheme is to ensure seamless adaptation between SharkNet and 5G protocols to support efficient and stable data transmission. The specific adaptation steps are as follows (the process is shown in Fig. 7):

(1) SharkNet protocol unpacking on the sending side: After receiving the verified SharkNet message frame, the module first unpacks it, removes the header, extracts key data, and temporarily stores it.
(2) 5G protocol packing on the sending side: the critical information from the stored SharkNet message frame is then encapsulated with a 5G protocol header, aligning it with the required format for 5G transmission.
(3) 5G protocol unpacking on the receiving side: The received 5G data frame undergoes 5G protocol unpacking, where the header is removed, and key data is extracted and temporarily stored.
(4) SharkNet protocol packing on the receiving side: The temporarily stored key data is then re-encapsulated with a SharkNet protocol header, reconstructing the SharkNet frame structure, followed by verification to ensure data integrity and protocol compatibility.

In this protocol adaptation scheme, the transmission reliability of the wireless link is ensured by detecting the retransmission method. This is because for SharkNet packets (10-byte basic packets), retransmission of a complete and correct packet is more time and computationally efficient than performing error correction. In addition, the 5G protocol has a multi-layer verification mechanism (e.g., acknowledgement mode and retransmission mechanism at the RLC layer) that automatically detects packet loss or transmission errors during wireless transmission. If there is a problem with a packet during wireless transmission, the protocol automatically initiates a retransmission request to ensure that the receiver receives the complete and correct packet.

As a result, the 5G-based wireless portion of the transmission remains highly reliable without a significant impact on SharkNet's data transmission. In addition, SharkNet itself includes a comprehensive set of authentication and retransmission mechanisms. After the SharkNet protocol has been repackaged, any incorrect packets are discarded without being passed on to the upper layers, and a retransmission request is automatically initiated. If the packet is correct, a confirmation response is sent to the sender. This double-checking mechanism

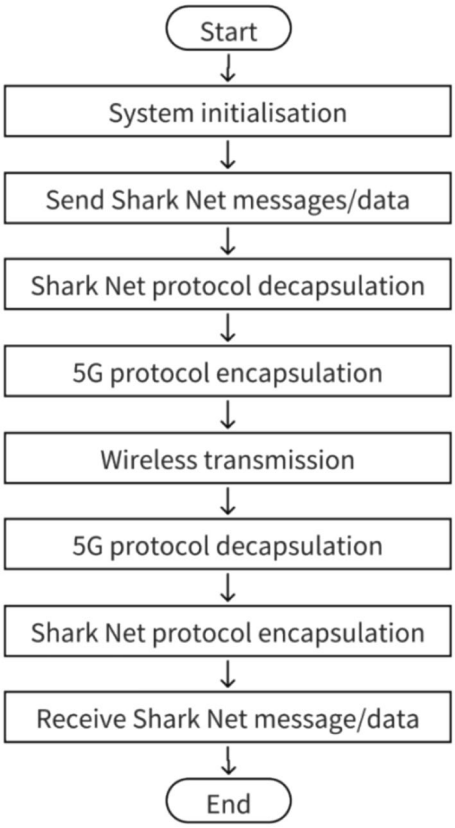


**Fig. 7**. SharkNet-5G protocol adaptation.

combines the advantages of 5G and SharkNet to ensure high reliability of data transmission in the protocol adaptation scheme to a certain extent, while keeping the computational overhead low and minimising the impact on the link and the strong real-time performance of the system. In conclusion, this adaptation scheme effectively ensures data interoperability between the two protocols, enabling efficient communication between SharkNet and 5G networks in a variety of application scenarios.

## 5G encapsulation and decapsulation of SharkNet PDU

Before the 5G protocol can encapsulate SharkNet protocol packets, the validity of the SharkNet frame structure must be rigorously verified to ensure the accuracy and integrity of the data transmission. This validation process includes step-by-step parsing and checking of the mode, address, parameter, control, and checksum fields, and discarding the packet and initiating an automatic retransmission if a field contained in a field is abnormal; otherwise, the next field is checked. After completing all verifications, the system allocates unpacking frames according to the bytes in the SharkNet frame structure and temporarily stores the unpacked PDU data. The parsed SharkNet PDU data will be encapsulated by the 5G protocol stack, ready for transmission over the wireless channel.

After unpacking the SharkNet frame structure, the SharkNet data is converted to 5G data through the 5G NR protocol stack. Figure 6 illustrates the encapsulation and decapsulation process within the 5G protocol. To enable transmission of SharkNet PDU data over the wireless channel, the data must pass through the data link layers of the 5G user plane protocol stack, including SDAP, PDCP, RLC, MAC, and the physical layer. The specific steps are as follows (The specific process is shown in Fig. 8):

(1) Application layer transmission: SharkNet PDU data is transferred to the application layer via the TCP/IP protocol.
(2) SDAP sub-layer mapping: At the application layer, each IP data packet is mapped to a Data Radio Bearer (DRB) through the SDAP sub-layer's QoS flow mapping. This mapping process selects different DRBs based on the QoS requirements of each service, ensuring differentiated quality of service (QoS) transmissionCP Sub-layer Processing[46].
(3) PDCP sublayer processing: where it undergoes IP header compression, encryption, and integrity protection to ensure data confidentiality and integrity[46].
(4) Rnsmission at the RLC Sub-layer: At the RLC sub-layer, data is encapsulated into RLC SDUs and transmitted in sequence over various logical channels. This sub-layer supports Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM). In AM, any erroneous packets trigger a retransmission mechanism, ensuring data reliability.

