Journal Pre-proof

How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities

Jinfang Jiang, Chuan Lin, Guangjie Han, Adnan M. Abu-Mahfouz, Syed Bilal Hussain Shah, Miguel Martínez-García

PII: S2352-8648(22)00142-0

DOI: https://doi.org/10.1016/j.dcan.2022.07.001

Reference: DCAN 474

To appear in: *Digital Communications and Networks*

Received Date: 25 April 2022

Revised Date: 12 June 2022

Accepted Date: 1 July 2022

Please cite this article as: J. Jiang, C. Lin, G. Han, A.M. Abu-Mahfouz, S.B.H. Shah, M. Martínez-García, How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities, *Digital Communications and Networks* (2022), doi: https://doi.org/10.1016/j.dcan.2022.07.001.

Digital Communications and Networks(DCN)

HOSTED BY

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/dcan

How AI-enabled SDN Technologies Improve the Security and Functionality of Industrial IoT Network: Architectures, Enabling Technologies, and Opportunities

Jinfang Jiang[a], Chuan Lin[b], Guangjie Han[*a], Adnan M. Abu-Mahfouz[c], Syed Bilal Hussain Shah[d], Miguel Martínez-García[e]

[a]**Department of Internet of Things Engineering, Hohai University, Changzhou, 213022, China**
[b]**Software College, Northeastern University, Shenyang, 110819, China**
[c]**Council for Scientific and Industrial Research (CSIR) and the Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, 2092, South Africa**
[d]**School of Computing and Mathematics, Manchester Metropolitan University, Manchester, M15 5RN, UK**
[e]**Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, LE11 3TT, UK**

Abstract

The ongoing expansion of the Industrial Internet of Things (IIoT) is enabling the possibility of effective Industry 4.0, where massive sensing devices in heterogeneous environments are connected through dedicated communication protocols. This brings forth new methods and models to fuse the information yielded by the various industrial plant elements and generates emerging security challenges that we have to face, providing ad-hoc functions for scheduling and guaranteeing the network operations. Recently, the large development of Software-Defined Networking (SDN) and Artificial Intelligence (AI) technologies have made feasible the design and control of scalable and secure IIoT networks. This paper studies how AI and SDN technologies combined can be leveraged towards improving the security and functionality of these IIoT networks. After surveying the state-of-the-art research efforts in the subject, the paper introduces a candidate architecture for AI-enabled Software-Defined IIoT Network (AI-SDIN) that divides the traditional industrial networks into three functional layers. And with this aim in mind, key technologies (Blockchain-based Data Sharing, Intelligent Wireless Data Sensing, Edge Intelligence, Time-Sensitive Networks, Integrating SDN&TSN, Distributed AI) and improve applications based on AI-SDIN are also discussed. Further, the paper also highlights new opportunities and potential research challenges in control and automation of IIoT networks.

KEYWORDS:
Industrial Internet of Things (IIoT), Industry 4.0, Artificial Intelligence (AI), Machine Intelligence, Software-defined Networking (SDN).

1. Introduction

Currently, we are witnessing an industrial revolution ranging term as Industry 4.0. Although this term may not be fully correct and involves a certain level of hype, the generalized implementation of autonomous decision making systems has become a new industry per se. The industry 4.0 is built by integrating networking capabilities that interconnect Artificial Intelligence (AI) agents in industrial plants, leading to the paradigms of *Industrial Internet of Things (IIoT)* and *smart manufacturing* [1, 2]. These subjects are attracting continuous attention from both academia and industry, and have been categorized in various prototype models [3, 4].

*Corresponding should be addressed to Guangjie Han (email: hanguangjie@gmail.com).

Fig. 1 displays a typical architecture for IIoT networks, integrating four functional layers: data sensing, data transfer, data processing, and application layers [5, 6]. The data sensing layer utilizes information acquisition and sensing technologies to collect heterogeneous data with different industrial attributes, and uploads them to the data transfer layer through advanced communication technologies, e.g., WiFi, Bluetooth, Internet of Things (IoT), 5G, etc. [7, 8]. As the intermediated layer, the data transfer layer (based on the Internet backbone) aims at uploading the industrial data to the data processing layer by deploying Traffic Engineering (TE) or data routing policies, according to the given requirements and constraints (e.g., Quality of Service (QoS), costs, lags, etc.) of the industrial data delivery services [9]. Based on the dedicated data computing schemes (e.g., cloud/edge computing, distributed computing), the data processing layer adopts data fusion algorithms to process the data in real-time, and it provides an open interface for the application layer, such that the diverse categories of industrial applications can be edited and deployed at the application layer according to the current needs [10].

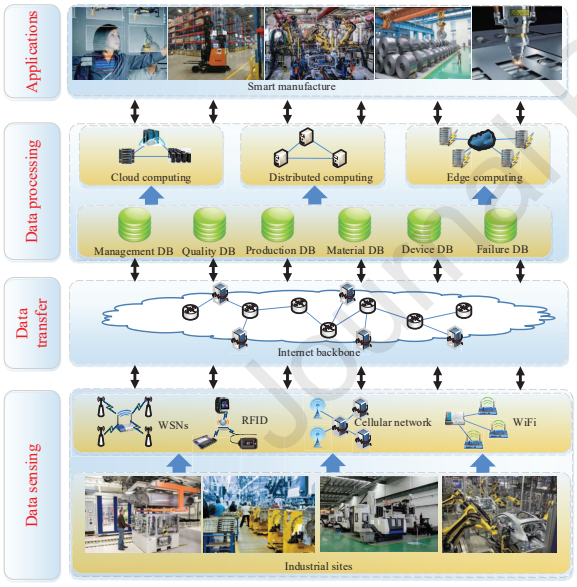

Fig. 1. A typical IIoT network architecture.

In IIoT networks, the frequent and synchronous industrial service requests are compute intensive, heterogeneous, and high-dimensional [11]. The new intelligent manufacturing technologies involve high-precision industrial manufacturing, processing and maintenance operations requests, which result in delay-sensitive operations – especially with respect to real-time surveillance, computation and cooperation among the different intelligent agents [12, 13]. In addition, different industrial applications are associated with different response time thresholds, representing the different delay-sensitivity requirements. For instance, compared with industrial data backup services, the data flow associated with industrial fault detection presents high degree delay-sensitivity [14]; it requires the network administrator to acquire the entire network states in real-time to determine comprehensive TE strategies according to the features of each industrial application, such that the Quality of Experience (QoE) of each industrial service can be satisfied [15, 16, 17]. Meanwhile, the openness and heterogeneity of IIoT has led to the exposure of massive security holes, making the IIoT networks are vulnerable to various categories of network attack, e.g., DDoS, Probing, R21, U2R, trojan, virus, worm, etc. [18, 19] Normally, the attackers falsify the features of abnormal traffic similar to normal traffic, which makes it impossible for network devices to detect the anomaly flow in IIoT network. Further, with the rapid development of IIoT, the category of network flow is becoming more and more diversified. And, different categories of IIoT services produce different flow patterns, making the entire network flow varies over time [20]. This results in the outdate of the anomaly detection models, thus misreporting new flow patterns or failing to detect abnormal traffic in IIoT networks. Hence, it is a non-trial task to improve both the Security and Functionality of IIoT Network.

However, the following factors hinder the secure data scheduling in IIoT networks of normal architecture: *i*) the IIoT network is a huge distributed control system integrating heterogeneous wired/wireless industrial Local Area Networks (LANs), which presents challenges with respect to scalable configuration [21, 22]; *ii*) current IIoT networks are still built based on traditional computing architectures and networks, i.e., the network control and data delivery planes are highly coupled. Thus centralized network administration is difficult, as is the deployment of unified network management strategies [23]; *iii*) the existing IIoT networks lack the ability of automatic control-management and display low adaptability with respect to the evolution of the increasing of industrial services; *iv*) although often neglected, the deployment of massive computing systems may increase the hidden environmental impacts of an industrial plant [24].

The Software-Defined Networking (SDN) is a recent paradigm that decouples the network control plane from the data plane (short for data forwarding plane) [25, 26, 27]. Different from the traditional computer networks, the switches in the data plane are only in charge of delivering the industrial data according to the policies determined at the control plane, while the SDN controller in the control layer functions as the network operator, and aims at managing each switch in the data layer through dedicated control standards, e.g., OpenFlow [28]. It can be inferred that, with the assistance of SDN, the management for IIoT networks can be simplified, and the network resources can be more efficiently utilized, leading to optimized global network policies that are temporarily deployed. For instance, in an IIoT network with heterogeneous ar-

