Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.040456
Review

Managing Smart Technologies with Software-Defined Networks for Routing and Security Challenges: A Survey

Babangida Isyaku[1,2] and Kamalrulnizam Bin Abu Bakar[2,*]

[1]Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor, 81310, Malaysia
[2]Department of Computer Science, Faculty of Computing and Information Technology, Sule Lamido University, P.M.B. 048, Jigawa State, Nigeria
*Corresponding Author: Kamalrulnizam Bin Abu Bakar. Email: knizam@utm.my
Received: 19 March 2023; Accepted: 09 May 2023; Published: 28 July 2023

Abstract: Smart environments offer various services, including smart cities, e-healthcare, transportation, and wearable devices, generating multiple traffic flows with different Quality of Service (QoS) demands. Achieving the desired QoS with security in this heterogeneous environment can be challenging due to traffic flows and device management, unoptimized routing with resource awareness, and security threats. Software Defined Networks (SDN) can help manage these devices through centralized SDN controllers and address these challenges. Various schemes have been proposed to integrate SDN with emerging technologies for better resource utilization and security. Software Defined Wireless Body Area Networks (SDWBAN) and Software Defined Internet of Things (SDIoT) are the recently introduced frameworks to overcome these challenges. This study surveys the existing SDWBAN and SDIoT routing and security challenges. The paper discusses each solution in detail and analyses its weaknesses. It covers SDWBAN frameworks for efficient management of WBAN networks, management of IoT devices, and proposed security mechanisms for IoT and data security in WBAN. The survey provides insights into the state-of-the-art in SDWBAN and SDIoT routing with resource awareness and security threats. Finally, this study highlights potential areas for future research.

Keywords: SDN; WBAN; IoT; routing; security

1 Introduction

Smart environment is a network of heterogeneous smart objects connected to the internet, including smart transportation, home appliances, surveillance equipment, and wearable e-healthcare devices [1]. Internet of things (IoT) devices are applied in these smart environments to gather and share the required information autonomously between other devices. The IoT has become a technological revolution representing the future of computing and communications [2]. It integrates every object for interaction via embedded systems, leading to a highly distributed network of devices communicating

with human beings as other devices [3]. The number of connected Internet of Things (IoT) devices is predicted to reach 83 billion by 2024 [4]. These heterogeneous devices generate traffic flows with different Quality of Service (QoS) requirements. The diversity of IoT devices and their associated applications makes it challenging to predict the amount and types of traffic flows that will be generated [5]. Routing traffic flows in IoT networks is a critical aspect of network management due to the limited resource exhibited by the devices [5]. They exhibit high computational power and energy with limited memory [6]. The device's energy is one of the most important resources, which may cause the network to experience intermittent connectivity and complicate the routing challenge in IoT [7]. The diversity of IoT devices, communication infrastructure, and protocols used in IoT pose significant challenges to establishing seamless communication and interoperability between different devices and networks. This complexity adds to the difficulty of managing traffic flows and ensuring security and privacy in the IoT ecosystem [8]. The most common IoT security attacks are Denial of Service (DoS) and energy depletion attacks [9].

Conversely, WBANs use tiny sensors to collect and process health data in real-time, which has greatly improved patient monitoring and diagnosis in hospitals and remote areas. These sensors can be attached to or implanted inside the body to monitor various physiological parameters, such as blood pressure, heart rate, glucose level, and temperature [10]. The data collected by these sensors is sent to a master node and then transmitted to a health facility. The communication within the WBAN network is known as intra-WBAN [11]. Communication between personal devices and the master node is referred to as Inter-BAN. It enables data exchange between different WBAN networks, which may have different devices and sensors operating at different frequencies, and with different protocols [12]. This communication allows healthcare professionals to gather data from multiple sources to get a more comprehensive view of a patient's health status, regardless of location. However, the diverse traffic pattern from various applications in WBAN makes it critical to address the communication requirement of different flows [13]. The successful deployment of WBANs is challenging due to the need to use appropriate technology, maintain strict security regulations, implement a suitable network architecture, manage traffic engineering, and handle data and QoS among inter WBANs [14].

Therefore, IoT and WBAN technologies exhibit similar weaknesses due to their architectural design and limited resources [15]. The latter and former network architectures are not designed to support scalable networks with various devices operating with different protocols [16]. Hence, routing and security challenges are among the main issues affecting WBAN and IoT systems [17]. A strong communication architecture with flexible, scalable, and dynamic control over IoT and WBAN operations is urgently required to improve the routing, security, and efficiency of managing data from various applications [18]. The emerging Software Defined Networks (SDN) paradigm could achieve an optimum solution to many of the challenges of WBANs and IoT. SDN are a promising technology that can provide solutions to improve network infrastructure management [19]. This way, SDN can optimize routing with resource awareness in smart technologies by enabling dynamic routing, programmable network policies, centralized management, and resource-aware routing decisions. By leveraging SDN in smart technologies, network administrators can ensure that their networks can handle the increased traffic generated by these technologies while remaining energy-efficient and cost-effective. SDN-based frameworks such as Software Defined Wireless Body Area Network (SDWBAN) and Software Defined Internet of Things (SDIoT) have been proposed to efficiently manage wireless sensors embedded in wearable devices and non-medical sensors.

Several routing challenges survey papers were presented for WBAN over the years [20]. Another article [5] discussed SDN and IoT security features. The works in [19,21] review IoT virtualization using SDN by classifying the literatureinto SDN designed for IoT, function virtualization for IoT networks,

and SDIoT networks. Reference [22] reviews incorporating SDN Architecture with IoT while focusing on managing IoT devices with SDN. The paper in [23] studies the SDN and fog computing-based solutions to overcome the IoT's main challenges. The survey in [24] extensively discussed SDN base technologies to address the requirement of IoT from different network scales, including the data centre. Challenges were also presented in the context of IoT and, finally, highlighted some future work. The works in [25,26] present a taxonomy of security threats that affect the existing solution and highlight their weaknesses. An in-depth analysis of how SDN/NFV (Network Function Virtualization) architecture is incorporated in IoT, Fog, and cloud computing with a security framework is presented in [27]. The paper in [28] reviewed the SDN framework to address IoT management issues concerning fault tolerance, energy management, scalability, load balancing, and security threat. While researchers are better with time. There is a lack of comprehensive surveys to cover the benefit of integrating SDN and other emerging technologies, such as smart healthcare and the city while focusing on routing with resource awareness and security concerns.

In contrast to the existing study, managing Wireless Body Area Networks (WBANs) and the Internet of Things (IoT) using SDN for routing and security challenges has not been fully covered. SDN is a promising technology that provides centralized network management and control, making it an ideal solution for managing complex IoT and WBAN networks. This survey paper explored different routing and security challenges faced by these networks and how SDN can be used to address these challenges. The paper explores how SDN can manage routing and security in WBANs and IoT. Various SDWBAN and SDIoT, routing and security solutions were discussed. The paper extensively discusses each solution and analyses their weakness. Future research directions were presented. Table 1 summarizes the related surveys and their differences from the present document. Table 2 present all the abbreviation used and their description.

Table 1: Comparison of related surveys

Related work	Year	Internet of Things	WBAN	SDN	Security threats and vulnerabilities	Routing with resource awareness	Scope of the work
Bera et al. [24]	2017	√	X	√	X	X	Discusses application area of SDN in IoT. Review related works
Salman et al. [23,21]	2018	√	X	√	√	X	The paper discussed incorporating SDN and fog computing to overcome the IoT's main challenges
Qu et al. [20]	2019	√	√	X	X	√	Analysis, prons, and cons of the routing protocol in WBAN
Farris et al. [5]	2019	√	X	√	√	X	discussed the security features provided for both SDN and IoT
Alam et al. [19]	2020	√	X	√	X	X	The authors discussed and categorized the used of SDN in IoT, VFN

(Continued)

Table 1 (continued)

Related work	Year	Internet of Things	WBAN	SDN	Security threats and vulnerabilities	Routing with resource awareness	Scope of the work
Dantas Silva et al. [25,26]	2020	√	X	√	√	X	Present SDN security taxonomy in IoT scenario
Sergio et al. [22]	2020	√	X	√	X	X	Review management of IoT devised with SDN
Ray et al. [27]	2021	√	X	√	X	X	Discussed how SDN is integrated with IoT, Fog, and cloud computing with other emerging technology
Siddiqui et al. [28]	2022	√	X	√	√	X	Reviewed SDN framework to address IoT management issues concerning fault tolerance, energy management, scalability, load balancing, and security threat
Present survey paper	2023	√	√	√	√	√	Extensively discussed SDN framework to address WBAN wearable devices management concerning Routing, fault tolerance, and security

Table 2: Summary of abbreviation

Abbreviation	Description
AAA	Authentication Authorization and Accounting
ARP	Address Resolution Protocol
BCM/MCM	binary and a multi-class classification module
SDIoT	Software Defined Internet of Things
SDWBAN	Software Defined Wireless Body Area Networks
QoS	Quality of Service
IoT	Internet of Things
SDN	Software Defined Networks
AP	Application Plane
CP	Control Plane
DP	Data Plane
API	Application Programming Interface

(Continued)

Table 2 (continued)

Abbreviation	Description
REST	Representational State Transfer
NOS	Network Operating System
NBI	Northbound Interface
ONIX	Online Information eXchange
DC	Distributed Controller
POF	Protocol-Oblivious Forwarding
ForCES	Forwarding and Control Elements
OVSDB	Open vSwitch Database Management Protocol
PAD	Programming Abstraction of Datapath
PP	Perception Plane
RFID	Radio Frequency Identification
WSN	Wireless Sensor Networks
DoS	Denial of Service Attack
DdoS	Distributed Denial of Service Attack
PDR	Packet Delivery Ratio
IEEE	Institute of Electrical and Electronics Engineering
MAC	Medium Access Control
PDA	Personal Digital Assistant
WiFi	Wireless Fidelity
EDT	Edge-based Decision-making and Task allocation
EE-TAR	Energy Efficient and Thermal Aware Routing Protocol for SDWBAN
SDNC	Software Defined Network Controller
EOCC-TARA	Energy Optimized Congestion Control based on Temperature Aware Routing Algorithm
EMSMO	Enhanced Multi-objective Spider Monkey Optimization
HMS	Healthcare Monitoring System's security and privacy
SS	Smart Spaces
AI-SDIN	AI-enabled Software-Defined IoT Network
HTTP	Hypertext Transfer Protocol
PHY	Physical
CNN	Convolutional Neural Network
MDP	Markov Decision Process
ML	Machine Learning
AMLSDM	Adaptive Machine Learning based SDN-enabled DdoS attacks Detection and Mitigation
MUD	Manufacturer Usage Description
DPI	deep packet inspection
MITM	Man-In-The-Middle
LFA	Link Flooding Attacks
NIDS	Intrusion Detection System
IP	Internet Protocol

(Continued)

Table 2 (continued)

Abbreviation	Description
TD	Threat Detection
PEM	policy-enforcement module
PoC	proof of concept
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
UTM	Universiti Teknologi Malaysia

Fig. 1 presents the overall structure of the manuscript, summarized as follows: Section 2 presents an overview of SDN. The background and research challenges are described in Section 3. In Section 4, the paper delves into the integration of SDN with smart technologies concerning routing and security. Section 5 covers the lessons learned regarding integrating these two technologies. Section 6 highlights future research directions. Finally, Section 7 concludes the paper.

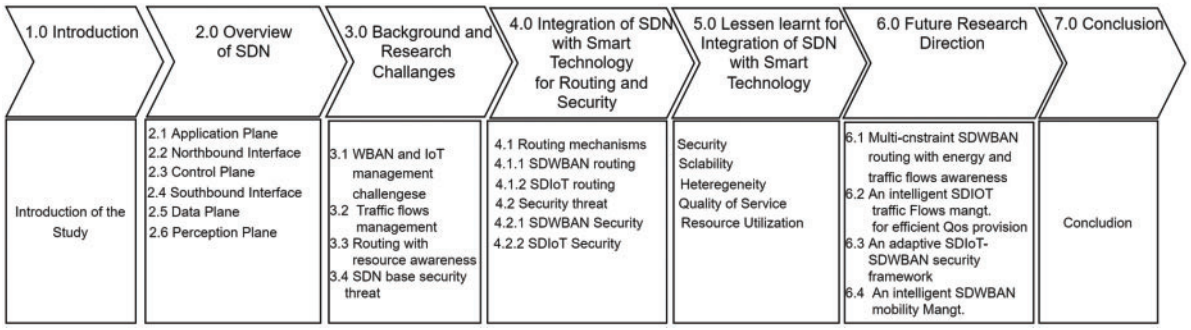

Figure 1: Structure of the manuscript

2 Overview of Software-Defined Networks

Software Defined Networks (SDN) is a new network paradigm that emerged to offer simple policy enforcement, network configuration, and Management by separating network control logic and data forwarding entities [29]. The SDN architecture comprises three (3) planes, as shown in Fig. 2: Application Plane (AP), Control Plane (CP), and Data Plane (DP). Each of these planes played a role in the network. The AP is the application repository that runs on top of the controller. A communication standard manages the interface between the AP and CP. The network operator programs the CP to manage DP devices automatically and optimize network resource usage. The CP instructs the DP based on network policy through an open interface/standard. This way, SDN offers a more flexible and programmable way to manage network traffic and resources, making it an increasingly popular approach to network architecture in enterprise and data centre environments. The following sub-section details each SDN component with its operating procedure. More information about SDN can be found at [30,31].

2.1 Application Plane

AP resides at the top layer in SDN architecture, consisting of various applications and services defining network behaviour. They are used for creating new rules using Application Programming Interfaces (APIs) for certain types of incoming packets that are passed to the controller when needed. The AP offers an end-to-end view of the entire network from various application domains, including routing, security, load balancing, healthcare, network mobility management, and many others for consumers or business applications [32]. For security, the network manager could define a set of security policies at the SDN controller that could be changed later, if necessary, based on changes in the underlying network's adversary model or business application requirements. Additionally, the controller provides several other advantages, including routing. The AP shares these applications as high-level policies with CP through Northbound Interface (NBI).

