A Survey on Network Management for xANET: Evolution, Challenges, Future Directions

Tong Li, Chungang Yang, Yao Wang, Lin Cai, Alagan Anpalagan, and Zhu Han

***Abstract*—The x ad hoc network (xANET) termed as a family of ad hoc networks, including mobile ad hoc network (MANET), vehicular ad hoc network (VANET), flying ad hoc network (FANET) and satellite ad hoc network (SANET), has found a wide range of applications in providing ubiquitous wireless services. Despite its broad utility, the dynamic nature and lack of a centralized controller pose significant challenges to effective and flexible network management for xANET. Conventional network management protocols face challenges such as scalability, security vulnerabilities, configuration complexity, robustness, and performance resilience. Recent efforts have presented different approaches, focusing on policy-based network management (PBNM) and intent-driven network management (IDNM). However, there is no comprehensive survey to clarify their concepts and classifications. This paper presents a survey of the network management evolution for xANET, covering configuration-based, policy-based and the latest intent-driven approaches. We first introduce the characteristics and applications of xANET. Meanwhile, we investigate the network management concepts and challenges. Moreover, we survey the evolution of management protocols for xANET, including simple network management protocol (SNMP), PBNM, and IDNM. Then, we follow the detailed network management of xANET from configuration-based to policy-based and intent-driven approaches. Through comparative analysis, it is found that IDNM employs a more intelligent management protocol, demonstrating higher efficiency and flexibility in handling complex tasks and dynamic network management. This makes it better suited to addressing the challenges of xANET management. Finally, we summarize the remaining challenges and possible future research directions.**

***Index Terms*—Ad hoc network, intent-driven network, network management, policy-based network management**

I. Introduction

Ad hoc networks have been widely deployed as a promising networking paradigm in various fields, such as disaster management and emergency response. As a self-organizing, decentralized, and multi-hop wireless network, it enables communication without relying on infrastructure [1]. Instead, it relies solely on the collaborative efforts of nodes to achieve wireless connectivity. This overcomes the geographical limitations inherent in conventional wireless network connections, allowing people to communicate with each other in any environment through simple setups [2].

The self-organizing networks can be classified into various types based on node characteristics and application scenarios, including mobile ad hoc network (MANET), vehicular ad hoc network (VANET), flying ad hoc network (FANET), and satellite ad hoc network (SANET) [3]. Specifically, MANET refers to a network where mobile wireless nodes connect in a self-organizing manner within their communication range. VANET is a specialized type of MANET where vehicles serve as mobile nodes [4]. FANET involves communication networks among unmanned aerial vehicles (UAVs) and between UAVs and control stations. Unlike conventional satellite networks, SANET forms a self-organizing network by combining multiple small satellites to enable the automatic construction, management, and optimization of satellite communication networks without central control. This is achieved through collaborative actions among nodes to allocate resources dynamically [5]. SANET represents the future form of satellite communication networks characterized by increased flexibility and adaptability. In this paper, to better distinguish the management characteristics of these networks, we collectively refer to MANET, VANET, FANET, and SANET as a family of ad hoc networks called x ad hoc networks (xANETs).

According to the united nations sustainable development goals (UN SDGs), xANETs have made significant contributions in various domains. Specifically, under SDG 9 (industry, innovation, and infrastructure), xANETs leverage their self-organizing and decentralized characteristics to provide reliable wireless connectivity in remote and underserved regions, even in the absence of stable network infrastructure [6]. Additionally, xANETs support SDG 11 (sustainable cities and communities) by enabling effective communication in urban environments and disaster-stricken regions [7]. This ensures that communication networks can be rapidly established in emergencies, enhancing response capabilities and laying a robust foundation for urban intelligence and sustainable development. The high flexibility and scalability of xANETs make them the preferred solution for communication in dynamic environments where conventional networks fail to operate [8]. However, the characteristics of xANET present the following challenges for effective network management.

- Firstly, nodes can join and leave the network at any mo-

Tong Li, Chungang Yang, and Yao Wang are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, China (emails: tongli1018@gmail.com; guideyang2050@163.com; yaow0518@gmail.com). Corresponding author Chungang Yang is with National Key Laboratory of Multi-domain Data Collaborative Processing and Control, Xi'an, 710068, China, and also with Hangzhou Institute of Technology of Xidian University, Hangzhou, 311231, China. This work was supported by the National Key Laboratory of Multi-domain Data Collaborative Processing and Control (Program No. MDPC20240401).

Lin Cai is with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada (email: cai@ece.uvic.ca).

Alagan Anpalagan is with the Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON M5B 2K3, Canada (email: alagan@ee.ryerson.ca).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446701, South Korea (email: hanzhu22@gmail.com).

ment. Therefore, network management approaches must rapidly detect changes in the status of these nodes and promptly update the network topology for automatic reconfiguration [9]. This involves effective node monitoring and management policies to ensure the network can adapt flexibly to changes in a dynamic environment.

- Secondly, many nodes in xANET may run with limited energy. As a result, minimizing network management overhead is essential for optimizing energy efficiency [10]. To achieve efficient energy utilization, reducing the number of nodes involved in sending, receiving, and processing is necessary [11]. However, this objective conflicts with the periodic updating requirements of the network topology.
- Thirdly, security is of utmost importance when the xANET is employed in any context. Network management should integrate highly robust security measures to counter various threats, including eavesdropping, sabotage, and intrusion [12]. Therefore, network management of the xANET should integrate encryption and authentication mechanisms to ensure secure communications [13]. When implementing encryption and authentication mechanisms, attention should be paid to their adaptability and flexibility to accommodate different application scenarios and security requirements.
- Fourthly, intelligent and automated management systems become crucial because of the dynamic variability of xANET [14]. The network management approach can effectively monitor the performance of various devices in xANET and adaptively configure them according to different application scenarios and requirements to ensure real-time and efficient scheduling of various network resources [15]. This enables higher-level network management and reduces the burden of manual management.

The conventional simple network management protocol (SNMP) adopts centralized management. When the network scale becomes large, various query information will generate too much signaling overhead, which is not suitable for xANET management [16]. With the development of intelligent technology, policy-based network management (PBNM) and intent-driven network management (IDNM) methods have emerged. However, the PBNM system requires establishing complex management policies [17]. It lacks a detailed and unified standardized expression method, and the management policies are static, which cannot adapt to the dynamic changes and complexity of xANET [18]. IDNM introduces automated and intelligent management methods to separate managers from network management and can meet the high dynamic and adaptive management requirements of xANET [19].

A. Motivation for this Survey

As a wireless ad hoc network covering air, space and ground, xANET has become an indispensable core component of future mobile communication technology. Its characteristics are that nodes in the network can move freely, and the topology changes dynamically at any time. xANETs are mainly employed in emergency, temporary, military mobile communications and other fields. Compared with conventional networks, xANETs are highly dynamic, limited resources, and poor security [20] [21]. These characteristics make xANET management more complex. Therefore, beginners entering this field should possess a solid foundation in network configuration protocols, wireless communication technologies, and network optimization techniques. At the same time, the rapid development of emerging technologies such as software-defined network (SDN), artificial intelligence (AI), blockchain, and intent-driven network (IDN) has accelerated network automation and intelligence, offering new approaches for managing complex networks [22]. Researchers should master and apply these emerging technologies to propose more intelligent and efficient network management approaches.

Current network management approaches include SNMP, PBNM, and IDNM [23]. Each has its advantages and disadvantages in different xANET scenarios. Conventional SNMP is often unable to effectively handle the management tasks of a large number of devices and massive data, which may cause performance bottlenecks and delays, limiting the scalability and efficiency of network management [24]. The PBNM approach uses static management policies and rules, which cannot adapt to dynamically changing network environments and requirements [25]. As an emerging network management approach, IDNM allows administrators to define high-level intents without focusing on low-level configuration details, simplifying the network management process. Additionally, IDNM employs a closed-loop verification mechanism to ensure that the network consistently adheres to the configurations and automatically adjusts based on real-time state [26]. Such intelligent and automated management is well-suited to the complex demands of xANET management, enabling it to maintain efficient and stable operations in a continuously evolving network environment.

Therefore, the main motivation of this survey is to provide a comprehensive survey of the xANET management approach, including xANET characteristics and applications, management concepts and challenges, the evolution of network management protocols and current research on xANET management. The survey also introduces the remaining challenges and future research directions for xANET management.

B. Related Survey Work

In recent years, researchers have investigated a variety of issues concerning xANETs. Among them, a large number of research results have been accumulated in the field of xANET management. However, most of the current work primarily focuses on individual management functionalities, and there is still a lack of a comprehensive summary report of xANET management capabilities. The topics of these research papers are summarized as follows.

In the realm of fault management, the study by [27] investigated fault management between layers in the SDN but did not consider other management issues. Another work, [28] reviewed various frameworks to address faults in wireless sensor networks, including cartelized, distributed, hierarchical, and hybrid. In configuration management, [29] provided a detailed exploration of utilizing a swarm of UAVs for network management in the 6th generation (6G) mobile communication

TABLE I: COMPARISON WITH EXISTING SURVEYS AND TUTORIALS

Research direction	Research field	Ref.	Main content	Limits
Management approach	Fault management	[27]	The cross-layer fault management problems and approaches in SDN.	It did not consider other management issues in SDN.
		[28]	Various frameworks to address faults in wireless sensor networks.	It did not explore the effectiveness of frameworks in dynamic environments.
	Configuration management	[29]	Utilizing a swarm of UAVs for network management.	The implementation scheme in complex configuration management was not considered.
		[30]	The QoS requirements for VANET and the existing QoS routing protocols.	The dynamic adjustment of configuration policies was not explored.
	Performance management	[31]	Monitoring network traffic and intent state to optimize network performance.	It did not examine scalability in large-scale dynamic networks.
		[32]	Selecting monitoring points and optimizing the location to improve network performance.	The possibility of dynamically adjusting monitoring points was not addressed.
	Security management	[33]	The network security situation awareness technology.	It did not explore adjusting defense strategies for new security threats.
		[34]	The automatic security configuration technology.	It did not discuss dealing with multi-level security policy conflicts.
Management protocol	Configuration	[36]	ANMP concept and three-layer management structure.	It did not discuss protocol performance in dynamic environments..
		[37]	The application and management functions of SNMP in IoT scenarios.	It did not consider the complexity of IoT scenarios.
	Policy	[18]	Policy refinement schemes in PBNM.	It did not explore adjusting the management policy dynamically.
		[38]	PBNM system offered automated policy implementation.	The policy conflict management and scalability issues were not considered.
	Intent	[35]	The latest developments and applications of IDN.	It did not explore the policy conflict handling and adjustment capabilities.
		[39]	IDNM approach achieves automated network management by transforming intents into implementable policies.	The deployment of IDNM in dynamic networks was not considered.

networks. Within VANETs, [30] provided an overview of key quality of service (QoS) requirements in VANETs and classified existing QoS routing protocols. However, it did not explore how to dynamically adjust the configuration policy to ensure QoS in resource-limited scenarios.

Regarding performance management, [31] explored how to improve the overall performance of the network by monitoring network traffic and intent states, detecting network performance bottlenecks and adopting reroute policies in the SDN environment. However, they did not examine scalability in large-scale dynamic networks. [32] studied select monitoring points in hybrid SDN network architecture to optimize the link delay measurement method, but adjusting monitoring points in a dynamic environment was not addressed. In security management, [33] reviewed network security situation awareness techniques covering the three stages: perception, understanding, and prediction. However, the ability to adapt to novel threats in real-time and self-learn was not discussed in detail. [34] reviewed the related technologies in network security configuration automation, covering firewall rule management and access control list (ACL) configuration to more advanced policy-based automatic security configuration methods. However, it did not discuss how to effectively deal with the multi-level security policy conflict or adapt the system in a dynamic environment.

Additionally, some literature reviews network management protocols, primarily including SNMP, PBNM, and IDNM. However, there is still lack of a comprehensive exploration of the concepts and classifications associated with these protocols. While authors in [35] summarized some management protocols, it was notable that these works did not conduct an exhaustive examination and reporting on the development of network management protocols. For instance, the ad hoc network management protocol (ANMP) was an SNMPv3-compatible one that employed clustering concepts and a three-layer management structure [36]. In the context of SNMP, [37] provided a comprehensive summary of the application and management functions of SNMP in internet of things (IoT) scenarios. SNMP is operated by polling device state information (such as CPU utilization, bandwidth usage, etc.) and transmitting these data to a centralized management platform while also enabling remote configuration and management of devices. However, as the number of IoT devices continued to increase and network structures became increasingly complex, the limitations of SNMP became more apparent.

With the evolution of intelligent systems, PBNM has become a well-known approach to address complex network management tasks. [18] reviewed existing policy refinemen-

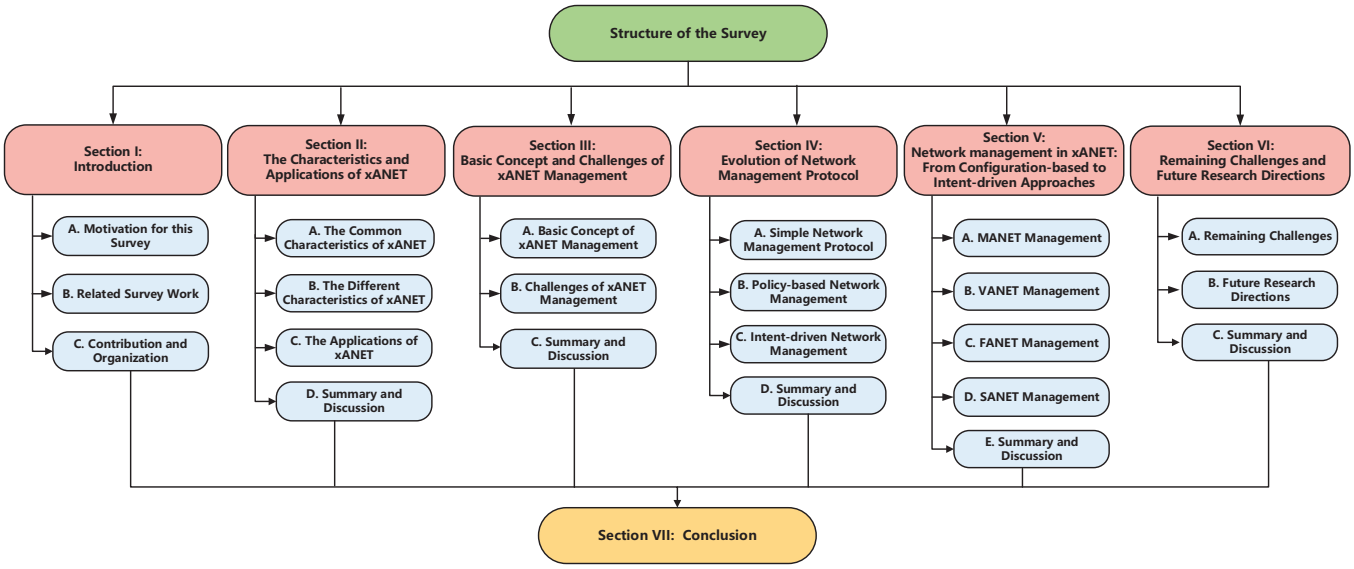

Fig. 1: Structure of this survey.

t schemes, categorizing them into rule-based transformation, classification-based refinement, case-based reasoning, and logic-based approaches. Described in [38] was a PBNM system specifically designed for ad hoc networks. This system offered the capability to express network requirements through high-level policies and automated implementation through intelligent agents in the network.

Furthermore, the emergence of IDN technology further elevates the intelligence of network management protocols. In [35], the authors summarized the latest developments and applications of IDN, extensively reviewing and classifying relevant works in the current research landscape. However, the application of IDN in network management was not deeply discussed. The intent was a user-expressible and understandable language form. As exemplified by [39], these high-level intents could map to multiple configuration policies. IDNM achieved automated network management by transforming intents into implementable policies and combining them with PBNM. IDNM, in terms of management paradigms and concepts, was a further development beyond PBNM.

As shown in Table I, we provide a comparative summary of the contents of existing surveys and tutorials. Although existing research has made progress in the field of xANETs management, there are still several shortcomings. First, most studies focus on isolated management issues, lacking in-depth exploration of the multi-dimensional and comprehensive management requirements in the complex and highly dynamic xANETs. Second, there is currently no survey that systematically reviews the evolution of existing management protocols. Most research emphasizes optimizing individual protocols or their application in specific scenarios. Current studies have yet to fully integrate the technical characteristics of xANETs to provide comprehensive technical assessments that can guide the design and development of next-generation network management protocols.

C. Contribution and Organization

As outlined in Section I-B, to address the aforementioned shortcomings, this survey presents the first systematic review of the characteristics and management requirements of xANETs. It provides an in-depth analysis of the complex challenges in xANETs management from the perspectives of fault management, configuration management, performance management, and security management. Furthermore, this survey explores the evolution of existing management protocols, including SNMP, PBNM, and IDNM, focusing on their technical transition towards automation and intelligent management. By synthesizing these research efforts, this survey establishes a theoretical foundation for developing future xANETs management protocols and offers strong support for the design and implementation of next-generation network management protocols. In particular, the main contributions of this work are the following:

- First, we systematically introduce the characteristics and applications of the xANET, including their common and different characteristics, as well as the applications of multiple xANETs coexisting.
- Second, the survey consolidates xANET management requirements from the perspectives of fault management, configuration management, performance management, and security management. It also extensively discusses the challenges currently faced by xANET management.
- Third, to address the aforementioned challenges, we investigate the developmental trajectory of the existing management protocols, encompassing SNMP, PBNM, and IDNM. We compare their architectures and concepts, illustrating their gradual evolution towards automation and intelligence.
- Fourth, we conduct a comprehensive survey of network management protocols in xANETs, evolving from configuration-based to policy-based and intent-driven approaches.

- Finally, we discuss the remaining challenges facing xANET management, including automation, cost-effectiveness, and QoS assurance, along with discussions on future research directions.

Fig. 1 gives the structure of this paper. In Section II, we introduce the characteristics and applications of the xANET. Then, in Section III, we summarize the basic concept and challenges of xANET management. Section IV highlights the evolution of network management protocols, including SNMP, PBNM, and IDNM. In Section V, we survey the management research for xANET, covering configuration-based, policy-based and intent-driven approaches. Section VI discusses remaining challenges and future research directions. Finally, we conclude this paper in Section VII.

II. The Characteristics and Applications of xANET

As an emerging network architecture, the space-air-ground integrated network necessitates high flexibility and adaptability, particularly in unplanned scenarios, where it must autonomously establish and maintain itself [40]. xANET has become an indispensable component within the space-air-ground integrated network. As illustrated in Fig. 2, xANET is subdivided into multiple sub-domains, including MANET, VANET, FANET, and SANET, according to the specific usage scenarios. In this Section, we introduce the characteristics and applications of xANET. By analyzing the characteristics of xANETs and the applications of multiple xANETs coexisting, network management can be implemented more effectively to ensure that specific communication requirements are effectively met. Section II-A summarizes the common characteristics of xANET, and Section II-B discusses the different characteristics of xANET. Furthermore, Section II-C considers the applications of xANET, and Section II-D summarizes and discusses this Section.

A. The Common Characteristics of xANET

As a self-organizing, decentralized, and multi-hop wireless network, xANET relies exclusively on the mutual coordination among nodes to achieve wireless connectivity. This communication framework discards the centralized structure present in conventional networks, creating a flexible and robust communication infrastructure [41]. While xANETs may exhibit diversity in various application scenarios, they collectively share some common characteristics that ensure the smoothness and reliability of network communication.

- Self-organization: xANETs exhibit the distinctive characteristic of self-organization, enabling nodes to collaborate autonomously and form a network without central control [42]. This decentralized capability allows the network to be dynamically established and reconfigured in real-time, at any location, and under diverse environmental conditions. Nodes can independently manage tasks such as routing, load balancing, and resource allocation, adapting to changes in network topology or node availability [43]. This attribute is particularly advantageous in rapid deployment scenarios like disaster recovery or military operations. It ensures seamless communication in highly dynamic and unpredictable environments, fulfilling robust, on-demand connectivity requirements.