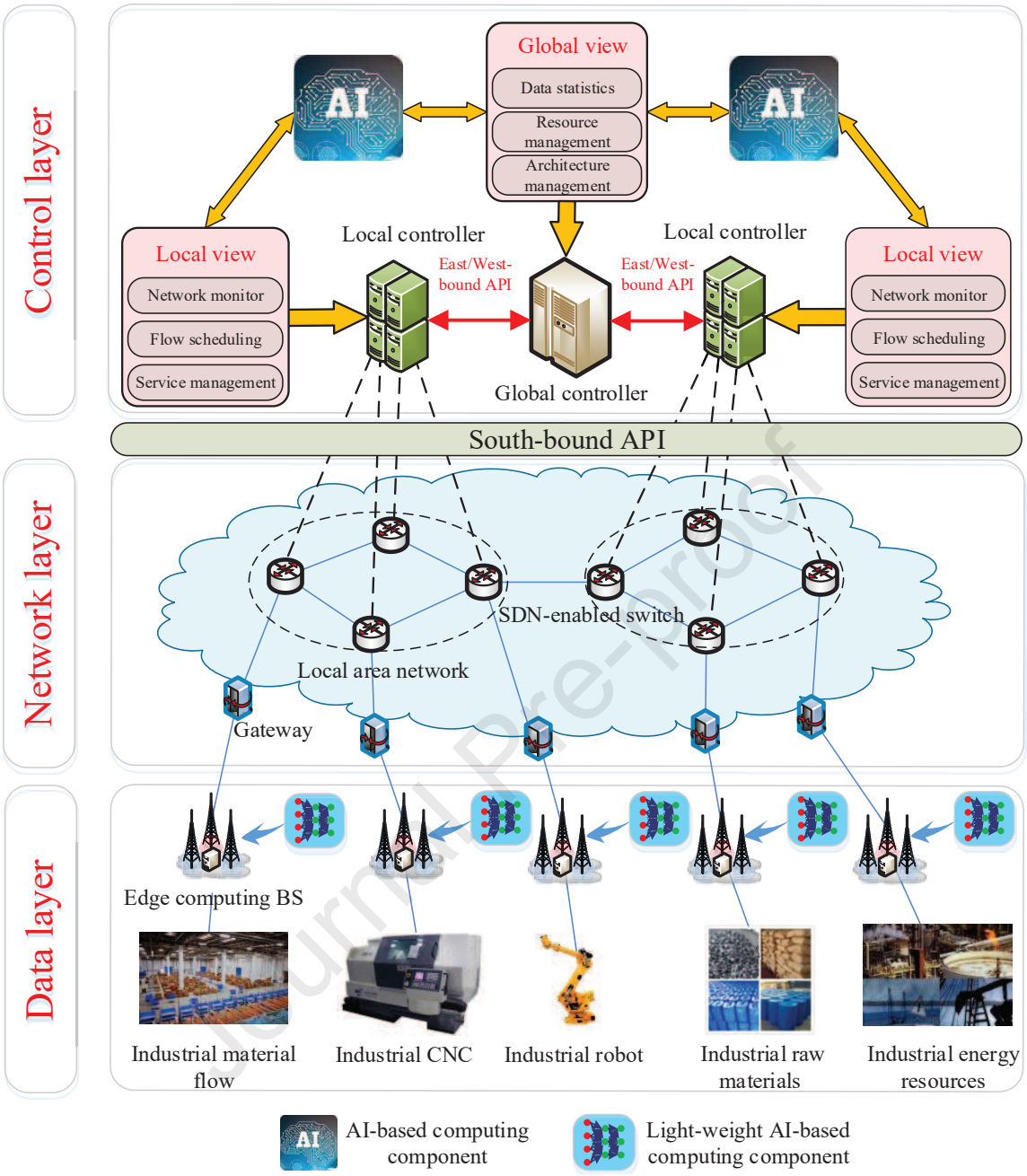

Fig. 2. Schematic of an AI-SDIN architecture

chitecture, the SDN technique can support or provide the network with an uniform control plane, such that all the IIoT devices can be monitored in real-time and globally optimal network policies can be determined and deployed.

At present, there is major academic focus on AI, which is resulting in significant industrial impacts [29]. AI is producing effective solutions to various monitoring and automation issues. Hence, AI can support intelligent network management in multiple ways; AI can assist the SDN controller with adaptive and smart network management – including automatic decision-making, data routing/TE determination, diagnostics, reconfiguration, etc. Integrating AI into SDN-based IIoT networks can potentially enhance the functionality of the IIoT networks [30, 31]. Hence, motivated by the rapid surge in SDN and AI technologies, this paper discusses how AI-enabled SDN technologies can improve the functionality of IIoT networks from the vantage points of network architectures, enabling technologies, application scenarios, and future research directions.

The remainder of this paper is organized as follows. The state-of-the-art about the subject is surveyed in Sec. 2. In Sec. 3, an architecture for AI-enabled Software-Defined IIoT Networks (AI-SDIN) is described. In Sec. 4, the enabling technologies for constructing AI-SDIN platforms is discussed. Sec. 5

presents multiple industrial applications that can be enhanced by AI-SDIN, while Sec. 6 analyzes the potential challenges and open research directions about the topic. Sec. 7 concludes the paper.

2. Background and Current Research Position

Recently, diverse research on IIoT networks has been undertaken, especially within the topics of protocols, security, communication technology, architectures, etc. [32, 33] IIoT networks are markedly different from the traditional computer networks. Some of the differences are highlighted in Tab. 1. The scale of IIoT networks is usually very limited because they are often deployed to guarantee data delivery in specific domains. This is different from the computer networks, which transfer various categories of multimedia data flow, each of which has different demand on QoS metrics – e.g., security requirement, delay, jitter, data loss, etc. [34, 35] Further, in IIoT networks most of the data is highly sensitive to delays, and one main target is to guarantee that the delay constraints of the data transmission process are satisfied. Thus, different from the traditional computer networks based on CSMA/CD, the MAC layer of the wired IIoT networks is usually built by way of the RapidRing protocol [36]. Since the data in the IIoT network typically corresponds to industrial manufacturing services, the data delivery requires to be guaranteed under high-level security policies [37]. In many industrial fields, e.g., coal mining industry, wind power generation, petrochemical industry, etc., the industrial sensors are distributed in unserviced areas, and the sensing information is collected and delivered by open wireless tunnels. This make the industrial sensors not only easy to be stolen and captured, but also vulnerable to eavesdropping. And the traditional security approaches, e.g., trust mechanism, identity authentication, information encryption, etc., cannot satisfy the requirement of industrial applications. Thus, efficient and secure data delivery has to be guaranteed in IIoT networks.

With the widespread implementation of IIoT applications, IIoT networks are evolving gradually towards wired/wireless hybrid network architectures. Tab 2 presents several candidate protocols for IIoT network communications – ZigBee, WirelessHART, ISA100.11a, WiFi, Bluetooth, LoRA are wireless communication protocols, while PROFINET, EthernetPOWERLINK, DeviceNET, Modbus, and CAN are wired protocols. The recent successful commercialization of 5G brings forth another innovation opportunity, upgrading the IIoT networks to High Bandwidth and Low Latency (HBLL). IIoT integrating 5G technology is more capable of real-time industrial data sensing, supporting timely data processing or analysis at the data computing center [38, 39]. Multiple related proposals can be found in [40, 41, 42]. Furthermore, edge computing has exceeded the conventional computing platform by efficiently allocating the computing resources and deploying the edge computing station at feasible places. It is acknowledged that edge computing will enhance the user experience of various industrial delay-sensitive applications, by finding the right balance between traditional stand-alone systems and cloud computing.

As a promising paradigm to improve the functionality and salability of IIoT networks, the SDN technique has been widely promoted and deployed in many famous or mature data center networks or the other networks. For instance, the Google B4 network separates the network's control plane form the data plane to enable fast deployment of new network control services and has been proved to significantly improve the system performance [43]. Further, on account of the SDN technique, there are many emergent paradigms that have been demonstrated to be successfully to be deployed in traditional computer networks, e.g., the OpenNetMon [44]. It can be speculated about that the successful deployment of these paradigms can provide valuable suggestions to the promotion of AI-SDIN.

As mentioned, current research progress is subject to the integration of the heterogeneous network with different communication protocols, diverse computing platforms, and other elements. And with respect to incorporating *machine intelligence* through AI, multiple applications already exist – from directly monitoring industrial systems through grey-box models and Convolutional Neural Networks (CNNs) [45, 46] to assessing the uncertainty in their response through probabilistic Recurrent Neural Networks (RNNs) [47]. Then, a wide range of AI sensor fusion techniques are surveyed in [48, 49], and the possible schemes for implementing *machine intelligence* in industrial plants in [50].

3. AI-SDIN Architecture

As a revolutionary technique to improve the scalability and robustness of network functionality, the SDN paradigm has been widely used in multiple types of networks – e.g., traditional computer networks, multi-agent networks, underwater acoustic sensor networks, etc. SDN utilizes standardized protocols (OpenFlow [28], ForCES [60], POF [61], etc.) between network control and packet forwarding components. By SDN, the network control unit can be intensely decoupled from the network data delivery devices, such as the router, leading to a centralized network control plane, i.e., the SDN controller. Breaking away with the traditional manner of individually configuring network devices, SDN controllers can support exact network monitoring and adaptively determine/deploy network policies, according to users' requirements and the network states [62, 63].

To yield intelligent policy decisions, AI-enabled computing elements can be deployed on the SDN con-

Features	IIoT networks	Traditional networks
Security	High-level demand	Low to high level demand
Network scale	Small	Large
Delay-sensitivity	High-level demand	Low-level demand
Robustness	High-level demand	Low-level demand
Protocol	RapidRing	CSMA/CD
Machine Intelligence	High-level	Low-level

Table 1
Comparison between IIoT networks and traditional networks.

Protocol	Standard	Description	Advantages	Disadvantages
ZigBee [51]	IEEE 802.15.4	Transmission range limit: 50 m; transmits data through a mesh network of intermediate devices.	low cost; low power.	Cannot run on large-scale networks.
WirelessHART [52]	IEEE 802.15.4	Utilize a time synchronized, self-organizing, and self-healing mesh architecture.	Robustness; dedicated to the industrial networks.	Incompatible with FieldBus-based wired communication standard.
ISA100.11a [53]	IEEE 802.15.4	Dedicated to particular wireless monitoring applications.	Low power; compatible with FieldBus-based wired communication standard.	Low rate; not widely used.
WiFi	IEEE 802.11a/b/g/n/ac	For Business consumer-level applications.	High rate; mature technology.	High power.
Bluetooth [54]	IEEE 802.15.1	Replaces RS-232 and RS-485.	Low power.	Short com. range
LoRA [55]	LoRAWAN	For IIoT networks.	Large com. range; low power; low cost.	Spectrum conflict.
PROFINET [56]	IEEE 802.3	For soft real-time applications.	Easy to deploy.	Not suitable for delay-sensitive industrial applications.
Ethernet POWERLINK	IEEE 802.3	Ethernet based; For real-time applications.	Open; high rate.	Complex; requires auxiliary protocols.
DeviceNET [57]	FieldBus	For transferring the frame of short length.	High scalability; widely used.	Low rate.
Modbus [58]	FieldBus	Open; support various interfaces, e.g., RS-485.	Easy access to Modicon or Honeywell systems.	Significant coding development.
CAN [59]	FieldBus	For transferring the frame of short length.	High interference immunity.	Low rate.