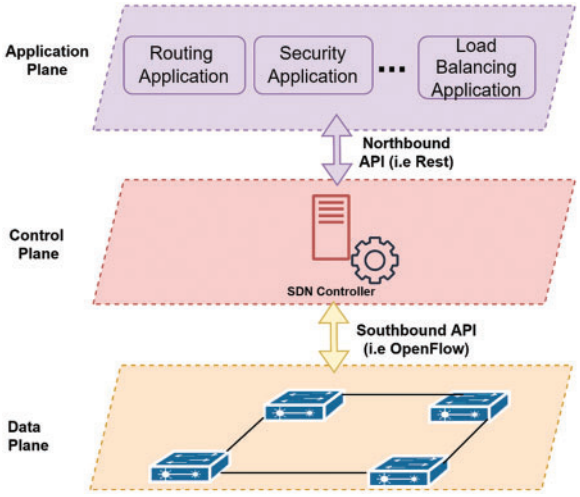

Figure 2: Software defined network architecture

2.2 North Bound Interface

North Bound Interface (NBI) Refers to an interface that enables the communication between lower- and higher-level components. In other words, it established the communication between the SDN controller and the applications or services that run on top of it. This allows applications or services to communicate with the SDN controller responsible for network infrastructure management. The North Bound Interface can be defined using protocols or APIs, such as REST APIs, NETCONF, YANG, etc. The choice of protocol or API depends on the application or service's specific requirements and use cases communicating with the SDN controller. The common northbound interface is still an open issue. More details about NBI can be found at [30,31].

2.3 Control Plane (CP)

The CP is the essential component of the SDN structure; it provides fine-grained control over the networking element at the DP. The CP receives the shared applications from AP, converts them inform of services into a clear set of instructions in the form of flow entries, and installs them in the data structure of DP. The controller manages communication between applications (business logic and intelligence) and network devices [33]. This way, it provides numerous network services such as network topology storage, routing computation, network state monitoring, state data storage,

enforcing security policies, and load balancing [31]. These fundamental functionalities are the critical enabler that most network applications require, increasing productivity while making life easier for application developers and network operators. The CP offered logically centralized network management, easing the burden of solving networking problems through a Network Operating System (NOS) [34].

Similarly to the traditional NOS, its critical value is providing abstractions, essential services, and common Application Programming Interfaces (APIs) to developers. The NOS can provide generic functionality such as network state and topology information, device discovery, and network configuration distribution. This way, the developer is no longer required to be concerned with the low-level details of data distribution among routing elements. There is various set of controllers with different architectural design [35–37]. Existing controllers can be classified in a variety of ways. One of the most critical architectural considerations is centralized or distributed [38]. The former is a single entity that manages all network forwarding devices. Unfortunately, it represents a single point of failure and may have scaling limitations [39]. A single controller may not be sufficient to manage a network with many data plane elements. Alternatively, a Distributed Controller (DC) can be applied to reduce the impact of a single controller failure. This way, it can be scaled to meet the needs of any environment, from small to large-scale networks, including IoT environments [24]. A DC could be a centralized cluster of nodes or a physically distributed set of elements. The most widely used examples of DC include Online Information eXchange (ONIX) [40], HyperFlow [41], DISCO [37], and Beacon [42]. The control and data plane communication is managed through Southbound Interface.

2.4 Southbound Interface

The Southbound Interface (SBI) refers to the interface between the SDN controller and the network infrastructure devices, such as switches and routers. The SBI enables network programmability and automation in an SDN environment. A standard interface for communication between the controller and network devices allows network administrators to configure, manage, and automate network functions more easily and efficiently. This way, it plays a critical role because building a switch from scratch typically takes up to two years to be ready for commercialization, while upgrade cycles can last up to nine months [31]. A new product's software development can take six months to a year [43]. The initial investment is substantial and risky. SBI, as a central component of its design, represents one of the significant barriers to introducing and accepting any new networking technology. In this context, SDN SBI emerged to unlock these hardships through open and standard protocols, which many researchers, including the industry, take as a welcome idea. There exist various SBI protocols in the literature; however, the earlier implementations of the SBI interface were Protocol-Oblivious Forwarding (POF) [44] and Forwarding and Control Elements (ForCES) [45]. Others include Open vSwitch Database Management Protocol (OVSDB) [46], Programming Abstraction of Datapath (PAD) [47], and OpenFlow [48]. These standards encourage interoperability by enabling network equipment from many vendors. However, The OpenFlow protocol provides three information sources to network operating systems. First, forwarding devices send event-based messages to the controller when a link or port change occurs. Second, flow statistics are generated by forwarding devices and collected by the controller. Third, packet-in messages are sent to the controller by delivering devices when they are unsure what to do with a new incoming flow or when there is an explicit "send to controller" action in the matched entry of the flow table. These channels are critical for providing flow-level information to the network operating system. As such, OpenFlow is adopted as the most widely used SBI in SDN [32]. Although, OpenState [49] has emerged as an extension of OpenFlow with two table solutions (state and legacy OpenFlow Flowtable) to reduce consulting controllers. However,

it has not been officially accepted as the SBI in SDN [50]. As such, OpenFlow-enabled equipment demonstrates interoperability which various network vendors have proved.

2.5 Data Plane

The Data Plane (DP) comprises a set of networking equipment (switches, middlebox appliances, access points, and routers), including other IoT devices attached to switches [24]. These devices are used as simpler forwarding entities with no software capable of controlling decisions. The network intelligence is removed from the DP to a logically centralized control system. The CP dynamically configures them to perform the switching, routing, and other task based on a decision made by the network control logic. The network forwarding element consults the SDN controller for any control decision. These new networks are theoretically built on open and standard interfaces (i.e., OpenFlow). An OpenFlow-enabled forwarding device is built on Flowtable [34]. A logical data structure in SDN switches decides how to manage the network. Flowtable comprises flow entries, each Flowtable entry consisting of three parts: (1) a matching rule, (2) actions to be performed on matching packets, and (3) counters to record the statistical information of the successfully matched packets. The Flowtable is populated with a set of flow entries by the CP through reactive or proactive mode [31]. The former installs entries in real-time based on the device's request, while the latter installs rule in advance before the occurrence of any event. For more details about the SDN architecture and Management of the Flowtable table, we refer the reader to the reference in [30].

2.6 Perception Plane

The Perception Plane (PP) comprises sensing devices and an aggregator. The sensing devices include medical sensors, smart cars, smart bicycles, smartphones, Radio Frequency Identification (RFID), smart meters, and many more. These devices allow communication with the IoT Gateway and are visualized as a perception layer below the data plane, as shown in Fig. 3. They sense and collect data from numerous devices intelligently. The aggregator, sink, absorbs information generated by the sensor layer. It typically includes one or more sink nodes that gather and publish data to the Internet via the IoT Gateway. An aggregator can combine sensing or actuating services in the local network and operate as a bridge to connect wireless sensors and the rest of the local network's nodes. SDN can provide centralized control and configuration, policy enforcement, and programming abstraction for large-scale IoT (and sensor) networks. Although, some research has been conducted on the softwarization of WSNs and IoT [51].

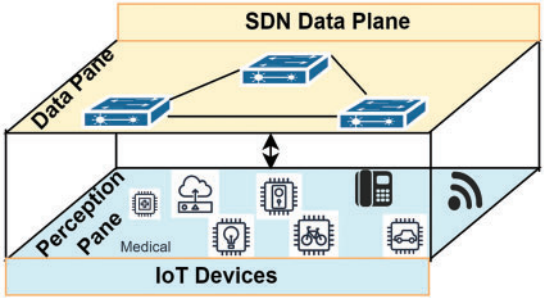

Figure 3: Integration of IoT with SDN architecture at the perception plane

However, Complexity is one of the issues affecting the perception plane because it requires a deep understanding of the underlying technology to configure and manage them correctly. Secondly, there is a lack of standardization in the industry to address the two interfaces efficiently. This can

lead to inconsistencies in how different vendors implement SDN, making it difficult to achieve interoperability and consistency in network behaviour. Finally, security is another critical concern affecting the integration of SDN and IoT devices at the perception plane. The programmability of SDN can introduce new vulnerabilities that must be carefully managed to prevent unauthorized access and attacks between the two interfaces. Therefore, it is required to have SBI for communicating with IoT devices. Unfortunately, extending the SBI into the perception plane beyond OpenFlow switches is a significant challenge [52].

3 Background and Research Challenges

The Internet of Things (IoT) and Wireless Body Area Networks (WBANs) are two emerging technologies that are rapidly gaining popularity [53]. IoT devices are embedded with sensors, processors, and communication capabilities, which allow them to connect to the internet and exchange data with other devices [54]. The Data traffic's proliferation among the sensor nodes and other devices exhibited variabilities such as on-demand, normal, and emergency data traffic. Delivering the required QoS for different data traffic is quite challenging due to the data traffic variabilities. The selection of an optimized route to cope with traffic variability and energy constraint while satisfying the QoS requirement is necessary. In addition, the wireless networks in WBAN are used to monitor and transmit health-related data from wearable devices to healthcare providers. In addition, data and devices in WBAN and IoT are prime targets for various attacks, such as spoofing attacks, intrusions, Denial of Service (DoS) attacks, distributed DoS (DDoS) attacks, eavesdropping, and jamming [55]. Therefore, the diverse number of devices in WBAN and IoT generate a massive amount of data which requires efficient management for better performance. However, the current WBAN and IoT architecture is critical, and it may not be efficient in managing the network without violating the QoS due to the inability to dynamic reconfiguration [56].

SDN allows network administrators to centralize the management and control of the network infrastructure, providing more flexibility and programmability to the network. IoT and WBAN devices generate sensitive data that needs to be transmitted securely over the network. Similarly, they often required battery-powered, making energy efficiency a crucial consideration. However, several challenges are associated with managing IoT and WBAN using SDN, including security, routing, energy efficiency, and managing devices. Therefore, SDN-based solutions need to optimize traffic routing and ensure that energy consumption is minimized and robust while guaranteeing security measures to protect this data. This section discusses various challenges affecting IoT, WBAN, and SDN, as shown in Fig. 4. The study focuses on managing WBAN and IoT devices, traffic flows management, routing with resource awareness, and SDN security challenges. The following subsections detail each of the challenges.

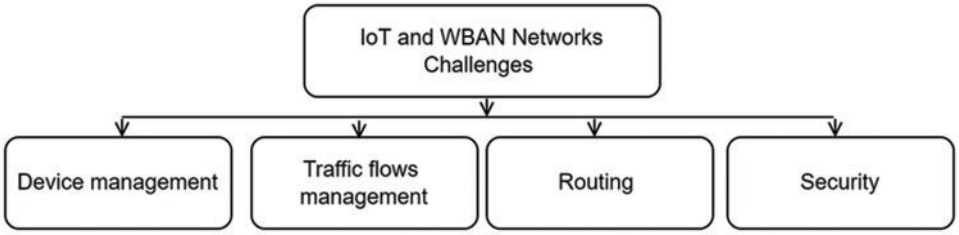

Figure 4: IoT and WBAN challenges

3.1 WBAN and IoT Management Challenges

WBANs and IoT are two emerging technologies that potentially transform the healthcare industry. Traditionally, network management in these technologies involves protocols that facilitate data sharing among users and networks. Routing decisions (control logic) and forwarding decisions are carried out at the switches. The wide variety of networked systems available on the Internet today controlled network modules with a wide range of storage, processing capacity, and energy usage. However, managing different devices from various vendors is difficult due to a lack of support for customization and adaptability. Consequently, this leads to under-utilization and, equivalently, over-provisioning network bandwidth. IoT network management must provide functionalities including frequent network monitoring status, configuring operating parameters, fault detection and recovery, collecting network performance data, and managing operations [28]. As a result of widespread Internet connectivity, traditional Wireless Sensor Networks (WSN)'s management challenges have now been passed on to the IoT domain [28]. The authors in [57] categorize these management challenges into security management, energy-aware routing, load balancing, interoperability, data management, and scalability. Addressing these management challenges will be crucial to the success of WBANs and IoT in healthcare. This way, healthcare providers can harness the power of these technologies to improve patient outcomes, reduce costs, and enhance the overall quality of care. Therefore, IoT network management solutions are required to incorporate the challenges mentioned above to provide diverse management functions to address these concerns. However, as uninterrupted service and security are essential in every network, we focused on routing with resource aware and security challenges.

3.2 Traffic Flows Management

Traffic management is a crucial aspect of modern cities; with the emergence of the IoT) and WBANs, the challenges faced by traffic management have become even more complex [58]. IoT and WBANs enable the integration of various sensors and devices to collect and transmit data. In traffic management, these technologies can monitor traffic conditions, collect data on traffic flow, and provide real-time information to drivers and traffic management authorities. One of the main challenges of traffic management in IoT and WBANs is the sheer volume of data generated by these technologies. The sensors and devices in these networks generate massive amounts of data, which can overwhelm traditional traffic management systems. The ability to process, analyze, and interpret this data in real time is critical to making informed decisions about traffic management. Another challenge is the need for standardization of data formats and protocols. Different devices and sensors may use different data formats and protocols, making it difficult to analyze the data from various sources. Privacy and security are also significant challenges in traffic management in IoT [59] and WBANs. The data collected by these networks may include sensitive information such as location and personal health information. Ensuring the privacy and security of this data is critical to protecting the rights of individuals and maintaining public trust in the technology.

Additionally, the reliability and availability of these networks are also important factors to consider in traffic management. Downtime or system failures can lead to significant disruptions in traffic flow and compromise public safety. Therefore, traffic management in IoT and WBANs presents several challenges that must be addressed. Standardization of data formats and protocols, privacy and security, and reliability and availability of the networks are key areas that need attention. Overcoming these challenges will require an adaptable emerging network to create a more effective solution. Therefore, integration of SDN with WBAN and IoT required efficient traffic management to optimize the network performance.

3.3 Routing with Resource Awareness

WBANs and IoT are the most promising wireless communication and networking technologies. WBANs are designed to provide real-time and continuous monitoring of various physiological parameters of the human body, while IoT connects multiple devices and sensors to the internet for efficient data sharing and analysis. However, these technologies also face several routing challenges that must be addressed to ensure their effective and reliable operation.

The battery life of the sensors and devices is a major challenge in WBANs, making energy-efficient routing critical [60]. Routing protocols that minimize the energy consumption of the devices and maximize their lifetime are needed to ensure the long-term operation of the WBAN. Another challenge is the sensors' limited communication range, making it difficult to establish a stable and efficient communication link with the gateway. To overcome this challenge, multi-hop routing protocols [61] often use intermediate nodes to relay data between the sensors and the gateway. This way, it can extend the communication range of the nodes beyond their direct transmission range. Besides, it helps to mitigate the impact of obstacles and signal attenuation, as the data packets can be routed through nodes with better connectivity. However, transmission latency is one of the major challenges of multi-hop routing. As the data packets have to be forwarded through multiple nodes, the time taken for the data to reach the destination node increases, leading to higher latency. This can be problematic in real-time applications such as healthcare monitoring, where delays in data transmission can have serious consequences. In addition, multi-hop networks are often more complex than those single-hop networks, as they have to consider the network's topology and the availability of the intermediate nodes. This can make the design and implementation of the routing protocol more challenging and require more computational resources.