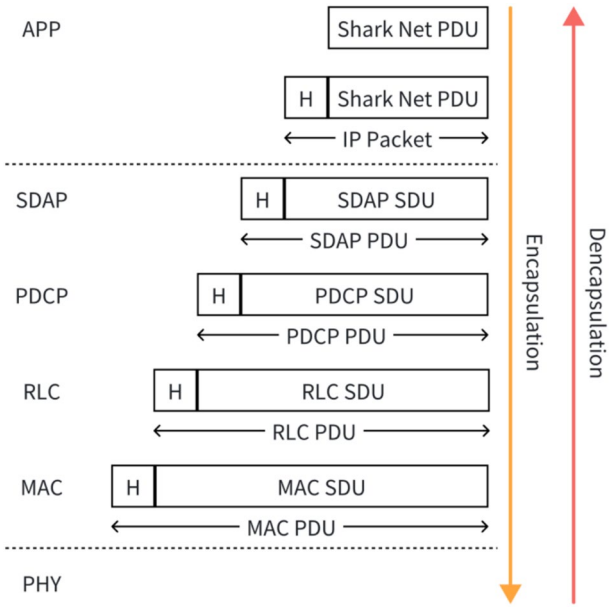


**Fig. 8**. Encapsulation and decapsulation process of the 5G Protocol.

(5) Link adaptation at the MAC Sub-layer: Through link adaptation, the data is passed to the MAC sub-layer, where the layer dynamically selects the appropriate transmission block size based on current network conditions, optimizing instantaneous throughput to meet the time-varying characteristics of wireless transmission[47].
(6) Physical lassion: After being encapsulated by the MAC layer, data enters the physical layer, where it undergoes modulation, coding, and error detection before being transmitted over the wireless channel.
(7) This layered encapsulation and decapsulation process ensures that SharkNet PDU data can be transmitted efficiently and securely within the 5G NR network.

## Discussion of NAT issues in wireless link networks

Since this study uses a SIM card, 5G public base station, and corresponding core network provided by a carrier, we found that, even with the 5G module connected to the public network and the IP address and port known, direct communication between devices remains unachievable. This is due to the carrier's core network utilizing NAT (Network Address Translation) and firewall mechanisms to manage devices. The known IP address is actually a private IP within the local network, which obstructs direct communication between devices.

*Solution 1: cloud server intermediary*

To address this issue, we implemented a cloud server as an intermediary for communication. In this setup, the cloud server performs network address translation between public and private networks, successfully establishing a communication link between the two 5G modules, thereby enabling bidirectional data transmission. As shown in Fig. 9a, the cloud server acts as a data relay, adapting and converting data streams between the SharkNet and 5G protocols.

The advantage of this approach is its simplicity and ease of rapid deployment. However, it increases communication latency due to reliance on the cloud server and incurs additional operational costs. This solution suits our current experimental environment and offers a quick and effective workaround.

*Solution 2: customized SIM card and carrier permissions*

Another option is to negotiate with the carrier to obtain a customized SIM card and enable permissions within the core network to allow direct device-to-device communication. This solution would fundamentally resolve the NAT issue, eliminate cloud server relay latency, and improve communication efficiency. However, the process of obtaining a customized SIM card is complex and time-consuming, involving deep customization of the carrier's network and adjustments to permissions, making it challenging to implement. Therefore, although this solution holds promise for the future, it is not suitable for our current experimental timeframe.

*Solution 3: private core network*

A third solution is to use a private SIM card and a dedicated core network, where devices in the system no longer need to connect to the commercial 5G public network, allowing direct communication between the two 5G modules (e.g., tested with the Ping command) without reliance on the cloud server for data relay, as illustrated in Fig. 9b. This approach eliminates latency and instability introduced by the public network, ensuring higher communication efficiency.

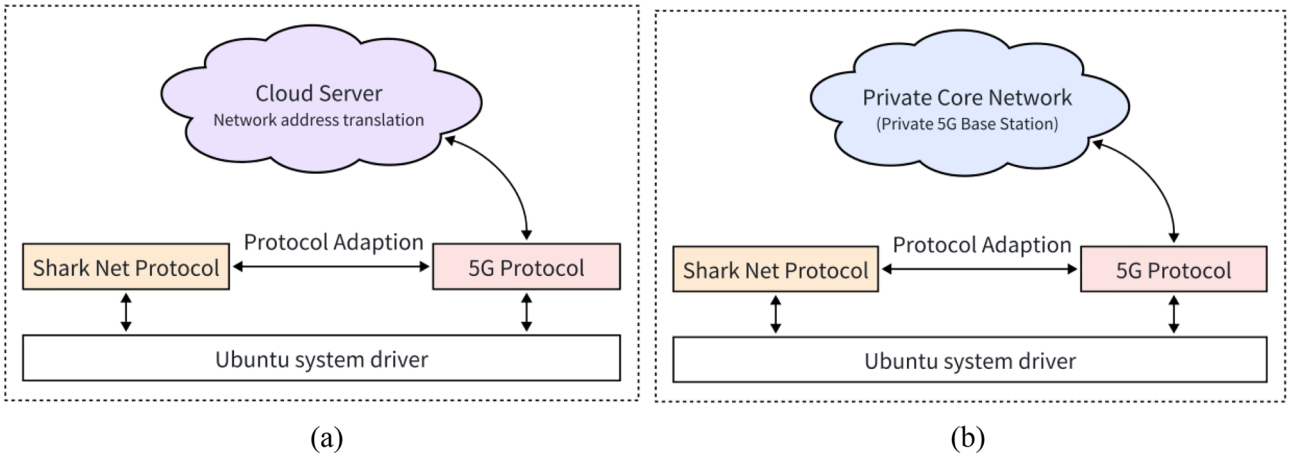


**Fig. 9**. (**a**) Software architecture of wireless link with public network connection (**b**) Software architecture of wireless link with private network connection.