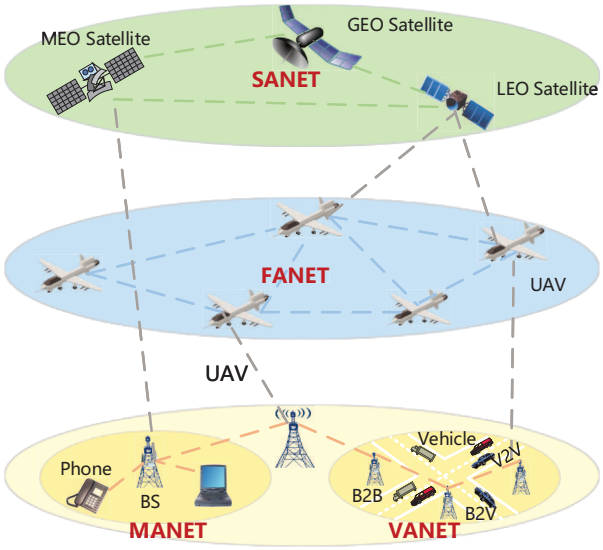

Fig. 2: Illustrations of xANET.

- Dynamics: xANETs are characterized by highly dynamic behavior, where nodes can join or leave the network flexibly and unpredictably. These nodes may move at varying speeds and follow different mobility patterns, leading to constant fluctuations in network topology [44]. The dynamic nature of xANETs results in frequent and unpredictable topology changes influenced by various factors such as node mobility, environmental conditions, and wireless channel variations. The constantly shifting topology affects key network parameters like link stability, communication paths, and bandwidth availability, making it difficult to predict the timing, frequency, and scale of these changes [45]. These dynamic variations necessitate adaptive routing protocols and real-time resource management to maintain reliable communication and optimize network performance under highly variable conditions.
- Multi-hop Communication: Multi-hop communication is a fundamental communication pattern in xANETs, where data is transmitted across multiple intermediate nodes to reach the destination [46]. Each node functions as both a source and relay, forwarding packets to neighboring nodes in a store-and-forward manner. This decentralized forwarding mechanism enables xANETs to extend communication beyond the direct transmission range of individual nodes, making the network highly adaptable in dynamic environments with frequently changing topologies [47]. The multi-hop architecture also provides fault tolerance. If some nodes move or go offline, alternative paths can be dynamically discovered and established using routing recovery or on-demand routing protocols, ensuring continuous connectivity.
- Distributed Network Control: In xANETs, nodes function simultaneously as hosts and routers, with each node having equal status within the network. A distributed

control approach allows nodes to make independent decisions, enabling each node to handle and forward data autonomously [14]. By using localized information and algorithms, nodes can autonomously manage routing tasks, dynamically adapting to changes in network conditions, such as node mobility or topology variations. This decentralized control mechanism significantly improves the network adaptability to frequent topology changes, as nodes can quickly recalculate routing in response to disruptions or mobility. The absence of a single point of failure makes xANETs inherently robust and resilient, ensuring that the network continues to operate effectively even when individual nodes fail, experience outages, or are compromised [48].

In conclusion, with their notable features, xANETs offer a flexible, adaptive, and robust solution in the field of communication. These features make xANETs particularly well-suited for dynamic and infrastructure-less environments. However, the heterogeneous nature of xANETs, encompassing various node types with differing capabilities and application-specific requirements, introduces unique challenges. To ensure optimal performance, adjustments to routing strategies, resource management protocols, and security mechanisms must be made to address the specific requirements of each application environment.

B. The Different Characteristics of xANET

Due to the diverse node types and extensive application scenarios covered by xANETs, they exhibit varied and distinctive features. The heterogeneous nature of nodes, with varying capabilities in terms of mobility, power, and computational resources, combined with the diverse operational environments, enables xANETs to adapt dynamically to different domains and complex environments [49].

1) MANET: As a type of ground network, MANET refers to a network where mobile wireless nodes connect in a self-organizing manner within their communication range without relying on fixed infrastructure for communication [50]. Each node in the network operates both as a host and a router, enabling it to dynamically forward data to other nodes while maintaining its communication capabilities [51]. This decentralized approach allows MANETs to adapt to topology and node mobility changes, making them suitable for various applications, such as emergency response operations, military communications, and remote area networking, where traditional infrastructure may be unavailable or impractical. In comparison to conventional wireless communication networks, MANET exhibits the following characteristics.

- Short Network Survival Time: MANET is primarily used to fulfill temporary communication requirements, where the network is dynamically formed to support ad hoc communication for a specific duration or task [52]. Once the usage is complete, the network environment is automatically dismantled. Therefore, the survival time of MANET is relatively short compared to other networks. The survival time of MANET is heavily influenced by factors such as node mobility, battery life, and the overall mission duration, which directly impact the network ability to maintain connectivity and sustain operation [53].
- Resource Constraints: The MANET terminals often include small, lightweight devices such as portable computers, handheld devices, or smartphones. These mobile terminals generally have limited system resources, including constrained memory and low processing power, which can impact their ability to handle large-scale data processing or complex computations [54]. Additionally, these terminals typically rely on consumable energy sources, such as batteries, which introduce further challenges in terms of energy efficiency and network longevity [55]. The reliance on battery power necessitates energy management policies, as the depletion of energy resources can lead to node failures, ultimately affecting the network overall performance, connectivity, and operational lifespan.

2) VANET: VANET is a specific form of MANET in which vehicles serve as mobile nodes operating within road traffic environments. While VANETs share general characteristics with conventional wireless networks, such as decentralization, distributed architecture, self-organization, scalability, and the ability to form temporary, flexible networks, they also exhibit unique characteristics due to their specific operational scenarios that differ from the MANET [56].

- Rich Sensing Information: Vehicles in VANETs are equipped with various sensors that provide valuable auxiliary information to enhance network functionality [57]. These sensors, in conjunction with advanced technologies such as global positioning system (GPS) and geographic information system (GIS), allow nodes to acquire precise data about their geographic location, speed, and direction, as well as real-time road conditions [58]. Integrating sensor data and geographic technologies is critical in enabling location-based services, improving routing efficiency, and supporting safety applications. By leveraging this rich data set, VANETs can deliver more reliable and context-aware communication, enhancing overall network performance in vehicular environments.
- Low Energy Constraint: VANET nodes benefit from the onboard power sources of vehicles, effectively eliminating the typical energy constraints found in other types of xANETs [59]. As vehicles are powered by their engines, they can continuously generate the necessary electrical power to support network operations. This abundant power supply allows VANET nodes to operate without the need for energy-saving mechanisms, which are often critical in battery-powered networks like MANETs [60]. Consequently, energy consumption is a less significant factor in the design of VANET protocols, allowing the focus to shift toward optimizing other performance aspects such as communication reliability, low latency, and high data throughput.
- Predictable Motion Trajectories: The operating environment for VANETs is primarily urban roadways, where the road network structure constrains vehicle movement. This results in relatively predictable mobility patterns [61]. Moreover, using vehicle-mounted GPS devices and

advanced navigation software enables the accurate prediction of a vehicle trajectory, destination, speed, and direction [62]. These tools provide real-time data that allow network protocols to anticipate node movements, optimize routing decisions, and improve communication efficiency.

3) FANET: FANET is a specialized type of aerial network consisting of a multi-hop MANET architecture formed by a cluster of UAVs. With its exceptional scalability and resilience, FANET enables efficient information sharing and coordination among network nodes, making it highly suitable for dynamic and complex environments such as battlefields or disaster response scenarios [63]. While FANET shares common characteristics with MANETs, it introduces unique demands due to the highly maneuverable nature of UAV nodes.

- Limited Node Energy: Most small and medium-sized UAVs in FANET are powered by batteries with limited energy storage capacity [64]. Given the relatively low energy density of current battery technologies and the constrained payload capacity of these UAVs, their operational flight time is significantly restricted [65]. The energy constraints directly affect the UAVs ability to maintain network connectivity, perform multi-hop relays, and execute complex maneuvers. As a result, energy consumption and management become key considerations in FANET management protocol design, influencing decisions on flight path optimization, duty cycling of nodes, and power-efficient communication policies.
- Limited Communication Bandwidth: In FANET, wireless communication quality is susceptible to noise, collisions, and routing control overhead. These factors can degrade the performance of the network and reduce the available communication bandwidth to levels lower than theoretical maximums [66]. Under heavy network loads, these issues can lead to congestion, packet loss, and increased latency, severely impacting data transmission reliability and throughput among UAVs. Consequently, it is necessary to develop robust congestion control mechanisms, efficient routing protocols, and adaptive communication strategies to ensure smooth and reliable data exchange in such environments.
- Real-time Data Transmission: The multi-hop transmission characteristic of FANETs can lead to various interferences during data transmission, such as signal fading, collisions, and increased routing overhead [67]. These interferences can result in packet delays and significant latency. However, achieving low-latency data transmission in FANET is crucial for effectively using UAVs in applications [68]. FANETs need optimized management protocols to meet these requirements that minimize delay, enhance route stability, and reduce overhead.

4) SANET: As a crucial form in space-based networking, SANET is a self-organizing network of interconnected satellites designed to facilitate wide-area communication in space [69]. SANET offers global coverage, enabling communication across distant and remote locations to meet diverse communication requirements [70]. SANET provides a reliable global communication solution for various applications, including scientific research, military communication, and global internet connectivity. Maintaining continuous, high-bandwidth communication makes it an essential solution for scenarios requiring persistent global coverage and robust data transmission across large geographical areas [71].

- Wide Coverage: While ground networks have rapidly developed, they are limited to only 20% of the Earth's land area and 5% of the ocean area [72]. In contrast, SANETs typically consist of dozens or even hundreds of satellites in various orbits, providing global coverage [73]. This makes SANET suitable for applications that require communication in remote or disaster-stricken areas. By leveraging the advantages of satellite technology, SANETs can maintain connectivity where terrestrial infrastructure is inadequate or non-existent, facilitating essential services such as emergency response, remote sensing, and global data access, even in challenging environments.
- Diverse Applications: With the advancement of information technology, conventional ground networks have become insufficient to meet information demands for reliable and high-speed communication. SANETs have gradually entered various emerging fields, providing crucial technical support for applications such as satellite navigation, space target observation, information transmission, and deep space exploration [74]. By utilizing advanced satellite constellations and innovative networking protocols, SANETs enable efficient data exchange and enhance operational capabilities [75].
- High Communication Latency: SANETs often encounter longer communication delays than terrestrial networks due to the distance between satellites. The delay in satellite systems can be divided into fixed delay and dynamic delay [76]. Specifically, for every 1000 km increase in satellite altitude, the one-way delay for a single hop increases by 20ms [77]. This latency can accumulate in multi-hop communication scenarios, leading to increased end-to-end delays that must be carefully managed to ensure the effectiveness of time-sensitive applications, such as real-time data transmission and remote sensing operations.

These diverse forms of xANETs collectively constitute the core components of the space-air-ground integrated network system. They provide essential and crucial support for achieving highly flexible and adaptive communication, ensuring the stable operation of the network in diverse and dynamic environments. Although these networks share some common characteristics, such as decentralization, dynamic topology, and autonomy, their differences arise from the scenarios and applications they face. Specifically, as illustrated in Table II, a deeper understanding of their similarities and differences can be gained by comparing their features.

C. The Applications of xANET

As task requirements become increasingly complex, the coexistence of various types of xANET is crucial for effective mission execution [78]. For instance, in surveillance tasks, the

TABLE II: THE COMPARISON OF MANET, VANET, FANET AND SANET

Network type	MANET	VANET	FANET	SANET
Overview	Mobile nodes establish connections.	Vehicles are mobile nodes.	UAVs are mobile nodes.	Satellites are mobile nodes.
Node type	Mobile node	Vehicle node	UAV node	Satellite node
Node mobility	Low	Medium to high	High	Low
Mobile model	Random movement model.	Regular movement model.	The conventional model and the special movement model.	The satellite moves along a predefined orbital path.
Node density	Low	High	Very low	Very low
Topological change rate	Slow	Fast	Fast	Slow
Radio propagation model	Line of sight (LoS) may not be accessible near the ground.	LoS may not be accessible when close to the ground.	LoS is accessible for most cases when higher than the ground.	LoS is accessible for most cases in orbit.
Energy limit	Most nodes are battery-powered and need to consider energy saving.	Most nodes are powered by vehicles with low energy constraints.	Small UAVs have power consumption limitations.	Nodes are powered by solar panels or sustainable energy sources.
Calculate ability	High	High	Limited	High
Node positioning	GPS	GPS, assisted global positioning system (AGPS), difference global positioning system (DGPS)	GPS, AGPS, DGPS, inertial measurement unit (IMU)	GPS
Service type support	Military communications, emergency rescue, field survey.	Traffic management, vehicle safety, intelligent transportation.	UAV monitoring, surveying, agriculture, logistics.	Scientific research, military communications, global Internet.

collaboration between FANET and MANET achieves comprehensive coverage of target areas and facilitates real-time data transmission through low-latency wireless links. The rapid deployment capabilities of FANET allow it to adapt flexibly to dynamic environments, such as those encountered in disaster response or military operations. At the same time, MANET establishes stable communication links among ground nodes, ensuring swift data aggregation and processing [79].

Moreover, in specific communication tasks, the integration of SANET with FANET leverages the broad coverage offered by satellites alongside the agility of UAVs to ensure efficient information transfer [80]. The global perspective satellites enable data to be transmitted over extensive geographic regions. At the same time, FANET can quickly adjust to complex terrains, ensuring rapid data flow between network edges and centralized nodes. This coexistence model enhances network robustness and improves mission flexibility and responsiveness.

By fully utilizing the unique functionalities provided by different xANETs, this coexistence approach allows for a more comprehensive methodology in task management, addressing diverse operational requirements. However, this diversified coexistence also presents a series of technical challenges for network management.

- Interoperability Issues: The differences in protocols, standards, and communication mechanisms among various xANETs pose significant challenges in achieving seamless communication [81]. Developing robust interfaces and integration strategies is essential to ensure compatibility and collaboration among different systems.
- Resource Management Complexity: Coordinating resource allocation among multiple xANETs can lead to resource conflicts and inefficiencies [82]. Effective resource management strategies must be implemented to optimize the utilization of shared resources, such as bandwidth, power, and computational capabilities.
- Management Overhead: The complexity of managing multiple types of xANET can significantly increase operational costs [83]. Network administrators should develop advanced management tools and strategies to effectively monitor and control these heterogeneous systems.

The coexistence of various xANETs is becoming increasingly vital for meeting the demands of complex tasks. However, this also introduces unique technical challenges that must be addressed through effective network management strategies to ensure optimal performance and security. By leveraging innovative solutions and technological advancements, the full potential of xANET can be realized, leading to more efficient and reliable task execution.

D. Summary and Discussion

Depending on the specific application scenarios, different types of xANETs exhibit distinct characteristics and functional

requirements, with variations in aspects such as calculating ability and network topology. This section summarizes the common and different characteristics of various types of xANETs and discusses the applications of multiple xANETs coexisting. Analyzing these characteristics provides a foundation for identifying the challenges faced in xANET management, laying the groundwork for addressing these challenges effectively.

III. Basic Concept and Challenges of xANET Management

The characteristics of xANET and its wide range of application scenarios clarify the functions of xANET management and introduce a series of challenges to network management. This Section delves into the basic concepts and challenges of xANET management. Section III-A summarizes the basic concept of xANET management in terms of fault management, performance management, security management, and configuration management. Section III-B discusses the challenges of xANET management based on the characteristics and management concepts of xANET. Section III-C summarizes and discusses this Section.

A. Basic Concept of xANET Management

Network management is an exceedingly complex and challenging task involving diverse tasks, depending on the specific application. The ISO/IEC 7498-4 document defines five fundamental functions of network management known as FCAPS management, which includes fault management, configuration management, accounting management, performance management, and security management [84]. In the case of xANET, its design aim is to facilitate dynamic, self-organizing communication between nodes rather than pursuing commercial objectives. Given the constant changes in network topology, dynamic additions and departures of nodes, and limitations in resources and wireless transmission, the management focus is predominantly on fault management, configuration management, performance management, and security management [85].

It is important to note that resource and energy management are critical components that intersect with these four management areas [86][87]. For instance, effective resource management falls under performance management, which involves optimizing bandwidth and computational resources to enhance overall network efficiency. Similarly, energy management can be considered part of configuration and performance management, where configuring network parameters to minimize energy consumption helps sustain the operation of energy-constrained devices. Therefore, while we primarily emphasize fault management, configuration management, performance management, and security management, we acknowledge that resource and energy management are essential for effectively operating xANETs in unstable environments, safeguarding communication security and enhancing network performance.

1) MANET Management: The management of MANETs involves the effective monitoring, control, and optimization of various aspects. This encompasses activities aimed at ensuring the stability and performance of MANET to meet diverse communication requirements. Due to the unique characteristics of MANET, such as node mobility, dynamic network topology, and limited resources, network management in this environment becomes inherently more intricate.

- Fault Management: Nodes connect and disconnect more frequently in MANET, so rapid fault detection and recovery are critical. Critical indicators involve the time required to identify faults, the network downtime length, and the fault recovery effectiveness [88]. Automatic routing recalculation is one of the possible solutions, as it helps identify alternate paths, and continuous monitoring of node states enables quick detection and isolation of failures. Furthermore, fault management leverages resource management by reassigning resources, such as bandwidth and power, from failed nodes to nearby nodes, optimizing network resilience under dynamic conditions [89].
- Performance Management: Performance management aims to optimize MANET operations by ensuring efficient data transmission and resource utilization. Throughput, delay, and packet delivery rates are among the essential performance indicators [90]. Solutions encompass network topology monitoring to track node locations and connectivity, allowing adaptive routing path adjustments. In addition, performance management involves resource allocation, balancing bandwidth among nodes to meet varying communication requirements, and energy management policy to maintain network connectivity over longer durations [91]. For example, energy-aware routing protocols adjust paths based on node battery levels, preventing network segments from becoming isolated due to node depletion [92].
- Configuration Management: Configuration management ensures that nodes are set up to meet specific tasks and environmental conditions. Evaluating metrics include the duration of configuration processes, adaptability to dynamic conditions, and efficient resource usage [93]. Autoconfiguration protocols are part of the solutions, allowing nodes to dynamically acquire configuration parameters based on the current state of the network [94]. Configuration management allocates bandwidth and power based on node roles and network requirements, optimizing MANET's ability to respond to fluctuating demands. Resource-aware configuration protocols help balance the network load, adjusting bandwidth and power distribution to avoid bottlenecks and improve overall efficiency [95].
- Security Management: MANET faces threats like malicious attacks, eavesdropping and data tampering. Security management employs multi-layered strategies, with key performance metrics including response time to security breaches, data integrity rates, and system availability [96]. Solutions include encryption to ensure data confidentiality, authentication methods to verify node legitimacy, and access control mechanisms to restrict unauthorized connections [97]. Resource and energy management are also integral. For instance, energy-efficient encryption

protocols are deployed to conserve node battery while providing necessary security, helping ensure data integrity and confidentiality without compromising the network's connectivity and resource availability [98].

2) VANET Management: VANET management encompasses managing various resources, services, and communication processes within the network. Its primary objective is to ensure the stability and performance of the communication network between vehicles and roadside units, meeting the operational requirements for urban traffic and road safety.