On the other hand, In IoT, heterogeneity of the devices and networks is one of the routing challenges. The devices and networks in IoT can have different capabilities, communication protocols, and data formats, which makes it challenging to design routing protocols that can handle the diverse requirements of IoT applications [62]. Another challenge is the scalability of the network, as the number of connected devices and sensors can grow rapidly, leading to increased network congestion and potential packet losses. To address this challenge, routing protocols that can dynamically adapt to the changing network conditions and balance the network load are needed.

Therefore, the routing challenges in WBANs and IoT require the development of a specialized routing scheme that can address the unique requirements and constraints of these technologies. Energy-aware routing and multi-hop routing protocols are essential in WBANs, while scalable and adaptable routing protocols are critical in IoT. Addressing these challenges will ensure these technologies' reliable and effective operation and enable innovative applications in healthcare, smart cities, and other domains [63]. As such, it is essential to consider these challenges with traffic flow quality of service demand while integrating SDN with WBAN and IoT.

3.4 SDN-Based Solution Security Threat

SDN is an innovative approach to network management that allows for centralized control and automation of network configurations. However, the benefit comes at the cost of new security threats that must be considered. SDN controller is always a prime target for the attack [64]. Unauthorized access to the controller is a significant security threat in SDN-based solutions. SDN-based solutions are susceptible to various attacks, including DoS, attacks software, Man in the Middle, and spoofing attacks, where attackers flood the network with traffic, causing it to crash or become unusable [65]. Man-in-the-middle attacks can intercept network traffic and can modify or steal data. Attackers attack

early access to the control plane and redirect traffic to a malicious node, allowing them to intercept and manipulate network traffic [9]. Similarly, insider threats, such as employees or contractors with access to the controller, can intentionally or unintentionally cause harm to the network. In addition, the switch Flowtable memory is constrained with limited storage space, making it another soft target for attack. Intuitive, SDN controller, and switch Flowtable storage are vulnerable to attacks. This can be particularly devastating in critical smart technologies applications. Therefore, network administrators must know these threats and take appropriate measures to secure their SDN-based solutions. Consequently, it is important for any SDN-based solutions to take proper steps to ensure their design considering these threats.

4 Integration of SDN with Emerging Technologies for Routing and Security

WBAN and IoT pose various challenges due to limited network resources, traffic variabilities, and static architectural design, as discussed in Sections 3.1–3.5. Emerging technologies can utilize several specific features of SDN. The most notable ones include centralized control logic, programmability, Open interface, traffic engineering, and security. These features are useful in dynamic and rapidly changing WBAN and IoT environments. For example, a centralized control plane can be beneficial for managing large-scale WBAN and IoT networks. Programmability provides a programmable infrastructure that allows network administrators to create and modify network policies and configurations in real-time. Open interfaces such as OpenFlow, NETCONF, and REST APIs can simplify the integration of WBAN and IoT networks with the SDN controller. While traffic engineering allows network administrators to control, traffic flows granularly, which can be useful in managing traffic in WBAN and IoT networks, particularly for applications that require low latency or high reliability. SDN provides several security features, such as access control, network segmentation, and network virtualization, that can be used to secure WBAN and IoT networks. Therefore, several researchers proposed integrating SDN with WBAN and IoT frameworks to benefit from the SDN features. This study categorized the literature into two parts: routing and security. We categorized the former into SDWBAN routing with resource awareness and SDIoT routing with flows management. Similarly, in the latter, we analyzed SDWBAN and SDIoT security-related solutions.

Some research questions were derived to systematically conduct the review, including what are the current routing solutions in SDWBAN and SDIoT frameworks? What are the existing security solutions in SDWBAN and SDIoT frameworks? How do these solutions account for the challenges in IoT, WBAN, and SDN, and their respective strengths and weaknesses are also key areas of interest? What can potential future research works be done to improve the routing and security in SDWBAN and SDIoT frameworks? A literature search was conducted using various key search terms to answer these questions. These terms included SDN, IoT, WBAN, routing, and security threats. Relevant academic research repositories were selected, including Science Direct, IEEE, Springer, Tech Science, and ACM Digital Library. A search strategy was developed using the identified search terms to retrieve relevant papers. Inclusion and exclusion criteria were set to ensure that only relevant articles were selected. Papers were included if they addressed the research questions and objectives and were published in peer-reviewed academic journals or conference proceedings. Non-English and documents outside the scope of the study were excluded. Relevant information from the selected articles was extracted and synthesized to address the research questions. Fig. 5 illustrates the taxonomy of the literature.

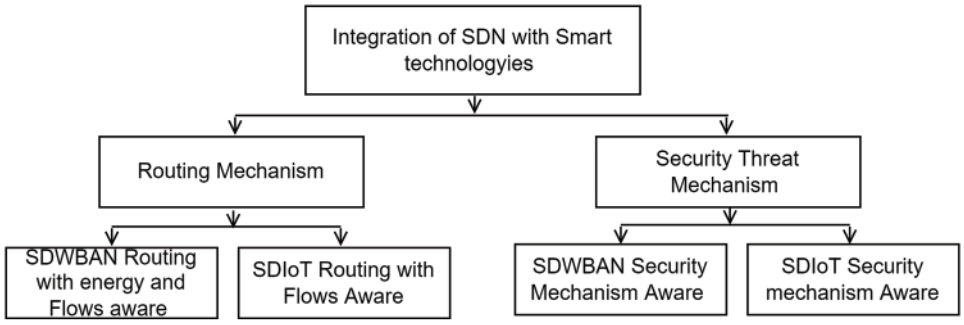

Figure 5: Integration of SDN with smart technology

4.1 Routing Mechanism

Routing protocols are crucial in discovering and maintaining network routes, dictating how messages are transmitted and received within a network. However, selecting an appropriate routing protocol depends on the nodes' specific requirements and capabilities for a given application. Several routing protocols have been proposed for WBAN and IoT. However, developing an efficient routing protocol for WBAN or IoT can be time-consuming and challenging due to these networks' specific characteristics and requirements. These challenges include topology, energy efficiency, limited resources, overheating and radiation absorption, data rate, usability, heterogeneous environments, Quality of Service (QoS), reliability and delay, path loss, mobility, network size, security, and privacy. Recently, researchers have leveraged SDN to introduce SDWBAN and SDIoT for better routing and security. This study categorized the routing into two parts: SDWBAN and SDIoT. The following section discusses various proposals from the literature to address these categories. Fig. 6. Present the taxonomy of the routing mechanisms.

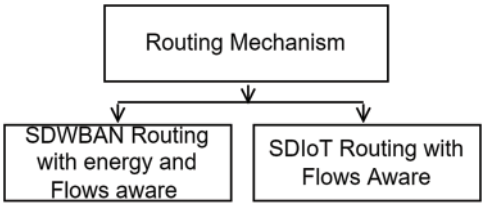

Figure 6: Routing mechanisms

4.1.1 SDWBAN Routing with Energy and Traffic-Aware Related Solutions

WBAN sensors usually monitor and collect health-related information for critical and non-critical patients. To meet the Quality of Service (QoS) demand for different patient data, traffic management and efficient Routing is vital in WBAN. However, the conventional WBAN communication framework can not guarantee the successful delivery of critical patient data due to administrative control and management to support and prioritize emergency data. To overcome these challenges, the work in [18] presents a novel framework incorporating the SDN with WBAN. A model was introduced to handle normal and emergency data packets to improve the QoS. Their Work achieved better network management; however, finding an optimal number of controllers and switches for WBAN to maintain the required QoS is challenging. WBAN is a network with different data flows; physiological data require different QoS to transmit without much loss and packet processing delay. Although, traffic

priority with QoS is proposed in WBAN [11] with multi-QoS metrics [10]. However, these works lack proper administrative control and centralized network management. An effort was made in [66] to incorporate SDN into healthcare using centralized controllers for health surveillance applications. However, the architecture lacks a detailed description of SDN functionalities and priority-based data traffic management, especially for emergency data flow. An SDN-based control system was proposed for managing emergency alerts in a smart city environment [58]. When an emergency occurs, this control system activates and dynamically modifies the routes of normal and emergency traffic to reduce the time required for emergency resources to arrive at the emergency location. The architecture is built on IoT devices such as traffic lights, cameras, and algorithms. The algorithm manages resource requests and route changes to facilitate the movement of emergency service units. The emergency traffic delay has been reduced. However, these works lack proper flow management to achieve better QoS. A smart healthcare systems traffic classification was presented in [67]. The authors leverage SDWBAN efficiently to manage the generated traffic from WBAN and divide WBAN traffic into three categories: emergency/periodic data, sensor health traffic, and environmental data. The proposed architecture used Personal Digital Assistant (PDA) to receive data from sensor nodes and categorize traffic types. The classified data is then sent to the appropriate server for further analysis. An SDN controller remotely configures (modifies Flowtables) using communication services such as WiFi or 3G/4G networks in accordance with the operator/network policies. Another solution in [15] proposed the SDWBAN framework that allows administrators to prioritize sensitive data over normal data flow. This way, an application classification algorithm and a modified version of the sector-based distance protocol were used to implement a data prioritization policy. The framework increased while decreasing delay. However, due to its architectural design, the work may not scale up with the desired performance on heterogeneous applications in large-scale networks. Although, their fellow up work [68] introduced a mathematical model to obtain the optimal number of controllers to achieve satisfactory performance. A higher packet delivery ratio with lower latency was achieved. Unfortunately, the optimization model may require a large solver to converge in a dynamic large-scale network. A Criticality-Aware Flow Control for SDN-Based Healthcare IoT was presented in [69]. The authors formulate a mathematical resource reallocation problem to optimize the network overhead while considering packet flows' criticality requirements. A controller application was developed to identify and predict critical packets from non-critical ones and locate the index using a machine learning approach. Although the scheme can reduce latency and overhead, it does not provide localized (i.e., edge node) multiple disease identification with healthcare-related decision-making, which is required for critical applications. To overcome this challenge, the approach in [70] proposed SD-Health, an Edge-based Decision-making and Task allocation (EDT) scheme. It uses machine learning techniques to the criticality of flows and location of mobile devices. Each packet is associated with sensed value at a particular time. The controller assigns the appropriate EDT module based on the predicted values to the edge node. The controller predicts an edge node's future healthcare-related decisions and prepares the module accordingly. The ML-based trajectory prediction allows for the prediction of mobile device locations in the network in the future. Once the mobile device's location is predicted, the edge node is dynamically assigned a set of computation tasks. However, it is quite challenging to feed the machine learning training module due to edge device resource constrained. The authors in [71] present traffic management for monitoring health application to handle a huge volume of dynamic data collected for the body area network and the surrounding are processed and routed intelligently by the SDN controller. The SDN controller monitors traffic flows and communicates traffic flow rules to sensors, wearables, and other devices for mobility and routing management. This way, the approach improved network performance with better reliability.

Maintaining network QoS is one of the critical challenges emerging in heterogeneous WBANs. The previous works are concerned with managing heterogeneous data flows on WBAN. However, higher network throughput, minimum delay, and maximum sensor battery lifetime are critical performance metrics required to achieve network QoS. Energy resources are limited in the compact architecture; efficiency and network lifetime are important factors in WBAN-based applications. It can be achieved by developing an effective routing mechanism that ensures QoS while reducing energy constraints on forwarding nodes and minimizing delay and path loss. The work in [72] proposed Energy Efficient and Thermal Aware Routing Protocol for SDWBAN (EE-TAR) to compute the least cost path from source to sink that provides timely data available for medical practitioners. Although, data flows could reach their destination through the shortest path. However, the solution may not cope with the behavior of frequent dynamic network changes. The approach performs better than the traditional Dijkstra algorithm regarding energy consumption ratio. It is important to provide effective communication between the sensors while prolonging the overall lifetime of the network with minimum energy consumption, especially for medical-related data. A routing algorithm that operates like a conventional one may not be suitable for providing the required service due to resource limitations. Table 3 summarized SDWBAN routing with energy and traffic flows aware.

Table 3: SDWBAN routing with energy and traffic flows aware

References	Method	Link/ switch resource	SDWBAN energy resource		Energy-aware Routing	Traffic management awareness	Weaknesses
			SDN resource	WBAN resource			
Hasan et al. [18]	A framework for incorporating SDN with WBAN	X	X	√	X	√	The optimal number of controllers and switches for WBAN to achieve Quality of Service was overlooked
Iqbal et al. [73]	Hyperelliptic Curve Cryptosystem (HECC) to protect patient data	X	X	√	X	X	It lacks proper classification to ensure the QoS of different WBAN data flows
Hasan et al. [15]	SDWBAN framework with sector-based distance	X	X	√	X	√	The number of controllers to achieve optimal performance is unknown.
Hasan et al. [68]	Optimization model	Link latency	X	√	X	X	Required large solver to converge in dynamic large-scale networks

(Continued)

Table 3 (continued)

References	Method	Link/ switch resource	SDWBAN energy resource		Energy-aware Routing	Traffic management awareness	Weaknesses
			SDN resource	WBAN resource			
Mehiar et al. [66]	Framework	X	X	X	X	√	It lacks a detailed description of SDN functionalities and priority-based data traffic management, especially for emergency data flow.
Rego et al. [58]	Flow management architecture	X	X	√	√	√	An ineffective Emergency detection system
Ahmed et al. [72]	Energy and thermal aware routing SWBAN	Distance	√	√	√	X	May not adapt to the dynamic network changes
Sallabi et al. [67]	System architecture	X	√	X	X	√	Periodic monitoring imposed extra processing load on the SDN controller.
Misra et al. [69]	Criticality-aware flow control	√	√	X	√	√	No localized (i.e., edge node) multiple disease identification
Saha et al. [70]	SD-health machine learning	X	√	X	X	√	It is quite challenging to feed the machine learning training module due to edge device resource-constrained
Ahmed et al. [74,75]	EOCC-TARA based on spider monkey optimization	Sensor	√	X	√	X	Required large solver to converge in dynamic large-scale network
Cicioğlu et al. [7,76]	SDWBAN inter WBAN routing	Sensor	X	√	√	X	It only supports inter WBAN
Al-Hubaishi et al. [77]	Energy routing fuzzy logic	Sensor	X	√	√	X	Can not support WBAN architecture ISO/IEEE 11073 service quality requirements