However, building a private core network involves significant costs and requires specialized equipment and custom network architecture. As a result, we decided not to adopt this solution at this time. Once the project is successfully deployed, we plan to further assess and potentially implement a private core network solution to support large-scale industrial applications.

In summary, at this stage, the cloud server intermediary solution is our primary approach. While it introduces some latency and additional costs compared to other options, it is relatively simple to implement and convenient for experimental deployment. The customized SIM card and private core network solutions offer greater potential for the future, but due to current time and cost constraints, we plan to evaluate and implement them in later phases.

To address communication issues in public network connections, we introduced NAT (Network Address Translation) technology in conjunction with the cloud server intermediary solution. When two wireless link modules connect to the core network, NAT maps the modules' private IP addresses and port numbers to a public IP and corresponding port number. This translation process ensures that devices within the local network can communicate over the Internet using a unique public IP, overcoming the limitation of private IP addresses that cannot be used directly on the public network.

By integrating NAT with the cloud server, the solution enables modules' private IP addresses and ports to be mapped to a public IP and port. This ensures that devices within the local network can communicate via a unique public IP address, thus avoiding the issue of private IP addresses being unusable on the public network. Figure 10 illustrates the application of NAT within the wireless link system, where the cloud server acts as a critical intermediary.

In this architecture, combining NAT with the cloud server, the cloud server manages communication and data forwarding with both modules through the public IP, resolving the issue of modules being unable to communicate directly on the public network. The cloud server not only facilitates wireless data exchange between the two modules but also provides a reliable remote communication link via the public network. This architecture ensures system security within a wide-area network and offers flexibility and scalability for future expansion, such as supporting additional devices or cross-regional link modules.

## Experimental evaluation

### Experimental preparation

To evaluate the performance of the proposed wireless link prototype system, we chose to test it in a random indoor environment (within 5G signal coverage) and selected link delay and reliability as representative key metrics for evaluation. Table 1 lists the main relevant parameters of the experiment and the system.

In terms of hardware, the system mainly adopts Raspberry Pi 4B as the main control platform, whose ARM Cortex-A72 architecture combines small size, high performance and low power consumption. This not only meets the design requirements of the system, but also provides flexibility for further scalability and future optimisation. Secondly, the system uses the RM500U-CN 5G module (supporting the 3GPP Release 16 standard), which can operate in both SA and NSA modes. In the study, the SIM card required by the module we use China Mobile SIM card to connect to the public network for related tests.

We compare two transmission methods: transparent transmission of SharkNet frames and protocol-adapted transmission. The end-to-end delay (based on the timestamp difference between the switch and the end system test node) and the link reliability (based on the message reception ratio of the messages received by the switch to those sent by the end system in the interval between the adapted control commands are sent) are measured and evaluated by four sets of experiments, and the average value of each set of experiments is used as the final result of the analysis. Transparent transmission is the transmission of SharkNet frames without unpacking and directly packetised by the 5G protocol; protocol adaptation is the transmission of SharkNet frames after unpacking and