- Fault Management: The dynamic nature of vehicle movement leads to frequent connections and disconnections, necessitating efficient fault management. Key indicators include the time to detect faults, the accuracy of localization, and the length of service interruptions [99]. Possible solutions include real-time monitoring of network topology to identify faults and utilizing efficient resource reallocation to redirect energy and bandwidth to maintain communication continuity [100]. For instance, if a roadside unit loses connectivity, neighboring units may redirect energy resources or extend their transmission range temporarily to cover the affected area, supporting critical tasks like cooperative driving and real-time traffic updates [101].
- Performance Management: Performance management ensures that the VANET provides high-quality services under all conditions to ensure efficient data transmission and resource utilization. Significant metrics for evaluation include how effectively bandwidth is used, the level of delay, overall throughput, and packet delivery success [102]. Performance management begins with monitoring changes in network topology to gain insights into vehicle locations and connectivity relationships. By implementing real-time monitoring systems, performance issues can be swiftly identified, allowing timely interventions [103]. Actions may include optimizing routing paths, increasing bandwidth, or dynamically adjusting resource allocation to resolve identified bottlenecks, ultimately enhancing the network's efficiency and responsiveness.
- Configuration Management: Effective configuration management ensures the correct and efficient setup of vehicles and nodes in VANET, which includes managing energy-efficient communication parameters to minimize power consumption and avoid conflicts. Performance indicators for configuration management may involve the time required for setup, uniformity across nodes, and the occurrence of errors [104]. Centralizing settings ensures uniformity in critical network parameters and reduces configuration error risk. Additionally, automatic configuration protocols help balance resource allocation based on network demands [105]. By maintaining configuration backups and setting up energy-saving modes for low-priority vehicles, the network can enhance availability and ensure critical services remain operational [106].
- Security Management: Security management in VANETs protects against unauthorized access and malicious activities, such as disinformation and denial-of-service (DoS) attacks [107]. Important performance metrics include response time to security incidents, false positive rates, and system availability [108]. By integrating resource management into security protocols, such as limiting bandwidth for unverified nodes or temporarily lowering transmission power, VANET can reduce vulnerabilities while conserving energy. Real-time traffic monitoring helps identify suspicious activities early, allowing for rapid response and the reallocation of energy resources. Security policies are continuously updated, integrating resource-saving measures to adapt to evolving security needs without compromising network sustainability [109].

3) FANET Management: FANET management involves the comprehensive administration of routing and path optimization, sensor data management, UAV status monitoring, and flight plan management. Due to the dynamic nature of UAVs, effective network management necessitates the continuous and adaptive adjustment of routing protocols and data transmission optimization based on the UAV positions, mission requirements and current environmental conditions.

- Fault Management: Faults can occur at all levels, from hardware failures to communication link problems, potentially impacting mission execution. System performance can be gauged through fault detection speed, recovery duration, and availability. This process involves automated monitoring of UAV status and communication links to ground stations or other UAVs [110]. By employing real-time monitoring systems, the exact location of the failure can be determined, and the cause analyzed. Flight path adjustments or switching to alternate communication links can be employed as solutions to maintain mission continuity. Additionally, effective resource management helps reallocate available bandwidth and processing capabilities during fault recovery, ensuring that critical communications can continue uninterrupted [111].
- Performance Management: Performance management focuses on optimizing the efficiency and performance of the FANET. Essential performance measures include altitude stability, speed consistency, throughput, and latency. Continuous monitoring of flight performance enables the assessment of UAV flight status, such as altitude, speed, attitude stability, and hovering ability [112]. This data is vital for planning optimal routing to ensure the UAV operates at peak performance while executing its mission [113]. Furthermore, to improve real-time performance, performance management also includes optimizing data transmission and energy management policies, ensuring critical information is delivered to designated locations as quickly as possible, minimizing energy consumption and prolonging the UAV's operational endurance [114].
- Configuration Management: FANETs require dynamic configuration of UAV flight plans, sensor settings, and communication parameters based on mission requirements and environmental conditions. Metrics such as configuration precision, responsiveness to environmental changes, and resource utilization efficiency are impor-

tant [115]. For instance, the UAV flight plan may need frequent adjustments in search and rescue missions to effectively cover a specific area [116]. Configuration management can be achieved remotely, allowing for real-time adjustments of UAV settings and parameters during flight. This dynamic configuration ensures that UAVs can adapt to changing mission objectives and optimizes resource utilization.

- Security Management: The security management of FANET encompasses identity authentication and access control, key management, and data encryption [117]. Crucial metrics for security include the frequency of unauthorized access attempts, the speed of responses to incidents, and the reliability of data integrity during transmission. Identity authentication and access control aim to prevent unauthorized nodes from joining the network [118]. Key management is responsible for generating, distributing, updating, and revoking keys, thus facilitating secure communication in dynamic environments [119]. Data encryption uses lightweight encryption algorithms to prevent data theft and tampering [120]. The FANET security management system enhances resilience, security, and self-healing capabilities in complex and dynamic environments by integrating advanced technologies such as blockchain and AI.

4) SANET Management: SANET management encompasses global resource allocation, optimization of delay-sensitive applications, bandwidth management, and security monitoring of communication links. Network management should optimize data transmission paths for delay-sensitive applications to reduce latency.

- Fault Management: Satellites may encounter failures such as space radiation and collision threats, leading to communication interruptions and functional anomalies. Evaluating performance involves measuring the time taken for fault detection, recovery efficiency, and periods of communication downtime. Fault management involves real-time monitoring of satellite status and communication link stability and identifying and locating faults [121]. In the event of a failure, the system must automatically switch to backup satellites or adjust communication paths to ensure continuity of communication. Research has shown that machine learning (ML) techniques can enhance fault detection and diagnosis capabilities in satellite systems. By analyzing satellite telemetry data, machine learning algorithms can automatically detect abnormal behaviors, thereby reducing reliance on manual monitoring and improving the efficiency and accuracy of fault management [122].
- Performance Management: SANETs require continuous monitoring of satellite performance and resource utilization, measuring parameters such as latency, bandwidth utilization and signal strength [123]. Significant performance indicators are throughput levels, the rate of packet loss, and energy consumption efficiency. Performance management is crucial in identifying resource bottlenecks, optimizing resource allocation, and enhancing network efficiency. Furthermore, it facilitates energy management by ensuring that satellite operations are energy-efficient, prolonging satellite lifespan and optimizing operational costs [124]. By monitoring and improving performance indicators, this management policy not only enhances user experience but also ensures the reliability and speed of data transmission.
- Configuration Management: Satellite and terminal equipment configurations may change frequently to adapt to various tasks and communication requirements. Configuration management ensures that these configurations are correct and consistent to meet communication requirements [125]. This requires flexible configuration management tools and automation techniques for fast and accurate configuration changes. Key indicators include the precision of configurations, system responsiveness to modifications, and the optimal utilization of resources. Additionally, resource management is essential to dynamically allocate configuration settings based on real-time usage and operational requirements, ensuring efficient resource utilization across the network [126].
- Security Management: SANET communication involves sensitive information, making security management paramount. Security management includes authentication mechanisms to ensure that only legitimate users and devices can access the network, thereby limiting the resources and operations available to users and preventing unauthorized access [127]. It also requires ongoing monitoring for potential intrusions and malicious attacks, and implementing defensive measures to protect the network. Moreover, energy management practices must be integrated into security protocols to ensure that security measures do not excessively drain satellite resources, thus maintaining overall operational integrity [24].

5) Summary and Discussion: As illustrated in Table III, different types of xANETs have distinct requirements, performance metrics, and solution approaches regarding fault management, performance management, configuration management, and security management. Appropriate management policies should be devised in practical applications based on specific network requirements and operational environments, with their effectiveness evaluated using key performance metrics. These solution approaches collectively aim to enhance the reliability, performance, adaptability, and security of xANETs, ensuring stable network operation in complex and dynamic environments while meeting the diverse communication quality demands of various application scenarios.

B. Challenges of xANET Management

As highlighted in the preceding sections, xANETs are inherently highly dynamic and formed through wireless links. Due to the mobility of nodes, these wireless links are susceptible to failures, or connections may be lost due to fluctuating wireless links. Consequently, the management of xANETs confronts numerous challenges.

1) MANET Management: The high mobility of nodes and the dynamic evolution of the topology in MANETs make conventional network management methods challenging to apply

TABLE III: xANETs MANAGEMENT REQUIREMENTS

Management type		Fault management	Configuration management	Performance management	Security management
MANET	**Requirements**	Rapid fault detection and recovery.	Ensure that the node configuration meets the task and environment.	Ensure efficient data transmission and resource utilization.	Prevent malicious attacks, eavesdropping and data tampering.
	Performance metrics	Fault identification time, network downtime, fault recovery efficiency.	Configuration duration, adaptability, resource utilization.	Throughput, delay, packet delivery rate.	Response time to breaches, data integrity rates, and system availability.
	Solution approaches	Routing recalculation, continuous monitoring, resource reassignment.	Autoconfiguration protocols, resource allocation.	Network topology monitoring, resource allocation.	Encryption, authentication, access control.
VANET	**Requirements**	Avoid frequent connections and disconnections.	Manage node parameters and automatic configuration.	Ensure high-quality services and efficient data transmission.	Prevent unauthorized access and malicious activities.
	Performance metrics	Fault detection time, localization accuracy, service interruption length.	Setup time, uniformity, and error occurrence.	Bandwidth utilization, delay, throughput, and packet delivery success.	Response time to incidents, false positive rates, and system availability.
	Solution approaches	Real-time monitoring, resource reallocation.	Centralized settings, automatic configuration protocols.	Real-time monitoring, optimized routing, dynamic resource allocation.	Resource allocation, real-time traffic monitoring, updated security policies.
FANET	**Requirements**	Avoid hardware failure, communication link problems.	Dynamic configuration of UAV flight plans, sensor settings, and parameters.	Optimize the efficiency and performance of the FANET.	Implement identity authentication, access control, and data encryption.
	Performance metrics	Fault detection speed, recovery duration, overall availability.	Configuration precision, responsiveness, resource utilization.	Altitude stability, speed consistency, throughput, latency.	Frequency of unauthorized access attempts, response speed, data integrity.
	Solution approaches	Real-time monitoring, flight path adjustment, resource reallocation.	Remote real-time adjustments based on mission requirements.	Flight performance monitoring, optimized routing, and energy management policies.	Blockchain, AI, lightweight encryption algorithms.
SANET	**Requirements**	Avoid communication interruption and functional anomalies.	Frequent configuration changes to adapt to the requirements.	Ensure the reliability and speed of data transmission.	Avoid loss of sensitive information.
	Performance metrics	Fault detection time, recovery efficiency, communication downtime.	Configuration precision, system responsiveness, resource utilization.	Latency, bandwidth utilization, signal strength, packet loss rate, energy consumption.	Unauthorized access attempt.
	Solution approaches	Real-time monitoring, backup satellite switching, ML-based fault detection.	Flexible configuration tools, automation techniques, and dynamic resource allocation.	Resource bottleneck identification, energy-efficient operations.	Authentication mechanisms, intrusion monitoring, energy-efficient security measures.

directly [55]. Therefore, innovative management solutions are necessary for MANET management to adapt to the continuously changing environment, ensuring stability, performance, and security. Addressing these challenges requires a deep understanding of node mobility, dynamic topology changes, and limited resources. It is important to adopt flexible and adaptive management policies to maintain effective communication in MANETs.

- Node Mobility: The emergence of 6G networks introduces unprecedented requirements for ultra-low latency and enhanced reliability, aiming to support an array of high-demand applications [129]. However, in the context of MANETs, high-speed node movement leads to frequent changes in network topology, complicating stable links' maintenance. While 6G technologies bring advanced features, including high-precision positioning and rapid handover capabilities, sustaining continuous, reliable communication remains a formidable task in such highly dynamic environments [130]. Therefore, MANET management systems need capabilities for real-time monitoring and adaptive topology adjustments to ensure the network remains functional and resilient across complex

scenarios.

- Resource Optimization: Massive connectivity of 6G significantly amplifies the resource management demands in MANETs, especially within ultra-dense environments [131]. The computational and energy resources of MANET nodes are typically limited, creating a need for efficient and adaptive resource allocation. While 6G introduces capabilities like edge computing and resource virtualization to enhance resource management, the frequent changes in node availability and the potential for resource conflicts among nodes add complexity to resource allocation and management [132]. Therefore, MANET management systems should have fine-grained spectrum and computational resource management capabilities.
- Security and Privacy: While 6G introduces advanced security technologies, such as quantum key distribution, distributed authentication, and error recovery mechanisms, the decentralized and self-organizing nature of MANETs still exposes nodes to potential threats [133]. Frequent topology changes and the lack of fixed infrastructure mean that security measures should be adaptable and distributed across the network. To safeguard communication in this dynamic environment, MANET management approaches should implement dynamic, distributed security policy updating that responds in real time to changes in network topology.
- Automation and Intelligence: In highly dynamic environments, MANETs are inherently difficult to manage manually due to their decentralized nature and frequent topology changes. AI-enhanced technologies offer critical support for automation, minimizing the need for human intervention [134]. However, given the unstructured data and complex, rapidly evolving network topologies, MANET management approaches should achieve high precision and stability in self-organization and automated decision-making [135]. To ensure effective operation, these management approaches should dynamically adjust communication parameters and resource allocations in response to real-time network changes.

2) VANET Management: The high speed of vehicles and the real-time requirements in VANETs present significant challenges for network management. Effectively managing VANETs requires addressing the continuous changes in vehicle positions while ensuring stable communication connections, real-time data transmission, and security. While 6G introduces enhanced connectivity, ultra-low latency, and AI-driven adaptability, managing VANETs requires ongoing attention to specific challenges.

- High-speed Mobility: The rapid movement of vehicles on highways requires instantaneous transmission of traffic information and robust safety mechanisms. Although 6G provides low latency and improved handover techniques, the challenge of maintaining stable communication links remains critical [136]. A fast and reliable communication management mechanism is essential, as even brief communication interruptions may lead to severe disruptions. Therefore, network management approaches should implement robust strategies to ensure continuous connectivity and real-time data integrity in high-speed scenarios.
- High-Density Environments: In urban settings, the dense concentration of vehicles heightens the risk of signal interference and resource contention. While 6G offers advanced spectrum sharing and interference management technologies, the challenge of effectively managing these resources in high-density scenarios persists [137]. Ensuring reliable and efficient data transmission amidst competing signals and potential congestion requires innovative spectrum allocation strategies and adaptive interference suppression techniques.
- Automated Management: The dynamic nature of VANETs, characterized by the continuous influx and departure of vehicles, complicates manual network management. Even with the automation capabilities provided by 6G, the complexity of real-time configuration management remains a challenge [138]. The management system must adapt to rapidly changing network conditions, ensuring seamless integration of new vehicles and consistent network performance. Practical automated configuration tools are essential for maintaining network continuity and optimizing resource use in this evolving environment.

3) FANET Management: The dynamic changes in communication topology and the real-time task requirements of UAVs render network management exceptionally complex in FANETs. Effectively managing FANETs necessitates overcoming the continuous changes in UAV positions and addressing dynamic relationships among UAVs, all while ensuring network stability, communication reliability, and adaptability to aerial environments.

- Three-dimensional Dynamic Topology: The three-dimensional movement of UAVs complicates network management due to frequent changes in position and orientation. While 6G enhances positioning accuracy and communication capabilities, the challenge of real-time fault management remains [139]. Continuous monitoring of UAV positions, speeds, and altitudes will still be essential, and effective communication path adjustments must be made based on mission requirements. The need for fast fault detection and recovery mechanisms persists, as any disruption in connectivity can have critical implications for mission success.
- Real-time Communication and Dynamism: The dynamism and operational diversity of UAVs require advanced network management for real-time path planning and rapid configuration adjustments. Although 6G supports ultra-low latency communication, the challenge lies in maintaining efficient data transmission under various flight conditions [140]. Performance management must evolve to address the complexities introduced by dynamic environments and changing operational demands.
- Security and Privacy: The sensitive nature of data involved in UAV missions underscores ongoing security challenges. While 6G brings enhanced security features, the risk of unauthorized access and data leakage still exists. Robust measures such as advanced encryption,

secure data transmission, and strong UAV identity authentication will continue to be critical for protecting sensitive information, particularly as threats evolve in increasingly complex operational landscapes [141].

- Automated Management: As FANETs grow more complex with the integration of more UAVs, automated network management capabilities will be essential. Although 6G introduces AI-driven tools for autonomous path planning and fault recovery, the challenge of adapting to dynamic environmental conditions and diverse task requirements remains [142]. Management systems must intelligently respond to changes in real time, ensuring continuity and performance without excessive reliance on manual intervention.

4) SANET Management: Global resource allocation, dynamic satellite orbits, and complex communication links contribute to the complexity of SANET management. Effectively managing SANETs requires overcoming continuous changes in satellite positions and orbits while ensuring communication stability on a global scale, optimizing delay-sensitive applications, and ensuring the security of communication links [143].

- Link Stability: The dynamic nature of satellite positions and environmental conditions significantly impacts communication links. While 6G enhances positioning accuracy and communication protocols, real-time monitoring of satellite trajectories and automated switching capabilities remain essential for ensuring link stability [144]. Continuous communication is critical for both fault management and performance optimization, particularly in scenarios where satellite movements can disrupt established connections.
- Dynamic Configuration Management: Different geographical regions and mission requirements necessitate adaptable network configurations. The ability to remotely and dynamically adjust configurations to meet evolving communication demands is vital for reducing manual intervention and enhancing network responsiveness, especially in rapidly changing operational environments.
- Performance Optimization: Effective real-time bandwidth management, route optimization, and data compression techniques are essential to maximize satellite resource utilization. Although 6G introduces improved communication capabilities, the ongoing challenge lies in ensuring efficient and reliable data transmission across diverse applications, particularly those sensitive to latency [145]. Optimizing performance in real-time remains a critical aspect of SANET management.
- Security and Privacy: The transmission of sensitive data within SANETs necessitates robust security measures. As 6G networks introduce enhanced security protocols, the need for comprehensive security management remains. Key measures such as data encryption, identity authentication, access control, and advanced defensive technologies are crucial for protecting data integrity and maintaining user privacy in satellite communications [146].
- Automation and Intelligence: SANETs require automated capabilities for state monitoring, satellite switching, configuration management, performance optimization, and security control [147]. While 6G facilitates greater automation, the ongoing challenge is to ensure that these systems can reliably adapt to various environments and mission requirements. The integration of AI-driven decision-making tools will be essential for enhancing network reliability and efficiency in the face of complex operational dynamics.

5) Summary and Discussion: As outlined above, the core challenges of managing xANETs encompass several aspects. First, the dynamic nature of the network poses significant challenges, as the frequent movement of nodes and continuous changes in network topology require the management approach to be highly adaptable and flexible. Second, real-time responsiveness and reliability are critical, particularly in mission-critical scenarios where the network must quickly react to changes and ensure accurate and timely data transmission. Additionally, efficient resource utilization is another key challenge. The limited spectrum, bandwidth, and energy resources in xANETs must be efficiently allocated and optimized to ensure long-term network stability. Lastly, scalability is also a core challenge in managing xANETs. As the number of nodes increases, network management approaches should provide robust scalability to handle the complexity and demands of large-scale networks.

C. Summary and Discussion

In this section, we introduce the basic concepts of xANETs management and the numerous challenges it faces. Our analysis reveals that the key issues xANETs management protocols must address include efficient collection of network management information, real-time topology updates, and automated handling of dynamic network configurations. To effectively address these challenges, new network management approaches must be adopted. These approaches should not only feature efficient data collection and adaptive processing mechanisms but also possess robust real-time decision-making capabilities. This will enable xANETs management systems to rapidly adjust in response to constantly changing network conditions, ensuring the stability and efficiency of communications.

IV. Evolution of network management protocol

The dynamic, distributed, and wireless characteristics of xANET pose several challenges to the most commonly used network management protocol, SNMP. Recent efforts have presented different types of management protocols. In this Section, we summarize these network management protocols, including SNMP, PBNM, and IDNM. For each protocol, we introduce its architecture and concepts. At the same time, the advantages and disadvantages of each protocol are analyzed based on the xANET scenario. Fig. 3 shows the level of intelligence of these network management protocols [19]. Section IV-A investigates the SNMP, Section IV-B recommends the PBNM, and Section IV-C introduces the IDNM. In Section IV-D, we provide the summary and discussion of the Section.