(Continued)

Table 3 (continued)

References	Method	Link/ switch resource	SDWBAN energy resource		Energy-aware Routing	Traffic management awareness	Weaknesses
			SDN resource	WBAN resource			
Cicioğlu et al. [56]	HUBsFlow interface protocol	Controller	√	√	X	X	Extending the SBI into the perception plane beyond OpenFlow switches is challenging.
Oliveiraet al. [78]	Controller energy efficiency	Controller	√	X	√	X	Overlooked switch TCAM power consumption
Isravel et al. [71]	SDWBAN	Switch	√	X	X	√	Frequent network monitoring introduced overhead

SDWBAN routing algorithm for healthcare applications was presented in [7,76]. This method leverages SDN centralized control panel to manage the structure for inter-WBAN communications for efficient routing. This way, an energy-efficient routing algorithm is proposed to improve the lifetime and residual energy of the network infrastructure. This method has shown performance gain by improving system throughput, decreasing delay, rate of successful transmission, and energy compared to the traditional models, which have lower consumption rates. However, it only supports Inter-WBAN communication, leaving the problem of forwarding nodes selection, and thermal dissipation is also avoided [74]. In addition, managing the communication between the controller and enable switches is challenging. Although, WSANFlow [12] was proposed to manage all communications between the SDN controller (SDNC) and the SDN-oriented end devices to optimize the network performance. The proposed SDNC can handle all network control and management tasks. As a result, by utilizing the WSANFlow interface protocol, the SDN controller can optimize the instructions to be delivered, manageable, and efficient to the end devices. However, WSANFlow is not standardized as the acceptable interface to manage SDN infrastructure. An SDN-enabled wireless sensor fuzzy-based routing algorithm was proposed in [77]. The algorithm has a new routing discovery mechanism that uses fuzzy logic to change the existing path during data transmission. However, the solution can not support WBAN architecture ISO/IEEE 11073 service quality requirements. A solution was proposed in [56] to integrate this requirement with the SDN approach. HUBsFlow interface protocol was implemented on the controller to provide the communications between the controller and HUBs in inter-WBAN communications. However, extending the SBI into the perception plane beyond OpenFlow switches is challenging. Table 4 summaries various SDWBAN solutions.

While congestion is one of the most common issues, it arises when the incoming traffic exceeds the node capacity or transmission capacity; unfortunately, references [7,74] have limitations in handling data transmission without congestion and controlling thermal dissipation in networks. To counter these challenges, the reference in [74] proposed a novel Energy Optimized Congestion Control based on Temperature Aware Routing Algorithm (EOCC-TARA) for SDN-based WBAN using Enhanced Multi-objective Spider Monkey Optimization (EMSMO). The algorithm aimed to improve energy efficiency, congestion-free communication, and reduce adverse thermal effects. EOCC-TARA routing algorithm considers temperature due to sensor node thermal dissipation and develops a strategy

to select forwarding nodes adaptively based on temperature and energy. The congestion avoidance concept is then combined with the energy efficiency, link reliability, and path loss concepts to model the cost function on which the EMSMO provides optimal Routing. This way, energy consumption is reduced with network lifetime and system throughput. However, it required a large solver to converge in a dynamic large-scale network.

Most of the existing literature focused on energy-aware routing, considering either sensor energy consumption or transmission link capacity at the expense of the processing power of the SDN controllers. In contrast to other literature, reference [78] focused on improving the energy efficiency of the network's control plane processing power. The authors used the parallel processing capabilities of modern off-the-shelf multicore processors to distribute the controller's many tasks across the cores. They show how a multicore controller can use an off-the-shelf multicore processor to save energy while maintaining service levels. By dividing tasks among homogeneous cores, one can reduce the frequency of operations, lowering overall energy consumption while maintaining the same level of service quality. Experimentally, their work achieved energy efficiency while lowering the core's frequency of operation.

4.1.2 SDIoT Routing with Flow Management-Related Solution

The proliferation of IoT devices with the rising development of smart cities generates many traffic flows with various Quality of Service demands. In this regard, the need for SDN resource distribution mechanisms is growing rapidly. Furthermore, network traffic management is important for optimizing IoT performance in smart cities. Due to poor traffic management, congestion is one of the most serious problems in many developing cities. It has a greater impact on commuters' daily lives. Although many researchers have addressed accident response, [79] large-scale incidents and emergencies remain relatively underdeveloped. The current traffic load on electric vehicles required an optimization model to travel paths based on recharging availability. The work in [80] introduced the multi-network controller architecture for heterogeneous IoT. MINA is a middleware with self-observing and adaptive capabilities that manages the pervasive heterogeneous network. It uses a layered architecture similar to SDN and flows matching principle to bridge the semantic gap between IoT and task definitions in a multi-network environment. This architecture optimizes the flow scheduling and management of Wi-Fi and WiMAX environments by utilizing resource sharing. However, the work focused on technological-based flow scheduling and overlooked application-based flows. SDN-based efficient flow control and mobility management in urban multi-networks were presented in [81]. The authors proposed the UbiFlow framework, which allows for integrating SDN and IoT using SDN distributed controllers. The IoT network is partitioned into small network chunks/clusters in the UbiFlow architecture. A physically distributed SDN controller manages each partition. For different data requests, the IoT devices in each partition may be connected to a different access point. MINA handles per-device flow management and access optimization. However, the works had to satisfy IoT flow requests to some extent while guaranteeing network performance in each partition. However, neither [80] nor the work in [81] addressed emergency road traffic effectively. In contrast, the work in [58,82] introduced an SDIoT-based platform that modifies normal and emergency road traffic routes to reduce the time it takes for resources to arrive at an emergency. This way, the delay of emergency traffic was improved.

Similarly, reference [83] designed a game-theoretic traffic-handling scheme to minimize delay and maximize throughput in software-defined IoT networks. However, IoT devices sensor generate different traffics flows with various QoS requirement, and delay only account for single QoS parameters. Other flows have different requirements; as sensors' use increases in various IoT applications, there is a need to address the resource allocation for handling these sensors generating critical data

while satisfying application QoS demand. To overcome these challenges, a value-based utility SDIoT traffic management was presented [84] to cope with QoS requirements in constrained sensor devices. The proposed algorithm ensures that the demand for sensor packets is satisfied by managing the traffic while allocating queue resources among flows through a centralized SDN controller, which utilizes network packet statistics. The effectiveness of the proposed algorithm is verified using the OpenFlow testbed. Various sensor devices were considered with different QoS requirements. The system's performance indicates that each sensor device achieved the required resource network utility level. However, periodic traffic monitoring introduced extra processing load on the SDN controller.

Most of the previously mentioned solutions lacked the intelligence to effectively managed traffic flows or IoT devices. Artificial intelligence (AI) aids in the dynamic management of resources and network traffic effectively. Different types of traffic flows can be discovered, and their patterns can also be obtained, which can then be applied to SDN control logic for proper decision-making. For example, multimedia traffic has drastically grown in the last few years, and smart city cameras add new traffic flows and applications. This has been overlooked in [58,82]. In [85], the authors presented an intelligent video surveillance system that utilizes SDN and AI. The design incorporates two primary AI modules for flow classification and resource estimation to ensure QoS and QoE based on delay and loss rate; these modules were built on top of the SDN application. The Controller periodically received flows from IoT devices. Afterwards, it requests the AI module to classify the flows. This way, multimedia flow is classified as critical traffic. The article also highlights the pre-processing standards for prioritizing the data set by categorizing it as essential and labelling it in increasing order, with 1 being non-critical traffic and 5 being essential traffic.

Similarly, the work in [86] devised an Intelligent traffic classification in SDN-IoT. This way traffics are classified based on bandwidth and latency requirement. The authors compared different classification algorithms while the impact of two feature selection methods is considered to reduce the number of features needed for classification. Periodic flow statistics collection imposed an extra processing load on the controller. Table 4 compares various SDIoT routing and flow management solutions.

Table 4: SDIoT routing and flow management solutions

Literature	Method	SDN controller mode	SDIoT energy resource		Energy-aware routing	Traffic management awareness	Weaknesses
			SDN resource	IoT resource			
Qin et al. [80]	Flows scheduling algorithm	X	X	√	X	√	The work focused on technologically based flows scheduling and overlooked an application based
Wu et al. [81]	UbiFlow system architecture	X	√	√	X	√	Overlooked flows management based on their emergency demand
Rego et al. [58,82]	Priority route for emergency service	X	X	√	√	√	The work does not indicate their SDN controller operational mode.

(Continued)

Table 4 (continued)

Literature	Method	SDN controller mode	SDIoT energy resource		Energy-aware routing	Traffic management awareness	Weaknesses
			SDN resource	IoT resource			
Alipio et al. [84]	VUTM algorithm	X	X	√	X	√	Periodic traffic monitoring introduced extra processing load on the SDN controller.
Rego et al. [85]	Flow classification and management	-	X	√	X	√	
Mondal et al. [83]	Game theory-based scheme	X	X	√	X	√	The optimization model takes time to converge in large-scale networks
Owusu et al. [86]	Machine learning model	X	√	√	X	√	Traffic statistics collection imposed overhead on Controller
Saha et al. [87]	Routing Optimization model	X	√	X	X	√	Computing K paths may increase the overhead on the controller
Tang et al. [88]	Deep learning model	X	X	√	X	√	The work did not clearly explain the adopted controller mode
Nguyen et al. [89]	Deep learning	Proactive	√	X	X	√	It focuses on managing SDN switch memory without considering IoT energy consumption
Kamboj et al. [90]	Multipath routing path	X	√	√	X	√	Frequent network monitoring affects the controller's performance
Ouhab et al. [61]	Q-learning routing model	X	X	√	√	X	Overlooked incorporating SDN resource power consumption
Naeem et al. [91]	QoS-enabled routing optimization max-flow min-cost problem,	X	X	√	√	X	Computing the K path more often introduced additional overhead on a controller,

A ubiquitous network of smart objects generates various types of traffic that necessitate a variety of QoS guarantees from the network. For instance, factory automation latency requirements can range from 0.25 to 10 ms, whereas process automation can tolerate delays of up to 100 ms [92]. As a result

of the diverse requirements, there is a need to maintain application-dependent QoS guarantees in the network. An SDIoT traffic-aware routing was presented in [87]. Traffic flows are classified into delay and loss-sensitive flows. A greedy approach based on Yen's K-shortest paths algorithm was devised to compute the optimal forwarding path while considering the QoS requirements of each flow to maximize the overall network performance.

Similarly, the work in [91] proposed an IoT-based SDN-based energy-efficient and QoS-aware parallel routing scheme. While characterizing medical services as jitter-sensitive, loss-sensitive, and delay-sensitive flows, the authors considered a max-flow-min-cost optimization problem with multi-constrained QoS parameters. The goal was to maximize flow gathering over active resources while minimizing bandwidth costs and meeting QoS requirements. However, Computing K paths may increase the overhead on the controller. In contrast, an SDIoT adaptive channel assignment scheme for periodic and busty IoT traffic was presented [88]. The proposed method employed a centralized SDN controller to calculate dynamic load via a deep Convolutional Neural Network (CNN). Afterwards, an adaptive channel assignment algorithm based on the load was used to reduce interference and improve transmission quality.

In contrast, online gaming and virtual reality necessitate the underlying network capable of fulfilling high bandwidth and low latency requirements. The works in [90,93] proposed a dynamic multipath routing scheme with QoS awareness for improving the QoS of high-bandwidth applications in an SDIoT. The proposed solutions consist of three phases flow splitting, multipath routing, and flow reordering. Flow splitting scheme to determine how to split incoming flows to enable multipath routing in the network. The cost function for routing the splittable sub-flows and formulating a min-cost routing problem as an integer linear program. Finally, flow reordering is used for sub-flows via multiple paths to maintain the desired flow sequence at the destination. This way, higher network throughput was achieved while reducing the QoS violation. However, frequent network monitoring affects the controller's performance. Although the works in [90,93] work well in a small network setting, they may not significantly increase network performance when the number of nodes becomes too large, especially in dynamic large-scale networks that generate huge amounts of data. Ouhab et al. [61] proposed a two-level control model routing protocol for low-power and lossy networks based on multi-hop clustering techniques to reduce energy consumption in the IoT. The authors devised intelligent Q routing for efficient QoS provisioning as a major concern for IoT devices. The use of this combined solution allows the network to save energy. End-to-end delay, packet delivery ratio, and energy consumption were improved. However, the solution overlooked the limited resource in SDN. SDN switches Flowtable have constrained resources that can easily overflow, resulting in QoS violations, such as high delay and low throughput. As a result, designing a dynamic flow rule placement mechanism capable of providing fine-grained traffic analysis while meeting QoS requirements of traffic flows and preventing Flowtable overflow at SDN switches is difficult. Unlike the previous work, Nguyen et al. [89] proposed adaptive flow rule placement at SDN switches to maximize the number of match fields in a flow rule to deal with the dynamics of IoT traffic flows. The authors use the Markov Decision Process (MDP) with a continuous action space to model system operation and formulate its optimization problem. A deep deterministic policy gradient-based algorithm to assist the system in determining the best policy. This way, the scheme minimizes the QoS violation ratio of traffic flows.

4.2 Security Threat Mechanism

The embedded wearable devices in WBAN, in other words, IoT devices, collect data from the sensors or other devices and transmit it for analysis and processing to a central server. In WBAN, the data varies from critical to emergency data. These devices carrying these data are resource constraints.

As such, An attacker can easily target them by sending forged requests. This way, they intercept data and manipulate valuable sensor data in transit or capture and transform a physical device into a zombie to launch attacks on other systems. The most common IoT attacks are Denial of Service (DoS) and energy depletion [94,2]. Implementing security defence mechanisms on these devices using a traditional approach in an open environment is challenging, as they add computation overhead on small IoT devices. In addition, security issues, such as network-based routing and botnet attacks, can potentially disrupt IoT services.

For this reason, IoT applications require trust management for reliable data fusion and enhanced information security [95]. Although Integrating SDN with IoT provides better network management, it is critical for network security and data transmission efficiency. The heterogeneous nature of IoT coupled with resource constraints has made the security functionality even more challenging. Traditional IoT security systems are ineffective and necessitate extensive adaptation. Therefore, it's required to have a more robust solution to deal with these unique security challenges. These solutions should also adapt to the nature of current traffic flows behaviour in WBAN. Table 5 presents various attack and security challenges on IoT-based networks. This study categorized security threats in smart technology into two parts, as shown in Fig. 7. SDWBAN and SDIoT security-related solutions. This way, the study surveyed each solution and discussed its strengths and weaknesses. Tables were presented to summarize each solution.