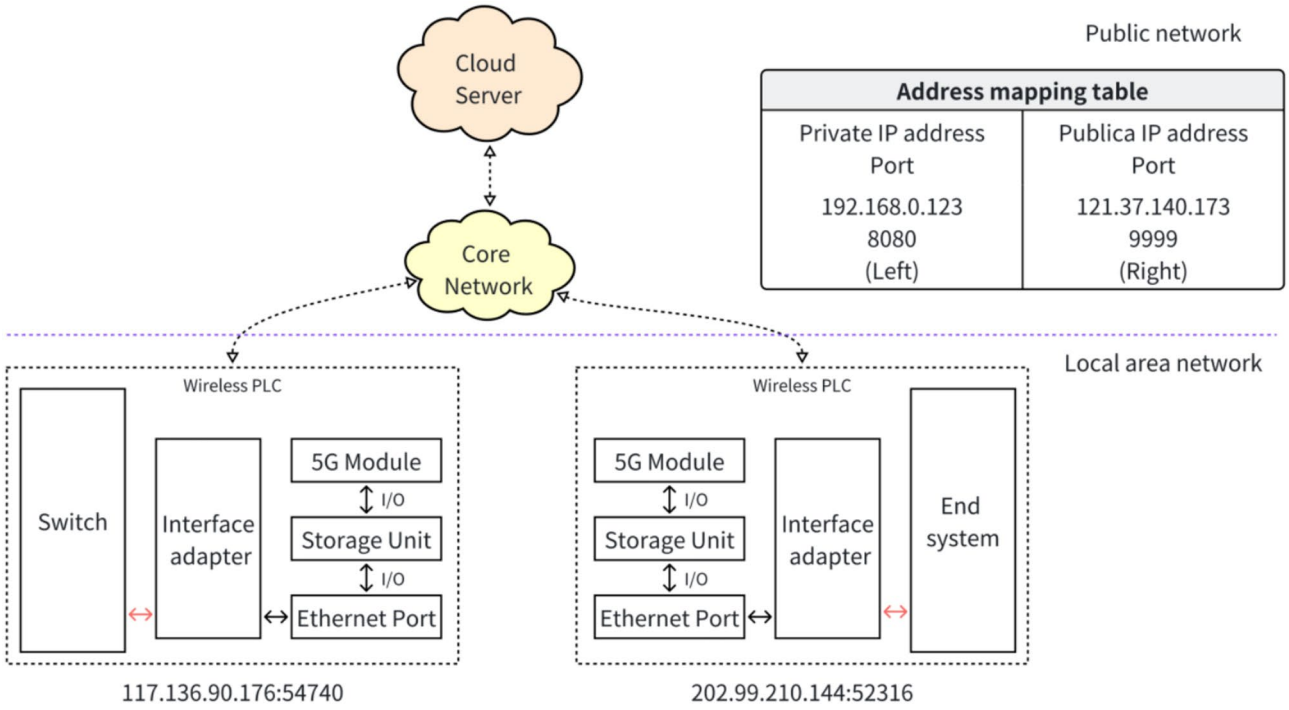


**Fig. 10**. Network address translation architecture for wireless link.

| Parameter | Value/Range |
|---|---|
| Test environment | Indoor laboratory setting |
| Test distance | Within 5G signal coverage |
| network Mode | Public 5G network (China Mobile) |
| Control platform | Raspberry Pi 4B (ARM Cortex-72) |
| 5G module type | RM500U-CN (Release 16) |
| 5G maximum upload speed | 1 Gbps (Based on SA mode) |
| 5G maximum download speed | 2 Gbps (Based on SA mode) |
| SharkNet frame size | 10 bytes |
| Control command interval | 10–100 ms |
| Data packet load range | 500–5000 packets |

**Table 1**. Key parameters of the wireless link system and experimental setup.

| Component | Operating mode | Power consumption |
|---|---|---|
| Raspberry Pi 4B | Active mode | Approx. 3.0–7.0 W (depending on load) |
| | Idle mode | Approx. 0.8–2.0W |
| RM500U-CN 5G module | Active mode | Approx. 2.4–4.2W |
| | PSM mode | Approx. 13.69mW |

**Table 2**. Transmission link power consumption composition analysis.

then packetised by the 5G protocol, and when the 5G packets are received at the receiving end, they are unpacked by the 5G protocol, and then packetised by the SharkNet into the SharkNet core network for transmission.

## Power consumption analyses

In order to assess the feasibility of the proposed link in real industrial applications, the power consumption characteristics of the wireless link system are analysed in this section. The main power consumption components of the system include the control platform (Raspberry Pi 4B) and the 5G communication module (RM500U-CN). Table 2 lists the power consumption data of each component in different operating modes.

Analysis of the power consumption data shows that the overall power consumption of the system is mainly composed of two parts: the Linux control platform and the 5G module. The control platform exhibits a large power consumption fluctuation range (3.0–7.0W) under different loads, which is mainly due to the computational load variation when handling tasks such as protocol conversion and data processing. The 5G module, on the other hand, achieves extremely low standby power consumption (< 14mW) through the PSM (Power Saving Mode) energy saving mode, which is important for improving the overall energy efficiency of the system.

For industrial application scenarios with long-term operation, the system adopts the following strategies to optimise energy efficiency performance. The control platform dynamically adjusts the CPU frequency according to the actual data processing requirements, reducing unnecessary power consumption while ensuring performance. 5G modules automatically enter PSM mode during data transmission intervals, significantly reducing standby power consumption, a strategy that is particularly suitable for industrial control scenarios with periodic data transmission. In addition, the system reduces the peak load on the control platform by optimising task scheduling for protocol conversion and data processing, thereby reducing maximum power consumption.

To further optimise the energy-efficient performance of the system, more fine-grained power control strategies can be introduced in the future, protocol conversion algorithms can be optimised to reduce processing loads, and dynamic power regulation mechanisms based on load prediction can be explored. With these optimisation measures, the system can achieve higher energy efficiency while ensuring performance, providing long-term stable operation in industrial sites.

## Result analysis and discussion

Figure 11 presents the end-to-end latency results for SharkNet with 5G protocol adaptation and transparent transmission. The experimental results clearly reveal an approximate 8 ms difference in latency performance between the transparent transmission and protocol adaptation schemes under various data packet loads.

As the number of data packets gradually increased from 500 to 5000, both schemes exhibited an upward trend in link latency. However, the protocol adaptation scheme demonstrated significantly lower latency than the transparent transmission scheme, with a more gradual increase. This outcome is primarily due to differences