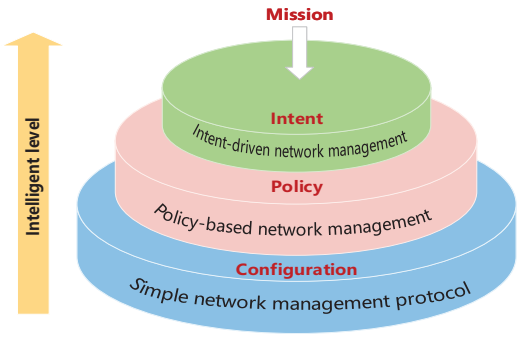

Fig. 3: The intelligent level of network management protocols [19].

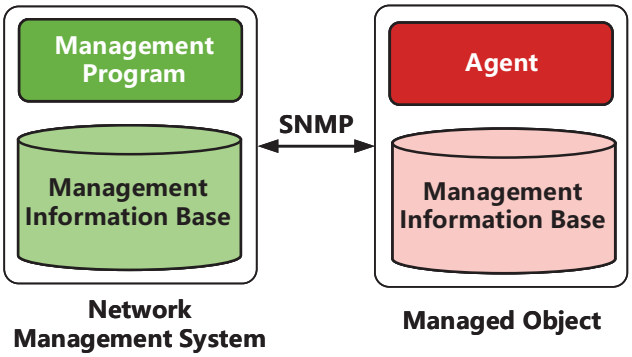

Fig. 4: SNMP structure.

A. Simple Network Management Protocol, SNMP

SNMP is the most predominant network management protocol that operates in the centralized management mode. This protocol is responsible for managing all network nodes through a single manager [16]. The SNMP comprises a range of specifications and protocol families, including SNMP protocol, database structure, and data objects. A network management system based on SNMP adopts a client-server (C/S) structure consisting of the network management system (NMS), the network managed object, the agent process, and the communication protocol [24]. Fig. 4 illustrates the network management object based on SNMP. In this system, the NMS utilizes the SNMP protocol to retrieve information from the managed object, and the software agent embedded in the managed object sends the data to the NMS via the SNMP protocol. Additionally, the management information base (MIB) is used to access data, which further enhances the efficiency and effectiveness of the network management system based on SNMP [148].

- NMS: The NMS is essential for network administrators, providing tools for configuration and data collection. Beyond manual oversight, it can automate data collection through management programs, thus streamlining operations. By receiving reports from agents, the NMS allows for real-time monitoring and proactive management of network performance [149]. Administrators can set alerts and thresholds to preemptively address potential issues, ensuring a reliable and efficient network infrastructure.
- Managed Object: Managed objects, which include devices like routers, switches, and hosts, are configured to support SNMP parameters that facilitate the collection and reporting of critical performance data [24]. This configuration enables network administrators to gain insights into the operational status of these devices, allowing for timely interventions before performance degradation occurs.
- Agent: The agent functions as a communication bridge between the NMS and managed objects, responding to requests from the NMS and providing essential performance data [37]. Additionally, agents can proactively report significant network events, enabling swift identification and resolution of issues.
- Communication Protocol: The SNMP is a comprehensive communication protocol that encompasses both the definition and identification of management information, as well as the communication protocol for exchanging this information between various entities within the network. The definition and identification of management information include the structure and identification of management information (SMI) and MIB [150]. SMI specifies the naming conventions and usage for managed objects, while MIB serves as a standardized repository for managing network devices [151]. MIB-II, defined in RFC1213, is currently the standard used in SNMP and establishes unique object identifiers for managed instances, organized in a hierarchical tree structure [15]. The SNMP communication protocol is critical in facilitating efficient communication between different entities. SNMP employs a variety of data operations, including Get, Getnext, Set, Response, and Trap [36]. These operations facilitate smooth data transmission between the NMS and the managed devices.

As networks evolve, particularly with the emergence of 6G technologies, the role of SNMP is increasingly under scrutiny. The growing complexity and data volume in xANETs presents significant challenges for SNMP. While effective in its simplicity, SNMP may struggle to adapt to these new demands.

One of the primary concerns with SNMP is its centralized management architecture [152]. This centralized approach does not effectively accommodate the decentralized nature of future network architectures, particularly in dynamic environments where devices frequently join and leave the network. As the number of managed devices increases, the volume of data generated can overwhelm SNMP's polling-based model, leading to excessive signaling overhead.

Furthermore, the polling mechanism to SNMP is not designed for the real-time adaptability that xANETs demand. In xANETs characterized by dynamic topologies and rapidly changing conditions, the ability of SNMP to manage and respond to real-time events is limited. Its reliance on periodic queries can introduce latency, making it unsuitable for applications requiring immediate feedback.

As the network landscape shifts towards more programmable and flexible architectures, integrating SNMP with SDN and network function virtualization (NFV) frameworks

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2025.3545254

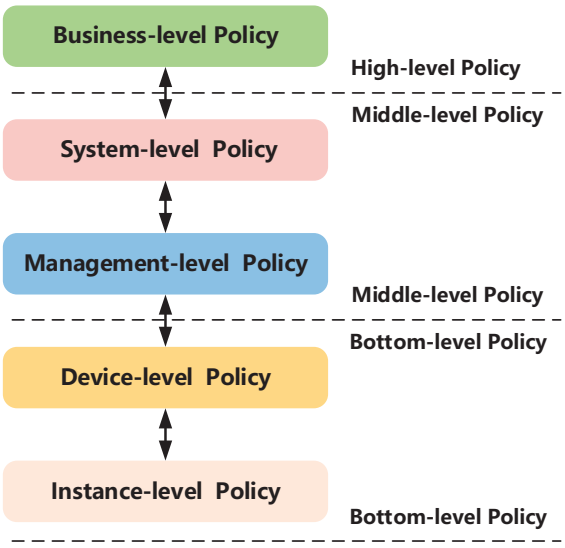

Fig. 5: Different abstraction levels of policy [157].

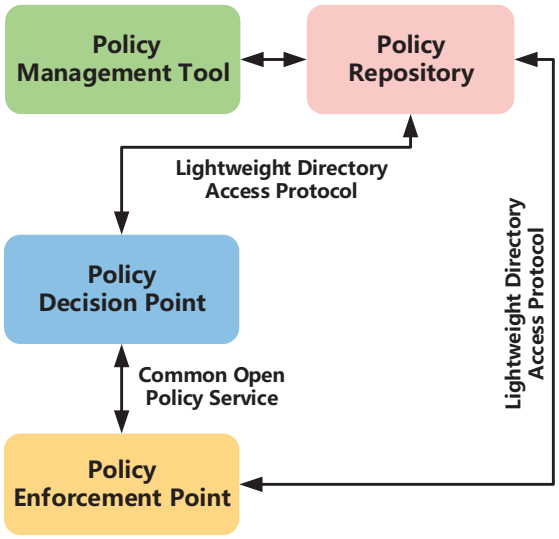

Fig. 6: PBNM architecture.

presents both challenges and opportunities. While SNMPv3 enhances security through improved authentication and encryption, it often finds itself overshadowed by protocols better suited for the complexities of network management. Protocols such as NETCONF/YANG and RESTCONF are increasingly favored in SDN and NFV contexts due to their programmability and ability to manage complex configurations more efficiently [153].

In summary, while SNMP has served as a foundational tool for network management, its limitations in scalability, real-time adaptability, and integration with emerging network architectures highlight the need for more advanced protocols. Future network management protocols can meet the evolving demands of future networks.

B. Policy-based Network Management, PBNM

PBNM is a network management approach that involves defining high-level management objectives in terms of policies implemented in the network. This approach empowers network administrators to specify policies customized to the unique requirements of the network, which ensures that network resources and services are allocated in an optimized manner to achieve the desired objectives [154].

1) Policy Basics: Policies serve as the basis of the PBNM system, providing the necessary structure to guide the network's operations effectively. Each policy consists of a series of conditions and actions, in the form of IF {conditions} THEN {actions} [155]. Conditions are used to determine whether to execute a particular set of actions based on the description or objects of the network. Upon triggering a policy rule, specific rules dictate the execution of one or more corresponding actions.

The design and implementation of policies can substantially influence network performance. Hence, it is of utmost importance to formulate and execute policies that align with the specific objectives and requirements of the network. However, the complexity inherent in policy design can pose challenges. During the network management process, policies are dynamic, and they evolve from initial formulation to final execution by the device [156]. Depending on the level of abstraction, policies can be categorized as bottom-level policies, middle-level policies and high-level policies, as illustrated in Fig. 5 [157].

- Bottom-level Policy: It focuses on individual network devices, which can be further classified into device-level policies and instance-level policies [158]. The device-level policy defines a group of devices with similar functions, outlining the policies that apply to the group. On the other hand, instance-level policies are directly applied to the specific operation implementation of the device, such as the command line interface (CLI).
- Middle-level Policy: It is independent of the device and cannot be directly utilized to operate the device. It is further divided into system-level policies and management-level policies [159]. System-level policies refer to the information model, such as the policy information model formulated by the IETF. Meanwhile, the management-level policy pertains to a generic or specific data model.
- High-level Policy: It is a business-level policy characterized by business terms. These policies are directly interfaced with users, and their descriptions and representations typically use a user-friendly representational language model similar to natural language [160]. High-level policies are not associated with specific configuration details and device operations.

Specifically, the expression of management policy can be classified into three distinct categories [161]. Table IV summarizes the content between different policy expressions.

- Event-Condition-Action (ECA) policy: These policies outline the rules that dictate the functioning of the system [162]. The rules are enforced by policy decision points (PDPs). Whenever an event occurs, the PDP examines if any policies include this event within their events section. When an event of a policy occurs, the policy

TABLE IV: THE EXPRESSION CONTENT OF THE POLICY

Type	Content	Overview
ECA	Event	Events serve as triggers for policies and represent noteworthy asynchronous occurrences in related domains.
	Condition	Conditions are employed to verify the truthfulness of specific expressions before executing the designated action.
	Action	Actions encompass various network management operations of configuring and monitoring network elements or services.
ACL	Subject	Subject is the entity requesting the decision.
	Request	Request describes the parameters of the request that needs to make a decision.
	Target	The target is the object on which the principal requests permission to operate.
	Conditions	Policy can specify conditions that limit the decision environment.
	Permit/Deny	It determines whether to allow or deny the request.
Configuration	User policy	User policies are expressions of high-level goals and objectives.
	Configuration policy	These policies encompass configuration information for networks, services, or protocols.

is activated. If there are multiple events, the priority of these events must be considered, and conflicts during the policy-triggering process must be resolved.

- ACL Policy: ACL policies specify and enforce whether a particular entity is authorized to perform specific actions [163]. These policies are enforced by PDPs, which provide decisions in response to policy enforcement points (PEPs). ACL policies specify the target, including the resource (the entity being accessed), the subject (the entity accessing the resource), and the action (the action performed by the subject and target), conditions (which describe conditions that allow or disallow access) and results ("allow" or "reject") [164].
- Configuration Policy: Configuration policies define specific parameters for network protocols, services and elements [165]. It can be divided into user policy and Configuration Policy. User policies express high-level goals and objectives. These policies include configuration information for software components, which impose operational constraints [166]. Configuration policies contain configuration details for network protocols, elements, or services, such as routing and QoS.

To conclude, policies are crucial in managing behavior in the PBNM system, and the design of effective policies is paramount to ensuring system performance and security. By continually improving and optimizing policies, network management systems can achieve efficiency, security, and better adaptability to the evolving intents of networks.

2) PBNM: In view of the shortcomings of SNMP, the IETF standardized PBNM as a more effective approach for managing and controlling large-scale networks [167]. The adoption of PBNM represents a significant transformation in network management, shifting the focus from "how to achieve" to "achieve goals". This approach allows administrators to focus primarily on the goals of network management and the necessary abstract behaviors to achieve those goals rather than getting involved in the intricate configuration and management operations of network devices [168]. As a result, administrators can more intuitively reflect their decision-making through policy formulation. The IETF has defined the PBNM architecture, including basic modules such as policy management tool (PMT), policy repository (PR), PDP, PEP, common open policy service (COPS), and lightweight directory access protocol (LDAP) [17]. The relationship of each module is shown in Fig. 6.

- PMT: PMT is the primary policy input module in the entire PBNM system. It provides a user-friendly policy editing interface to build and modify policies [169]. Additionally, it also checks and confirms the policy to ensure that there are no conflicts with any other policies in the system.
- PR: The PR module is responsible for storing policy information. It can be implemented as a directory server or a database server [170]. In addition to storing the policy information edited by the administrator, it can also store other network information and system parameters.
- PDP: PDP is a logical entity and the core component of the policy control system. The performance of a policy is evaluated by the PDP, which ensures the execution of the appropriate policy based on its assessment [171].
- PEP: PEP is the network element entity responsible for implementing the policies determined by the PDP. It is responsible for feeding back information to the PDP, reporting network state information and policy implementation [172].
- COPS Protocol: The COPS protocol is used to communicate policy information in the response-request mode between the PDP and the PEP [173]. COPS establishes a TCP connection and uses the C/S communication. COPS allows PDP to actively send configuration information to PEP or notify the deletion of invalid configuration information.
- LDAP: The LDAP provides a standard means of accessing the PR. The PDP/PEP in the PBNM framework

TABLE V: THE TYPE OF INTENTS

Intent type	Project	Content	Ref.
Technical	Merlin	It can express the intent related to the specified path of data packets, data packet classification, and processing functions.	[178]
	PGA	It can express routing, flow monitoring and access control-related intents.	[179]
	Janus	It supported more dynamic intent representations such as time-varying, triggering, and QoS.	[180]
	Pyretic	It realized related business intents through network programming language of an imperative nature.	[181]
Non-technical	Charting	Request described the parameters of the request that needs to make a decision.	[182]
	LUMI	It can refine and deploy advanced policies in large-scale heterogeneous networks.	[183]

accesses the policy and network information in the PR according to LDAP [174].

Despite its potential, PBNM is not without limitations. As xANETs evolve with increasingly complex tasks and highly dynamic environments, the management complexity faced by PBNM protocols has rapidly escalated. Policy management should address multi-dimensional demands across diverse nodes and tasks, complicating the creation, verification, conflict detection, and resolution of policies. Additionally, interdependencies between policies can increase management complexity, creating further challenges for network administrators.

Furthermore, the PBNM architecture typically relies on a centralized PDP to analyze and enforce policies [175]. However, as the number of nodes in xANETs grows, the load on the PDP increases significantly. In large-scale networks requiring rapid response, the centralized control model may introduce latency, which can inhibit decision-making speeds and make it challenging to meet the real-time requirements of dynamic environments.

Additionally, although PBNM can be applied to policy management within SDN/NFV environments, its relatively static policy configurations and fixed management structures limit its flexibility in adapting to real-time orchestration and dynamic resource allocation. In situations where network conditions frequently change, policies struggle to adjust promptly, leading to execution delays that degrade overall service quality.

In summary, while PBNM holds considerable advantages in conventional network management, its applicability is limited in future dynamic and virtualized environments. Future management approaches should incorporate real-time monitoring and response mechanisms, as well as more flexible policy definitions and management methods, to improve adaptability and responsiveness. These advancements would enable PBNM to meet the demands of complex xANETs environments better, optimizing performance in highly dynamic and resource-diverse settings.

C. Intent-driven Network Management, IDNM

As PBNM continues to standardize and evolve, a new network management approach has emerged called IDNM. This approach enables users to specify their desired outcomes or objectives while allowing the underlying network infrastructure to determine the best way to achieve them [19]. This can enhance the efficiency of network management in the xANET, which is inherently complex and dynamic. Therefore, the IDNM is a promising approach for improving the management of the xANET.

1) IDN Basics: IDN is designed to simplify the deployment and management of network services and applications based on high-level requirements. The core concept of IDN is the intent, which is a declarative description of the network requirements. Intent serves as a high-level abstraction of policy, allowing users to specify their requirements more intuitive and natural manner [39]. By leveraging intent translation, policy mapping, intent verification, and state-aware technologies, IDN can automatically derive and configure the network state that aligns with the intent [176]. The intent and IDN are further described as follows.

Intent: The intent represents the specific requirements for various network services. Essentially, intent provides a higher-level abstraction of network configuration, abstracting away the low-level implementation details [177]. Numerous researchers have conducted various studies on intent, which can be categorized into external and internal intent according to its source [23]. External intent refers to the desired purpose directly expressed by the user, which can be expressed in natural language, voice, and other forms. The internal intent refers to the potential demand within the network.

Furthermore, intents can be mainly classified into technical intents and non-technical intents. Technical intent is mainly aimed at network administrators with professional network knowledge. They can participate in network management and application development using the programming languages of northbound interfaces [178–181]. In contrast, non-technical intent is closer to natural language, which is convenient for users to understand and for the network to parse [182][183]. Table V illustrates the research progress of technical and non-technical intents.

For instance, Merlin [178] was a technical intent language that could express the intent related to the specified path of data packets, data packet classification, processing functions, and set bandwidth requirements. PGA could express routing, flow monitoring, and access control-related intents [179]. It can support dynamic intents but not QoS intents and can express and realize the creation of virtual networks. In [180], it supported more dynamic intent representations such as time-

varying, triggering, and QoS intents. Pyretic realized related business intents through network programming language of imperative nature [181].

To achieve non-technical intent description, the expression of tuples to divide the basic unit of intent description had been proposed [182]. Tuples typically consist of keywords such as objects, operations, and ranges. Objects generally refer to resource nodes, such as nodes A and B, which are common objects in tuples. Operations refer to the type of action, such as node A and node B performing link communication and other operations. The ranges are used to constrain the operation or represent the constraints on resource attributes such as bandwidth and delay in the network. The authors in [183] proposed an innovative intent framework called LUMI for refining and deploying advanced policies in large-scale heterogeneous networks. It utilizes a DialogFlow chat interface for user interaction, and the generated intents can be exported as JSON files.

As a new network model, IDN has been proposed in several studies and related experiments. The ultimate goal of IDN is to facilitate network management and reduce the burden on network administrators by liberating users from the complexity of underlying network configurations [26]. Users can submit intent requirements, and the network system will automatically complete the configuration and realization of intents.

At present, IDN has attracted significant attention from various communities, including the standards community, academia, and open-source communities. The open networking foundation (ONF) was the first to propose IDN in 2015. It defined the key characteristics of "intent" in network management, outlining the role and attributes of the intent interface and its primary implementation architecture [184]. In 2017, the authors in [185] provided a specific definition of IDN, including four key modules: translation and verification, automatic implementation, network state awareness and assurance, and dynamic optimization or repair. The IDN architecture white paper of Cisco defined three important components of IDN: intent translation, intent realization, and service assurance [186]. Meanwhile, the IETF had discussed use cases for IDN, including intents focused on network measurement and network slicing [187]. Additionally, there are some IDN efforts also ongoing in other forums, including at ETSI [188] and in the wireless space [189]. Recently, a new network architecture called state-action-intent (SAI) was proposed in [190], which combines AI technology with various functional modules of IDN. This approach has the potential to enhance the capabilities of IDN, making it even more efficient and reliable.

In IDN, administrators can express their intent, which can be translated into multiple network policies to realize their intent. Network policies are subsequently translated into instructions that configure and operate devices using the current network management architecture. The relationship between intent, policy, and configuration is depicted in Fig. 7 [191]. As network scale and technical complexity increase, the continuous improvement of abstraction helps shield intricate technical details. It enables network management at the highest level of abstract intent, creating a mapping from "business intent" to "system policy" to the final "detailed configuration".

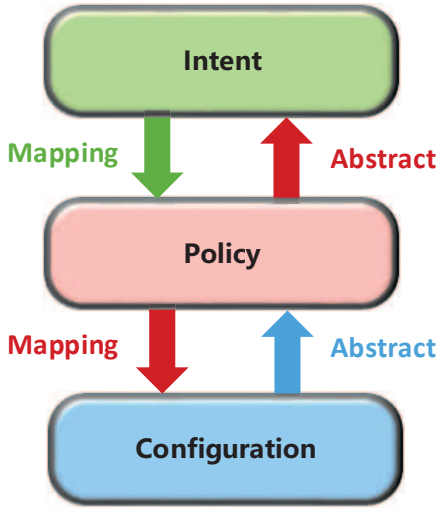

Fig. 7: The relationship between intent, policy, and configuration.