Table 5: Security threats and vulnerabilities

IoT layer	Components	Security issues and attacks	Effect
Perception layer	Sensor, Cameras, Smart Devices, RFID,	Denial and distributed denial of services attacks, Fake node, and radio interference, RFID spoofing	Data leakage, message destruction, unfair resource allocation, network congestion and data privacy violation
Network Layer	Sensor, wired, and wireless technologies	Network attack: Denial and distributed denial of services attack Data attacks: Data Inconsistency and Data Breach	Network crashes and network Flooding. Data leakage and data privacy violation
Application Layer	Web services, Directorate Services	Software attack: Worm, spyware, virus, trojan horses, and adware Physical attack: Tampering, malicious code injection, fake node injection, sleep denial attack, permanent denial of service, and RF interference/jamming	Infect data and resource destruction

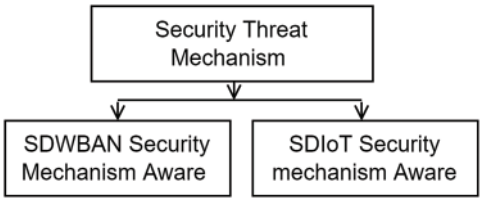

Figure 7: Taxonomy of security threat mechanisms

4.2.1 SDWBAN Security Threat and Vulnerabilities-Related Solutions

Several efforts were made over the years to provide QoS to satisfy WBAN application constraints and ensure security within WBAN. Various security mechanisms have considered the WBAN nodes' characteristics. Security mechanisms like trust management should be lightweight to avoid affecting the WBAN application's QoS. Integrating SDN with WBAN helps in the real-time monitoring of patient data as well as the agility required to move the data from different endpoints. Varadharajan et al. [96] proposed an SDN-based framework for secure patient monitoring in hospital settings. The proposed method can provide fine-grained security policies for communications while also tracking the locations of patients who exhibit critical health behavior. The scheme periodically monitors the patient's location and deals with attacks on the hospital network. Policy-based security was enforced to differentiate healthcare-related traffic and others to prioritize healthcare traffic. A trust-based method was used to resist insider attacks [97]. Although the proposed approach can detect malicious healthcare devices, it is not intended for WBANs-based systems and is only effective against network insider attacks, not outsider attacks. A security and privacy healthcare monitoring framework is proposed in [98] for both inside and outside attacks. The authors investigated the challenges and concerns regarding the traditional Healthcare Monitoring System's security and privacy (HMS).

Afterward, a model was proposed to monitor the elderly and patients. This guarantees the data protection and privacy of various delivered services. Interestingly, the authors consider local and remote patients on hospital grounds, benefiting patients without wireless coverage. However, the paper lacks detailed implementation or build evaluations. Medical data must be transmitted securely for a reliable system, as each information is personal to the patient. An efficient data delivery system was presented in [99]. The authors use 'Kerberos,' a secure networking protocol for authentication and a fast data delivery system for secure virtual hospitals. SDN controllers are used to classifying traffic, which is authenticated using the Kerberos protocol, and enough bandwidth is allocated to meet QoS requirements by delivering data on time. Sensitive data is encrypted and stored in a private cloud with Kerberos, whereas periodic health data is stored in a public cloud with a firewall and an access list. Encapsulated packets authenticate and establish a secure connection for downlink transmission of medical data from the hospital or examiner. Biometric authentication, path selection, and bandwidth allocation optimization techniques can improve the proposed system's performance even further.

On top of the optimized path selection, additional security, privacy, monitoring mechanisms, and efficient management of IoT devices are required for the new vision of smart infrastructure. This problem becomes more complicated and challenging when dealing with several smart infrastructure objects distributed across different network locations, known as Smart Spaces (SS), and evolving management rules that may be unique to each SS. To overcome these challenges. Jaouhari et al. [100] deployed different centralized security controls for various SS locations on other networks. This way, users were given access to the resources anytime and anywhere. Security mechanisms were employed,

starting from low-level checks through filtering and controlling all flows going in and out firewall by dynamically modifying the rules based on the need. This way, efficient data protection is ensured.

Although, the references [97–100] tried their best to improve the security in SDWBAN. However, it is quite challenging to devise an effective security strategy for patients relying on the conventional WBAN to monitor their health are related information due to the confined nature of the WBAN environment. As such, they lacked the effectiveness to mitigate these attacks adequately. Artificial intelligence seems to be the promising solution to control scalable and secure WBAN devices. AI-enabled Software-Defined IioT Network (AI-SDIN) is embedded in [101] to improve applications based on AI-SDIN based on three functional layers to yield intelligent-based decision-making. The AI algorithm was used to identify and isolate malicious attacks, while the data forwarding entities focused on data transmission. Although the AI-based solution is promising, the lack of standard protocol for communication among wearable IoT devices made security measures quite challenging. The Lightweight security protocols are incapable of providing optimal protection against prevalent powerful cyberthreats affecting devices. Similarly, Mandal et al. [102] proposed provably secure certificateless protocol to enable sensitive information with confidentiality and privacy. The authors developed a certificateless authenticated key agreement protocol with low computational cost and higher security. This way, achieves anonymity, resistance to key escrow issues, and mutual authentication between sensor nodes attached to patients and the application provider.

Other researchers [103] leverage deep learning techniques to introduce an anomaly detection system. However, deep learning requires many datasets for training and has poor generalization abilities due to its inability to interact with the environment. These factors make optimizing the performance of dynamic networks difficult. The proposed solution would alleviate the burden of security configuration files on network devices.

Some existing studies impose an extra overhead on medical sensors, which could decrease the stability of the real-time transmission systems. Haseeb et al. [104] proposed a machine-learning model to predict network resource consumption and improve sensor data delivery. An unsupervised machine learning technique was used to classify medical things into various collections. Afterward, dynamic metrics were used to predict the status of link states based on updated network information. Finally, a security algorithm was developed on top of the SDN controller to efficiently manage the consumption of the IoT nodes and protect them from unidentified occurrences. This way, the model improved system throughput and data drop ratio.

Most of the current studies focus on the security of the wearable device but overlook the limited resource on SDN. It also poses various security threats because of its limited resource. In contrast, Hadem et al. [105] focus on Detecting anomalous traffic and network intrusion using the PACKET_IN event at the controller. The scheme periodically fetches the flow statistics from the OpenFlow switches. They leverage Selective logging of suspicious flows during a PACKET IN event. It allows for an IP traceback in the event of an attack, which a network administrator can initiate via a Hypertext Transfer Protocol (HTTP)-based web console. This way, high detection accuracy was achieved. However, frequent flow statistics monitoring imposed extra processing load on the controller. Table 6 summarizes various SDWBAN security solutions.

Table 6: SDWBAN security solutions

Related work	Type of attack	Method	SDWBAN Attack facility		Weakness
			WBAN based devices	SDN based devices	
Varadharajan et al. [96]	Cyber attack	Attack signature and behavior detection	√	X	A frequent network monitor can easily affect the SDN controller's performance
Meng et al. [97]	Insider attacks	Bayesian inference	√	X	It is not intended for WBANs-based systems and is only effective against network insider attacks
Shayokh et al. [99]	Hijacking attack	Kerberos Authentication model	√	X	The system is weak due to its architectural design. Further optimization is required to improve the system's performance
Khayat et al. [98]	Cyber attack	Security framework	√	X	The paper lacks detailed implementation or build evaluations.
El Jaouhari et al. [100]	External threats	Security framework architecture	√	X	It can only manage limited users while exhibiting load imbalance among SDN controller
Haseeb et al. [104]	Attack on sensors	Machine learning technique	√	X	The scheme overlooked incorporating the resource constraints of the controller, an attack on the controller can easily bring the network down.
Jiang et al. [101]	Malicious attacks	Artificial intelligence	√	X	The paper lacked implementation details for further reproducibility
Hadem et al. [105]	Anomalies traffic detection	Selective logging of suspicious packets	X	√	Frequent flow statistics monitoring imposed extra processing load on the controller.
Wani et al. [103]	Anomalies detection	Deep learning model	√	X	The model has poor multi-layered abilities due to its inability to interact with the environment
Mandal et al. [102]	Data adverse attacks	Elliptic curve cryptosystem	√	X	The system only applies to WBAN but may not be compatible with SDN architecture.

4.2.2 SDIoT Security Threat-Related Solution

IoT provides benefits in terms of time efficiency, cost savings, and improved quality of life; however, it poses security risks because IoT devices can become entry points to many critical infrastructures. This way, it provides hackers and cyber criminals with more opportunities to exploit sensitive information. The system may become more vulnerable as automation increases. In other words, more data will be transferred via IoT for automation purposes. The more sensitive data we send over the internet, the greater the risk of data and identity theft, device manipulation, data falsification, IP theft, and server/network manipulation. However, the SDN paradigm provides opportunities to solve IoT security-related issues. Although, the SDN gateway plays a significant role in monitoring the traffic originating from and directed to IoT-based devices. Unfortunately, it does not entirely eradicate the security challenges. An SDN-based IoT gateway was proposed to detect and mitigate anomalous behavior [106]. The SDN gateway monitors traffic coming from and going to IoT devices. The gateway-designed adaptive mechanism will perform dynamic analysis on these traffic patterns to determine when devices act maliciously or are being exploited externally. When it detects abnormal behavior, it takes one of three possible mitigation actions (blocking, forwarding, or applying Quality of Service) to deal with it. However, monitoring a high volume of IoT devices with high heterogeneity magnifies the processing load on the SDN controllers.

Besides, the lack of standard protocols for continuous monitoring and adaptive decision-making poses another challenge. SoftThings [95] was introduced to address these challenges by detecting abnormal behaviors and attacks as early as possible and mitigate as appropriate. SoftThings consists of three functional modules Learning Classification and Flow management modules. The first two modules focus on detecting IoT traffic anomalies, and the last one is responsible for implementing flow rule replacement at the SDN devices. A Machine Learning (ML) algorithm was developed on top of the SDN controller to learn the behavior of IoT devices over time to detect and mitigate an attack. This way, SoftThings can detect attacks on IoT with high precision. However, their evaluation is limited to simulated traffic in Mininet that does not represent the behavior of real IoT devices [107].

IoT-related data can be time sensitive or highly confidential, depending on the application domain. As such, early DDOS attack mitigation remains vital. Cherian et al. [108] devised a framework to collect IoT live data and send it through secure SDN into the cloud platform. Unfortunately, Their work was tested on the RYU controller only. It may not guarantee the same performance on a controller lower than RYU.

In contrast, Hamza et al. [107] leverage Manufacturer Usage Description (MUD) to devise security measures to reduce an IoT device's attack surface by formally defining its expected network behavior. It is a framework developed by the Internet Engineering Task Force (IETF) for vendors to officially specify the intended network behavior of the IoT devices they put into the market. Unfortunately, the MUD specification has not been formally adopted.

Aslam et al. [109] proposed an Adaptive Machine Learning based SDN-enabled DdoS attacks Detection and Mitigation (AMLSDM) framework. An adaptive multi-layered was used to feed-forwarding the framework with three layers. The first layer used a support vector machine, naïve Bayes, Random Forest, K-Nearest Neighbour, and Logistic Regression classifiers to build a model for detecting DDoS attacks from the training and testing environment-specific datasets. The second layer focuses on the ensemble voting algorithm, which accumulates the performance of the first layer classifiers. The final layer focuses on adaptive frameworks that measure real-time live network traffic to detect DDoS attacks in the network traffic. This way, higher detection accuracy was achieved. Deep Learning approaches are helpful for intrusion detection mechanisms in combating malicious

IoT devices. The authors [110] provided an IoT-based work that recognizes the efficacy of a DL-based algorithm (LSTM) for botnet attack detection. The study analyzed data from various IoT devices from the N IoT 2018 dataset, which had a detection rate of 99.90%.

Similarly, a hybrid DL-driven framework for intrusion detection in IoT devices was presented in [111,112]. The schemes developed various intelligent models for efficiently identifying multi-class malware families in IoT infrastructure. However, due to its high computational complexity, the model may not be promising in Dynamic large-scale networks. IoT infrastructures are affected by various security threats, especially in large-scale networks. Reference [113] proposed a secure architecture with NFV in smart buildings. It used a policy-based cyber-security framework capable of resisting active and passive attacks. This includes replay/masquerading attacks, tampering attacks, malware injection, zero-day vulnerabilities, man-in-the-middle attacks, distributed DoS attacks, sniffing/eavesdropping via Authentication Authorization Accounting (AAA) system, and log analysis. Attacks on IoT infrastructure are launched coordinated, such as brute force. The hacking end-user login credential is another way for bad guys to target a specific victim. However, most existing studies defense mechanisms against such attacks are carried out individually and independently, resulting in ineffective and weak defense. Grigoryan et al. [114] proposed an SDIoT security architecture to quickly share the attacking information with peer controllers and block the attacks cooperatively. However, it may introduce controller placement problems. SDN enables centralized logical control over the network, but its centralized architecture exposes the network to potential vulnerabilities. Reference [115] implements entropy in the central controller to improve its usage of resources.

Similarly, an entropy-based solution was proposed to detect and mitigate DoS and DDoS attacks in IoT scenarios [116]. The scheme consists of three stages Traffic flow monitoring, Anomaly Detection, and Mitigation. The former focus on monitoring the network periodically to obtain network information which will be used to feed the detection algorithm based on an entropy calculation algorithm. Anomaly detection analyses the received data to detect malicious flow, while the mitigation stage protects end-users when a malicious attack is detected. To some extent, the technique has mitigated the attack. However, a frequent network monitor can easily stress the SDN controller, consequently, can become another target. Besides, enforcing manual security configuration on SDN facilities without formal verification could also increase the number of attacks in SDIoT. To mitigate this problem, Bringhenti et al. [117] proposed Maximum Satisfiability Modulo Theories (MaxSMT) to automatically compute a formally correct and optimized allocation scheme and configuration of SDN switches by refining security policies, user-defined or derived from detected attacks. This mechanism complies with the primary characteristics of virtualized IoT-based networks, such as the presence of numerous interconnected devices simultaneously and strict latency requirements. In a realistic use case, the feasibility and performance of the framework developed to implement this methodology were validated.