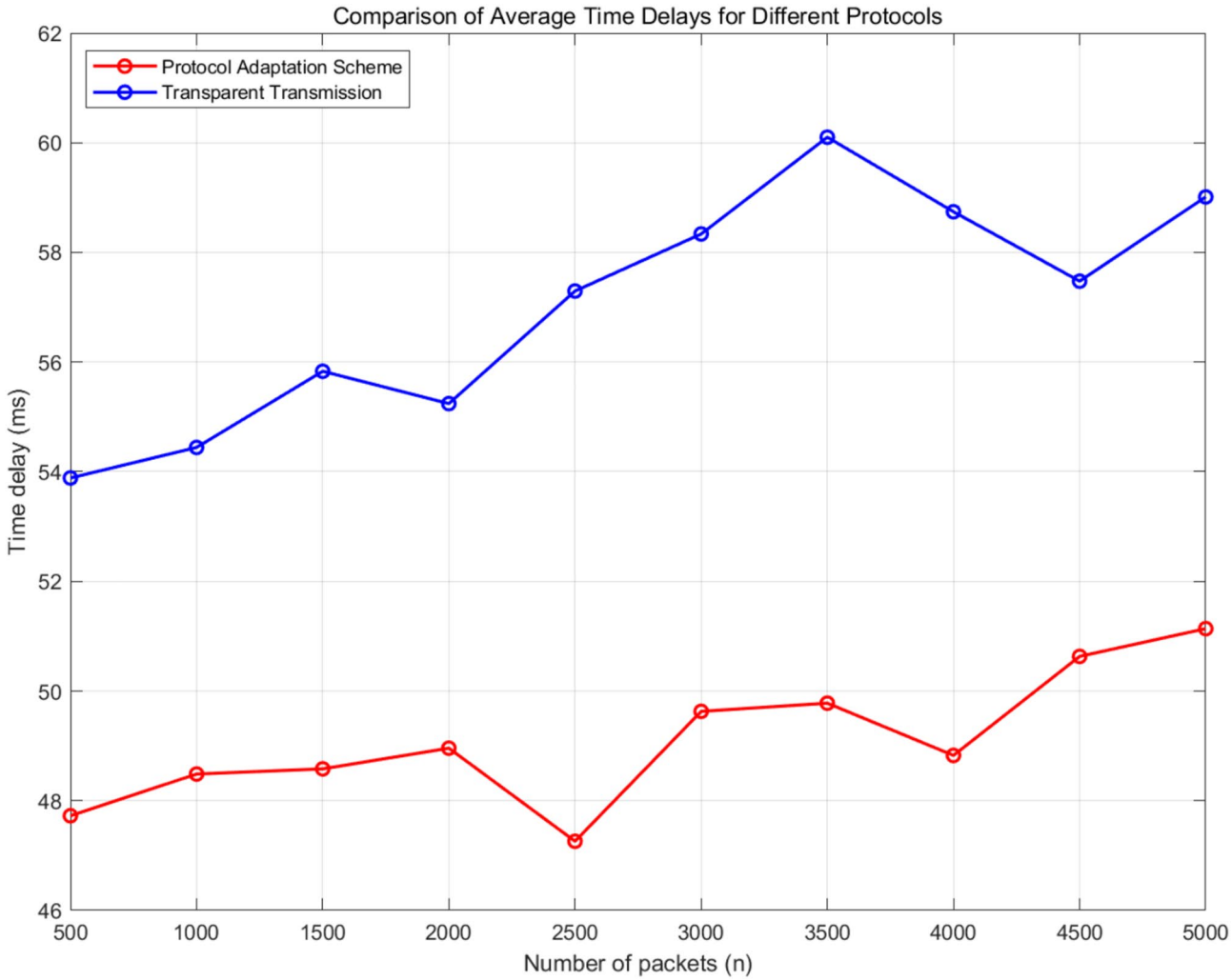


**Fig. 11**. End-to-end latency comparison between SharkNet protocol adaptation and transparent transmission.

in their transmission mechanisms: in transparent transmission, SharkNet data packets are directly encapsulated within the 5G protocol, while in the protocol adaptation scheme, SharkNet packets are first unpacked and then re-encapsulated within the 5G protocol. Consequently, each packet in the protocol adaptation scheme contains fewer bytes, resulting in smaller packet sizes. Additionally, the protocol adaptation scheme incorporates improved packet scheduling and timing optimization within the link, effectively reducing latency accumulation, even under high load conditions.

By optimizing packet format and communication timing, the protocol adaptation scheme minimizes additional latency during protocol switching and wireless transmission. The experiments indicate that latency remains relatively stable across different loads with the protocol adaptation scheme, demonstrating its higher adaptability and resilience under heavy packet loads.

Furthermore, the data reveals fluctuations and occasional spikes in link latency. This instability may be attributed to several factors: the cloud server's intermediary instability, uncertainties in the commercial 5G network, and dynamic user load variations within the 5G base station coverage area. These factors can impact latency, causing fluctuations in transmission delay.

In addition, the data shows fluctuations and occasional spikes in link latency. In addition, we can see from Fig. 11 that the current link latency is higher than 46 ms and its link latency composition is shown in Fig. 12. We can see that instabilities such as link latency and jitter can be mainly attributed to the cloud server intermediary, the instability and uncertainty of the public 5G network, and the dynamic user load variations in the 5G base station coverage area.

In summary, the protocol adaptation scheme can significantly reduce data transmission latency in large-scale industrial control scenarios, enhancing system real-time performance. In industrial control systems, low latency directly affects the timely execution of control commands and system responsiveness. Compared with the transparent transmission scheme, the protocol adaptation scheme maintains low latency and high stability while effectively managing uncertainties caused by load fluctuations, providing superior performance for industrial wireless communication. Overall, the latency advantage of the protocol adaptation scheme not only improves SharkNet's communication efficiency but also enhances its resilience in complex environments. Supported by 5G URLLC technology, the network's low-latency characteristics are further amplified, laying a solid foundation for the real-time performance and reliability of future industrial control systems.

To test the reliability of the wireless link prototype, we used a smooth spline function to fit the discrete data of six known test nodes to a continuous curve, thereby estimating values for other unknown test nodes. Figure 13 presents the reliability comparison between the SharkNet with 5G protocol adaptation and the transparent transmission schemes under different control cycles. The experimental results indicate that as the control command interval increases from 50 to 100 ms, both the transparent transmission and protocol adaptation schemes show improved reliability, yet with notable differences.

Under a 50 ms control cycle, the reliability of the protocol adaptation scheme is slightly higher than that of transparent transmission. As the control interval lengthens, the reliability of transparent transmission gradually increases, while the protocol adaptation scheme reaches comparable reliability levels more quickly and shows a faster rate of improvement. The reliability curve of the transparent transmission scheme exhibits slower growth in shorter control cycles (50 to 70 ms), suggesting its limitations in handling data within shorter intervals. In contrast, the protocol adaptation scheme demonstrates greater adaptability and responsiveness, maintaining high reliability even under shorter control cycles. This advantage stems from improvements in protocol conversion, packet optimization, and timing adjustments within the protocol adaptation scheme, enabling it to maintain link stability effectively and complete data packet transmission within shorter timeframes, even under high-frequency data transmission conditions.