Table 2
Prominent candidate communication protocols for IIoT networks.

troller, so that smart network control and functions are executed. For instance, AI algorithms can assist in identifying and isolating malicious attacks in a software-defined network [30, 64]. Thus, SDN applications gives to IIoT networks an scalable platform that can deploy complex network policies, while AI, functioning as *machine intelligence*, can compute smart and self-adapting network policies. A typical architecture for AI-SDIN is showcased in Fig. 2, where the network is divided into three distinct functional layers.

3.1. Data Layer

The data layer of the AI-SDIN generates large amounts of data (related to various categories of industrial devices, resources, etc.). These valuable data can be sensed and gathered by advanced IIoT techniques and industrial sensors [50]. In particular, the widely utilized Radio Frequency IDentification (RFID) system makes intelligent data sensing more straightforward, with the data being automatically sensed and exchanged among different devices [65]. Tab. 2 summarizes some popular wireless communication protocols for IIoT sensors, e.g., PROFINET, DeviceNET.

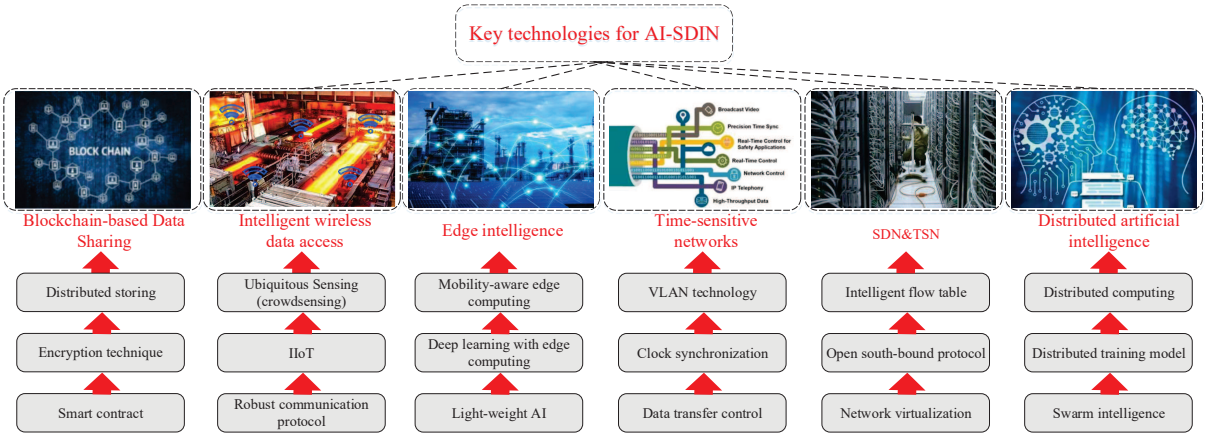

Fig. 3. Key technologies in AI-SDIN.

It is worth noting that the recently emergent LoRA has become one of the most prominent protocols for IIoT networks, due to its larger communication range and low power/cost. Moreover, at the edge of an IIoT network, a Fog Computing-based Base Station (BS) equipped with light-weight AI computing component can be deployed to provide light-weight data processing and filtration, especially for delay or security sensitive industrial services [66, 67].

3.2. Network Layer

The network layer of the AI-SDIN is dedicated to connecting the elements of the network, resulting in a unified data delivery plane that allows for efficient data sharing, especially for massive data. In the network layer, the data is accessed through LANs and aligns the services that the edge computing cannot provide. The LAN integrates a set of particular switches following the pre-defined south-bound protocols, e.g., OpenFlow, Protocol Oblivious Forwarding (POF) [68], etc. For instance, the Pica8's P series switch has received wide acceptance by the industrial consumers. Different from the IIoT-based data layer, the LAN of network layer is built through specialized wired communication protocols, including industrial Ethernet and FieldBus (Tab. 2). In addition, the forwarding devices in the network layer are only in charge of data delivery, and provide open API following the south-bound protocol to the control layer of the AI-SDIN.

3.3. Control Layer

The control layer is regarded as the *machine intelligence* nucleus of the AI-SDIN platform. In the control layer, the forwarding devices in the network layer are controlled and programmed by pre-defined protocols. For instance, in the normal OpenFlow v1.3-based control plane – e.g., Ryu, the standardized *Packet_In*/*Packet_Out*, *Flow_Mod* messages of OpenFlow, etc., are used to control the operations of the forwarding devices, by deploying the policies determined within the control plane. In the classical architectures as those proposed in [69, 70, 71], within the control plane of AI-SDIN, the *machine intelligence* is embedded, to bring decision-making capabilities to the system. Thus, the control plane can be an intelligent agent, and complex industrial applications can be efficiently supported and executed, e.g., threat identification or network adaptive adjustment. For example, in [72], an AI-based two-stage intrusion detection scheme was proposed for software-defined industrial IoT networks; the proposed scheme can exactly detect the potential network attacks based on the synchronized information at the SDN controller.

In addition, as shown in Fig. 2, the control plane supports the distributed network management. That is, each local controller supports the devices at each LAN, while the global controller deals with the operations across multiple LANs. Hence, by the north-bound protocol, cooperative industrial services can be modified and supported at the application layer. For the sake of brevity, we do not present the legend for the application layer in Fig. 2.

4. Involved Key Technologies

In Fig. 3, various key enabling technologies applicable to building an AI-SDIN system are displayed. These are discussed next.

4.1. Blockchain-based Data Sharing

The booming development and promotion of digital cash has distinguished the blockchain technique. Normally, Blockchain is considered to be a traceable, distributed and nontamperable ledger. Each node in Blockchain share information and keeps updating and maintaining the ledger. It as well guarantees data consistency by utilizing consensus mechanisms. It can be foreseen Blockchain will play a crucial part in data science especially in terms of privacy protection, tamper-proofing and temporal ordering. Thus, employing

blockchain technique in IIoT has proved to be quite feasible and beneficial [73]. As a hotspot technique, the Blockchain technique can be integrated with operations, production, sales and management in smart factories. In IIoT networks, the Blockchain can be employed to coordinate and track the interconnected network devices. For instance, Fig. 4 display an architecture for software-defined IIoT network embedding Blockchain.

In smart factories, the industrial data can be shared in the whole manufacturing process, e.g., fund flow, production/sales data, inventory information, etc. These time series data requires to be surveyed and tracked during, in case of being traceable, tamper-proof and nonduplicative. The features of Blockchain satisfy the security and efficiency requirements of data sharing in IIoT networks towards smart factories. It can be inferred that Blockchain will contribute to improve the security of IIoT network, by providing secure data sharing, robust data aggregation and guaranteeing data confidentiality, etc. For instance, in [74], the authors employ Blockchain technique and propose an improved industrial data access/sharing prototype supporting private key dynamic generation to resist and identify collusion attacks in IIoT networks.

4.2. *Intelligent Wireless Data Sensing*

Intelligent wireless data sensing involves three key sub-components: robust communication technologies, IIoT, and ubiquitous sensing. To provide continuous data-driven industrial services, robustness communication technologies should be employed, thus avoiding potential wireless eavesdropping or man-in-the-middle attacks [75].

Besides the ubiquitous digital signature and identity authentication technologies, the recent widespread adoption of AI has accelerated the development of security checking and data encryption technologies – applicable to industrial wireless data sensing [76]. For instance, in [77], the authors propose an encryption/decryption module that can secure complex cryptography the communication with limited computation capability, so that the traditional Supervisory Control And Data Acquisition (SCADA) systems can be enhanced. In [78], to make IEEE 802.15.4 protocol adapt to the IIoT networks, the authors propose the utilization of the best radio channels while still providing deterministic performance and to group the links per timeslot, allocating them either to the same whitelist or even appropriately reordering them to avoid collisions.

Acting as the intermediate layer in industrial wireless services, the IIoT aims to integrate and interconnect each working *island* (partially isolated subsystems). This can assist the network administrator in constructing an abstract view for analyzing all the industrial data related to material, logistics, machinery information, etc. Thus, stable and QoS-aware communication protocols are indispensable to provide industrial services access, especially for data-driven industrial applications. For instance, in [79], the authors propose to share the communication resource among the wireless stations to satisfy the QoS and security requirement of different industrial applications or users and propose an approach named QWIN by offloading their priority queues into the IIoT network and deploying cooperation and security mechanisms.

Furthermore, to confront the challenges of industrial big data and the rapid growth in industrial mobile users, ubiquitous sensing monitoring has become an active research field; Crowd-Sensing is a paradigm that support industrial data sensing by constructing dynamic sensing networks [80]. Through Crowd-Sensing, the industrial data can be co-jointly sensed, and the analyzed result can be efficiently shared in real time.

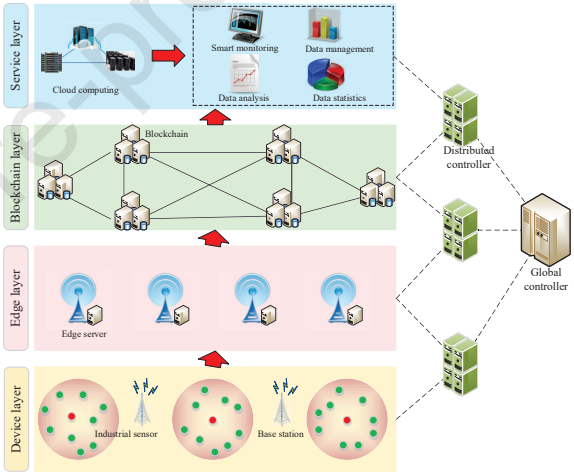

Fig. 4. Software-defined IIoT network embedding Blockchain.