IDN mainly includes four modules that work together seamlessly to achieve the desired network behavior: the intent translation module, policy mapping module, intent verification module, and state awareness module [161]. The intent translation module converts natural language expressions of intent into network-recognizable intent. The policy mapping module combines the network state with the intent to convert it into corresponding configuration policies. The intent verification module ensures that the policies are accurately executed. The state awareness module is responsible for continuously monitoring network state information to ensure the realization of the intent. The entire operation process of IDN is closely tied to intent, and users only need to describe their desired state without describing how to realize that intent [192] [193].

In conclusion, IDN is an emerging network architecture that can simplify network management and improve network performance. The extensive research and development efforts by various communities demonstrate its potential to revolutionize network management and pave the way for the development of more advanced network architectures in the future.

2) IDNM: As mentioned above, IDN offers an innovative approach to network management. The authors in [19] introduced IDN into network management, termed IDNM. This management approach enables administrators to clearly express their intents and requirements through interaction with the management system. The authors in [23] presented an intent-driven autonomous network management scheme and built the IDNM prototype. The prototype subsequently analyzes these intents automatically and transforms them into configurable policies. These policies not only possess adaptive capabilities to manage network conditions in real time but also align with established performance metrics, ensuring the stability and efficiency of the network in dynamic environments.

As shown in Fig. 8, IDNM mainly consists of three layers, namely the application layer, management layer and infrastructure layer [113]. This model aligns network operations with

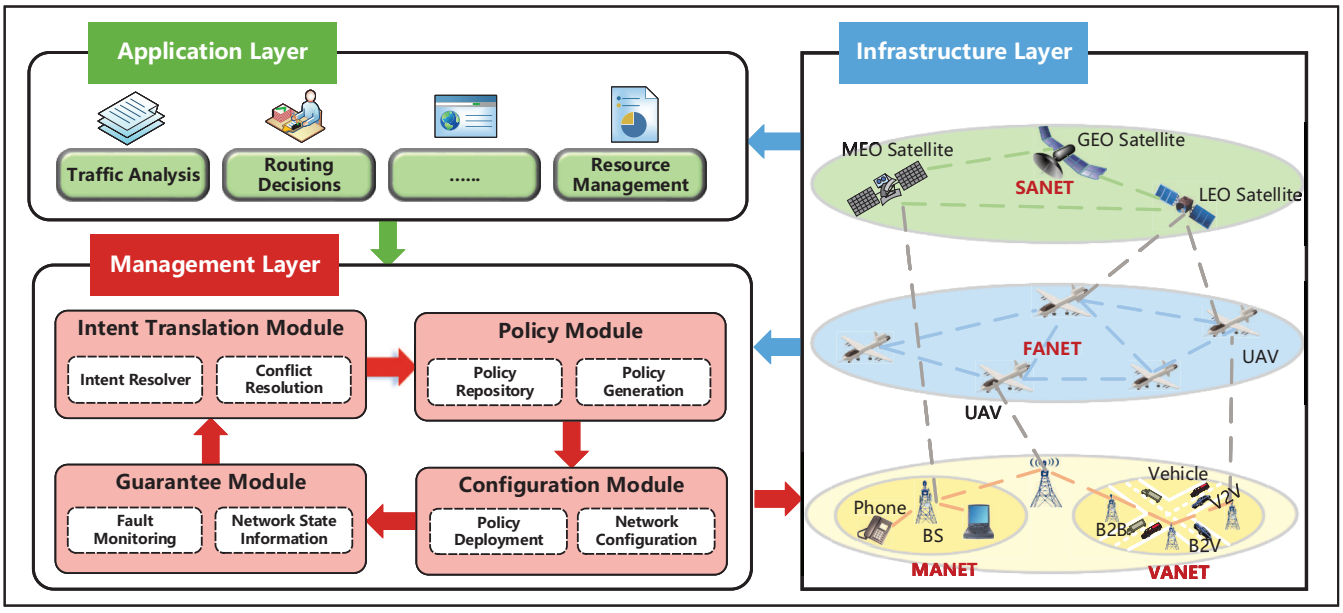

Fig. 8: Intent-driven xANET management system.

the observation-orientation-decision-action (OODA) loop, dynamically adjusting policies based on real-time feedback.

- Application Layer: It comprises management intents within the xANET. The sources of management intents are categorized into two categories: intents output by managers and need to be fed back by the network.
- Management Layer: It autonomously processes intent, policy and configuration, forming a closed loop that minimizes manual intervention. Key modules include the intent translation, policy, configuration, and guarantee modules.
- Infrastructure Layer: It consists of network nodes and resources in MANET, VANET, FANET and SANET. Nodes execute the policies from the management layer, and real-time feedback allows the system to adjust policies as network conditions evolve.

Management Layer contains intent translation, policy, configuration and guarantee modules [113]. These four modules form a closed loop that enables autonomous configuration management of the network and eliminates the need for human intervention.

- Intent Translation Module: It converts natural language or structured intent expressions into network-recognizable formats, including intent resolver and conflict resolution techniques. This module refines intent expressions, mapping them to optimal configurations in line with the latest network state. The authors in [160] classified intent refinement from various perspectives, such as the target users, refinement schemes, and input methods. Furthermore, knowledge graph-enabled intent-driven network [194] proposed a knowledge graph-based intent translation technique. The authors in [195] implemented a structured intent module and a clear representation of network information using graph-based techniques to solve the intent conflict.
- Policy Module: It comprises the PR and policy generation. Policies are logical commands that trigger configuration actions and are stored in the PR as ECA rules. When the policies in the PR cannot fully realize the management intent, AI technologies are used to generate new policies that better align with the management intent. The authors in [196] converted the intents and policies of network administrators into specific network configuration and operation instructions. The authors in [176] decomposed intents into a hierarchical policy structure using predefined policy templates and introduced a closed-loop feedback mechanism, employing a finite state machine (FSM) to execute policies and deploy intents.
- Configuration Module: It contains policy deployment and network configuration, where the configuration policies are sent to the network nodes that require configuration and connection using standard interfaces. From the perspective of the OSI seven-layer model, the configuration management in xANET mainly pertains to the lower three layers, namely the physical layer, the data link layer and the network layer. To achieve policy configuration in xANET, a local management node must be set in each subnet to share the configuration tasks in network management [197]. The local management node configures the remaining nodes in the subnet.
- Guarantee Module: It contains fault monitoring and network state information. Feedback-driven lifecycle verification further ensures that policies respond to network changes. In [198], verification techniques for IDN were clearly defined and classified from different perspectives. A full-lifecycle verification framework with feedback is proposed to verify the access control policies of network functions.

Despite its numerous advantages, IDNM faces a series of challenges in practical application. First, the highly dynamic

TABLE VI: COMPARISON OF NETWORK MANAGEMENT PROTOCOLS

Characteristics	SNMP	PBNM	IDNM
Management Complexity	Simple, but unsuitable for complex networks.	Moderate, supports policy-driven management.	Complex, but highly automated.
Configuration Flexibility	Low, relies on manual configuration.	Moderate, partially automated.	High, supports intent-driven automation.
Dynamic Adaptability	Low, slow response, requires manual intervention.	Moderate, some policies can be adjusted.	High, real-time adjustments, automatically adapts to network changes.
Intelligent Capability	Low, based on a simple MIB structure.	Moderate, policy-based on predefined rules.	High, leverages AI/ML for intelligent decision-making.
Scalability	Limited, suitable for small-scale networks.	Moderate, supports medium to large-scale networks.	High, suitable for large-scale and complex networks.
Fault Recovery Capability	Low, requires manual intervention.	Moderate, supports limited automated recovery.	High, features automatic detection and self-healing.
Security	Basic security mechanisms, limited support.	Moderate, policies can enhance security.	High, supports advanced security policies and real-time threat response.
Applicable Scenarios	Suitable for simple, static networks.	Suitable for medium-sized enterprise networks.	Suitable for dynamic, complex, large-scale networks.
Suitability for xANETs Management	IDNM>PBNM>SNMP		

and heterogeneous nature of xANETs increases the complexity of management. The IDNM approach must handle various network nodes, task requirements, and resource constraints, making the expression, translation, and execution of intents more challenging. IDNM management technology requires high adaptability and generalizability to address diverse situational demands effectively.

Second, the scalability of the IDNM management architecture is crucial. As network scale and management demands grow, IDNM must support extensive upper-level management demands and complex lower-level policy configurations. It should rapidly detect and adapt to real-time changes in network states, dynamically adjusting management policies to ensure stability and efficiency in network performance.

Finally, while IDNM can leverage the flexible resource orchestration capabilities of SDN/NFV technologies and their dynamic resource allocation, effectively managing intent within these novel network architectures remains a pressing challenge [189]. It is essential to ensure that intents are accurately translated into specific configuration policies to achieve seamless and efficient integration.

Therefore, future research on IDNM should focus on optimizing the architecture's generalizability and dynamic responsiveness. Developing more intelligent intent translation and policy generation mechanisms will better address the varying demands within xANETs, further enhancing network adaptability and intelligence.

D. Summary and Discussion

As network management demands continue to evolve, Section IV reviews three approaches: SNMP, PBNM, and IDNM. Table VI presents a detailed comparison of the characteristics and practical performance of each approach. IDNM stands out in terms of flexibility, intelligent management, and dynamic adaptability, making it clearly more aligned with the complex requirements of xANETs management and more effective in addressing the challenges of a constantly changing network environment.

V. NETWORK MANAGEMENT IN XANET: FROM CONFIGURATION-BASED TO INTENT-DRIVEN APPROACHES

This Section carefully surveys existing work in the field of xANET management, focusing on approaches from configuration-based to policy-based to intent-driven. Section V-A provides an overview of MANET management. Section V-B summarizes the current work of VANET management. Section V-C focuses on FANET management, and Section V-D delves into the status of SANET management. Section V-E provides the summary and discussion of this Section. By summarizing these works, we aim to comprehensively understand the current work of xANET management and provide a deeper understanding of future development.

A. MANET Management

Due to the constant mobility of nodes and the dynamic changes in network topology, MANET management has become exceedingly complex. In this dynamic environment, effective MANET management is crucial for ensuring network performance and reliability. As illustrated in Table VII, a substantial body of literature has already delved into and discussed MANET management issues from various perspectives, aiming to identify effective solutions that can adapt to this intricate environment. In this work, we provide a comprehensive overview of the current research from the standpoint of SNMP, PBNM, and IDNM management protocols.

TABLE VII: THE OVERVIEW OF THE MANET MANAGEMENT

Management protocols	Overview	Limits	Ref.
SNMP	The ANMP introduced cluster-based and hierarchical structures to improve scalability.	The hierarchical structure increases message overhead, reducing its responsiveness.	[199]
	A management system using static and mobile agents to monitor node status and manage resources.	Mobility introduces extra complexity and control overhead in managing agents.	[200]
	An SNMP-based management framework was used to optimized routing protocols like AODV and DSR.	The polling nature and message congestion limit the scalability and performance.	[201]
	SNMP framework was extended to integrate QoS metrics based on QoRA.	Frequent data collection for QoS monitoring introduces additional overhead.	[202]
	It provided an overview of current network management architectures and major trends.	SNMP exists high message overhead or the absence of management functionality in certain nodes.	[203]
PBNM	PBNM simplifies network management by predefined policies to monitor and trigger actions.	PBNM requires significant initial effort to define policy and leads to rigidity.	[17]
	A policy-based security management framework defines the security policies.	It may fail to account for novel security threats not considered during policy formulation.	[204]
	The PAIT method incorporates policies into message metadata to control message access.	PAIT introduces delays in message transmission as each message undergoes policy validation.	[205]
	A policy-based trust management framework monitored nodes and isolated malicious nodes.	Continuous monitoring and policy adjustments may strain devices with limited processing power.	[206]
	A colored time petri net model integrated context-awareness into policy management.	Constant monitoring of context information is resource-intensive.	[207]
	A policy-based route framework applied policy rules into route selection.	This approach can lead to suboptimal route selection.	[208]
	It integrates security and QoS considerations into routing policies.	Maintaining accurate trust evaluations can be resource-intensive.	[209]
	P2P technology is applied to network management to manage tasks across multiple domains.	Frequent changes can impact network stability and the timeliness of management tasks.	[168]
	A policy-based clustered routing framework collects node information to implement routing policies.	Mobile agents for collecting and distributing policy data can introduce delays and additional load.	[210]
IDNM	PEMR model adjusts routing strategies based on SLA and real-time network conditions.	Intent-based routing increases processing overhead.	[174]
	A QoS-guaranteed routing protocol incorporates QoS parameters to optimize routing selection.	It may require significant processing resources.	[211]
	CONAIR architecture selected optimal communication links by real-time QoS evaluation.	Continuous QoS monitoring can introduce overhead.	[212]
	A hybrid congestion control policy considered network state and packet loss to refine congestion.	The reliance on dual-layer metrics increases computational and communication overhead.	[213]

1) SNMP: The SNMP is a widely adopted protocol for network management, facilitating the exchange of management information between network managers and agents. SNMP-based methods have been applied to MANETs to create lightweight protocols compatible with SNMP's foundational structure, addressing the need for adaptability in resource-limited, highly dynamic environments. In an early approach, the authors in [199] proposed the ANMP, by introducing cluster-based and hierarchical structures while maintaining SNMP's protocol data unit (PDU) and MIB structures. The cluster-hierarchy approach of ANMP was innovative for improving scalability in MANETs. However, it encountered challenges related to message overhead and responsiveness under high mobility conditions, limiting its applicability in very large or fast-moving networks.

In an alternative approach to MANET management, the author in [200] introduced a MANET management system based on agents (NMSA). This method employed both static agents (SA) and mobile agents (MA) to monitor node status and manage resources autonomously in dynamic environments. The strengths lie in its use of mobile agents, which adapt to network topology changes by relocating and cooperating with other agents, providing resilience against node failures. However, while the mobility and intelligence of agents enhance flexibility, they also introduce additional control overhead and complexity, as agents require protocols to prevent redundant or conflicting actions in highly dynamic networks.

Building on the conventional SNMP framework, [201] proposed an SNMP-based management framework explicitly tailored for MANETs. This framework optimized routing

protocols like AODV and DSR to address the overhead, latency, and network throughput issues typical in MANETs. By adapting routing protocols, the framework aimed to enhance routing efficiency, though improvements were limited by the fundamental constraints of SNMP, such as its polling-based nature and potential message congestion in dense networks. The framework was further extended in [202] to integrate QoS metrics, incorporating a QoS routing algorithm based on ant colony optimization (QoRA). This algorithm enabled adaptive routing by collecting real-time QoS data such as latency, bandwidth, and packet loss, then dynamically updating routing tables to optimize network performance. While QoRA was effective at improving stability and efficiency, its reliance on frequent data collection could introduce overhead, particularly in bandwidth-constrained environments.

The evolution of network management architectures in MANETs has led to a spectrum of approaches, including centralized, distributed, and hybrid models [203]. It introduces significant trends in MANET management, transitioning from SNMP-based approaches to PBNM and eventually embracing self-management to address the dynamic nature and resource scarcity challenges in MANETs. The SNMP-based hierarchical management model provides a more accurate execution of complex tasks in management and decision-making. However, there exists high message overhead or the absence of management functionality in specific nodes. The policy-based approach is the second available model, which provides this functionality by implementing and executing policies defined by network administrators. Alternatively, the complexity of establishing the control makes its implementation challenging. The third model is referred to as the self-management model. One drawback of this method is that it may be overly complex for computing nodes with limited resources, and sensor nodes might require specialization for specific management functions.

Overall, while SNMP-based and agent-based models offer foundational frameworks for MANET management, emerging trends indicate a need for highly adaptable, efficient, and intelligent solutions to accommodate the inherent challenges of MANET environments. The integration of adaptive algorithms and decentralized management mechanisms remains crucial to advancing MANET performance and sustainability in real-world applications.

2) PBNM: Conventional network management approaches are effective for individual devices, such as the SNMP. However, if the number of hosted nodes is significantly large, this can become a resource-intensive process. PBNM offers a promising solution to address these challenges, particularly in the dynamic and resource-constrained environments. It simplifies management in large-scale systems by automating the execution of predefined policies that monitor network conditions and trigger actions autonomously [17]. However, a key limitation is the initial effort required to define a comprehensive set of policies that can handle the wide range of network conditions in dynamic environments. Additionally, predefined policies can lead to rigidity if conditions change unpredictably, potentially causing operational inefficiencies.

The authors in [204] proposed a policy-based security management framework for message protection, defining security policies that automatically enforce actions like encryption and authentication. This framework enabled real-time security adaptation based on network conditions, providing robust protections for data confidentiality and integrity. However, the framework's dependency on predefined policies might limit its effectiveness against novel security threats that were not accounted for during initial policy formulation. [205] proposed a policy-based information transfer (PAIT) method, which incorporated policies into message metadata to control message access and restrict certain nodes from receiving sensitive data. The message creator specified the nodes, both recipients and restricted nodes. Although PAIT provided strong privacy controls, its policy-driven approach may introduce delays in message transmission, particularly in dense networks where each message must undergo additional policy validation at the receiving end, which could impact real-time communication needs.

A distributed policy-based trust management framework was further designed for monitoring node behavior to enforce trust and security in MANETs [206]. By using predefined policies to identify and isolate malicious nodes, the system enhanced the security and resilience against insider threats. The distributed framework allowed it to operate effectively in a decentralized network. However, it could be resource-intensive, as continuous monitoring and policy adjustments may strain devices with limited processing power.

The authors in [207] presented a colored time petri net model that integrated context-awareness into policy management, enabling real-time adjustments based on dynamic changes in MANETs. The model formalized the policy execution process using colored time petri nets, allowing for flexible adjustment and updating of policies based on dynamic network changes and context information. While this approach enhanced adaptability, the constant monitoring of context information could be demanding in terms of processing power and bandwidth, potentially impacting network efficiency in resource-limited devices or highly active networks.

MANET nodes may have multiple routes to a destination, each with different reliability and security characteristics. The authors in [208] designed a policy-based route framework that applied policy rules related to security and connection reliability requirements to route selection. By assessing trustworthiness and stability across available routes, this model selected routes through authenticated, trusted nodes with low failure rates. This approach ensured data security and connection reliability. However, it may inadvertently lead to suboptimal route selection in dynamic environments where trusted nodes are not always available, limiting routing flexibility and efficiency in rapidly changing networks. In the realm of trust-based routing, [209] integrated security and QoS considerations into routing policies, enabling the network to make routing decisions based on trust levels and QoS parameters. However, maintaining accurate trust evaluations could be resource-intensive, requiring frequent updates and verifications that may impose additional computational and communication overhead.

The authors in [168] reviewed the application of peer-to-

peer (P2P) technology in network management, referred to as P2P-based network management (P2PBNM). P2PBNM leveraged a decentralized approach, constructing overlay networks with strong self-organizing properties to manage tasks across multiple management domains. However, frequent changes in node connectivity can impact overall network stability and the timeliness of management tasks. A policy-based clustered routing framework was designed, in which mobile agents collected node status information and implemented routing policies based on real-time data [210]. By clustering nodes and using mobile agents, this framework distributes routing and management tasks efficiently, reducing overhead and balancing loads. The clustering model allows nodes to predict resource availability based on neighboring patterns, but the overhead introduced by mobile agents in gathering and distributing policy data could cause delays and additional network load.

In conclusion, PBNM provides automation and adaptability to manage the complexities of MANET, significantly reducing manual intervention and enhancing system security and reliability. However, PBNM's reliance on predefined policies can lead to insufficient responsiveness in rapidly changing conditions. Additionally, techniques such as distributed trust management, P2P architectures, and mobile agent technology enhance network resilience and scalability through decentralization and dynamic resource allocation. However, they introduce additional bandwidth and computational costs. Future research should focus on the deep integration of dynamic policy updates and environment-aware mechanisms to develop a more intelligent and resource-efficient management framework for MANETs.