In summary, the protocol adaptation scheme demonstrates superior reliability not only in long control cycles but also under short cycles. This reliability advantage is particularly critical for industrial control systems, especially in scenarios with high-frequency control commands, where the protocol adaptation scheme better ensures the stability of the communication link and the integrity of data transmission, preventing control delays or system response errors due to transmission failures. Overall, the protocol adaptation scheme outperforms the transparent transmission approach in terms of reliability, reaching ideal reliability levels more quickly in short-cycle, high-frequency communication environments, demonstrating greater adaptability and interference resistance. Supported by 5G URLLC technology, the protocol adaptation scheme provides more robust real-time performance and reliability assurance for industrial control systems, serving as an effective tool for enhancing communication reliability.

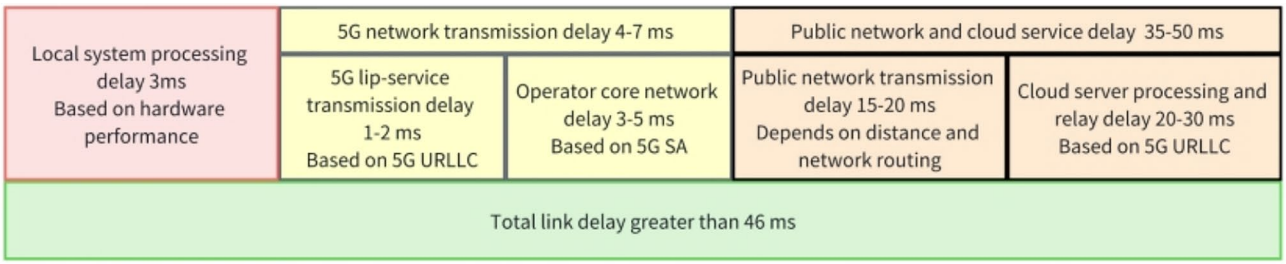


**Fig. 12**. Schematic diagram of link delay composition.

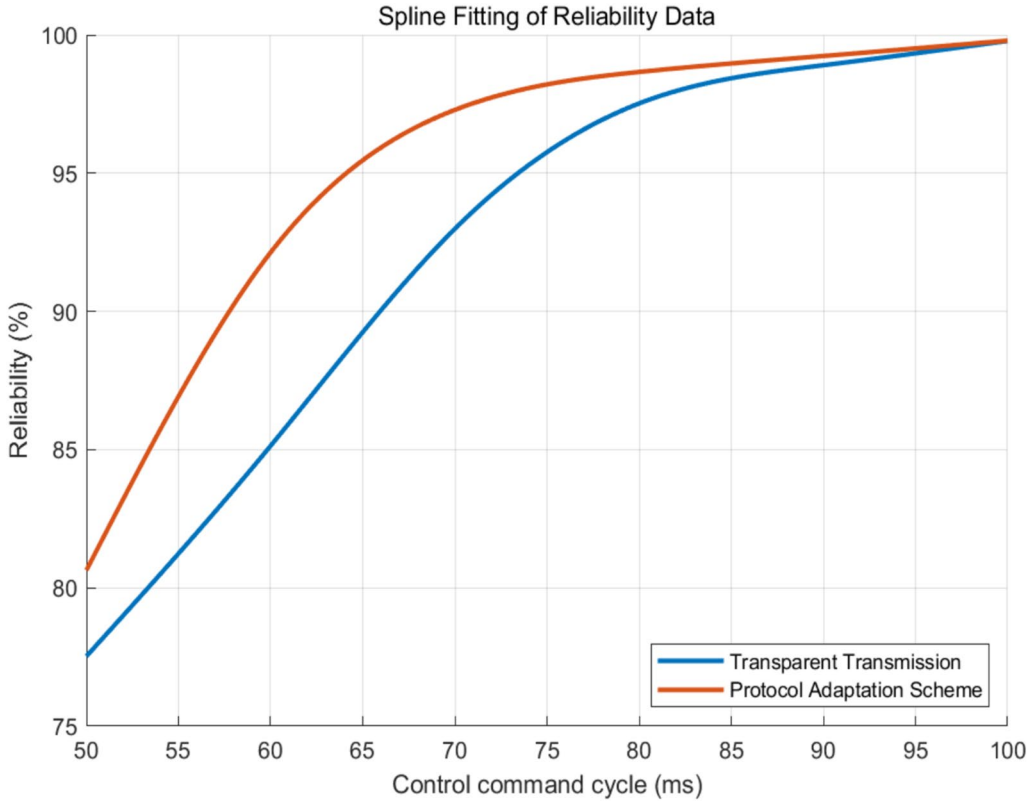


**Fig. 13**. Reliability comparison between SharkNet protocol adaptation and transparent transmission.

## Conclusions

This paper presented a novel wireless communication link protocol adaptation scheme that combines 5G URLLC technology with the SharkNet industrial fieldbus. By designing a protocol parsing and conversion mechanism, this scheme addresses the limitations of traditional wired SharkNet communication, such as complex wiring, limited coverage, and low flexibility, enabling efficient wireless adaptation. This approach not only significantly enhances communication flexibility and real-time performance but also expands system coverage capabilities.