4.3. *Edge Intelligence*

An IIoT system may generate large amounts of data and consume a lot of energy and resources [24]. This may result in unfeasible requests to IIoT networks in terms of bandwidth, especially for security/delay sensitive industrial applications that the cloud computing platform cannot satisfy [81]. The edge computing and Mobile Edge Computing (MEC) paradigms have emerged to unload the computing requirements of cloud computing centers. By means of edge computing, the processing delays of industrially generated data the required network communication resources (e.g., the bandwidth) can be reduced. This results in improved network efficiency through a cooperation architecture (*Edge-to-Cloud*). One example is when the edge computing component aims at processing lightweight delay-sensitive tasks and tasks that would involve massive data communication to the cloud centre, while the cloud centre deals with large-scale tasks with lower delay-sensitivity. For instance, in [82], the

authors present an blockchain and edge intelligence-enabled Industrial Internet of Things network that can support secure and flexible edge service administration. On account of the proposed framework, the authors propose as well a cross-layer resource sharing scheme that can only deployed in the centralized network management platform, e.g, the SDN-enabled networks. To support continuous and stable data processing services, the mobility-aware edge computing technique can be employed for ensuring that the mobile users (industrial robots) can seamlessly switch among the different edge computing components [83]. Furthermore, in recent years, integrating AI techniques such as deep learning into edge computing (referred to as *edge intelligence*) has opened new research directions towards incrementing the computing ability and scalability of edge computing systems [84]. For instance, to enable edge intelligence, the authors in [85] present a network architecture (named by OpenEI) that is a software-based framework where the edge computing unit consists of data computing and communication component, and can provide scalable deployment for complex artificial intelligence policies, e.g., deep learning, reinforcement learning, etc.

4.4. Time-Sensitive Networks

Time-Sensitive Networks (TSNs) constitute a new industrial communication technology that holds sustained attention from both academia and industry. TSNs allow the periodic and aperiodic data to be concurrently transferred within the same network. This brings the advantages of deterministic transmission to Ethernet. For instance, in [86], the authors take a deep study on the theoretical foundation of queue management in TSN data deliver devices especially in IEEE 802.1Qbv standards-based IIoT networks. The authors have proved the queue scheduling and assignment issues for real-time data delivery on time sensitive IIoT networks with both dynamic and static priority scheduling is NP-hard issue. By formulating the problem by satisfiability modulo theory, the authors have proposed two heuristics to address the issues that are easy to realize. At present, IEEE, IEC, and other organizations are formulating the underlying interoperability standards and specifications for IIoT networks based on TSN. TSN integrates a series of technical standards, mainly including clock synchronization, scheduling strategy for data flow, and network configuration. We note that TSN operates in the MAC layer of the ISO/OSI model [87, 88]. To standardize and realize the TSNs, one of the most challenging issues that have to be solved is to optimize and determine the scheduling mechanism. For instance, in [89], to improve the performance of no-wait scheduling algorithms in TSNs, the authors propose no-wait scheduling mechanism and joint algorithm for message fragmentation in TSNs. In particular, on account of the optimization modulo theories, the authors propose a specification for the joint problem and utilize off-the-shelf solvers to address the problem.

4.4.1. VLAN

TSN is standardized based on the Virtual Local Area Network (VLAN) approach and the priority mechanism in the IEEE 802.1q protocol [90, 91]. The IEEE 802.1q supports QoS provisioning and can also support network performance predictability. Furthermore, it can efficiently allocate the network resources (e.g., bandwidth) to satisfy the QoS of the industrial users.

4.4.2. Clock Synchronization

For delay-sensitive industrial control, all the tasks are time-stamped, thus, accurate clock synchronization is indispensable. TSN consists is composed of the IEEE 802.1as and IEEE 802.1as-rev, which are specifically developed for industrial applications. Note that the IEEE 802.1as is based on the IEEE 1588 V2 precise clock synchronization protocol, which is referred to as Generalized Precision Time Protocol (gPTP). gPTP operates via a distributed master-slave structure and synchronizes all the clocks in each gPTP network node [92].

4.4.3. Data Transfer Control

With the control of the scheduling mechanism in TSNs, the data passes through the receiving port to perform frame filtering, flow metering, and frame queuing. In particular, the IEEE 802.1q defines different sharpers to realize the scheduling mechanism [93, 94]. Thus, it is actually a Transmission Selection Algorithm (TSA) where each algorithm corresponds to a scheduling mechanism, which is suitable for different industrial application scenarios.

4.5. Integrating SDN&TSN

Integrating SDN and TSN requires three essential techniques: specialized south-bound protocol, network virtualization, and protocol realization [95]. The Network Configuration Protocol (Netconf) together with OpenFlow are suitable candidate protocols – OpenFlow aims at deploying intelligent flow tables, and Netconf is dedicated to configuring and updating TSN-related protocol. An architecture for integrating SDN and TSN is presented in Fig. 5; in the figure, the *queuing* and *priority* features from the OpenFlow table are utilized to set the delivery priority of each data flow, and to limit the transmission rate at each port of the SDN-based switches, respectively. Further, in [96], the authors argue the OpenFlow protocol is the key technique in SDN-based IIoT network and can as well provide the TSN-embedded SDN with a global view. To adapt the TSN feature to SDN, the authors propose a control mechanism called TSNu that can provide exact time-slot scheduling for the data delivery in TSNs. In [97], the authors argue that the SDN

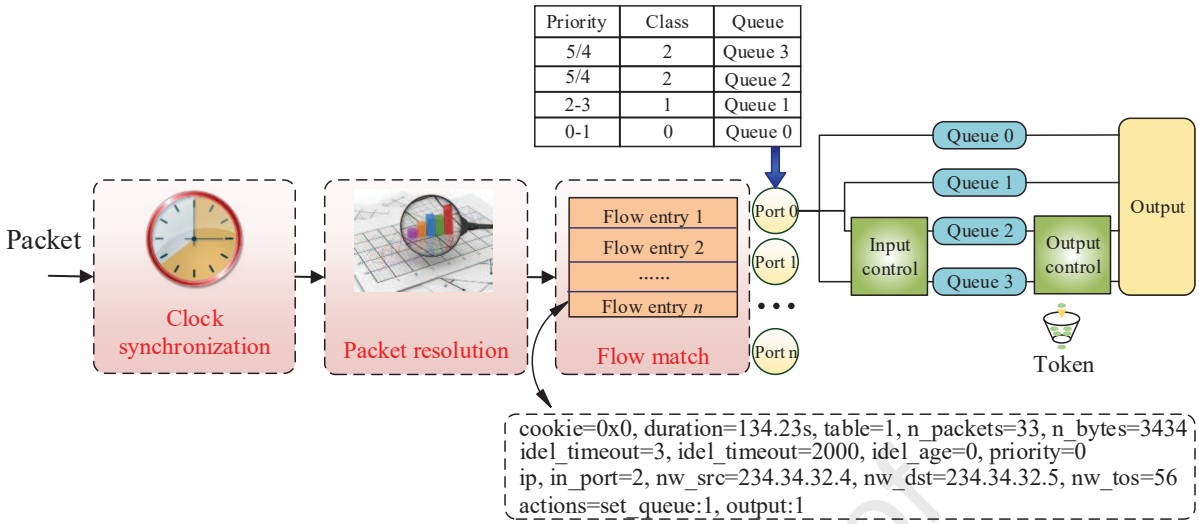

Fig. 5. An architecture integrating SDN and TSN.

technique or paradigm can be utilized to tackle the configuration challenges in TSN. On account of the IEEE 802.1 Qcc standard, the authors propose the design of the Centralized Network Configuration (CNC) based on a micro-service architecture. And, the authors develop as well a utility maximization approach to optimize the data routing, resource scheduling, etc. Further, the OpenFlow Meter table can also be leveraged to limit the data delivery speed, as to guarantee the delay-sensitivity of the data from the TSN network. Furthermore, to address the suitability issues due to differentiated protocols and interfaces, the head of the packet requires to be re-written, such that the data at the gateway can be switched. A candidate solution to this is that of revising the Priority Code Point (PCP) field of the VLAN to realize the priority matching among different domains.

4.6. Distributed AI

In a multi-agent system, distributed AI aims at controlling each agent to perform cooperative tasks intelligently. For the AI-SDIN based on hierarchical network architecture (Fig. 2), the distributed AI can be deployed within each local controller, such that the network policies – e.g., the TE policies, can be distributed computed and determined at each local controller [98]. It is worth mentioning that the distributed AI framework is performed under the control of the global controller. The architecture for distributed AI-SDIN offers the natural advantage of deploying a distributed AI computing framework, where each local controller can share the computing resources with the others through a robust communication tunnel. In addition, the communication among the local controller follows the West-East interface, and it can be dynamically switched with the monitoring and scheduling ability of the global controller. For instance, in [99], the authors propose ADDAI (Anomaly Detection using Distributed AI) which can distribute the data computation mission among a set of IIoT devices. It can satisfy the requirement from any industrial user and address the a single point of failure with high probability, by deploying distributed AI framework. Further, in [100], the authors regard the cloud-to-thing as a continuum and propose a framework to deploy the AI in a scenario with cooperative edge computing. In particular, the authors propose approaches to improve the communication efficiency to accelerate the learning efficiency of the cooperative AI.

5. Improved Applications based on AI-SDIN

The SDN technique is complex to implement to achieve widespread adoption in traditional computer networks, displaying heterogeneous and encapsulation features. Hence, the AI-SDIN is in low technology readiness level state. As a practical manner to achieve actual Industry 4.0 implementations, it can be inferred that the AI-SDIN will play an important role in accelerating the digitalization and integration in industrial manufacturing [50]. In [101], the authors give a comprehensive survey about how to utilize the SDN technique to realize and improve the operations of IIoT networks. The paper also discusses the possible application scenarios by means of software-defined IIoT networks. On the other hand, in this section, we emphasize smart industrial applications under the AI-SDIN architecture. In particular, we align the discussion around the following six aspects: trustworthy data sensing, sustainable logistics, smart industrial materials scheduling, smart sales, secure healthcare, and smart agriculture.