3) IDNM: IDNM empowers networks to autonomously handle configuration, optimization, and repair in response to high-level objectives set by administrators. For example, the authors in [174] introduced a performance and event management routing (PEMR) model designed to adjust routing strategies based on SLA requirements and real-time network conditions. The adaptive routing capabilities include rapid rerouting and automatic recovery. This model supports each node in making decisions autonomously, driven by predefined intents and monitored network information, which optimizes response times and network resilience. However, intent-based routing may increase processing overhead, which could impact scalability in larger MANETs.

The application of IDNM in MANETs shows promising advancements, particularly in enhancing QoS. In [211], a QoS-guaranteed routing protocol for WSN-MANET was proposed, which embedded QoS requirements within the routing process. This was achieved by incorporating QoS parameters directly into the cost function, optimizing routing selection for various applications. While this approach enables precise QoS management and path optimization, it may require significant processing resources, particularly in MANETs with frequent topology changes.

To address congestion issues, an advanced and dynamic congestion-aware intent-based routing (CONAIR) architecture was introduced, which efficiently selected optimal communication links by evaluating QoS parameters in real-time [212]. This proactive approach enabled the network to predict and mitigate congestion before it occurred, thus enhancing reliability and reducing delays. However, continuous QoS monitoring can introduce overhead in highly dynamic environments where resources are constrained. Further refining congestion management, a novel hybrid congestion control policy was presented that considered the network state and packet loss [213]. By factoring in both current network conditions and application-layer intents, this approach enables robust congestion management that aligns closely with upper-layer service expectations. However, its reliance on dual-layer metrics may increase computational requirements.

Through mechanisms like adaptive routing, QoS optimization, and congestion-aware resource management, IDNM helps MANETs maintain efficient performance and reliability under dynamic conditions. However, the inherent characteristics of MANETs, such as frequent topology changes and limited bandwidth, significantly complicate real-time intent translation and adaptive decision-making processes. Balancing resource overhead with network management performance is a critical challenge. Developing lightweight intent translation models and efficient decision algorithms will be essential for achieving robust, scalable IDNM frameworks within MANET.

B. VANET Management

In the face of challenges such as mobility, security, and resource demands, managing VANETs becomes highly intricate. Effectively addressing the dynamic changes in network topology and the instability of routing paths is crucial, especially when ensuring communication among vehicles and maintaining network performance. To tackle these management issues, researchers have proposed a series of protocols, as shown in Table VIII, including SNMP, PBNM, and IDNM. The design of these protocols aims to monitor and control VANET, achieving effective management of network performance, status, and behavior. Through the implementation of these protocols, network administrators can continuously monitor the network performance and status, taking necessary actions to ensure reliability and security while optimizing resource utilization and management.

1) SNMP: SNMP, a protocol widely utilized for managing fixed networks, is instrumental in enabling NMS to collect operational data from managed devices by issuing requests through defined SNMP messages. This process relies on the MIB, which outlines all accessible management objects for monitoring and controlling network devices. The NMS oversees overall network functionality, sustaining connectivity and device status across the network. However, applying SNMP to VANETs presents unique challenges, given the intermittent connectivity and high variability.

To address these limitations, the authors in [214] introduced an SNMP-based vehicular delay-tolerant network (VDTN) model. This model adapted SNMP for VANETs by implementing a delay-tolerant architecture. SNMP could gather load-related data from VDTN nodes and leverage a centralized NMS to manage distributed devices efficiently. While effective for delay-tolerant scenarios, this model has limitations in environments where real-time data access is essential, potentially delaying response actions during critical incidents. Building

TABLE VIII: THE OVERVIEW OF THE VANET MANAGEMENT

Management protocols	Overview	Limits	Ref.
SNMP	VDTN model adapts SNMP for VANET by implementing a delay-tolerant architecture.	It causes delays in real-time data access during critical incidents.	[214]
	It explores MIB specifications for OBUs.	Increased data volume from continuous sensor monitoring lead to network performance overhead.	[215]
	SNMP is used to execute atomic processes via functional service modules.	Reliance on limited message types restricts adaptability for complex network tasks.	[216]
	The QoRA integrates SNMP for optimal routing paths and congestion management.	It added computational complexity and the requirement for constant SNMP manager access.	[217]
PBNM	A policy enforcement framework used DNF for expressive access control and a conflict resolution mechanism.	Complexity may lead to overhead and potential delays in enforcing policies.	[218]
	Policy-based security mechanisms include access control, data encryption, and key management.	Complexity and processing overhead may introduce delays.	[219] [220]
	A distributed resource management solution uses XACML and smart contracts to manage policies.	Dependency on smart contracts introduces latency and resource consumption challenges.	[221]
	PBNM for managing QoS and QoE for video streaming, improving reliable routing in the IOV.	It required substantial computational resources.	[222] [223]
IDNM	A automation framework incorporates an intent-based traffic offloading solution.	The reliance on SDN added complexity in managing edge device configurations and vulnerability risks.	[224]
	The ACO-AODV protocol used intent-based networks for routing and network parameter selection.	Maintaining accurate intent tracking in real-time introduces additional overhead.	[225]
	LocJury scheme controls malicious location access by predicting and monitoring location access intents.	Dependency on virtual currency limited scalability and acceptance.	[226]
	IUCB algorithm enables long-term optimal task offloading while meeting URLLC constraints.	It requires significant computational resources.	[227]
	The intent-based network control framework configures network policies using intent controllers.	Coordination between SDN controllers and policies complicates management and execution processes.	[228]

upon SNMP adaptations in VANETs, [215] explored a method for creating and testing MIB specifications in on-board units (OBUs). These specifications were designed to allow fast, secure access to sensor data from vehicles, addressing configuration and error management challenges. However, the increased data volume from continuous sensor monitoring may introduce overhead, impacting network performance if not managed efficiently.

Further extending the application, [216] explored SNMP role in executing atomic processes through functional service modules. Utilizing MIB to transmit management information with sufficient semantic context provided a structured approach to process execution, simplifying service management in distributed networks. However, reliance on limited message types may restrict its adaptability to diverse network tasks, posing a challenge in handling more complex service demands.

On another note, the authors in [217] proposed the quality of service routing algorithm (QoRA) to address congestion issues in ad hoc networks. Leveraging ant colony optimization, QoRA sought optimal routing paths while avoiding congestion, integrating SNMP and QoRA units to ensure path selection based on real-time quality data. While this approach enhances routing reliability, it added computational complexity and required constant SNMP manager access.

SNMP has been adapted for use in VANET to facilitate effective network management. These studies highlight the adaptability of SNMP in VANET. However, continuous communication may not align well with the sporadic connectivity of vehicular environments, potentially leading to delays in data collection and response. Moreover, the increased volume of data from various sensors can create overhead. As VANETs evolve, future research must focus on developing more adaptive management mechanisms that can handle the dynamic nature of these networks while minimizing latency and resource consumption to ensure robust and responsive network management.

2) PBNM: PBNM offers a flexible framework that enables network administrators to guide network behavior by defining policies. In the dynamic context of VANET, which is marked by frequent node mobility and fluctuating communication conditions, PBNM becomes essential for effective network management. Administrators can formulate policies tailored to various traffic scenarios, thus facilitating adaptive vehicle communication and mobility management.

The authors in [218] proposed a policy enforcement framework for secure data dissemination. This framework empowered highly mobile data-sending vehicles and strategically positioned roadside units (RSUs) to establish access control policies, thereby safeguarding data transmission collaboratively. A notable feature of this framework is its use of

disjunctive normal form (DNF) to articulate expressive access control policies that cater to diverse data security needs. Moreover, the inclusion of a conflict resolution mechanism based on confidence-weighted priorities allows the system to adapt dynamically in the face of conflicting policies, ensuring both system stability and data security. However, while this framework enhances security, its complexity may lead to increased overhead and potential delays in policy enforcement.

Additionally, [219] introduced policy-based security mechanisms, including access control, data encryption, and key management, to tackle security challenges within VANETs. Another paper proposed a policy-based approach for detecting and mitigating malicious behavior by analyzing the communication history among vehicles to evaluate their creditworthiness and trustworthiness [220]. While these security measures enhanced the overall integrity of the network, they could introduce additional complexity and processing overhead, which may impact real-time decision-making.

In a different approach, the authors in [221] proposed a distributed resource management solution for VANETs utilizing smart contracts. This method employed secure policy deployment processes and access control policies grounded in the extensible access control markup language (XACML) standard. By leveraging the XACML framework, this approach facilitated the entire lifecycle of access control policies, including creation, updating, revocation, and evaluation. Although this method enhanced the robustness and flexibility of resource management, the reliance on smart contracts could introduce latency and resource consumption challenges in real-time environments.

Furthermore, the authors in [222] emphasized QoS management for video streaming in VANET, delving into various QoS and quality of experience (QoE) metrics. Additionally, the SURFER1 and SURFER2 protocols were improved upon the ROAMER protocol for the internet of vehicles (IOV), thereby offering more secure and reliable routing options [223]. While these enhancements can significantly improve the performance of video streaming applications, they may also require substantial computational resources, potentially limiting their applicability in resource-constrained environments.

In summary, PBNM plays a pivotal role in enhancing the adaptability and efficiency of VANETs by enabling network administrators to define and implement policies that govern network behavior. However, the inherent complexity of implementing and managing numerous policies can lead to increased overhead, potentially resulting in delays and resource inefficiencies. Future research on management approaches should balance effective network management with resource constraints.

3) IDNM: IDNM automates the configuration, optimization, and management of network resources by leveraging the intent information generated by nodes within the network. This approach leads to more intelligent and efficient network operations. In VANETs, IDNM identifies and understands diverse intents of vehicles, such as lane changing, deceleration, or acceleration. By continuously monitoring the real-time intents of vehicles, IDNM improves traffic management, reducing congestion and enhancing overall traffic flow. Additionally, it optimizes network resource allocation based on the intents and communication requirements of vehicles, thereby facilitating real-time communication among vehicles and driving the continuous development of intelligent transportation systems.

Currently, relevant researchers have successfully integrated IDNM into VANETs. For instance, the authors in [224] introduced a novel automation and orchestration framework utilizing SDN control from edge networks to vehicles. This framework incorporated an intent-based traffic offloading solution that enhanced QoE through instantiated policy settings. However, the reliance on SDN introduced complexities in managing edge device configurations and required robust security measures against potential vulnerabilities.

In the context of IoV, the network topology dynamically changes based on the driver's destination, intents, vehicle movements, and road structures. The authors in [225] presented the ACO-AODV routing protocol, which employed an intent-based network for real-time selection of optimal network parameters. However, while this method improved routing selection, it may also introduce additional overhead due to the complexity of maintaining accurate intent tracking in real time.

For IoCV, location served as the foundational data for various mechanisms and functionalities. Existing location privacy protection mechanisms (LPPMs) mostly relyed on biased threat models and lack adaptability to IoCV scenarios. The location privacy protection scheme, named LocJury, was introduced to monitor and predict the intent of location access by transforming given commands or business intents into executable operations, generating location access connections and relevant traffic [226]. Effectively controlling malicious location access through a virtual currency-based regulatory mechanism, LocJury provided an innovative security solution for IoCV scenarios. However, its dependency on virtual currency may raise concerns regarding scalability and acceptance among users in diverse scenarios.

In the field of air-ground integrated vehicular edge computing (AGI-VEC), the authors in [227] introduced the intent-aware learning-based confidence (IUCB) algorithm. IUCB enabled user vehicles (UVs) to learn long-term optimal task offloading policies while meeting long-term ultra-reliable low latency communication (URLLC) constraints. This intelligent task management mechanism enhanced the efficiency of AGI-VEC systems but required significant computational resources, which could be a challenge in resource-constrained vehicular environments. The intent-based network control framework was designed for data dissemination in the ecosystem of vehicular edge computing [228]. This framework configured network policies using intent-based controllers according to application requirements. However, it necessitated coordination between SDN controllers and intent-based policies, which could complicate the overall management and execution processes.

In summary, IDNM is increasingly applied in VANETs to facilitate intelligent and efficient network operations. By leveraging real-time intent information from vehicles, IDNM enables adaptive routing and traffic offloading strategies that respond dynamically to changing vehicular intents. However,

the dynamic nature of vehicular environments introduces complexity in accurately tracking and interpreting vehicle intents in real-time. Additionally, as the demand for resource efficiency increases, IDNM should balance computational overhead with effective decision-making capabilities. Future research directions should focus on enhancing the adaptability of the IDNM approach and improving intent translation accuracy to safeguard vehicular communication.

C. FANET Management

As the size of the FANET continues to grow, network management faces numerous challenges. Node management becomes incredibly complex due to the extensive number of nodes and their wide distribution within the FANET. Tasks such as state monitoring, configuration, maintenance, and fault diagnosis of nodes become increasingly challenging. The dynamic nature of the FANET also presents challenges in topology management, as nodes frequently move, join, and leave the network, resulting in frequent changes in the network topology. Real-time adjustments to the network topology architecture are critical to ensure reliable and effective data transmission. In addition, resource management and route management are also crucial issues that require attention in FANET management. Currently, researchers have proposed several effective solutions, as shown in Table IX, including SNMP, PBNM, and IDNM. These solutions are vital in resolving FANET management issues and providing reliable technical support for the stable operation and efficient communication of the FANET. By implementing these protocols, network managers can monitor the state of the nodes, diagnose faults, and adjust network topology in real-time, ensuring optimal performance of the FANET.

1) SNMP: As a standard management framework, SNMP enables network administrators to monitor FANET nodes in real-time, execute configuration changes, and troubleshoot issues. This provides an effective means for network managers to ensure the stable operation and efficient communication of FANETs. The study in [229] extensively explored the application of the SNMP, demonstrating its capability not only to collect data such as traffic statistics and topological information but also to facilitate network configuration.

SNMP was employed through agents to monitor QoS parameters specifically targeting UAV systems [230]. The protocol retrieved essential QoS data, including routing information from the cloud to UAVs, incoming and outgoing packet counts, and network interface statistics. This application highlighted the critical function of SNMP in maintaining network performance and ensuring service quality. However, it may struggle to provide real-time updates in environments where UAVs frequently change locations or operational states.

The authors in [231] provided a detailed exploration of cluster-based control plane message management. It emphasized that SNMP enables controllers to predict UAV information through UAV contextual data. This capability facilitated intelligent UAV management without necessitating constant real-time control messages. However, this method faced challenges in accuracy if the context information was outdated or insufficiently granular, potentially leading to suboptimal decision-making.

On another note, the QoRA algorithm was presented to prevent congestion during data transmission [232]. The algorithm utilized two components to address congestion, leveraging SNMP and the MIB to determine optimal routing aligned with QoS requirements. However, it may introduce additional complexity in managing the MIB, requiring careful configuration and maintenance.

Despite its advantages, SNMP is not without its challenges. As discussed in [233], a cause for concern emerged in 2022 when SNMP encountered severe vulnerabilities. These vulnerabilities resulted in successful DoS attacks that compromised UAV operations, highlighting an urgent need for ongoing enhancements in SNMP security. The identification of five specific vulnerabilities that could lead to successful attacks emphasizes the necessity for proactive security measures, as the reliance on SNMP for critical network management tasks could expose networks to significant risks. A total of five protocol vulnerabilities that could lead to successful DoS attacks were identified, emphasizing the imperative for ongoing efforts to enhance SNMP protocol security.

In summary, studies have demonstrated SNMP utility in managing QoS parameters for FANET, facilitating intelligent control without the need for constant real-time updates, and optimizing data transmission paths to prevent congestion. However, the reliance on a centralized model can lead to bottlenecks in highly dynamic environments typical of FANETs. Future research should focus on enhancing SNMP security protocols and exploring decentralized management approaches that could mitigate these risks while maintaining effective network management capabilities.

2) PBNM: The introduction of PBNM has significantly changed FANET management. Network administrators can automatically configure, adjust, and maintain the FANET based on predefined policies, providing an efficient and sustainable management approach for the complex FANET.

One of the major challenges in FANETs is maintaining robust communication links among UAVs, primarily due to their high mobility and dynamic topologies. Given that existing routing protocols partially fail to detect changes in network topology, a novel SDN-based hybrid dynamic routing policy was proposed in [4]. This policy integrated topology control, data collection, and routing computation within the SDN controller, meeting multiple requests from UAVs and effectively addressing network dynamics to accomplish tasks collaboratively. However, it introduced overhead associated with the management of the SDN controller and the requirement for continuous monitoring, potentially impacting response times under extreme conditions.

Conventional MANET technologies are overly complex and unable to construct and dynamically adapt to application requirements rapidly. The work by [234] further highlighted the potential of SDN combined with blockchain technology, resulting in a UAV network called SUV. The SUV architecture decoupled the control and data planes for each UAV, allowing for a logically centralized but physically decentralized control structure. However, it faced challenges such as the complexity

TABLE IX: THE OVERVIEW OF THE FANET MANAGEMENT

Management protocols	Overview	Limits	Ref.
SNMP	SNMP enables monitoring, configuration, and troubleshooting of FANET nodes.	Centralized SNMP models lead to bottlenecks in highly dynamic environments.	[229]
	SNMP was used to monitor QoS parameters.	It struggles to provide real-time updates.	[230]
	SNMP enables intelligent management by predicting UAV information using contextual data.	Accuracy issues arise when contextual data is outdated or insufficiently granular.	[231]
	The QoRA algorithm uses SNMP to determine optimal routing aligned with QoS requirements.	It introduces complexity in managing the MIB.	[232]
	SNMP faced critical vulnerabilities that led to DoS attacks, highlighting security concerns.	Vulnerabilities in SNMP lead to DoS attacks.	[233]
PBNM	A SDN-based routing policy integrates topology control, data collection, and routing computation.	It introduces overhead from SDN controller management and requires continuous monitoring.	[4]
	The SUV architecture decouples control and data planes.	Blockchain implementation and ensuring network security is complex.	[234]
	The policy-based protocol uses policy definitions and traffic engineering to optimize routing.	The reliance on policy definitions and routing overhead limits its effectiveness.	[235]
	A policy-based distributed mechanism encompassed policy definition and attack detection components.	The effectiveness relied on the detection of spoofing attempts and required computational resources.	[236]
IDNM	IMF system used technologies like intent translation, policy management, and state awareness.	It relied on accurate intent detection and robust policy verification mechanisms.	[113]
	The FMS system used standardized intent languages for air-to-air and air-to-ground communications.	Reliance on standardized protocols limited flexibility.	[237]
	A traffic intent-aware protocol allocated time slot allocation based on traffic intent.	It only considered the allocation of time slot resources.	[238]

of implementing blockchain for real-time applications and ensuring network security.

In wireless self-organizing networks, strategic communication and configuration management are highly complex, especially in dynamically distinguishing different flow types and their routing to ensure desired performance. To address this challenge, a policy-based routing protocol was introduced for FANET, which was built upon the Babel routing protocol [235]. It encompassed policy definition, routing selection, and traffic engineering. By identifying policies based on the type-of-service field, the enhanced Babel protocol allowed for the selection of optimal paths according to application requirements. However, the reliance on accurate policy definitions and potential routing overhead during high-traffic conditions could limit its effectiveness.

Moreover, most FANET applications depend on GPS-based location information, which is shared with other UAVs, ground control stations, and central service operators in real-time. However, GPS spoofing is a typical attack in FANET, leading to erroneous navigation solutions in global navigation satellite system (GNSS) receivers. To mitigate this risk, the authors in [236] proposed a policy-based distributed detection mechanism that encompassed both policy definition and attack detection components. This mechanism improved flight safety by enabling FANETs to recover their intended paths during GPS spoofing attacks. However, its effectiveness relied on the timely and accurate detection of spoofing attempts, and the implementation may require additional computational resources from UAVs.

In summary, by allowing network administrators to define and implement policies that govern various aspects of network operations, PBNM enhances the adaptability of FANETs to rapidly changing environments. However, there remain some challenges in ensuring security, minimizing overhead, and maintaining robustness in dynamic environments. Addressing these challenges will be critical for the continued evolution and effectiveness of PBNM in FANET applications.