Furthermore, a 5G and SharkNet-based wireless link prototype system was developed and validated, achieving successful end-to-end transmission and automatic protocol adaptation. Experimental results have shown effective verification of seamless interoperability between SharkNet and 5G protocols. This prototype system offers an important technical reference and support for the development of similar wireless communication applications in the industrial control field. Through extensive experiments, the study evaluated the performance of the proposed protocol adaptation scheme. Results have shown that compared with the transparent transmission method, the protocol adaptation scheme significantly reduces communication latency, while maintaining high reliability and exhibiting superior transmission stability and anti-interference capabilities. These results highlight the practical application potentials of the scheme in complex industrial environments, effectively enhancing the real-time performance and reliability of industrial control systems and providing a technical foundation for optimizing and advancing wireless communication in future IIoT applications.

However, this study has certain limitations. First, the system relies on a cloud server for data relay, which may introduce network uncertainties, resulting in latency fluctuations that can affect high real-time performance. To address this issue, customized SIM card plans negotiated with carriers or deployment of a private core network could reduce reliance on cloud servers. Second, the design and implementation complexity of the protocol adaptation scheme increases system development and maintenance costs. Finally, experiments were primarily conducted in a controlled indoor environment. Although the effectiveness of the scheme was verified, further testing and optimization are required for more complex industrial environments (e.g. strong electromagnetic interference or large-scale network scenarios) to validate and enhance the scheme's applicability and stability.

## Data availability

Data are provided in the manuscript.

Received: 30 October 2024; Accepted: 27 May 2025
Published online: 31 May 2025

## References


1. Diao, Z. & Sun, F. Application of internet of things in smart factories under the background of industry 4.0 and 5G communication technology. *Math. Probl. Eng.* **2022**, 4417620 (2022).
2. Yu, H., Zeng, P. & Xu, C. Industrial wireless control networks: from WIA to the future. *Engineering* **8**, 18–24 (2022).
3. T. Müller and H.D. Doran, Protecting PROFINET cyclic real-time traffic: A performance evaluation and verification platform In: *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. 1–4, (2018).
4. Li, Q. et al. An enhanced time synchronization method for a network based on Kalman filtering. *Sci. Rep.* **14**, 21271 (2024).
5. Devan, P. A. M., Hussin, F. A., Ibrahim, R., Bingi, K. & Khanday, F. A. A survey on the application of WirelessHART for industrial process monitoring and control. *Sensors* **21**, 4951 (2021).
6. Khorov, E., Kiryanov, A., Lyakhov, A. & Bianchi, G. A tutorial on IEEE 802.11 ax high efficiency WLANs. *IEEE Commun. Surveys Tutorials* **21**, 197–216 (2018).
7. Wollschlaeger, M., Sauter, T. & Jasperneite, J. The future of industrial communication: automation networks in the era of the internet of things and industry 4.0. *IEEE Ind. Electron. Mag.* **11**, 17–27 (2017).
8. J. Åkerberg, M. Gidlund and M. Björkman, Future research challenges in wireless sensor and actuator networks targeting industrial automation. In: *2011 9th IEEE International Conference on Industrial Informatics*. 410–415, (2011).
9. Lopez-Perez, D., Garcia-Rodriguez, A., Galati-Giordano, L., Kasslin, M. & Doppler, K. IEEE 802.11 be extremely high throughput: the next generation of Wi-Fi technology beyond 802.11 ax. *IEEE Commun. Mag.* **57**, 113–119 (2019).
10. Au, E. A short update on 3GPP release 16 and release 17 [standards]. *IEEE Veh. Technol. Mag.* **15**, 160 (2020).
11. Park, J., Samarakoon, S., Bennis, M. & Debbah, M. Wireless network intelligence at the edge. *Proc. IEEE* **107**, 2204–2239 (2019).
12. Varga, P. et al. 5G support for industrial IoT applications—challenges, solutions, and research gaps. *Sensors* **20**, 828 (2020).
13. M. Wei, C. Li and C. Li, An IPv6 internet accessing architecture and approach for industrial wireless network. In: *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*. 1–6, (2020).
14 Gil, S., Zapata-Madrigal, G. D., García-Sierra, R. & Cruz Salazar, L. A. Converging IoT protocols for the data integration of automation systems in the electrical industry. *J. Electr. Syst. Inform. Technol.* **9**(1), 2022 (2022).
15. V. Kulik and R. Kirichek, The heterogeneous gateways in the industrial internet of things. In: *2018 10th International congress on ultra modern telecommunications and control systems and workshops (ICUMT)*. 1–5, (2018).
16. H. Shi, L. Niu and J. Sun, Construction of industrial internet of things based on MQTT and OPC UA protocols. In: *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*. 1263–1267, (2020).
17. C.R.M. Silva and F.A.C.M. Silva, An IoT gateway for Modbus and MQTT integration, In: *2019 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)*. 1–3, (2019).
18. J.G.Z. Botero, J.A.H. Cuartas and S.I.S. Garces, Communication Profibus-ZigBee using low cost gateway. In: *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. 1–4, (2015).
19. Y. Zhou, W. Xiao, M. Liu and X. Li, "Design of the embedded gateway for 4G and PROFIBUS-DP based on FPGA," In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. 748–752, (2017).
20. X. Wu and L. Xie, "On the wireless extension of EtherCAT networks," In *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*. 235–238 (2017).
21. A. Morato, S. Vitturi, A. Cenedese, G. Fadel and F. Tramarin, The Fail Safe over EtherCAT (FSoE) protocol implemented on the IEEE 802.11 WLAN. In: *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. 1163–1170, (2019).
22. X. Wu and L. Xie, On the wireless extension of PROFINET networks. In: *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. 1–5, (2019).
23. D. Trancă, A.V. Păläcean, A.C. Mihu and D. Rosner, ZigBee based wireless modbus aggregator for intelligent industrial facilities. In: *2017 25th Telecommunication Forum (TELFOR)*. 1–4, (2017).
24. M. Yang, S. Lim, S. Oh and J. Shin, An uplink transmission scheme for TSN service in 5G industrial IoT. In: *2020 international conference on information and communication technology convergence (ICTC)*. 902–904 (2020).
25. K. Nikhileswar, K. Prabhu, D. Cavalcanti and A. Regev, Time-sensitive networking over 5G for industrial control systems. In: *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*. 1–8 (2022).
26. Z. Satka, D. Pantzar, A. Magnusson, M. Ashjaei, H. Fotouhi, M. Sjödin, M. Daneshtalab and S. Mubeen, Developing a translation technique for converged TSN-5G communication. In: *2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)*. 1–8, (2022).
27. Khoshnevisan, M. et al. 5G industrial networks with CoMP for URLLC and time sensitive network architecture. *IEEE J. Select Areas Commun.* **37**, 947–959 (2019).
28. M. Ghassemian, P. Muschamp and D. Warren, Experience building a 5G testbed platform. In: *2020 IEEE 3rd 5G World Forum (5GWF)*. 473–478, (2020).
29. Ansari, J. et al. Performance of 5G trials for industrial automation. *Electronics* **11**, 412 (2022).
30. D. Koziol and H. Määttänen, "Network architecture and NR radio protocols," 5G New Radio: A Beam-based Air Interface, 25–93, 2020.
31. Le, T., Salim, U. & Kaltenberger, F. An overview of physical layer design for ultra-reliable low-latency communications in 3GPP releases 15, 16, and 17. *IEEE Access* **9**, 433–444 (2020).
32. Parkvall, S., Dahlman, E., Furuskar, A. & Frenne, M. NR: The new 5G radio access technology. *IEEE Commun. Stand. Magazine* **1**, 24–30 (2017).
33. Siddiqui, M. U. A. et al. Urllc in beyond 5g and 6g networks: An interference management perspective. *IEEe Access* **11**, 54639–54663 (2023).
34. Feng, D. et al. Ultra-reliable and low-latency communications: applications, opportunities and challenges. *Sci. Chin. Inf. Sci.* **64**, 1–12 (2021).
35. Q. He, G. Dán and G.P. Koudouridis, Semi-persistent scheduling for 5G downlink based on short-term traffic prediction. In: *GLOBECOM 2020–2020 IEEE Global Communications Conference*. 1–6, 2020.
36. N.H. Mahmood, S. Böcker, A. Munari, F. Clazzer, I. Moerman, K. Mikhaylov, O. Lopez, O. Park, E. Mercier and H. Bartz. White paper on critical and massive machine type communication towards 6G. Preprint at https://arxiv.org/abs/2004.14146 (2020).
37. J. Park, S. Samarakoon, H. Shiri, M.K. Abdel-Aziz, T. Nishio, A. Elgabli and M. Bennis. Extreme URLLC: Vision, challenges, and key enablers. Preprint at https://arxiv.org/abs/2001.09683 (2020).
38. Ke, M., Gao, Z., Wu, Y., Gao, X. & Wong, K. Massive access in cell-free massive MIMO-based internet of things cloud computing and edge computing paradigms. *IEEE J. Select Areas Commun.* https://doi.org/10.1109/COMST.2021.3067807 (2020).
39. Wijethilaka, S. & Liyanage, M. Survey on network slicing for internet of things realization in 5G networks. *IEEE Commun. Surveys Tutorials* **23**, 957–994 (2021).
40. Gao, J., Zhuang, W., Li, M., Shen, X. & Li, X. MAC for machine-type communications in industrial IoT—Part I: Protocol design and analysis. *IEEE Internet Things J.* **8**, 9945–9957 (2021).
41 Saha, R. K. & Cioffi, J. M. Dynamic spectrum sharing for 5G NR and 4G LTE coexistence-a comprehensive review. *IEEE Open J. Commun. Soc.* https://doi.org/10.1109/OJCOMS.2024.3351528 (2024).
42. Hussain, H. et al. A survey on resource allocation in high performance distributed computing systems. *Parallel Comput.* **39**, 709–736 (2013).