Hypertext Transfer Protocol (HTTP) is more susceptible to Man-In-The-Middle (MITM) attacks. It is another type of critical attack that is hard to defend. Hayajneh et al. [118] present a model to effectively protect IoT devices that can only use HTTP against such attacks. The authors applied traffic separation techniques using deep packet inspection (DPI). Raspberry Pi was used as the IoT device. Afterward, Kodi Media Center was the software media center, while OpenFlow managed the communication between SDN planes. This way, their solution provides confidentiality and integrity and mitigates various risks without modifying the IoT devices. However, their design solution is limited to IoT devices that only use HTTP. Most famous network attacks, such as Distributed Denial of Service (DDoS) and Link Flooding Attacks (LFA), are launched by spoofing the Internet Protocol (IP) or the Address Resolution Protocol (ARP).

In contrast to the other solutions, the authors in [119] proposed a novel Network-based Intrusion Detection System (NIDS) architecture model to address spoofing attacks for the IoT system. The model operates based on the MapReduce approach in the context of distributed detection. The model also incorporated a multi-faceted detection technique based on anomaly-based and misuse-based NIDS agents. DN-based IoT architecture to manage and reduce ARP spoofing attacks by deploying a new machine near the SDN controller to handle address resolution questions. Although the work has made some performance gains, the overall network's performance can be enhanced while safeguarding against IoT threats. In addition, most proposed methods can be time-consuming and resource-exhausting, especially in dynamic large-scale networks, as they use complex algorithms. A lightweight secure Threat Detection (TD) and Rule Automation (RA) framework were presented in [120] to effectively detect and mitigate different cyber-security threats in an SDIoT infrastructure.

The authors introduced a binary and a multi-class classification module (BCM/MCM) for IoT threat detection and a policy-enforcement module (PEM) for attack mitigation. It is used to recognize and mitigate a broad range of cyber-security threats. However, multi-technology networks, network externality, and device heterogeneity in SDN-IoT may seriously affect the flow or application-specific QoS requirements. Which, in turn, highly influences security adoption in a network of interconnected IoT nodes. In addition, a dynamic SDIoT environment comprising hardware and software heterogeneity poses severe and challenging issues. A framework was presented for transforming SDN controllers into homogeneous groups and enhancing their security concerns by retaining th' SDN's robust security features [121]. The authors analyze controller response time and validate the approach using a mathematical model and a proof of concept (PoC) in a virtual SDN ecosystem. This way, the model enhances the system QoS with better security. However, high mathematical computation in large-scale networks may affect the system convergence time. Table 7 presents various SDIoT security solutions.

Table 7: SDIoT security solutions

Related work	Type of attack	Method	SDIoT attack facility		Weakness
			IoT based devices	SDN based devices	
Xu et al. [122]	TCP and ICMP flood-based attacks	Attack mitigation	X	SDN gateway	Frequent network monitoring introduced extra processing load on the controller
Bhunia et al. [95]	DDoS	Machine learning	√	SDN controller	The evaluation is limited to simulated traffic in Mininet that does not represent the behavior of real IoT devices
Hamza et al. [107]	DoS, reflective TCP/UDP/ICMP flooding, and ARP spoofing	Machine learning	√	X	MUD specification has not been officially adopted

(Continued)

Table 7 (continued)

Related work	Type of attack	Method	SDIoT attack facility		Weakness
			IoT based devices	SDN based devices	
Cherian et al. [108]	DDOS	SDIoT DDOS detection Architecture	√	X	Their work was tested on the RYU controller only. It may not guarantee the same performance on a controller lower than RYU
Al Hayajneh et al. [118]	Man in the middle attack	Raspberry Pi, Kodi Media Center	√	X	It is limited to IoT that can only use HTTP
Hasan et al. [110]	DoS and DDoS	Deep learning	√	X	Overlooked an attack on critical SDN infrastructure such as switch Flowtable memory constraints, which is vulnerable to various attack
Javeed et al. [111,112]	DOS	Hybrid Deep learning	√	X	The model may not be promising in Dynamic large-scale networks to its high computational complexity
Aldabbas et al. [119]	spoofing attacks	Attack mitigation	√	X	The solution focuses on protecting IoT facility only. They did not consider SDN infrastructure.
Lahlou et al. [120]	DoS and DDoS	Machine learning model	√	X	The solution may not perform well in large-scale network
Sood et al. [121]	Cyber attack	Mathematical model	√	X	high mathematical computation in large-scale networks may affect the system convergence time.
Molina Zarca et al. [113]	Man in the middle, DDOS attack	Security architectural design	√	X	The solution focuses on protecting IoT facility only. They did not consider SDN infrastructure.
Grigoryan et al. [114]	Cyber attack	SDIoT security framework	√	X	The scheme may introduce controller place issues
Sambanda et al. [115,116]	DDOS	Entropy algorithm	X	√	Computing threshold entropy value more often may affect the s'stem's performance in large-scale networks.
Bringhenti et al. [117]	Cyber attack	Maximum Satisfiability Modulo Theories	X	√	The scheme exhibit trade-off between performance and new optimization targets

(Continued)

Table 7 (continued)

Related work	Type of attack	Method	SDIoT attack facility		Weakness
			IoT based devices	SDN based devices	
Aslam et al. [109]	DDoS attack	Adaptive Machine Learning framework	X	√	The framework is limited to DDoS attacks only. Other attacks, such as phishing, were overlooked, and the SDN controller could also become prime for an attack.

5 Lesson Learnt in the Integration of SDN for Smart Technologies

Various lessons have been learned from integrating SDN with other smart technologies. Although integration of SDN with other smart technologies can enable new opportunities for innovation and transformation across various domains, it is expected to play a crucial role in the future of networking and computing. However, based on the literature review on SDWBAN and SDIoT for routing and security challenges, we derive a set of key post-mortem challenges to be considered. Most existing solutions leverage SDN's features to improve the IoT and WBAN technologies without carefully considering these challenges. It's required to address these challenges for successfully integrating SDN with IoT and WBAN

5.1 Heterogeneity

Heterogeneity: As mentioned earlier, the heterogeneity of devices, protocols, and domains involved poses a major challenge for integration. Different devices may use different communication protocols, data formats, and security mechanisms, making achieving interoperability and seamless communication difficult. Since IoT and WBAN devices are categorized under the perception layer in SDN. The literature has made some effort to introduce various frameworks for managing these two layers. However, no widely accepted standard protocol is currently being used for communication between the SDN data plane and the perception plane [52]. Therefore, this issue should be considered when integrating SDN with other smart technologies. This could be considered an open research problem that needs further attention from the research community.

5.2 Scalability

The massive number of devices and data generated by IoT and WBAN networks require scalable and efficient network infrastructures. SDN can provide dynamic and flexible resource allocation but also introduces new scalability challenges such as efficient traffic engineering, load balancing, and network slicing. As the number of traffic flows and policies increase, the scalability of traffic engineering becomes a challenge. The network may become difficult to manage and optimize, and the performance may degrade due to congestion and routing inefficiencies. In addition, SDN switches maintain flow tables that store information about the traffic flows and the associated forwarding rules. IoT and WBAN technologies generate a dense number of traffic flows; as the number of flows and rules increases, the size of the Flowtable also increases. Unfortunately, the Flowtable is a constraint with limited space, and the scalability of the switch becomes a challenge. The switch may run out of memory or processing capacity to store and process the flow table. Hence, affect the system's

performance. Therefore, the successful integration of SDN with other smart technologies should carefully consider this limited resource from SDN. Unfortunately, most existing SDWBAN and SDIoT routing solutions overlooked the Flowtable memory limitations. This resource constraint should be carefully considered because SDN is a flow-based network, and each flow requires corresponding flow rules in the switch flowtable. This could be a potential research area using articial intelligence.

5.3 Security

Integrating SDN with IoT and WBAN exposes new security risks such as unauthorized access, data leakage, and attacks on network controllers. Securing communication between devices, controllers, and applications is crucial for ensuring the privacy and integrity of data. Besides, the Flowtable memory limitation also introduced another security concern. An attacker can easily inject flows to refuse writing legitimate forwarding rules in the switch Flowtable. This may affect the communication between the SDN data and the perceptions plane. Such challenges should be given special consideration for better network performance. However, it was learnt most SDIoT and SDWBAN have neglected these challenges and focus on the security challenges of IoT and WBAN. Ignoring the SDN component security challenges may not always yield the desired security solution. Integrating both technologies' security challenges may give the best security solution. We refer readers to reference [123] for more intelligent security solutions.

5.4 Mobility Management

Mobility management is a critical challenge in integrating SDN with wireless body area networks (WBANs) and IoT devices. The mobility of users and devices in SDWBANs can introduce several challenges related to network management, data transmission, and user experience. Handover management is one of the key challenges in SDWBANs [124]. As users move between different WBANs or access points, SDN must manage the handover process seamlessly to ensure uninterrupted connectivity and QoS. SDN must provide efficient and fast handover mechanisms that optimize the network performance and user experience. Similarly, network topology changes more often. An effective SDWBAN needs to support the dynamic and unpredictable network topology of SDWBANs, which can frequently change due to user mobility and device connectivity. Therefore, providing an efficient and adaptive mechanism for managing and optimizing the network topology to ensure efficient data transmission and resource utilization is paramount.

5.5 QoS Optimization

QoS Optimization: QoS is a critical challenge in integrating SDN with IoT and WBAN, as it determines the performance, reliability, and efficiency of the applications and services [125]. Traffic flows exhibit variabilities with different QoS demands. Although SDN has the potential to provide efficient QoS management mechanisms that can optimize the network performance and user experience in SDWBANs. However, the heterogeneity, scalability, security, and mobility management. These challenges need proper attention to optimize the QoS of the applications and services. The QoS management mechanisms need to be adaptive to changing network conditions and user requirements to ensure efficient data transmission and user satisfaction.

5.6 Potential Innovation

Integrating SDN with IoT can enable the Industrial Internet of Things (IIoT) to enhance industrial processes' efficiency, flexibility, and productivity. SDN can provide real-time monitoring, control, and automation of manufacturing systems, supply chain management, and asset tracking.

Another potential innovation that could arise from integrating SDN with IoT and WBAN is the development of new applications and services. By leveraging the flexibility and programmability of SDN, developers can create customized network services tailored to the specific requirements of IoT and WBAN devices. This can lead to the development of new applications and services that were previously impossible. However, it also requires a flexible and agile network infrastructure to support rapid prototyping, testing, and deployment of new solutions.

6 Future Research Direction

Various schemes have leveraged the benefit and flexibilities of SDN to manage various IoT devices considering different objectives. Creating a model to maintain health facility data while preserving patient privacy and control over how their data is quite challenging. Other researchers used the SDN to manage different data in wearable devices on WBAN. Several routing algorithms were proposed to meet various applications' QoS. Different security mechanisms were introduced over the years to safeguard IoT [126] devices and sensitive data in WBAN using SDN. The following subsections have highlighted some future research works.

6.1 Multi-Constraint SDWBAN Routing with Energy and Traffic Flows Awareness

Incorporating SDN in WBAN applications indicates promising benefits in dealing with traffic and network management challenges. However, the existing SDWBAN solution focuses on either managing traffic or using SDN controllers to improve the WBAN infrastructure energy consumption. However, they neglect to incorporate the energy consumption of the SDN controller while managing WBAN traffic to achieve efficient energy routing. It would be an interesting research direction to devise energy and traffic-aware routing considering composite routing metrics from SDN and WBAN technology using fuzzy logic.

6.2 An Intelligent SDIOT Traffic Flows Management for Efficient QoS Provision

Several works have been proposed to integrate SDN with IoT to efficiently manage traffic for optimal network performance. However, most existing studies do not properly explain the adopted SDN controller mode. SDN controllers operate reactively and proactively. Control traffic consumes bandwidth and degrades the IoT devices' spectral efficiency. Also, the battery power is highly vulnerable to this massive control traffic. While traffic flows exhibit variabilities with different QoS demands. It would be interesting research to classify flows based on their QoS requirement. This way, flows can be routed through a path with sufficient bandwidth or energy awareness considering reactive and proactive controller modes using artificial intelligence.

6.3 An Adaptive SDIoT-SDWBAN Security Framework

The emerging technology leveraged the innovation in SDN to address the specific issues related to IoT devices management or WBAN architectural management. Unfortunately, the benefit comes with additional security threats most existing studies overlook. SDN controller is a prime attack target, while the SDN switches are constrained with limited space and high power consumption. Therefore, it would be exciting research to incorporate the challenges in SDN with IoT or WBAN in devising any security mechanism, possibly using a game theory model.

6.4 An Intelligence SDWBAN Mobility Management

WBAN sensors are often attached to the human body and can move with the person. This presents a challenge in mobility management, as the network needs to adapt to changes in the location and

movement of the sensors. Ensuring seamless handoff between network access points and maintaining the quality of service is essential to avoid disruption to network operations. It would be interesting research to devise an intelligent SDWBAN load balancing among the network access point.

7 Conclusion

This survey paper examines the integration of SDN with IoT and WBAN technologies to manage challenges presented by heterogeneous devices with limited resources and security threats. The existing solutions for SDWBAN routing with resource awareness and SDWBAN security solutions, the SDIoT framework for devices, traffic management, and SDIoT security solutions were reviewed. As such, integrating SDN with these emerging technologies presents a promising approach to managing the challenges these devices present. However, based on the summary of the literature in the tables, the existing solutions are critically evaluated, and the study highlighted some limitations. For instance, some reviewed studies focused on specific applications or scenarios, which may not be generalizable to other use cases. Others did not consider the full spectrum of security threats that could affect IoT and WBAN networks. Secondly, the limited resources of IoT and WBAN devices and the need for real-time data processing pose significant challenges for implementing SDN frameworks. As a result, this study suggests that future research should focus on developing more comprehensive and flexible frameworks to address the diverse needs of IoT and WBAN devices and explore new security approaches like machine learning and blockchain.

Although integrating SDN with IoT and WBAN technology offers new opportunities. However, some post-event considerations such as performance monitoring, security management, scalability, network segmentation, and resource allocation should keep in mind to ensure that the integrated network functions efficiently, securely, and optimally. This way, network performance has to be periodically monitored to ensure the effectiveness of device usage. Besides, allocating network resources such as bandwidth and compute power should be considered to ensure that critical IoT applications receive the necessary resources. Which in turn will assist in minimizing congestion. In conclusion, we provide a foundation for further investigation and highlight the need for more comprehensive and flexible solutions to address the unique challenges of these technologies. The suggested future directions for research are particularly valuable, as they provide a roadmap for further investigation in this promising area of study.