3) IDNM: IDNM represents an advanced approach to network management, enabling automatic configuration and optimization of network resources by comprehending the intent information of network nodes. This innovation introduces new possibilities for enhancing FANET management. IDNM not only addresses complex network tasks but also dynamically adjusts the network topology based on the intent of UAVs, providing a more intelligent and adaptive solution for network management.

The authors in [113] introduced an intent-driven network management system (IMF) specifically designed for FANETs. This system enhanced the automation of network management through technologies such as intent translation, policy management, policy verification, and state awareness. By converting high-level network management intents at lower-level UAV nodes into machine-operable policies, the IMF effectively simplified the complexity of network management. However, the success of this approach heavily relied on the accuracy of intent translation and the robustness of policy verification

mechanisms.

Furthermore, the functionalities of the FANET management system enable ground operators to focus on higher-level tasks, allowing for the holistic management of extensive UAVs. In response to the limitations of existing UAV operations, which often isolate flights to confined airspace, the authors in [237] introduced an integrated two-tier autonomous mode UAV flight management system (FMS) structure. This FMS facilitated collaborative operations by enabling UAVs to communicate through standardized intent languages across air-to-air and air-to-ground channels. However, the reliance on standardized protocols may restrict flexibility in diverse operational scenarios, potentially leading to inefficiencies if the protocols do not adapt well to specific mission requirements.

Additionally, the authors in [238] applied IDN technology to FANET, proposing a dynamic resource allocation protocol based on traffic intent awareness. This protocol dynamically adjusted time slot allocation parameters based on traffic intent, featuring self-analysis and self-configuration capabilities to meet the practical demands of FANETs. However, it depended on accurate and timely detection of traffic intents and only considered the allocation of time slot resources.

In summary, IDNM facilitates the translation of high-level operational intents into actionable policies at the UAV level, thereby reducing the complexity of network management and allowing ground operators to focus on strategic oversight rather than low-level configurations. However, the accuracy and robustness of related technologies are crucial, as incorrect interpretations can lead to inefficient resource utilization or communication breakdowns. Furthermore, ensuring the flexibility of communication protocols to accommodate diverse operational scenarios remains a challenge.

D. SANET Management

Compared with conventional terrestrial networks, SANETs have many different problems, such as transmission delay, node mobility and power limitations. As illustrated in Table X, various innovative management methods and architectures have been proposed by researchers to address the automation, intelligence, and complexity aspects of satellite network management.

1) SNMP: The SNMP demonstrates outstanding performance in LAN/WAN and network interface monitoring. However, it encounters significant challenges in configuration management and control, particularly within satellite networks characterized by long transmission delays, high node mobility, and limited power resources. These inherent complexities render conventional static management systems inadequate for the dynamic nature of satellite communications.

Recent research has sought to enhance the SNMP to address the unique requirements of satellite networks better. The authors in [239] developed a multi-element multi-domain network management protocol (MMMP). This protocol emphasized a holistic approach to network management by segmenting tasks into platform management, user management, performance management, security management, node management, and business management. The MMMP improved overall network management efficiency by allowing for tailored strategies across different domains, though its complexity may lead to increased overhead in resource-limited environments.

Another contribution, the authors in [240] proposed an SNMP-based spacecraft network monitoring system designed for real-time status monitoring of spacecraft networks. This system not only collected configuration and performance data from key nodes but also supported remote monitoring, fault detection, and resource allocation. While this application demonstrates SNMP's versatility in maintaining network stability and efficiency, it may struggle with latency issues inherent to satellite communications, which could delay the response times for critical management tasks. Moreover, the SNMP was utilized to collect data from different platforms, facilitating fault detection and diagnosis in satellite networks [241]. However, reliance on SNMP for comprehensive fault management may be limited by the scalability.

Moreover, the authors in [242] discussed a distributed network traffic detection architecture based on SNMP. This architecture allowed for near-real-time collection of traffic and related information specifically for the Beidou navigation satellite system. While this solution enhanced data gathering capabilities, it may introduce additional complexity and latency in processing, thereby potentially impacting overall network performance.

In summary, SNMP has been adapted for SANET to address the unique challenges posed by satellite communication, such as long transmission delays, high node mobility, and limited power resources. However, the static nature may hinder its effectiveness in rapidly changing environments, necessitating the development of more adaptive management solutions.

2) PBNM: In order to enhance automation and intelligence in satellite network management, the authors in [243] proposed a multi-layered management framework. This framework incorporated global and local controllers. This setup enabled centralized control, mobile management, resource allocation, and business management in an integrated satellite-terrestrial network. A significant advantage of this multi-layered approach lied in its hierarchical design, which balanced centralized control with the adaptability of local controllers, thus optimizing response times for resource and mobility management. However, the architecture may face scalability challenges, especially in dense network deployments, as the central controllers can become bottlenecks if not properly distributed.

Further exploring policy-based management, the authors in [170] developed a dynamic hierarchical structure that integrated an LPDP between the PDP and PEP. By configuring LPDP on satellite network management agents with administrative capabilities, LPDP could facilitate the exchange of policy information with PEP, resulting in enhanced network management efficiency. This hierarchical model provided localized policy decisions, which was beneficial in minimizing latency for time-sensitive operations. However, additional LPDP nodes could increase the overhead for policy synchronization, especially in fast-changing network environments.

The authors in [244] successfully applied policy network management to integrated satellite information networks. It

TABLE X: THE OVERVIEW OF THE SANET MANAGEMENT

Management protocols	Overview	Limits	Ref.
SNMP	A MMMP segmented tasks into multiple domains.	Increased complexity leads to higher overhead.	[239]
	An SNMP-based network monitoring system could monitor status, detect faults, and allocate resources.	Satellite communication latency can delay SNMP's response time.	[240] [241]
	A SNMP-based traffic detection system designed for the Beidou navigation satellite system.	It may introduce additional complexity and latency in processing.	[242]
PBNM	A multi-layered management framework incorporated global and local controllers.	The architecture may face scalability challenges.	[243]
	A hierarchical structure integrates an LPDP to facilitate the exchange of policy information.	Additional LPDP nodes increase the overhead for policy synchronization.	[170]
	A satellite network management architecture uses XML-based policy descriptions.	XML's verbosity led to increased processing times and bandwidth use.	[244]
	A policy-driven resource allocation framework combined with a DRL model.	DRL models required extensive training data and computational resources.	[245]
IDNM	An intent-driven CoX scheme uses intent decomposition, collaborative intent management, and cooperative resource management.	It led to overhead in managing intent and resource coordination.	[246]
	An intent-driven architecture for satellite network service management provided a user-centric and customizable service delivery mechanism.	Customization process introduced latency and required additional computational resources.	[247]
	Intent-driven network addressed resource management issues in LEO satellite networks.	It faltered in unforeseen situations or during extreme network conditions.	[248]
	An intent detection method analyzed user requirements and airborne interfaces.	It required substantial initial calibration and ongoing adjustments.	[249]

designed a policy-based network management architecture tailored for satellite networks using XML-based policy descriptions. This customization to satellite networks allowed for greater specificity in managing satellite information flows and addressing unique operational constraints, such as power limitations and orbital mechanics. While XML offered flexibility and readability, its verbosity led to increased processing times and bandwidth use, which could be a disadvantage in bandwidth-constrained satellite links.

To further adapt to dynamic conditions and user demands, the authors in [245] proposed a policy-driven resource allocation framework combined with a deep reinforcement learning (DRL) model. This framework allowed for the dynamic optimization of resources such as bandwidth and power by adjusting resource allocation policies based on real-time network conditions and communication demands. A notable benefit of this approach was its self-learning capability, enabling adaptive and efficient resource management in heterogeneous satellite networks. However, DRL models often require extensive training data and computational resources, which could be challenging to gather and process in real-time satellite operations.

In summary, through a multi-layered management framework, PBNM effectively addresses the high node dynamics and long delays in satellite networks, enabling intelligent network management and adaptive resource allocation. However, the complexity of PBNM may lead to issues of policy consistency and synchronization, particularly in scenarios with frequent node changes. Additionally, the delays that may be introduced during policy formulation and execution, especially on bandwidth-constrained satellite links, could impact the quality of real-time communication.

3) IDNM: The authors in [246] addressed the challenge of resource scarcity in space networks by proposing an intent-driven CoX scheme aimed at more effectively aligning resources with tasks. This scheme offered several advantages, including coordinated intent decomposition, collaborative intent management, and cooperative resource management. These features enable the network to meet complex task demands and provide on-demand network services. However, the complexity of implementing such a scheme may lead to overhead in managing intent and resource coordination, particularly in rapidly changing environments.

To address the complexities and efficiency challenges introduced by service function chains (SFC) in satellite networks, the authors in [247] proposed an intent-driven architecture for satellite network service management and an SFC deployment scheme. This scheme not only provided a user-centric and customizable service delivery mechanism but also significantly enhanced the flexibility of service delivery and deployment. The main advantage of this architecture was its ability to adapt services based on user requirements. However, the customization process may introduce latency and require additional computational resources, potentially affecting overall performance.

Addressing resource management issues in LEO satellite networks, the authors in [248] integrated intent-driven network with resource management. This integration reduced

the complexity of manual operations, enabling intelligent resource management policies. The approach simplified decision-making processes and improved efficiency, but it could falter in unforeseen situations or during extreme network conditions.

Furthermore, the authors in [249] proposed a universal intent detection method within the framework of intent-driven satellite networks. It analyzed various characteristics, such as user service quality requirements and airborne interfaces for different satellite types, achieving a more intelligent management approach to the satellite network. However, it required substantial initial calibration and ongoing adjustments to account for varying network conditions and user expectations.

In summary, IDNM can enhance the flexibility and scalability of SANET, enabling on-demand network services, efficient SFC deployment, and intelligent resource management. However, the variability in user demands and network conditions may complicate the adaptive nature of IDNM, and the dynamic characteristics of SANETs impose reliability requirements on intent-based decision-making.

E. Summary and Discussion

In this section, we survey the research progress on various network management approaches applied in different xANET scenarios. In general, IDNM demonstrates superiority over SNMP and PBNM. IDNM adopts a more intelligent management protocol, which enables real-time monitoring and prediction of network state and automates troubleshooting and performance optimization. These capabilities significantly enhance the reliability and efficiency of the network. Additionally, IDNM can support multiple types of network nodes and devices, providing flexibility in addressing the various complexities of xANET. From a practical application perspective, the IDNM protocol is better adapted to meet the management requirements of xANET. It can enhance network reliability and performance, thereby facilitating the rapid development and utilization of the network. By leveraging the intelligent and automated management capabilities of IDNM, network administrators can promptly respond to changes in network conditions and maintain better control over the network, thereby improving the user experience and total network performance.

VI. Remaining Challenges and Future Research Directions

As discussed in the sections summarized earlier, we have investigated the concept, challenges, and approaches for xANET management. Nevertheless, there are remaining challenges and novel research directions, such as automation, low overhead, and QoS guarantees. Section VI-A discusses the remaining challenges, and Section VI-B proposes the future research directions of xANET management. Section VI-C provides the summary and discussion of this Section.

A. Remaining Challenges

The management of xANETs presents a unique set of challenges due to their highly dynamic and decentralized nature. Unlike traditional wired networks, xANETs consist of mobile nodes with constantly changing positions, intermittent communication links, and varying network conditions. As a result, the network management protocols must be agile, adaptable, and resource-efficient to handle the diverse and rapidly evolving requirements. In this subsection, we discuss the important technical challenges of network management for the xANETs.

1) Automation: Automation remains one of the most pressing challenges in xANET management. The highly dynamic and unpredictable nature of the network topology makes manual configuration of xANETs impractical, highlighting the need for fully automated network management systems. One of the most significant challenges in automating xANET management is the frequent and unpredictable failures that occur across various layers of the protocol stack. These failures could range from physical layer disruptions due to environmental factors to higher-layer failures related to routing and application performance [250]. Each of these failure points requires tailored mechanisms to detect, diagnose, and recover from them, which further complicates the automation process. Fast failure recovery mechanisms are crucial to maintaining QoS guarantees, especially in mission-critical scenarios where delays in recovery could lead to severe service degradation. Therefore, the inherent challenges of dynamic topologies, unpredictable failures, and limited resources make achieving full automation a technically demanding task.

2) Low Overhead: In high-density xANETs, where a large number of nodes are continuously moving, the volume of control traffic required for maintaining network awareness can become overwhelming. This leads to a scalability issue, as the sheer amount of control messages increases with the number of nodes. As the density of nodes rises, the frequency of these control messages also increases [251]. The control traffic overload can result in network congestion, which in turn degrades the overall service quality, causing delays in routing decisions, increased packet loss, and diminished throughput. Also, constant updates are necessary to keep the network state current and to enable dynamic adaptation, but overly frequent updates can lead to excessive control overhead. Therefore, striking a balance between timely network awareness and minimizing control traffic overhead is a key challenge.

3) Quality of Service Assurance: Ensuring QoS in xANETs is especially challenging due to the heterogeneous nature, variable node mobility, and diverse application requirements across different domains. Traditional QoS mechanisms such as RSVP and DiffServ face limitations when applied to xANETs. RSVP, which is designed to reserve bandwidth for applications, is particularly inefficient in xANETs due to its reliance on end-to-end signaling and the requirement for stable routes between nodes [252]. DiffServ assumes a relatively stable network with predictable traffic flows and well-defined node behaviors, which is not the case in highly mobile and unpredictable environments like xANETs [253]. Therefore, the network management protocol should adjust the QoS parameters based on real-time network conditions and the specific requirements of the applications running on the network.

As xANETs continue to evolve and expand, network man-

agement will remain a significant technical challenge. Automating network operations, ensuring low overhead while maintaining network awareness, and providing reliable QoS assurance in dynamic environments will be crucial for enabling the effective deployment and operation of xANETs. Addressing these challenges will be key to achieving scalable, efficient, and resilient network management for next-generation xANETs.

B. Future Research Directions

As the fields of xANETs continue to evolve, it becomes evident that the future of network management must be intertwined with the latest advancements in emerging technologies. The ability to effectively manage the growing complexity, dynamic nature, and heterogeneity of xANETs will increasingly depend on the integration of advanced computational tools such as AI, generative AI (Gen-AI), edge computing, blockchain, terahertz (THz) Communication and advanced antenna technologies. These technologies hold the potential to significantly enhance the adaptability, efficiency, and intelligence of network management systems, enabling them to handle the vast and unpredictable dynamics of future xANETs autonomously. In this subsection, we discuss future research directions that focus on how xANETs can leverage these technologies to address their ongoing management challenges.

1) AI-Driven Network Management for Dynamic Adaptation: One of the most promising directions for xANET management is the integration of AI-based systems to manage network behavior autonomously. Traditional methods of network configuration and optimization are often based on predefined rules or algorithms. They are not flexible enough to cope with the dynamic and rapidly changing nature of xANETs. Particularly, ML and deep learning (DL) offer a powerful solution to this challenge by enabling systems to learn from data, adapt to network changes, and optimize decisions in real-time [254].

- Topology Discovery and Network Optimization: AI algorithms can be applied to optimize network topologies in real-time, learning from the ongoing changes in node positions, link quality, and other environmental conditions [255]. These AI algorithms can continuously adjust routing, power control, and bandwidth allocation decisions based on the network current state, maximizing throughput, minimizing latency, and ensuring reliability without requiring manual intervention.
- Failure Prediction and Recovery: AI models can be used to predict network failures before they occur by analyzing patterns in network behavior and correlating them with potential failure events. By utilizing predictive modeling, these systems can preemptively adjust routing protocols or reallocate resources to prevent disruptions. For example, by learning from historical data, AI systems can anticipate failure based on the node's mobility pattern and proactively adjust the network configuration, thus reducing downtime and improving network resilience [256].

2) Leveraging Generative AI for Adaptive Network Configuration: Gen-AI, which includes advanced models like generative pre-trained transformers (GPT) and other large-scale neural networks, can significantly contribute to network management tasks in xANETs. When trained on massive amounts of network data, Gen-AI models can generate network configurations and recommend optimized strategies based on dynamic input.

- Automated Policy Generation and Configuration: Network management often involves complex decision-making processes, such as the assignment of resources, setting priorities for traffic, or defining security policies. Traditionally, these tasks require extensive human intervention, especially in dynamic environments where network parameters are constantly changing. The deployment of Gen-AI models has already begun to revolutionize the way complex network decisions are made [257]. Gen-AI models can generate context-specific network policies that reflect real-time conditions and allow for rapid adjustments to network configurations.
- IDNM: IDNM can be used to autonomously translate high-level operational goals or intents into low-level network configurations. For example, Gen-AI models can understand the specific requirements of applications running in an xANET, such as low latency for real-time communications or high bandwidth for data-heavy services, and automatically generate appropriate QoS policies, routing decisions, and resource allocations [258].

3) Integrating Edge and Cloud Computing: The decentralized and distributed nature of xANETs makes it challenging to rely solely on a centralized control system for network management. Integrating edge computing and cloud-based resources into the xANET management framework presents a promising avenue for future research.

- Edge-AI for Localized Decision Making: By combining AI with edge computing, the network management system can offload specific tasks to edge devices located closer to the nodes [259]. This setup reduces the dependency on distant centralized servers, thereby lowering latency and enabling faster decision-making processes. Edge-AI can be helpful for local network health monitoring, failure detection, and autonomous configuration without requiring global coordination.
- Cloud-Assisted Global Network Orchestration: While edge computing handles localized tasks, cloud computing can provide global network orchestration [260]. By using cloud resources, the management system can gain a comprehensive view of the entire xANET. Cloud-based orchestration also allows for inter-network cooperation, where multiple xANETs can collaborate on resource sharing, improving coverage and ensuring seamless inter-network operation [81].

4) Blockchain for Trust and Security: Security and trust issues remain critical for xANET management, especially as the network becomes more autonomous and decentralized. The integration of blockchain technology could provide a robust solution for ensuring data integrity, secure communication, and trustworthy decision-making within the network [261]. In scenarios where xANETs are highly decentralized and involve

many independent nodes, blockchain can enable trustless collaboration. By recording all actions and decisions in a distributed ledger, blockchain ensures that network operations are transparent and verifiable, preventing malicious actors from compromising the network's integrity [262].

5) Terahertz Communication: xANETs have stringent application requirements for high bandwidth and low latency. THz communication can provide extremely high bandwidths, supporting higher data transmission rates and reducing congestion during data transmission, thereby ensuring the efficient flow of data in large-scale, high-density xANET deployments [263]. Additionally, the high frequency of the THz band offers shorter wavelengths, enabling more precise directional transmission, effectively reducing signal interference and attenuation, and improving the signal quality and coverage [264].

6) Advanced Antenna Technologies: The highly dynamic characteristics of xANETs pose significant challenges to network stability and communication quality. Advanced antenna technologies, such as RIS and MIMO, have become crucial for optimizing the performance of xANETs. Massive MIMO improves spatial diversity by increasing the number of antennas, which enhances signal quality and communication reliability [265]. Particularly in areas with high node density and mobility, MIMO technology can effectively improve network throughput and coverage, helping the network adapt to complex environments and dynamic changes. Meanwhile, RIS uses software-controlled metasurfaces to manipulate the propagation path of electromagnetic waves intelligently, providing stronger interference resistance in environments with severe multipath interference and signal attenuation. This optimizes signal quality and coverage in the network [266]. Additionally, combining RIS technology with AI allows for the intelligent adjustment of signal reflection paths, further enhancing network adaptability and resource utilization.

C. Summary and Discussion

With the development of xANETs, we have explored the key challenges and future research directions in this section. The dynamic and decentralized nature of xANETs introduces significant challenges, including automation, low overhead management, and QoS assurance. Future research should focus on leveraging emerging technologies such as AI, Gen-AI, large models, edge computing, blockchain, THz Communication and advanced antenna to address these challenges. The ongoing development of these technologies will be crucial for the evolution of self-organizing, self-healing networks capable of efficiently managing resources and ensuring QoS in next-generation communication systems.