5.1. Trustworthy Data Sensing

One of the most critical applications and functions in AI-SDIN is the data sensing and collection. The

mass production of low-cost sensors has made more possible than ever their integration in industrial environments, including the usage of redundant sensors to increase the security and robustness of the system. Powered by the abilities of IIoT including ubiquitous sensing, identification, and stable communication, the trustworthy data sensing of AI-SDIN is capable of the following features:

5.1.1. Integrated Correlation Analysis

Focused on the critical sensing elements including people, machines, industrial raw materials, and logistics, integrated correlation analysis models can perform data fusion for analyzing each category of industrial data. This mitigates the data island effect that limit traditional industrial IIoT networks. And it can as well improve the authenticity of the industrial data. For instance, in [102], to enable sustainable development for enhancing industrial production output, the authors propose a data-driven approach for optimizing and evaluating the efficiency of the industrial system. The system utilizes an uniform platform to collect and process the data from the aspect of emergy. And the evaluation model and the correlation analysis between efficiency and the corresponding factors can be built to achieve the quantitative evaluation.

5.1.2. Service-Oriented Data Analysis

Smart data sensing can also be applied to yield service-oriented data analyses, by fully integrating each potential analysis engine. For instance, to provide industrial fault recognition services [14], the analysis results from different recognition engines can be collated to compute the optimal solution according to the service type.

5.2. Sustainable Logistics

It is expected that the AI-SDIN will also play an important role in sustainable logistics and transportation. As mentioned, the IIoT framework of AI-SDIN can be widely deployed in multiple ecosystems, including industrial logistics or transportation systems. In particular, with the rapid development of industrial sensors integrating advanced wireless communication, power, sensing components, etc. (Sec. 5.1), the Internet of Vehicles (IoV) paradigm is being considered as a way to tackle traffic congestion. The IoV can provide seamless and real-time information sharing among the vehicles or between vehicles and humans. This can accelerate other vehicular-based industrial applications such as semi-autonomous driving [103], contributing to the development of industrial logistics and intelligent transportation.

For instance, the AI-SDIN is able to monitor the states of each road, the drivers, and track the location of each vehicle. It can assist the vehicles with smart parking and provide the vehicles with adaptive navigation to avoid potential traffic jams. For sustainable logistics towards industrial services, the AI-SDIN is capable of scheduling transportation resources to guarantee the transportation of industrial materials through platooning trucks. In particular, industrial materials can be ranked with different priorities according to their physical or security characteristics. Thus, based on the timely monitoring of the traffic flow, the traffic policies can be timely determined at the traffic control department. For example, to ensure the transportation safety for industrial oil and gas resources, the planned paths for the trucks need to bypass potential hazardous conditions. By comparison, first responders have strict delay requirements. Hence, their scheduling should have the highest priority.

Fig. 6. Improved applications based on AI-SDIN.

5.3. Smart Industrial Materials Scheduling

The existing supply chain systems include three links: upstream material supply, production, and downstream sales. The management of each link is often more or less independent. Integrating each link to execute timely information sharing can be challenging. AI-SDIN integrates each category of information from each component of the entire chain. As one of the most important applications in the future IIoT networks, smart industrial materials scheduling can be performed based on the smart logistics abilities of AI-SDIN.

Through AI-SDIN, the suppliers' yield information and the downstream sales are gathered at one integrated monitoring system. This enables the manufacturers to interchange information (about the industrial materials) in real-time, to determine the required sales strategy; based on the statistical information about the bins of industrial materials and the predicted sales information in the next period, the corresponding purchasing policy can be determined. Then, feasible material suppliers are selected that satisfy the computed purchasing policy.

5.4. Smart Sales

Within the practical applications of AI-SDIN, the exact computation and prediction ability of the *machine intelligence* provides additional value to the industrial chain; enterprises can concentrate on user's requirements and experience, and the sales model is innovated from inventory backlog to pre-sale – possibly via A/B testing. Thus, rapid delivery and comprehensive monitoring for industrial production can be realized. AI-SDIN promotes deep integration of human, machine, and physical objects, and ensures the integrity of enterprises' upstream and downstream supply chains, so that the resources are optimally allocated. For instance, in [104], the authors propose the paradigm of *cloud sales platform*, which can be expanded in IIoT networks; it can promptly summarize the customer's requirement in advance, and automatically link the customer's requirements with the enterprise that could satisfy their requirement. Then, after the sales are accomplished, multi-dimensional sales reports are automatically generated. This enables the visualization of the entire sales procedure and the integration of *research-production-marketing*.

5.5. Secure Healthcare

The healthcare industry is undergoing an AI revolution [48], which can be further accelerated by AI-SDIN. Although the approach also has its dangers [24]. The interconnection ability of AI-SDIN can as well connect each component (including medical organization, medical equipment, doctors, and patients) into an unified control/monitoring system, such that the globally optimal healthcare policies can be determined and deployed. Furthermore, in recent years, the rapid development of wearable sensors have resulted in the Body Area Network (BAN) framework, standardized by the IEEE 802.15.6 [105]. The BAN aims to connect each wearable device (e.g., heart rate monitor) into an integrated network for long-term monitoring and recording of human health signals. It can be inferred that the AI-SDIN will accelerate the popularization of intelligent healthcare, especially with respect to medical assistance and security protection. For instance, in [106], the author propose a high-performance affine cipher-based key encryption technology aiming at supporting serious secret key protection. Their proposal is dedicated to providing a prototype that can guarantee secure data delivery in BAN. However, their approach does not clarify how to encrypt the key words, which leaves a future work for AI-driven encryption engine.

5.6. Smart Agriculture

The paradigm of smart agriculture is innovating the classical agricultural model. Smart agriculture aims at applying IIoT technologies in traditional agriculture ecosystems, by using advanced industrial sensors (e.g., humidity or CO_2 monitoring sensor) and software to control agricultural production through centralized computing platforms (e.g., edge computing). By AI-SDIN, the agricultural information can be made more transparent and accurate. Each agent or production device in the agricultural industry can be intelligently scheduled to perform cooperative tasks. For instance, in [107], the authors propose a smart agriculture framework integrating different categories of monitoring systems, unmanned aerial vehicles, automatic irrigation systems, VR techniques, etc. Further, in [108], the authors argue that the IIoT technique is able to improve the agricultural production and propose a multi-model-based data delivery model for the integration of multi-vendor agricultural production systems. And their model utilizes the Data Distribution Service (DDS) middleware to enable communication between heterogeneous production systems to perform farming operations in a coordinated manner.

6. Opportunity and Further Research Directions

It can be witnessed that the AI and SDN technologies, together with their applications in IIoT networks, are still at the early stage. It is still not understood how well AI can generalize [103] and its ethical implications [24]. To realize AI-SDIN, there are still many challenging issues that the researchers have to confront, ranging from technical challenges to implementation issues. Ultimately, if implemented poorly, it may result in an over-complex highly-coupled systems which can lead to unpredictable incidents [109]. Furthermore, possible future work should also consider potential changes in industrial applications, which may result in model drift (i.e., concept and data drift) to build AI-SDIN systems with an adaptable layer. The following are some potential opportunities and research directions that can leverage towards implementing the AI-SDIN paradigm.

6.1. Light-Weight AI

Even if deep learning-based frameworks are powerful and dominant for most data analysis tasks, they are computationally expensive, and difficult to deploy on low-power devices. For instance, the edge computing components of AI-SDIN cannot support high-performance and high-complexity online data training schemes, since these devices have usually limited capabilities. As a result, new generations of light-weight AI schemes must be developed. This has led to the emergence of high-efficiency networks – e.g., Tiny YOLO [110], MobileNet [111], ShuffleNet [112], some of which are tiny counterparts of mainstream models. However, as for the learning performance, these light-weight AI schemes lag far behind their full-fledged counterparts. Hence, balancing the computing performance and energy consumption is

still main challenge in edge intelligence. Further, distributing the deployment of AI schemes among several cooperative edge computing components is also a hot research topic.

6.2. Network Management

As an open research topic, network management in AI-SDIN encompasses multiple aspects: network reconfiguration, network resource management, etc. In future smart factories, mobile agents will be frequently relocated under the control of different edge computing components [50], which can produce instabilities. Hence, it is indispensable to design robust handover or network reconfiguration protocols that ensure smooth message delivery for controlling industrial mobile agents. In addition, the introduction of SDN and AI models in IIoT networks have revolutionized network resource management. This diverts the burden from the data forwarding devices to the SDN controller, that is in charge of managing each corresponding data forwarding service. Thus, the computing resources on SDN controllers have to be feasibly scheduled for diverse network policies (e.g., the TE policies), especially when the features (QoS, priority, etc.) of the network services are considered.

6.3. Network Operation

AI-SDIN integrates diverse functions in each functional layer of the network architecture, and supports various wired and wireless communication protocols. The traditional south-bound protocol, e.g., OpenFlow, ForCES, cannot directly support the deployment of these network operations even when the wired part of the AI-SDIN is neglected. For instance, current south-bound protocols cannot support hard QoS guarantee and exact flow deployment at hybrid LAN switches. With the promotion of the Network Function Virtualization (NFV) technique in SDN, the current south-bound protocol needs to be adapted to the diverse functions and architectures. The will be even more challenging when the industrial applications across multi-domains are taken into account.