43. Akyildiz, I. F., Lin, S. & Wang, P. Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation. *Comput. Netw.* **93**, 66–79 (2015).
44. F.Z. Yousaf, M. Gramaglia, V. Friderikos, B. Gajic, D. Von Hugo, B. Sayadi, V. Sciancalepore and M.R. Crippa, Network slicing with flexible mobility and QoS/QoE support for 5G Networks. In: *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*. (2017)
45. Saibharath, S., Mishra, S. & Hota, C. Joint QoS and energy-efficient resource allocation and scheduling in 5G network slicing. *Comput. Commun.* **202**, 110–123 (2023).
46. Rinaldi, F., Raschella, A. & Pizzi, S. 5G NR system design: A concise survey of key features and capabilities. *Wireless Netw.* **27**, 5173–5188 (2021).
47 Mwakwata, C. B. et al. Narrowband internet of things (NB-IoT): from physical (PHY) and media access control (MAC) layers perspectives. *Sensors* **19**(2613), 2019 (2019).

## Author contributions
Author Yanzhang Xie researched the project and wrote the manuscript; authors Wenyi Liu and Qingping Yang provided multifaceted guidance; all authors reviewed the manuscript.

## Funding
Postgraduate Innovation Project of Shanxi Province,2023SJ214

## Declarations

## Competing interests
The authors declare no competing interests.

## Additional information
**Correspondence** and requests for materials should be addressed to W.L.

**Reprints and permissions information** is available at www.nature.com/reprints.

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.