Acknowledgement: We thank Universiti Teknologi Malaysia for supporting this research through the Post-Doctoral Fellowship Scheme under Grant Q.J130000.21A2.06E03 and Q.J130000.2409.08G77.

Funding Statement: We appreciate Universiti Teknologi Malaysia for funding this research work through Grant Q.J130000.21A2.06E03 and Q.J130000.2409.08G77.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] X. Chang, P. Ren, P. Xu, Z. Li, X. Chen *et al.,* "A comprehensive survey of scene graphs: Generation and application," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 45, no. 1, pp. 1–26, 2023.

[2] K. K. Karmakar, V. Varadharajan, S. Nepal and U. Tupakula, "SDN-Enabled secure IoT architecture," *IEEE Internet Things J*, vol. 8, no. 8, pp. 6549–6564, 2021.

[3] L. Zhang, X. Chang, J. Liu, M. Luo, Z. Li *et al.,* "TN-ZSTAD: Transferable network for zero-shot temporal activity detection," *IEEE Transaction Pattern Analysis & Machine Inteligence*, vol. 45, no. 3, pp. 3848–3861, 2023.

[4] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi and L. Vangelista, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Communication Survey Tutorials*, vol. 23, no. 3, pp. 1693–1720, 2021.

[5] I. Farris, T. Taleb, Y. Khettab and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commununication Survey Tutorials*, vol. 21, no. 1, pp. 812–837, 2019.

[6] B. Ozbek, Y. Aydogmus, A. Ulas, B. Gorkemli and K. Ulusoy, "Energy aware routing and traffic management for software defined networks," in *Proc. IEEE Network Softwarization and Workshops*, Seoul, Korea (South), pp. 73–77, 2016.

[7] M. Cicioğlu and A. Çalhan, "SDN-based wireless body area network routing algorithm for healthcare architecture," *ETRI Journal*, vol. 41, no. 4, pp. 452–464, 2019.

[8] W. Bekri, R. Jmal and L. Chaari Fourati, "Internet of things management based on software defined networking: A survey," *International Journal of Wireless & Infrasturacture Networks*, vol. 27, no. 3, pp. 385–410, 2020.

[9] B. B. Gupta and C. Chaturvedi, "Software defined networking (SDN) based secure integrated framework against distributed denial of service (DDoS) attack in cloud environment," in *Proc. Int. Conf. on Communication and Electronics Systems*, Coimbatore, India, pp. 1310–1315, 2019.

[10] F. T. Zuhra, K. B. A. Bakar, A. A. Arain, U. A. Khan and A. R. Bhangwar, "MIQoS-RP: Multi-constraint intra-ban, qos-aware routing protocol for wireless body sensor networks," *IEEE Access*, vol. 8, no. 1, pp. 99880–99888, 2020.

[11] F. T. Zuhra, K. B. A. Bakar, A. A. Arain, K. M. Almustafa, T. Saba *et al.,* "LLTP-QoS: Low latency traffic prioritization and qos-aware routing in wireless body sensor networks," *IEEE Access*, vol. 7, no. 1, pp. 152777–152787, 2019.

[12] A. B. Al-Shaikhli, C. Çeken and M. Al-Hubaishi, "WSANFlow: An interface protocol between sdn controller and end devices for SDN-oriented WSAN," *Wireless & Personal Communication*, vol. 101, no. 2, pp. 755–773, 2018.

[13] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza *et al.,* "A survey on the challenges and opportunities of the internet of things (IoT)," in *Proc. Int. Conf. on Sensing Technology*, Sydney, NSW, Australia, pp. 1–5, 2017.

[14] S. Memon, J. Wang, A. R. Bhangwar, S. M. Fati, A. Rehman *et al.,* "Temperature and reliability-aware routing protocol for wireless body area networks," *IEEE Access*, vol. 9, no. 1, pp. 140413–140423, 2021.

[15] K. Hasan, K. Ahmed, K. Biswas, M. Saiful Islam and O. Ameri Sianaki, "Software-defined application-specific traffic management for wireless body area networks," *Future Generation Computing System*, vol. 107, no. 1, pp. 274–285, 2020.

[16] M. Salayma, A. Al-Dubai, I. Romdhani and Y. Nasser, "Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence," *Association of Computing Machinery*, vol. 50, no. 3, pp. 1–38, 2017.

[17] Z. Shah, A. Levula, K. Khurshid, J. Ahmed, I. Ullah *et al.,* "Routing protocols for mobile internet of things (Iot): A survey on challenges and solutions," *Electronics*, vol. 10, no. 19, pp. 1–29, 2021.

[18] K. Hasan, X. W. Wu, K. Biswas and K. Ahmed, "A novel framework for software defined wireless body area network," in *Proc. Int. Conf. on Intelligent Systems, Modelling and Simulation*, vol. 20, no. 1, pp. 114–119, 2018.

[19] I. Alam, K. Sharif, F. Li, Z. Latif, M. M. Karim *et al.,* "A survey of network virtualization techniques for Internet of Things using SDN and NFV," *Association of Computing Machinery*, vol. 53, no. 2, pp. 1–40, 2020.

[20] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji *et al.,* "A survey of routing protocols in WBAN for healthcare applications," *Sensors*, vol. 19, no. 7, pp. 1–24, 2019.

[21] H. Zemrane, Y. Baddi and A. Hasbi, "SDN-based solutions to improve IOT: Survey," in *Proc. Colloquium in Information Science and Technology*, Marrakech, Morocco, pp. 588–593, 2018.

[22] M. B. Sergio, M. León, P. Torres-carrión, M. Zambrano and G. P. Vásquez Eds, "Applied technologies," in *Proc. Int. Conf. on Applied Technologies (ICAT)*, Quito, Ecuador, pp. 1–4, 2020.

[23] O. Salman, I. Elhajj, A. Chehab and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Computer Networks*, vol. 143, no. 2018, pp. 221–246, 2018.

[24] S. Bera, S. Misra and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994–2008, 2017.

[25] F. S. Dantas Silva, E. Silva, E. P. Neto, M. Lemos, A. J. Venancio Neto *et al.,* "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," *Sensors*, vol. 20, no. 11, pp. 1–28, 2020.

[26] P. J. B. Pajila and E. G. Julie,"Detection of DDoS attack using SDN in IoT: A survey," in *Proc. Intelligent Communication Technologies and Virtual Mobile Networks*, LNDECT, pp. 438–452, 2020.

[27] P. P. Ray and N. Kumar, "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review," *Computer Communication*, vol. 169, no. 1, pp. 129–153, 2021.

[28] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba *et al.,* "Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects," *IEEE Access*, vol. 10, no. 6, pp. 70850–70901, 2022.

[29] B. Isyaku, K. Bin, A. Bakar, W. Nagmeldin, A. Abdelmaboud *et al.,* "Reliable failure restoration with Bayesian congestion aware for software defined networks," *Computer Systems Science and Engineering*, vol. 46, no. 3, pp. 3729–3748, 2023.

[30] B. Isyaku, M. Soperi, M. Zahid and M. B. Kamat, "Software defined networking flow table management of openflow switches performance and security challenges: A survey," *Future Internet*, vol. 12, no. 9, pp. 147, 2020.

[31] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky *et al.,* "Software-defined networking: A comprehensive survey," *IEEE*, vol. 103, no. 1, pp. 1–61, 2014.

[32] X. Nguyen, D. Saucez, C. Barakat and T. Turletti, "Rules placement problem in openflow networks: A survey," *IEEE Communication Survey & Tutorials*, vol. 18, no. 2, pp. 1273–1286, 2016.

[33] B. Isyaku, A. Bakar, F. A. Ghaleb, M. Soperi and M. Zahid, "Path selection with critical switch-aware for software defined networking," in *Proc. Int. Symp. of Wireless Technology & Application*, Shah Alam, Malaysia, pp. 22–26, 2021.

[34] M. Alsaeedi, M. M. Mohamad and A. A. Al-roubaiey, "Toward adaptive and scalable openflow-sdn flow control: A survey," *IEEE Access*, vol. 7, no. 1, pp. 107346–107379, 2019.

[35] S. A. Shah, J. Faiz, M. Farooq, A. Shafi and S. A. Mehdi, "An architectural evaluation of SDN controllers," in *Proc. IEEE Int. Confrence Communication*, Budapest, Hungary, pp. 3504–3508, 2013.

[36] S. Scott-Hayward, "Design and deployment of secure, robust, and resilient SDN controllers," in *Proc. Network Softwarization and Workshops*, London, UK, pp. 1–5, 2015.

[37] K. Phemius, M. Bouet and J. Leguay, "DISCO: Distributed multi-domain sdn controllers," *Thales Communications & Security*, vol. 10, no. 1, pp. 9–12, 2013.

[38] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark *et al.,* "Advancing software-defined networks: A survey," *IEEE Access*, vol. 5, no. 1, pp. 25487–25526, 2017.

[39] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, "A survey on software-defined networking," *IEEE Communication Survey & Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[40] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski *et al.,* "Onix a distributed control platform for large.pdf," *USENIX Confrence of Operating Systems Design and Implement*, vol. 10, pp. 1–14, 2010.

[41] A. Tootoonchian and Y. Ganjali, "HyperFlow: A distributed control plane for OpenFlow," in *Proc. USENIX Conf. on Operating Systems Design and Implementation*, Berkeley, CA, USA, pp. 1–6, 2010.

[42] M. Priyadarsini, P. Bera and R. Bhampal, "Performance analysis of software defined network controller architecture-A simulation based survey," in *Proc. Int. Conf. on Wireless Communications, Signal Processing and Networking*, Chennai, India, vol. 18, no. 1, pp. 1929–1935, 2018.

[43] T. Kato, M. Kawakami, T. Myojin, H. Ogawa, K. Hirono *et al.,* "Case study of applying SPLE to development of network switch products," in *Association of Computing Machinery Int. Conf. Proc. Series*, Tokyo, Japan, pp. 198–207, 2013.

[44] H. Song, "Protocol-oblivious forwarding," in *Proc. of the Second Association of Computing Machinery SIGCOMM Workshop on Hot Topics in Software Defined Networking*, New York, NY, USA, pp. 127–132, 2013.

[45] E. Haleplidis, J. Hadi Salim, J. M. Halpern, S. Hares, K. Pentikousis *et al.,* "Network programmability with ForCES," *IEEE Communication Survery & Tutorials*, vol. 17, no. 3, pp. 1423–1440, 2015.

[46] S. Sharma, D. Staessens, D. Colle, D. Palma, J. Goncalves *et al.,* "Implementing quality of service for the software defined networking enabled future internet," in *Proc. European Workshop on Software-Defined Networks*, Budapest, Hungary, pp. 49–54, 2014.

[47] B. Belter, A. Binczewski, K. Dombek, A. Juszczyk, L. Ogrodowczyk *et al.,* "Programmable abstraction of datapath: Advanced programmability of heterogeneous datapath elements through hardware abstraction," in *Proc. European Workshop on Software-Defined Networks*, Budapest, Hungary, pp. 7–12, 2014.

[48] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson *et al.,* "OpenFlow: Enabling innovation in campus networks," *Association of Computing Machinery Computing Communication Review*, vol. 38, no. 2, pp. 69, 2008.

[49] G. Bianchi, M. Bonola, A. Capone and C. Cascone, "OpenState: Programming platform-independent stateful openflow applications inside the switch," *Association of Computing Machinery Computing Communication Review*, vol. 44, no. 2, pp. 44–51, 2014.

[50] A. Malik, B. Aziz, A. Al-haj and M. Adda, "Software-defined networks: A walkthrough fault tolerance," *PeerJ*, vol. 1, no. 1, pp. 1–26, 2019.

[51] H. I. Kobo, A. M. Abu-Mahfouz and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, no. 1, pp. 1872–1899, 2017.

[52] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas *et al.,* "A comprehensive survey of interface protocols for software defined networks," *Journal of Network and Computer Applications*, vol. 156, no. 1, pp. 102563, 2020.

[53] M. Li, P. Y. Huang, X. Chang, J. Hu, Y. Yang *et al.,* "Video pivoting unsupervised multi-modal machine translation," *IEEE Transaction Pattern Analysis & Machine Intelligence*, vol. 45, no. 3, pp. 3918–3932, 2023.

[54] C. Yan, X. Chang, Z. Li, W. Guan, Z. Ge *et al.,* "ZeroNAS: Differentiable generative adversarial networks search for zero-shot learning," *IEEE Transaction Pattern Analysis & Machince Intelligence*, vol. 44, no. 12, pp. 9733–9740, 2022.

[55] E. Barka, S. Dahmane, C. A. Kerrache, M. Khayat and F. Sallabi, "Sthm: A secured and trusted healthcare monitoring architecture using SDN and blockchain," *Electronics*, vol. 10, no. 15, pp. 1–15, 2021.

[56] M. Cicioğlu and A. Çalhan, "HUBsFLOW: A novel interface protocol for SDN-enabled WBANs," *Computer Networks*, vol. 160, no. 1, pp. 105–117, 2019.

[57] R. Amin, M. Reisslein and N. Shah, "Hybrid SDN networks: A survey of existing approaches," *IEEE Communication Survey & Tutorials*, vol. 20, no. 4, pp. 3259–3306, 2018.

[58] A. Rego, L. Garcia, S. Sendra and J. Lloret, "Software defined network-based control system for an efficient traffic management for emergency situations in smart cities," *Future Generation Computer System*, vol. 88, no. 1, pp. 243–253, 2018.

[59] M. Waqas, S. Tu, J. Wan, T. Mir, H. Alasmary *et al.,* "Defense scheme against advanced persistent threats in mobile fog computing security," *Computer Networks*, vol. 221, no. 1, pp. 109519, 2023.

[60] V. Sharma, M. Z. Khan, S. Batra, A. Alsaeedi and P. Srivastava, "Optimizing storage for energy conservation in tracking wireless sensor network objects," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1211–1231, 2023.

[61] A. Ouhab, T. Abreu, H. Slimani and A. Mellouk, "Energy-efficient clustering and routing algorithm for large-scale SDN-based IoT monitoring," in *Proc. IEEE Nternational Conf. on Communications*, Dublin, Ireland, 2020.

[62] R. K. Santhanaraj, S. Rajendran, C. A. T. Romero and S. S. Murugaraj, "Internet of things enabled energy aware metaheuristic clustering for real time disaster management," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1561–1576, 2023.

[63] M. A. Hamza, A. H. A. Hashim, D. H. Elkamchouchi, N. Nemri, J. S. Alzahrani *et al.,* "Energy-efficient routing using novel optimization with tabu techniques for wireless sensor network," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1711–1726, 2023.