6.4. Robustness and Security

As discussed, the mobile industrial objects may be frequently disconnected and connected to the edge computing components. This may result in the packet transmission tunnels being vulnerable to disruption and distraction, due to the complex electromagnetic and communication environment. In addition, some industrial applications require strict QoS (e.g., packet loss) provisioning on the related data flow delivery. Hence, the stability or robustness of the data layer in AI-SDIN has to be ensured. Thus, it requires adaptive spectrum sensing and network topology prediction approaches, able to guarantee the data delivery among the switches or the tunnels – between edge computing components and industrial mobile agents.

Further, the AI-SDIN must face challenges due to control plane instabilities. For instance, due to software errors (bugs) or glitches, NFVs implemented in software are more vulnerable than hardware middleware [113]. Since the AI-SDIN exhibits a complex hierarchical control plane, it is challenging to guarantee stable network management by cooperating with each SDN controller. Thus, there is active research in the subject.

6.5. Adaptive TE

Beyond robustness factors, packet delivery or routing in AI-SDIN is a know complex issue due to the multiplicity of features in IIoT networks. The complex features that may affect packet delivery efficiency include frequent high-speed mobility, multi-protocol, and multi-service data flow coexistence. These factors are more noticeable when the industrial services' scale up and the generated data become larger. For instance, in a small-scale LAN of AI-SDIN, three types of data flow are concurrently requested for delay-sensitive data processes. When complex data routing protocols, such as multi-path routing protocol, have to be taken into account, the *machine intelligence* is required to determine TE policies for adaptively allocating the network resources to each industrial service, so that the requirement of each service can be satisfied. In [114], on account of OpenFlow, the authors propose a real-time network monitoring platform that can monitor the link-delay, bandwidth, delay jitter of each network link. By their approaches, complex QoS routing algorithms can be realized and deployed for performing industrial data delivery. In [115], the authors propose a destination-aware adaptive traffic flow rule aggregation (DATA) mechanism for facilitating traffic flow monitoring in SDN-based IIoT networks. The proposed method adapts the number of flow table entries in SDN switches according to the level of detail of traffic flow information that other mechanisms (e.g. for traffic engineering, traffic monitoring, intrusion detection) require. It also prevents performance degradation of the SDN switches by keeping the number of flow table entries well below a critical level.

7. Conclusion

Although the paradigm of IIoT networks promotes the progress of smart manufacture towards achieving reduced costs and increased efficiency, IIoT networks present the constraints of network heterogeneity and scalability. Current network architectures integrate computing units of *low-intelligence*, which cannot support the scheduling for diverse and complex industrial flow – especially for case scenarios with delay-sensitivity requirements. In this paper, we argued that these issues can be addressed by utilizing an AI-enabled SDN technique, and we have presented a formal architecture named by AI-SDIN to achieve

this vision. Within the presented architecture, the IIoT networks are divided into three functional layers: data layer, network layer, and control layer. In the latter, advanced *machine intelligence* can be deployed to improve the security and functionality of the network. Then, we have surveyed possible key technologies towards actual implementation – e.g., Blockchain-based data sharing, intelligent wireless data sensing, edge intelligence, TSN&SDN, distributed AI, etc. We have also presented potential enhanced industrial applications based on AI-SDIN ranging from logistics to agriculture. Finally, the paper has indicated challenges and areas where further research is required. Our paper aims at revealing that the AI-SDIN leads the future of smart manufacture to be clear and bright. With AI-SDIN, industrial manufacture will be supermatic with less manufacture time and intelligent logistics, supporting fast production and marketing.

Acknowledgements

This work was supported by the Natural Science Foundation of China (No. 62002045), China Postdoctoral Science Foundation (No. 2021M690565), and Fundamental Research Funds for the Central Universities (No. N2117002).

References

[1] M. Ghobakhloo, Industry 4.0, digitization, and opportunities for sustainability, Journal of Cleaner Production 252 (4) (2020) 119869.
[2] C. Zhang, Y. Chen, A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics, Journal of Industrial Integration and Management 5 (01) (2020) 165–180.
[3] W. Khan, M. Rehman, H. Zangoti, M. Afzal, N. Armi, K. Salah, Industrial internet of things: Recent advances, enabling technologies and open challenges, Computers & Electrical Engineering 81 (01) (2020) 106522.
[4] F. Zhu, J. Gao, J. Yang, N. Ye, Neighborhood linear discriminant analysis, Pattern Recognition 123 (3) (2022) 108422.
[5] K. Tange, M. De Donno, X. Fafoutis, N. Dragoni, A systematic survey of industrial internet of things security: Requirements and fog computing opportunities, IEEE Communications Surveys & Tutorials 22 (4) (2020) 2489–2520.
[6] M. Faheem, M. Umar, R. A. Butt, B. Raza, M. A. Ngadi, V. C. Gungor, Software Defined Communication Framework for Smart Grid to Meet Energy Demands in Smart Cities, in: 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 51–55.
[7] X. Wu, M. D. Soltani, L. Zhou, M. Safari, H. Haas, Hybrid LiFi and WiFi networks: A survey, IEEE Communications Surveys & Tutorials 23 (2) (2021) 1398–1420.
[8] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, S. W. Kim, The future of healthcare internet of things: a survey of emerging technologies, IEEE Communications Surveys & Tutorials 22 (2) (2020) 1121–1167.
[9] C. Lin, Y. Bi, H. Zhao, Z. Liu, S. Jia, J. Zhu, DTE-SDN: A dynamic traffic engineering engine for delay-sensitive transfer, IEEE Internet of Things Journal 5 (6) (2018) 5240–5253.
[10] G. Premsankar, M. Di Francesco, T. Taleb, Edge computing for the Internet of Things: A case study, IEEE Internet of Things Journal 5 (2) (2018) 1275–1284.
[11] S. Kharb, A. Singhrova, A survey on network formation and scheduling algorithms for time slotted channel hopping in industrial networks, Journal of Network and Computer Applications 126 (1) (2019) 59–87.
[12] T. Ma, Y. Wang, W. Hu, D. El-Banna, K. Zhang, Evaluation of flexilink as unified real-time protocol for industrial networks, in: Proc. IEEE ICIEA), Wuhan, China, 2018, pp. 123–128.
[13] C. Sauer, E. Lyczkowski, M. Sliskovic, M. Schmidt, Real-time alarm dissemination in mobile industrial networks, in: Proc. IEEE ICIT, Valencia, Spain, 2021, pp. 1152–1156.
[14] M. Martínez-García, Y. Zhang, K. Suzuki, Y.-D. Zhang, Deep recurrent entropy adaptive model for system reliability monitoring, IEEE Transactions on Industrial Informatics 17 (2) (2020) 839–848.
[15] W. Li, P. Spachos, M. Chignell, A. Leon-Garcia, L. Zucherman, J. Jiang, A quantitative relationship between application performance metrics and quality of experience for over-the-top video, Computer Networks 142 (9) (2018) 194–207.
[16] Z. Duanmu, A. Rehman, Z. Wang, A quality-of-experience database for adaptive video streaming, IEEE Transactions on Broadcasting 64 (2) (2018) 474–487.
[17] F. Zhu, Y. Ning, X. Chen, Y. Zhao, Y. Gang, On removing potential redundant constraints for svor learning, Applied Soft Computing 102 (4) (2021) 106941.
[18] Q. Yan, W. Huang, X. Luo, Q. Gong, F. R. Yu, A multilevel ddos mitigation framework for the industrial internet of things, IEEE Communications Magazine 56 (2) (2018) 30–36.
[19] Y. Zhou, G. Cheng, Y. Zhao, Z. Chen, S. Jiang, Toward proactive and efficient ddos mitigation in iiot systems: A moving target defense approach, IEEE Transactions on Industrial Informatics 18 (4) (2022) 2734–2744.
[20] H. Qi, J. Wang, W. Li, Y. Wang, T. Qiu, A blockchain-driven iiot traffic classification service for edge computing, IEEE Internet of Things Journal 8 (4) (2021) 2124–2134.
[21] Y. Hu, M. Serror, K. Wehrle, J. Gross, Finite blocklength performance of cooperative multi-terminal wireless industrial networks, IEEE Transactions on Vehicular Technology 67 (7) (2018) 5778–5792.
[22] A. Neumann, M. Ehrlich, L. Wisniewski, J. Jasperneite, Towards monitoring of hybrid industrial networks, in: Proc. IEEE WFCS, Trondheim, Norway, 2017, pp. 1–4.
[23] L. Leonardi, M. Ashjaei, H. Fotouhi, L. L. Bello, A proposal towards software-defined management of heterogeneous virtualized industrial networks, in: Proc. IEEE INDIN, Aland Espoo, Finland, 2019, pp. 1741–1746.
[24] K. Crawford, The Atlas of AI, Yale University Press, 2021.
[25] I. Alam, K. Sharif, F. Li, Z. Latif, M. M. Karim, S. Biswas, B. Nour, Y. Wang, A survey of network virtualization techniques for Internet of Things using SDN and NFV, ACM Computing Surveys (CSUR) 53 (2) (2020) 1–40.
[26] A. Mishra, N. Gupta, B. Gupta, Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller, Telecommunication systems 77 (1) (2021) 47–62.
[27] Y. Jiang, K. Zhang, Y. Qian, R. Q. Hu, Efficient and Privacy-Preserving Distributed Learning in Cloud-Edge Computing Systems, in: Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning, New York, NY, USA, 2021, p. 25–30.
[28] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, OpenFlow: enabling innovation in campus networks, ACM SIGCOMM computer communication review 38 (2) (2008) 69–74.
[29] J. Lu, L. Feng, J. Yang, M. M. Hassan, A. Alelaiwi, I. Humar, Artificial agent: The fusion of artificial intelligence and a mobile agent for energy-efficient traffic control in wireless sensor networks, Future Generation Computer Systems 95 (6) (2019) 45–51.
[30] Q. Zhang, X. Wang, J. Lv, M. Huang, Intelligent content-aware traffic engineering for SDN: An AI-driven approach, IEEE Network 34 (3) (2020) 186–193.
[31] H. Wu, J. Chen, C. Zhou, W. Shi, N. Cheng, W. Xu,

W. Zhuang, X. S. Shen, Resource management in space-air-ground integrated vehicular networks: SDN control and AI algorithm design, IEEE Wireless Communications 27 (6) (2020) 52–60.

[32] M. Masud, M. Alazab, K. Choudhary, G. S. Gaba, 3P-SAKE: privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks, Computer Communications 175 (7) (2021) 82–90.

[33] S. Zhu, S. Xiao, A multi-service adaptive wireless communication protocol for industrial networks, in: Proc. IEEE ICCSNT, Dalian, China, 2017, pp. 371–374.

[34] S. R. Pokhrel, Y. Qu, L. Gao, QoS-aware personalized privacy with multipath tcp for industrial iot: Analysis and design, IEEE Internet of Things Journal 7 (6) (2020) 4849–4861.

[35] M. Serror, E. Wagner, R. Glebke, K. Wehrle, QWIN: Facilitating QoS in Wireless Industrial Networks Through Cooperation, in: Proc. IFIP Networking Conference, Paris, France, 2020, pp. 386–394.

[36] L. Song, Y. Liao, K. Bian, L. Song, Z. Han, Cross-layer protocol design for CSMA/CD in full-duplex WiFi networks, IEEE Communications Letters 20 (4) (2016) 792–795.

[37] M. M. Hassan, A. Gumaei, S. Huda, A. Almogren, Increasing the trustworthiness in the industrial iot networks through a reliable cyberattack detection model, IEEE Transactions on Industrial Informatics 16 (9) (2020) 6154–6162.

[38] M. H. C. Garcia, A. Molina-Galan, M. Boban, J. Gozalvez, B. Coll-Perales, T. Şahin, A. Kousaridas, A Tutorial on 5G NR V2X Communications, IEEE Communications Surveys & Tutorials 23 (3) (2021) 1972–2026.

[39] L. Chettri, R. Bera, A Comprehensive Survey on Internet of Things (IoT) toward 5G Wireless Systems, IEEE Internet of Things Journal 7 (1) (2019) 16–32.

[40] R. Zhohov, D. Minovski, P. Johansson, K. Andersson, Real-time performance evaluation of LTE for IIoT, in: Proc. IEEE LCN, Chicago, USA, 2018, pp. 623–631.

[41] H. Huang, S. Ding, L. Zhao, H. Huang, L. Chen, H. Gao, S. H. Ahmed, Real-time fault detection for iiot facilities using gbrbm-based dnn, IEEE Internet of Things Journal 7 (7) (2019) 5713–5722.

[42] S. Nuratch, The IIoT devices to cloud gateway design and implementation based on microcontroller for real-time monitoring and control in automation systems, in: Proc. IEEE ICIEA, Siem Reap, Cambodia, 2017, pp. 919–923.

[43] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hölzle, S. Stuart, A. Vahdat, B4: Experience with a globally-deployed software defined wan, in: Proc. ACM SIGCOMM 2013, New York, NY, USA, 2013, p. 3–14.

[44] N. L. M. van Adrichem, C. Doerr, F. A. Kuipers, Opennetmon: Network monitoring in openflow software-defined networks, in: Proc. IEEE Network Operations and Management Symposium (NOMS), Dallas, TX, USA, 2014, pp. 1–8.

[45] Y. Zhang, M. Martínez-García, R. S. Kalawsky, A. Latimer, Grey-box modelling of the swirl characteristics in gas turbine combustion system, Measurement 151 (2020) 107266.

[46] M. Martínez-García, Y. Zhang, J. Wan, J. Mcginty, Visually interpretable profile extraction with an autoencoder for health monitoring of industrial systems, in: 2019 IEEE 4th International Conference on Advanced Robotics and Mechatronics (ICARM), IEEE, 2019, pp. 649–654.

[47] M. Martínez-García, Y. Zhang, K. Suzuki, Y. Zhang, Measuring system entropy with a deep recurrent neural network model, in: 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Vol. 1, IEEE, 2019, pp. 1253–1256.

[48] S. Wang, M. E. Celebi, Y.-D. Zhang, X. Yu, S. Lu, X. Yao, Q. Zhou, M.-G. Miguel, Y. Tian, J. M. Gorriz, et al., Advances in data preprocessing for biomedical data fusion: An overview of the methods, challenges, and prospects, Information Fusion.

[49] S. Shen, C. Yu, K. Zhang, J. Ni, S. Ci, Adaptive and Dynamic Security in AI-Empowered 6G: From an Energy Efficiency Perspective, IEEE Communications Standards Magazine 5 (3) (2021) 80–88.

[50] J. Wan, X. Li, H.-N. Dai, A. Kusiak, M. Martínez-García, D. Li, Artificial-intelligence-driven customized manufacturing factory: key technologies, applications, and challenges, Proceedings of the IEEE 109 (4) (2020) 377–398.

[51] Y. Li, Z. Chi, X. Liu, T. Zhu, Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption, in: Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems, New York, NY, USA, 2018, p. 159–171.

[52] Reliability and temporality optimization for multiple coexisting wirelesshart networks in industrial environments.

[53] Z. Padrah, C. Pop, E. Jecan, A. Pastrav, T. Palade, O. Ratiu, E. Puschita, An ISA100.11a Model Implementation for Accurate Industrial WSN Simulation in ns-3, in: 2020 International Workshop on Antenna Technology (iWAT), Bucharest, Romania, 2020, pp. 1–4.

[54] D. Antonioli, N. O. Tippenhauer, K. Rasmussen, BIAS: Bluetooth Impersonation AttackS, in: 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 549–562.

[55] G. Premsankar, B. Ghaddar, M. Slabicki, M. Di Francesco, Optimal configuration of lora networks in smart cities, IEEE Transactions on Industrial Informatics 16 (12) (2020) 7243–7254.

[56] G. S. Sestito, A. C. Turcato, A. L. Dias, M. S. Rocha, M. M. da Silva, P. Ferrari, D. Brandao, A method for anomalies detection in real-time ethernet data traffic applied to PROFINET, IEEE Transactions on Industrial Informatics 14 (5) (2017) 2171–2180.

[57] A. Serhane, M. Shraif, H. Chehadi, A. Harb, A. Mohsen, Optimizing solar systems using DeviceNET, in: Proc. IEEE ICM, Beirut, Lebanon, 2017, pp. 1–4.

[58] W. You, H. Ge, Design and implementation of modbus protocol for intelligent building security, in: Proc. IEEE ICCT, Xi'an, China, 2019, pp. 420–423.

[59] M. Bozdal, M. Samie, I. Jennions, A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions, in: 2018 International Conference on Computing, Electronics Communications Engineering (iCCECE), 2018, pp. 201–205.

[60] E. Haleplidis, J. H. Salim, J. M. Halpern, S. Hares, K. Pentikousis, K. Ogawa, W. Wang, S. Denazis, O. Koufopavlou, Network programmability with ForCES, IEEE Communications Surveys & Tutorials 17 (3) (2015) 1423–1440.

[61] X. Wang, Y. Tian, M. Zhao, M. Li, L. Mei, X. Zhang, PNPL: Simplifying programming for protocol-oblivious SDN networks, Computer Networks 147 (12) (2018) 64–80.

[62] E. F. Castillo, O. M. C. Rendon, A. Ordonez, L. Z. Granville, IPro: An approach for intelligent SDN monitoring, Computer Networks 170 (4) (2020) 107108.

[63] M. Faheem, R. A. Butt, B. Raza, M. W. Ashraf, M. A. Ngadi, V. C. Gungor, Energy Efficient And Reliable Data Gathering Using Internet of Software-Defined Mobile Sinks for WSNs-based Smart Grid Applications, Computer Standards & Interfaces 66 (10) (2019) 103341.

[64] F. Zhu, J. Gao, C. Xu, J. Yang, D. Tao, On selecting effective patterns for fast support vector regression training, IEEE Transactions on Neural Networks and Learning Systems 29 (8) (2018) 3610–3622.

[65] Y. Zhang, M. Mukherjee, C. Wu, M.-T. Zhou, Advanced industrial networks with IoT and big data, Mobile Networks and Applications 24 (3) (2019) 947–949.

[66] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. Rodrigues, M. Guizani, Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay, IEEE communications magazine 56 (2) (2018) 44–51.

[67] X. Li, J. Wan, H.-N. Dai, M. Imran, M. Xia, A. Celesti, A hybrid computing solution and resource scheduling strategy for edge computing in smart manufacturing, IEEE Transactions on Industrial Informatics 15 (7) (2019) 4225–4234.

[68] H. Song, Protocol-Oblivious Forwarding: Unleash the Power

of SDN through a Future-Proof Forwarding Plane, in: Proc. ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, New York, NY, USA, 2013, pp. 127—-132.

[69] R. Amin, M. Reisslein, N. Shah, Hybrid SDN networks: A survey of existing approaches, IEEE Communications Surveys & Tutorials 20 (4) (2018) 3259–3306.

[70] A. A. Barakabitze, A. Ahmad, R. Mijumbi, A. Hines, 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges, Computer Networks 167 (1) (2020) 106984.

[71] F. Tang, B. Mao, Z. M. Fadlullah, N. Kato, On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT, IEEE Communications Magazine 56 (9) (2018) 80–86.

[72] J. Li, Z. Zhao, R. Li, H. Zhang, Ai-based two-stage intrusion detection for software defined iot networks, IEEE Internet of Things Journal 6 (2) (2018) 2093–2102.

[73] J. Sengupta, S. Ruj, S. Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot, Journal of Network and Computer Applications 149 (1) (2020) 102481.

[74] K. Yu, L. Tan, M. Aloqaily, H. Yang, Y. Jararweh, Blockchain-enhanced data sharing with traceable and direct revocation in iiot, IEEE Transactions on Industrial Informatics 17 (11) (2021) 7669–7678.