[64] A. Mishra, N. Gupta and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," *Telecommunication System*, vol. 77, no. 1, pp. 47–62, 2021.

[65] K. Bhushan and B. B. Gupta, "Detecting DDoS attack using software defined network (SDN) in cloud computing environment," in *Proc. Int. Conf. of Signal Processing & Integrated Networks*, Noida, India, pp. 872–877, 2018.

[66] D. Mehiar, H. Bechir, G. Mohsen and R. Ammar, "Structure and design of software-defined nettworks," *IEEE Communication Magazine*, vol. 22, no. 6, pp. 67–75, 2015.

[67] F. Sallabi, F. Naeem, M. Awad and K. Shuaib, "Managing IoT-based smart healthcare systems traffic with software defined networks," in *Proc. Int. Symp. on Networks, Computers and Communications*, Rome, Italy, pp. 1–5, 2018.

[68] K. Hasan, K. Ahmed, K. Biswas, M. S. Islam, A. S. M. Kayes *et al.,* "Control plane optimisation for an SDN-based wban framework to support healthcare applications," *Sensors*, vol. 20, no. 15, pp. 1–19, 2020.

[69] S. Misra, R. Saha and N. Ahmed, "Health-flow: Criticality-aware flow control for sdn-based healthcare IoT," in *2020 IEEE Global Communication Conf.*, Taipei, Taiwan. pp. 1–5, 2020.

[70] R. Saha, N. Ahmed and S. Misra, "SDN-controller triggered dynamic decision control mechanism for healthcare IoT," in *Proc. IEEE Global Communication Conf.*, Madrid, Spain, pp. 1–6, 2021.

[71] D. P. Isravel, S. Silas and E. B. Rajsingh, "Sdn-based traffic management for personalized ambient assisted living healthcare system," *Advance Intelligence System & Computing*, vol. 1167, no. 1, pp. 379–388, 2021.

[72] A. Ahmed, X. Wang, A. Hawbani, M. U. Farooq, T. Qureshi *et al.,* "EE-TAR: Energy efficient and thermal aware routing protocol for software defined wireless body area networks," in *Proc. Int. Conf. on Information, Communication and Networks*, Xi'an, China, pp. 51–55, 2020.

[73] J. Iqbal, M. Adnan, Y. Khan, H. Alsalman, S. Hussain *et al.,* "Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis," *Journal of Healthcare Engineering*, vol. 2022, no. 9210761, pp. 1–19, 2022.

[74] O. Ahmed, F. Ren, A. Hawbani and Y. Al-Sharabi, "Energy optimized congestion control-based temperature aware routing algorithm for software defined wireless body area networks," *IEEE Access*, vol. 8, no. 1, pp. 41085–41099, 2020.

[75] O. Ahmed, M. Hu and F. Ren, "PEDTARA: Priority-based energy efficient, delay and temperature aware routing algorithm using multi-objective genetic chaotic spider monkey optimization for critical data transmission in WBANs," *Electronics*, vol. 11, no. 1, pp. 1–127, 2022.

[76] M. Cicioğlu and A. Çalhan, "Energy-efficient and SDN-enabled routing algorithm for wireless body area network," *Computer Communication*, vol. 160, no. 6, pp. 228–239, 2020.

[77] M. Al-Hubaishi, C. Çeken and A. Al-Shaikhli, "A novel energy-aware routing mechanism for SDN-enabled WSAN," *International Journal of Communication System*, vol. 32, no. 17, pp. 1–17, 2019.

[78] T. F. Oliveira, S. Xavier-De-souza and L. F. Silveira, "Improving energy efficiency on SDN control-plane using multi-core controllers," *Energies*, vol. 14, no. 11, pp. 1–20, 2021.

[79] J. Steenbruggen, P. Nijkamp and M. Van Der Vlist, "Urban traffic incident management in a digital society. An actor-network approach in information technology use in urban Europe," *Technology Forecasting Society Change*, vol. 89, no. 1, pp. 245–261, 2014.

[80] Z. Qin, G. Denker, C. Giannelli, P. Bellavista and N. Venkatasubramanian, "A software defined networking architecture for the Internet-of-Things," in *Proc. Network Operations and Management Symp.*, Krakow, Poland, pp. 1–5, 2014.

[81] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin and J. A. McCann, "UbiFlow: Mobility management in urban-scale software defined IoT," in *Proc. IEEE INFOCOM*, Hong Kong, China, pp. 208–216, 2015.

[82] A. Rego, L. Garcia, S. Sendra and J. Lloret, "Software defined networks for traffic management in emergency situations," in *Proc. Int. Conf. on Software Defined Systems*, Barcelona, Spain, pp. 45–51, 2018.

[83] A. Mondal, S. Misra and A. Chakraborty, "TROD: Throughput-optimal dynamic data traffic management in software-defined networks," in *Proc. IEEE Globecom Workshop*, Abu Dhabi, United Arab, pp. 1–6, 2019.

[84] M. I. Alipio, A. G. A. Co, M. F. C. Hilario and C. M. C. Pama, "SDN-enabled value-based traffic management mechanism in resource-constrained sensor devices," in *Proc. Int. Conf. Infrasturacture Network*, Kuala Lumpur, Malaysia, pp. 248–253, 2019.

[85] A. Rego, A. Canovas, J. M. Jimenez and J. Lloret, "An intelligent system for video surveillance in IoT environments," *IEEE Access*, vol. 6, no. 1, pp. 31580–31598, 2018.

[86] A. I. Owusu and A. Nayak, "An intelligent traffic classification in SDN-IoT: A machine learning approach," in *Proc. IEEE Int. Black Sea Conf. Commununication Networking, BlackSeaCom*, Odessa, Ukraine, pp. 2–7, 2020.

[87] N. Saha, S. Member, S. Bera and S. Member, "Sway: Traffic-aware QoS routing in software-defined IoT," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 390–401, 2021.

[88] F. Tang, Z. M. Fadlullah, B. Mao and N. Kato, "An intelligent traffic load prediction-based adaptive channel assignment algorithm in SDN-IoT: A deep learning approach," *IEEE Internet Things Journal*, vol. 5, no. 6, pp. 5141–5154, 2018.

[89] T. G. Nguyen, T. V. Phan, D. T. Hoang, H. H. Nguyen and D. T. Le, "DeepPlace: Deep reinforcement learning for adaptive flow rule placement in software-defined IoT networks," *Computer Communication*, vol. 181, no. 9, pp. 156–163, 2022.

[90] P. Kamboj, S. Pal, S. Bera and S. Misra, "QoS-Aware multipath routing in software-defined networks," *IEEE Transaction Network Science Engineering*, vol. 10, no. 2, pp. 1–10, 2022.

[91] F. Naeem, M. Tariq and H. V. Poor, "SDN-enabled energy-efficient routing optimization framework for industrial internet of things," *IEEE Transaction Industrial Informatics*, vol. 17, no. 8, pp. 5660–5667, 2021.

[92] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis *et al.,* "Latency critical IoT applications in 5 g: Perspective on the design of radio interface and network architecture," *IEEE Communication Magazine*, vol. 55, no. 2, pp. 70–78, 2017.

[93] P. Kamboj, S. Pal and A. Mehra, "A QoS-aware routing based on bandwidth management in software-defined IoT network," in *Proc. Int. Conf. on Mobile Ad Hoc and Smart Systems*, Denver, CO, USA, pp. 579–584, 2021.

[94] L. A. B. Pacheco, J. J. C. Gondim, P. A. S. Barreto and E. Alchieri, "Evaluation of distributed denial of service threat in the internet of things," in *Proc. Int. Symp. on Network Computing and Applications*, Cambridge, MA, USA, pp. 89–92, 2016.

[95] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *Proc. Int. Telecommunication Networks and Applications Conf.*, Melbourne, VIC, Australia, pp. 1–6, 2017.

[96] V. Varadharajan, U. Tupakula and K. Karmakar, "Secure monitoring of patients with wandering behavior in hospital environments," *IEEE Access*, vol. 6, no. 1, pp. 11523–11533, 2017.

[97] W. Meng, K. K. R. Choo, S. Furnell, A. V. Vasilakos and C. W. Probst, "Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks," *IEEE Transaction Network Service Management*, vol. 15, no. 2, pp. 761–773, 2018.

[98] M. Khayat, E. Barka and F. Sallabi, "SDN_based secure healthcare monitoring system (SDN-SHMS)," in *Proc. Int. Conf. on Computer Communication and Networks*, Valencia, Spain, pp. 1–6, 2019.

[99] M. Al Shayokh, A. Abeshu, G. B. Satrya and M. A. Nugroho, "Efficient and secure data delivery in software defined WBAN for virtual hospital," in *Proc. Int. Conf. on Control, Electronics, Renewable Energy, and Communications*, Bandung, Indonesia, pp. 12–16, 2017.

[100] S. El Jaouhari and A. Bouabdallah, "Dynamic security management of smart wot infrastructures using SDN," in *Proc. IEEE Vehicle Technology Conf.*, Chicago, IL, USA, pp. 1–7, 2018.

[101] J. Jiang, C. Lin, G. Han, A. M. Abu-Mahfouz, S. B. H. Shah *et al.,* "How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities," *Digital Communication Networks*, vol. 1, no. 1, pp. 1–10, 2022.

[102] S. Mandal, "Provably secure certificateless protocol for wireless body area network," *Wireless Networks*, vol. 4, no. 1, pp. 1421–1438, 2022.

[103] A. Wani, S. Revathi and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 3, pp. 281–290, 2021.

[104] K. Haseeb, I. Ahmad, I. I. Awan, J. Lloret and I. Bosch, "A machine learning SDN-enabled big data model for iomt systems," *Electronics*, vol. 10, no. 18, pp. 1–13, 2021.

[105] P. Hadem, D. K. Saikia and S. Moulik, "An SDN-based intrusion detection system using SVM with selective logging for ip traceback," *Computer Networks*, vol. 191, no. 3, pp. 1–11, 2021.

[106] P. Bull, R. Austin, E. Popov, M. Sharma and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *Proc. Int. Conf. on Future Internet of Things and Cloud*, Vienna, Austria, pp. 157–163, 2016.

[107] A. Hamza, H. H. Gharakheili, T. A. Benson and V. Sivaraman, "Detecting volumetric attacks on IoT devices via SDN-based monitoring of MUD activity," in *Proc. Symp. on SDN Research*, San Jose CA USA, pp. 36–48, 2019.

[108] M. Cherian and S. Verma, "Integration of IoT and sdn to mitigate ddos with ryu controller," *Lecture Notes Data Engineering Communication Technology*, vol. 66, pp. 673–684, 2021.

[109] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif *et al.,* "Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT†," *Sensors*, vol. 22, no. 7, pp. 1–28, 2022.

[110] T. Hasan, A. Adnan, T. Giannetsos and J. Malik, "Orchestrating SDN control plane towards enhanced IoT security," in *Proc. IEEE Conf. on Network Softwarization: Bridging the Gap Between AI and Network Softwarization*, Ghent, Belgium, pp. 457–464, 2020.

[111] D. Javeed, T. Gao, M. T. Khan and I. Ahmad, "A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)," *Sensors*, vol. 21, no. 14, pp. 1–18, 2021.

[112] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari *et al.,* "A hybrid deep learning approach for bottleneck detection in IoT," *IEEE Access*, vol. 10, no. 5, pp. 77039–77053, 2022.

[113] A. Molina Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos *et al.,* "Security management architecture for NFV/SDN-aware IoT systems," *IEEE Internet Things Journal*, vol. 6, no. 5, pp. 8005–8020, 2019.

[114] G. Grigoryan, Y. Liu, L. Njilla, C. Kamhoua and K. Kwiat, "Enabling cooperative IoT security via software defined networks (SDN)," in *Proc. IEEE Int. Conf. Communication*, Kansas City, MO, USA, pp. 1–6, 2018.

[115] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert and C. Kemp, "User behavior anomaly detection for application layer ddos attacks," in *Proc. Int. Conf. on Information Reuse and Integration*, San Diego, CA, USA, pp. 154–161, 2017.

[116] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors (Switzerland)*, vol. 20, no. 3, pp. 1–18, 2020.

[117] D. Bringhenti, J. Yusupov, A. M. Zarca, F. Valenza, R. Sisto *et al.,* "Automatic, verifiable and optimized policy-based security enforcement for SDN-aware IoT networks," *Computer Networks*, vol. 213, no. 6, pp. 109123, 2022.

[118] A. Al Hayajneh, M. Z. A. Bhuiyan and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, pp. 1–14, 2020.

[119] H. Aldabbas and R. Amin, "A novel mechanism to handle address spoofing attacks in SDN based IoT," *Cluster Computing*, vol. 24, no. 4, pp. 3011–3026, 2021.

[120] S. Lahlou, Y. Moukafih, A. Sebbar, K. Zkik, M. Boulmalf *et al.,* "TD-RA policy-enforcement framework for an SDN-based IoT architecture," *Journal of Network & Computer Application*, vol. 204, no. 3, pp. 103390, 2022.

[121] K. Sood, K. K. Karmakar, S. Yu, V. Varadharajan, S. R. Pokhrel *et al.,* "Alleviating heterogeneity in SDN-IoT networks to maintain QoS and enhance security," *IEEE Internet Things Journal*, vol. 7, no. 7, pp. 5964–5975, 2020.

[122] G. Xu, B. Dai, B. Huang, J. Yang and S. Wen, "Bandwidth-aware energy efficient flow scheduling with SDN in data center networks," *Future Generation Computer System*, vol. 68, no. 1, pp. 163–174, 2017.

[123] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas *et al.,* "The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges," *Artificial Intelligence Review*, vol. 55, no. 7, pp. 5215–5261, 2022.

[124] A. F. S. Devaraj, T. S. Murthy, F. Alenezi, E. L. Lydia, M. A. M. Zawawi *et al.,* "Enhanced metaheuristics with trust aware route selection for wireless sensor networks," *Computer System Science Engineering*, vol. 46, no. 2, pp. 1431–1445, 2023.

[125] D. Sharma, S. Jain and V. Maik, "Optimized tuning of loading routing protocol parameters for IoT," *Computer System Science Engineering*, vol. 46, no. 2, pp. 1549–1561, 2023.

[126] B. Gong, G. Zheng, M. Waqas, S. Tu and S. Chen, "LCDMA: Lightweight cross-domain mutual identity authentication scheme for Internet of Things," *IEEE Internet Things Journal*, vol. 11 pp. 1–13, 2023.