[75] A. Singh, D. Kumar, J. Hötzel, IoT Based information and communication system for enhancing underground mines safety and productivity: Genesis, taxonomy and open issues, Ad Hoc Networks 78 (8) (2018) 115–129.

[76] F. Sutton, R. D. Forno, J. Beutel, L. Thiele, BLITZ: Low latency and energy-efficient communication for event-triggered wireless sensing systems, ACM Transactions on Sensor Networks (TOSN) 15 (2) (2019) 1–38.

[77] D. Upadhyay, S. Sampalli, SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations, Computers & Security 89 (1) (2020) 101666.

[78] V. Kotsiou, G. Z. Papadopoulos, P. Chatzimisios, F. Theoleyre, Whitelisting Without Collisions for Centralized Scheduling in Wireless Industrial Networks, IEEE internet of things journal 6 (3) (2019) 5713–5721.

[79] M. Serror, E. Wagner, R. Glebke, K. Wehrle, QWIN: Facilitating QoS in Wireless Industrial Networks Through Cooperation, in: 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 386–394.

[80] N. Jiang, D. Xu, J. Zhou, H. Yan, T. Wan, J. Zheng, Toward optimal participant decisions with voting-based incentive model for crowd sensing, Information Sciences 512 (1) (2020) 1–17.

[81] Q. Li, Y. Yue, Z. Wang, Deep robust cramer shoup delay optimized fully homomorphic for IIoT secured transmission in cloud computing, Computer Communications 161 (8) (2020) 10–18.

[82] K. Zhang, Y. Zhu, S. Maharjan, Y. Zhang, Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things, IEEE Network 33 (5) (2019) 12–19.

[83] F. Alvarez, D. Breitgand, D. Griffin, P. Andriani, S. Rizou, N. Zioulis, F. Moscatelli, J. Serrano, M. Keltsch, P. Trakadas, et al., An edge-to-cloud virtualized multimedia service platform for 5G networks, IEEE Transactions on Broadcasting 65 (2) (2019) 369–380.

[84] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, A. Y. Zomaya, Edge intelligence: the confluence of edge computing and artificial intelligence, IEEE Internet of Things Journal 7 (8) (2020) 7457–7469.

[85] X. Zhang, Y. Wang, S. Lu, L. Liu, L. xu, W. Shi, OpenEI: An Open Framework for Edge Intelligence, in: IEEE 2019 International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 2019, pp. 1840–1851.

[86] Y. Lin, X. Jin, T. Zhang, M. Han, N. Guan, Q. Deng, Queue Assignment for Fixed-Priority Real-Time Flows in Time-Sensitive Networks: Hardness and Algorithm, Journal of Systems Architecture 116 (2021) 102141.

[87] K. M. Shalghum, N. K. Noordin, A. Sali, F. Hashim, Network Calculus-Based Latency for Time-Triggered Traffic under Flexible Window-Overlapping Scheduling (FWOS) in a Time-Sensitive Network (TSN), Applied Sciences 11 (9) (2021) 3896.

[88] S. B. H. Said, Q. H. Truong, M. Boc, SDN-based configuration solution for IEEE 802.1 time sensitive networking (TSN), ACM SIGBED Review 16 (1) (2019) 27–32.

[89] X. Jin, C. Xia, N. Guan, P. Zeng, Joint Algorithm of Message Fragmentation and No-Wait Scheduling for Time-Sensitive Networks, IEEE/CAA Journal of Automatica Sinica 8 (2) (2021) 478–490.

[90] D. A. J. AL-Khaffaf, Improving LAN Performance Based on IEEE802. 1Q VLAN Switching Techniques, Journal of University of Babylon for Engineering Sciences 26 (1) (2018) 286–297.

[91] F. Smirnov, F. Reimann, J. Teich, M. Glaß, Automatic optimization of the VLAN partitioning in automotive communication networks, ACM Transactions on Design Automation of Electronic Systems (TODAES) 24 (1) (2018) 1–23.

[92] H. Puttnies, P. Danielis, D. Timmermann, Ptp-lp: Using linear programming to increase the delay robustness of ieee 1588 ptp, in: Proc. IEEE GLOBECOM, Abu Dhabi, United Arab Emirates, 2018, pp. 1–7.

[93] T. Gerhard, T. Kobzan, I. Blöcher, M. Hendel, Software-defined flow reservation: Configuring IEEE 802.1 Q time-sensitive networks by the use of software-defined networking, in: Proc. IEEE ETFA, Zaragoza, Spain, 2019, pp. 216–223.

[94] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi, C. Wang, X. Shao, M. Reisslein, H. Elbakoury, Performance Comparison of IEEE 802.1 TSN Time Aware Shaper (TAS) and Asynchronous Traffic Shaper (ATS), IEEE Access 7 (3) (2019) 44165–44181.

[95] L. Silva, P. Pedreiras, P. Fonseca, L. Almeida, On the adequacy of SDN and TSN for Industry 4.0, in: Proc. IEEE ISORC, Valencia, Spain, 2019, pp. 43–51.

[96] V. Balasubramanian, M. Aloqaily, M. Reisslein, An SDN Architecture for Time Sensitive Industrial IoT, Computer Networks 186 (2021) 107739.

[97] H. Chahed, A. J. Kassler, Software-Defined Time Sensitive Networks Configuration and Management, in: 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Heraklion, Greece, 2021, pp. 124–128.

[98] S. Alrubei, E. Ball, J. Rigelsford, The Use of Blockchain to Support Distributed AI Implementation in IoT Systems, IEEE Internet of Things Journal.

[99] M. Zolanvari, A. Ghubaish, R. Jain, ADDAI: Anomaly Detection using Distributed AI, in: IEEE International Conference on Networking, Sensing and Control (ICNSC), Xiamen, China, 2021, pp. 1–6.

[100] C. Mwase, Y. Jin, T. Westerlund, H. Tenhunen, Z. Zou, Communication-Efficient Distributed AI Strategies for the IoT Edge, Future Generation Computer Systems 131 (2022) 292–308.

[101] D. Henneke, L. Wisniewski, J. Jasperneite, Analysis of realizing a future industrial network by means of software-defined networking (sdn), in: Proc. IEEE WFCS), Aveiro, Portugal, 2016, pp. 1–4.

[102] C. Liu, M. Gao, G. Zhu, C. Zhang, P. Zhang, J. Chen, W. Cai, Data Driven Eco-Efficiency Evaluation and Optimization in Industrial Production, Energy 224 (2021) 120170.

[103] M. Martínez-García, R. S. Kalawsky, T. Gordon, T. Smith, Q. Meng, F. Flemisch, Communication and interaction with semiautonomous ground vehicles by force control steering, IEEE transactions on cybernetics.

[104] C. Sung, B. Zhang, C. Y. Higgins, Y. Choe, Data-Driven Sales Leads Prediction for Everything-as-a-Service in the Cloud, in: Proc. IEEE DSAA, Montreal, QC, Canada, 2016, pp. 557–563.

[105] F. Niaz, M. Khalid, Z. Ullah, N. Aslam, M. Raza, M. Priyan,

A bonded channel in cognitive wireless body area network based on IEEE 802.15. 6 and internet of things, Computer Communications 150 (1) (2020) 131–143.

[106] M. Azees, P. Vijayakumar, M. Karuppiah, A. Nayyar, An Efficient Anonymous Authentication and Confidentiality Preservation Schemes for Secure Communications in Wireless Body Area Networks, Wireless Networks 27 (3) (2021) 2119–2130.

[107] C. Lin, G. Han, X. Qi, J. Du, T. Xu, M. Martinez-Garcia, Energy-Optimal Data Collection for Unmanned Aerial Vehicle-Aided Industrial Wireless Sensor Network-Based Agricultural Monitoring System: A Clustering Compressed Sampling Approach, IEEE Transactions on Industrial Informatics 17 (6) (2021) 4411–4420.

[108] B. Almadani, S. M. Mostafa, IIoT Based Multimodal Communication Model for Agriculture and Agro-Industries, IEEE Access 9 (1) (2021) 10070–10088.

[109] C. Perrow, Normal Accidents: Living with High Risk Technologies-Updated Edition, Princeton university press, 2011.

[110] Yolov3, `https://arxiv.org/abs/1804.02767.pdf`.

[111] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, L.-C. Chen, Mobilenetv2: Inverted residuals and linear bottlenecks, in: Proc. IEEE CVPR, Salt Lake City, UT, USA, 2018, pp. 4510–4520.

[112] X. Zhang, X. Zhou, M. Lin, J. Sun, Shufflenet: An extremely efficient convolutional neural network for mobile devices, in: Proc. IEEE CVPR, Salt Lake City, UT, USA, 2018, pp. 6848–6856.

[113] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, M. Wang, Fog-computing-enabled cognitive network function virtualization for an information-centric future Internet, IEEE Communications Magazine 57 (7) (2019) 48–54.

[114] N. L. Van Adrichem, C. Doerr, F. A. Kuipers, Opennetmon: Network monitoring in openflow software-defined networks, in: Proc. IEEE NOMS, Krakow, Poland, 2014, pp. 1–8.

[115] T. V. Phan, M. Hajizadeh, N. T. Khi, T. Bauschert, Destination-aware Adaptive Traffic Flow Rule Aggregation in Software-Defined Networks, in: 2019 International Conference on Networked Systems (NetSys), Munich, Germany, 2019, pp. 1–6.

We declared that there is no conflict of interest in this paper (Title: How AI-enabled SDN Technologies Improve the Security and Functionality of Industrial IoT Network: Architectures, Enabling Technologies, and Opportunities).

Jinfang Jiang, Chuan Lin, Guangjie Han, Adnan M. Abu-Mahfouz, Syed Bilal Hussain Shah, Miguel Martínez-García