VII. Conclusion

The xANETs are complex and dynamic systems with various mobile nodes interacting to perform communication tasks. The management of these networks is encountering significant challenges, as the nodes are highly mobile, and there is no central node to manage their operations. While conventional approaches such as SNMP are still utilized, they become less effective as xANET becomes more extensive and more complex. Autonomous approaches are an improvement over conventional approaches. In this paper, we provided a survey of the network management approach evolution for xANET, from configuration-based to policy-based and intent-driven approaches. We began with the characteristics and applications of xANET, including their common and different characteristics, and the application of multiple xANETs coexisting. Subsequently, we provided a comprehensive overview of the concepts and challenges associated with xANET management. Next, we highlighted the evolution of management protocols from architectures and concepts, including SNMP, PBNM, and IDNM, respectively. Moreover, the paper surveyed the management research from different protocols in xANET. We overviewed the existing literature on network management approaches employed in various scenarios within MANET, VANET, FANET and SANET. Notably, each approach offers distinct advantages, but it is clear that IDNM stands out as the most promising protocol, as it enables autonomous, adaptive, and scalable management that aligns with the needs of large-scale and highly dynamic xANETs. Finally, our survey concluded with remaining challenges and future research directions that need further investigation. We believe that future research on network management approaches will incorporate emerging technologies such as AI to achieve more intelligent, resilient, and self-optimizing network management.

References

[1] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture,* vol. 105, pp. 101701–101729, May 2020.

[2] S. Yogarayan, "Wireless ad hoc network of manet, vanet, fanet and sanet: A review," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 13, no. 4, pp. 13–18, Dec. 2021.

[3] M. A. Al-Absi, A. A. Al-Absi, M. Sain and H. Lee, "Moving ad hoc networks-a comparative study," *Sustainability,* vol. 13, no. 11, pp. 6187–6218, May 2021.

[4] A. T. Albu-Salih, S. A. H. Seno and S. J. Mohammed, "Dynamic routing method over hybrid SDN for flying ad hoc networks," *Baghdad Science Journal,* vol. 15, no. 3, pp. 361–369, Sep. 2018.

[5] G. Wang, J. Zhang, Y. Zhang, C. Liu and Z. Chang, "Performance evaluation of routing algorithm in satellite self-organizing network on OMNeT++ platform," *Electronics,* vol. 13, no. 19, pp. 3963–3979, Oct. 2024.

[6] R. B. Swain and S. Ranganathan, "Modeling interlinkages between sustainable development goals using network analysis," *World Development,* vol. 138, pp. 105136–105150, Feb. 2021.

[7] W. L. Filho, A. L. Salvia and J. H. P. P. Eustachio, "An overview of the engagement of higher education institutions in the implementation of the UN sustainable development goals," *Journal of Cleaner Production,* vol. 386, pp. 135694–135703, Feb. 2023.

[8] Q. Wang, W. Li, Z. Yu, Q. Abbasi, M. Imran, S. Ansari, Y. Sambo, L. Wu, Q. Li and T. Zhu, "An overview of emergency communication networks," *Remote Sensing,* vol. 15, no. 6, pp. 1595–1631, Mar. 2023.

[9] S. T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. Devetsikiotis and F. H. P. Fitzek, "A theoretical discussion and survey of network automation for IoT: Challenges and opportunity," *IEEE Internet of Things Journal,* vol. 8, no. 15, pp. 12021–12045, Aug. 2021.

[10] M. Ozger, F. Alagoz and O. B. Akan, "Clustering in multi-channel cognitive radio ad hoc and sensor networks," *IEEE Communications Magazine,* vol. 56, no. 4, pp. 156–162, Apr. 2018.

[11] X. Zhou, X. Yang, J. Ma and K. I. -K. Wang, "Energy-efficient smart routing based on link correlation mining for wireless edge computing in IoT," *IEEE Internet of Things Journal,* vol. 9, no. 16, pp. 14988–14997, Aug. 2022.

[12] O. Singh, R. Vinoth, A. Singh and N. Singh, "Navigating security threats and solutions using AI in wireless sensor networks," *Interna-*

tional Journal of Communication Networks and Information Security, vol. 16, no. 4, pp. 411–427, Dec. 2024.

[13] M. Y. Arafat, S. Poudel and S. Moh, "Medium access control protocols for flying ad hoc networks: A review," *IEEE Sensors Journal,* vol. 21, no. 4, pp. 4097–4121, Oct. 2020.

[14] T. Qiu, N. Chen, K. Li, M. Atiquzzaman and W. Zhao, "How can heterogeneous internet of things build our future: A survey," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 3, pp. 2011–2027, 3rd Quart. 2018.

[15] S. T. Arzo, R. Bassoli, F. Granelli and F. H. P. Fitzek, "Multi-agent based autonomic network management architecture," *IEEE Transactions on Network and Service Management,* vol. 18, no. 3, pp. 3595–3618, Sep. 2021.

[16] S. I. Saheb and A. Rasool Md, "Auto-discovery and monitoring of network resources: SNMP-based network mapping and fault management," *Smart Computing Techniques and Applications, Springer,* vol. 225, pp. 643-653, Jul. 2021.

[17] C. Tang, X. Fu and P. Tang, "Policy-based network access and behavior control management," *IEEE 20th International Conference on Communication Technology (ICCT),* Nanning, China, Oct. 2020.

[18] A. C. Riekstin, G. C. Januario, B. B. Rodrigues, V. T. Nascimento, T. C. M. de Brito Carvalho and C. Meirosu, "A survey of policy refinement methods as a support for sustainable networks," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 222–235, 1st Quart. 2016.

[19] C. Yang, X. Mi, Y. Ouyang, R. Dong, J. Guo and M. Guizani, "SMART intent-driven network management," *IEEE Communications Magazine,* vol. 61, no. 1, pp. 106–112, Jan. 2023.

[20] R. Sultana, J. Grover and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications,* vol. 27, pp. 100284–100307, Jan. 2021.

[21] S. Singh, A. Pise, O. Alfarraj, A. Tolba and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," *Sustainable Cities and Society,* vol. 79, pp. 103483–103493, Apr. 2022.

[22] W. Quan, Z. Xu, M. Liu, N. Cheng, G. Liu, D. Gao, H. Zhang, X. Shen and W. Zhuang, "AI-driven packet forwarding with programmable data plane: A survey," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 1, pp. 762–790, 1st Quart. 2022.

[23] T. Li, C. Yang, Y. Song, L. Cai, R. Zheng, X. Liu, Z. Ji and S. Liu, "Architecting autonomous network management and control via intent-driven decoupled network," *IEEE Network,* vol. 38, no. 6, pp. 361–369, Nov. 2024.

[24] H. Wang, "Improvement and implementation of wireless network topology system based on SNMP protocol for router equipment," *Computer Communications,* vol. 151, pp. 10–18, Feb. 2020.

[25] F. Deng, Z. Yu, W. Liu, X. Luo, Y. Fu, B. Qiang, C. Xu and Z. Li, "An efficient policy evaluation engine for XACML policy management," *Information Sciences,* vol. 547, pp. 1105–1121, Feb. 2021.

[26] J. Wang, L. Zhang, Y. Yang, Z. Zhuang, Q. Qi, H. Sun, L. Lu, J. Feng and J. Liao, "Network meets chatgpt: Intent autonomous management, control and operation," *Journal of Communications and Information Networks,* vol. 8, no. 3, pp. 239–255, Sep. 2023.

[27] Y. Yu, X. Li, X. Leng, L. Song, K. Bu, Y. Chen, J. Yang, L. Zhang, K. Cheng and X. Xiao, "Fault management in software-defined networking: A survey," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 349–392, Sep. 2018.

[28] E. Moridi, M. Haghparast, M. Hosseinzadeh and S. J. Jassbi, "Fault management frameworks in wireless sensor networks: A survey," *Computer Communications,* vol. 155, pp. 205–226, Apr. 2020.

[29] M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Żywiołek and I. Ullah, 'Swarm of UAVs for network management in 6G: A technical review," *IEEE Transactions on Network and Service Management,* vol. 20, no. 1, pp. 741–761, Mar. 2023.

[30] F. Belamri, S. Boulfekhar and D. Aissani, "A survey on QoS routing protocols in vehicular ad hoc network (VANET)," *Telecommunication Systems,* vol. 78, no. 1, pp. 117–153, Jun. 2021.

[31] P. Monika, R. M. Negara and D. D. Sanjoyo, "Performance analysis of software defined network using intent monitor and reroute method on ONOS controller," *Bulletin of Electrical Engineering and Informatics,* vol. 9, no. 5, pp. 2065–2073, Oct. 2020.

[32] Y. Tian, W. Chen and C. T. Lea, "Monitor placement for link latency measurement in hybrid SDNs," *IEEE Transactions on Network and Service Management,* vol. 17, no. 2, pp. 750–763, Jun. 2020.

[33] J. Zhang, H. Feng, B. Liu and D. Zhao, "Survey of technology in network security situation awareness," *Sensors,* vol. 23, no. 5, pp. 2608–2633, Feb. 2023.

[34] D. Bringhenti, G. Marchetto, R. Sisto and F. Valenza, "Automation for network security configuration: State of the art and research trends," *ACM Computing Surveys,* vol. 56, no. 3, pp. 1–37, Oct. 2023.

[35] E. Zeydan and Y. Turk, "Recent advances in intent-based networking: A survey," *IEEE Vehicular Technology Conference (VTC),* Antwerp, Belgium, May 2020.

[36] A. Ito and H. Hatano, "A study on a protocol for ad hoc network based on bluetooth low energy," *Cognitive Infocommunications, Theory and Applications,* vol. 13, pp. 433–458, Aug. 2018.

[37] S. Sinche, D. Raposo, N. Armando, A. Rodrigues, F. Boavida, V. Pereira and J. S. Silva, "A survey of IoT management protocols and frameworks," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1168–1190, 2nd Quart. 2020.

[38] M. M. S. Bait Ali Sulaiman, "Intelligent mobile ad hoc network management system," *PhD thesis, Brunel University London,* 2016.

[39] N. Saraiva, N. Islam, D. A. L. Perez and C. E. Rothenberg, "Policy-driven network traffic rerouting through intent-based control loops," *Proceedings of the XXIV Workshop on Management and Operations of Networks and Services, SBC,* Porto Alegre, RS, Brasil, Sep. 2019.

[40] J. Liu, Y. Shi, Z. M. Fadlullah and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 4, pp. 2714–2741, 4th Quart. 2018.

[41] M. Tosun, U. C. Cabuk, E. Haytaoglu, O. Dagdeviren and Y. Ozturk, "CoRMAC: A connected random topology formation with maximal area coverage in wireless ad-hoc networks," *IEEE Internet of Things Journal,* vol. 10, no. 14, pp. 12379–12392, Jul. 2023.

[42] H. Luo, Y. Wu, G. Sun, H. Yu and M. Guizani, "ESCM: An efficient and secure communication mechanism for UAV networks," *IEEE Transactions on Network and Service Management,* vol. 21, no. 3, pp. 3124–3139, Jun. 2024.

[43] J. Guo, H. Gao, Z. Liu, F. Huang, J. Zhang, X. Li and J. Ma, "ICRA: An intelligent clustering routing approach for UAV ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 2, pp. 2447–2460, Feb. 2023.

[44] N. Temene, C. Sergiou, C. Georgiou and V. Vassiliou, "A survey on mobility in wireless sensor networks," *Ad Hoc Networks,* vol. 125, pp. 102726–102756, Feb. 2022.

[45] P. Goyal, V. Rishiwal and A. Negi, "A comprehensive survey on QoS for video transmission in heterogeneous mobile ad hoc network," *Transactions on Emerging Telecommunications Technologies,* vol. 34, no. 7, pp. 4775–4797, Apr. 2023.

[46] G. Feng, X. Li, Z. Gao, C. Wang, H. Lv and Q. Zhao, "Multi-path and multi-hop task offloading in mobile ad hoc networks," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 6, pp. 5347–5361, Jun. 2021.

[47] D. Zhang, H. Ge, T. Zhang, Y. Y. Cui, X. Liu and G. Mao, "New multi-hop clustering algorithm for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 20, no. 4, pp. 1517–1530, Apr. 2018.

[48] D. S. Lakew, U. Saąfad, N. N. Dao, W. Na and S. Cho, "Routing in flying ad hoc networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1071–1120, 3nd Quart. 2020.

[49] A. M. Rahmani, S. Ali, E. Yousefpoor, M. S. Yousefpoor, D. Javaheri, P. Lalbakhsh, O. H. Ahmed, M. Hosseinzadeh and S. W. Lee, "OLSR+: A new routing method based on fuzzy logic in flying ad-hoc networks (FANETs)," *Vehicular Communications,* vol. 36, pp. 100489–100506, Aug. 2022.

[50] J. Shanthini, P. Punitha and S. Karthik, "Improvisation of node mobility using cluster routing-based group adaptive in MANET," *Computer Systems Science & Engineering,* vol. 44, no. 3, pp. 2619–2636, Mar. 2022.

[51] I. Banerjee, M. Warnier and F. M. T. Brazie, "Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices," *Complex Adaptive Systems Modeling,* vol. 8, no. 1, pp. 7–28, 3nd Quart. 2020.

[52] A.H. Azni, R. Ahmad, Z. A. M. Noh, F. Hazwani and N. Hayaati, "Systematic review for network survivability analysis in MANETS," *Procedia-Social and Behavioral Sciences,* vol. 195, pp. 1872–1881, Jul. 2015.

[53] F. Safari, I. Savic, H. Kunze, J. Ernst and D. Gillis, "The diverse technology of MANETs: A survey of applications and challenges," *International Journal of Future Computer and Communication,* vol. 12, no. 2, pp. 37–48, Jun. 2023.

[54] Z. Chen, W. Zhou, S. Wu and L. Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," *IEEE Access,* vol. 8, pp. 44760–44773, Mar. 2020.

[55] D. Ramphull, A. Mungur, S. Armoogum and S. Pudaruth, "A review of mobile ad hoc network (MANET) protocols and their applications," *International conference on intelligent computing and control systems (ICICCS),* Madurai, India, May 2021.

[56] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani and A. S. Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs)," *International Congress on Human-computer Interaction, Optimization and Robotic Applications (HORA),* Ankara, Turkey, Jun. 2020.

[57] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay and A. R. Khan, "Vehicular ad hoc network (VANET) localization techniques: A survey," *Archives of Computational Methods in Engineering,* vol. 28, pp. 3001–3033, Sep. 2020.

[58] A. Rasheed, S. Gillani, S. Ajmal and A. Qayyum, "Vehicular ad hoc network (VANET): A survey, challenges, and applications," *Vehicular Ad-Hoc Networks for Smart Cities: Second International Workshop,* Singapore, Mar. 2017.

[59] Q. Pan, J. Wu, J. Nebhen, A. K. Bashir, Y. Su and J. Li, "Artificial intelligence-based energy efficient communication system for iIntelligent reflecting surface-driven VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 10, pp. 19714–19726, Oct. 2022.

[60] S. Sharma and A. Kaul, "VANETs cloud: Architecture, applications, challenges, and issues," *Archives of Computational Methods in Engineering,* vol. 28, pp. 2081–2102, Jun. 2021.

[61] M. Ye, L. Guan and M. Quddus, "TDMP: Reliable target driven and mobility prediction based routing protocol in complex vehicular ad-hoc network," *Vehicular Communications,* vol. 31, pp. 100378–100413, Oct. 2021.

[62] Q. Liu, G. Chuai, J. Wang and J. Pan, "Proactive mobility management with trajectory prediction based on virtual cells in ultra-dense networks," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 8, pp. 8832–8842, Aug. 2020.

[63] M. Fogli, C. Giannelli and C. Stefanelli, "Software-defined networking in wireless ad hoc scenarios: Objectives and control architectures," *Journal of Network and Computer Applications,* vol. 203, pp. 103387–103395, Jul. 2022.

[64] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," *Computer science review,* vol. 39, pp. 100359–100387, Feb. 2021.

[65] G. Faraci, S. A. Rizzo and G. Schembra, "Green edge intelligence for smart management of a FANET in disaster-recovery scenarios," *IEEE Transactions on Vehicular Technology,* vol. 72, no. 3, pp. 3819–3831, Mar. 2023.

[66] G. Amponis, T. Lagkas, P. Sarigiannidis, V. Vitsas, P. Fouliras and S. Wan, "A survey on FANET routing from a cross-layer design perspective," *Journal of Systems Architecture,* vol. 120, pp. 102281–102301, Nov. 2021.

[67] X. Qiu, Y. Yang, L. Xu, J. Yin and Z. Liao, "Maintaining links in the highly dynamic fanet using deep reinforcement learning," *IEEE Transactions on Vehicular Technology,* vol. 72, no. 3, pp. 2804–2818, Mar. 2023.

[68] M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk and H. Song, "A systematic survey: Security threats to UAV-aided IoT applications, taxonomy, current challenges and requirements with future research directions," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 2, pp. 1437–1455, Feb. 2023.

[69] H. Al-Hraishawi, H. Chougrani, S. Kisseleff, E. Lagunas and S. Chatzinotas, "A survey on nongeostationary satellite systems: The communication perspective," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 1, pp. 101–132, 1st Quart. 2023.

[70] G. Mushet, G. Mingotti, C. Colombo and C. Mcinnes, "Self-organising satellite constellation in geostationary earth orbit," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 51, no. 2, pp. 910–923, Apr. 2015.

[71] M. Khammassi, A. Kammoun and M. S. Alouini, "Precoding for high-throughput satellite communication systems: A survey," *IEEE Communications Surveys & Tutorials,* vol. 26, no. 1, pp. 80–118, 1st Quart. 2024.

[72] B. Al Homssi, A. Al-Hourani, K. Wang, P, Conder, S, Kandeepan, J, Choi, B. Allen and B. Moores, "Next generation mega satellite networks for access equality: Opportunities, challenges, and performance," *IEEE Communications Magazine,* vol. 60, no. 4, pp. 18–24, Apr. 2022.

[73] N. Pachler, I. del Portillo, E. F. Crawley and B. G. Cameron, "An updated comparison of four low earth orbit satellite constellation systems to provide global broadband," *International Conference on Communications Workshops (ICC Workshops),* Montreal, QC, Canada, Jun. 2021.

[74] E. Turan, S. Speretta and E. Gill, "Autonomous navigation for deep space small satellites: Scientific and technological advances," *Acta Astronautica,* vol. 193, pp. 56–74, Apr. 2022.

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

[76] L. Zong, H. Wang, Y. Bai and G. Luo, "Cross-regional transmission control for satellite network-assisted vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 7, pp. 9692-9701, Jul. 2022.

[77] R. Wang, M. A. Kishk and M. S. Alouini, "Stochastic geometry-based low latency routing in massive LEO satellite networks," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, no. 5, pp. 3881–3894, Oct. 2022.

[78] E. Chauhan, M. Sirswal, D. Gupta and A. Khanna, "A critical review: SANET and other variants of ad hoc networks," *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020,* Springer, Singapore, Jul. 2020.

[79] F. Pasandideh, J. P. J. da Costa, R. Kunst, N. Islam, W. Hardjawana and E. Pignaton de Freitas, "A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies," *Remote Sensing,* vol. 14, no. 18, pp. 4459–4484, Sep. 2022.

[80] Y. Lu, W. Wen, K. K. Igorevich, P. Ren, H. Zhang, Y. Duan, H. Zhu and P. Zhang, "UAV ad hoc network routing algorithms in space-air-ground integrated networks: Challenges and directions," *Drones,* vol. 7, no. 7, pp. 448–482, Jul. 2023.

[81] P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom and H. Olufowobi, "Survey of interoperability challenges in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 12, pp. 22838–22861, Dec. 2022.

[82] H. Lu, Y. Zhang, Y. Li, C. Jiang and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 6, pp. 3521–3532, Jun. 2021.

[83] M. S. Peelam, Naren, M. Gera, V. Chamola and S. Zeadally, "A review on emergency vehicle management for intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems,* vol. 25, no. 11, pp. 15229–15246, Nov. 2024.

[84] A. Widjajarto, M. Lubis and M. R. Syahputra, "Optimization performance management with FCAPS and ITILv3: Opportunities and obstacles," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 17, no. 1, pp. 281–290, Jan. 2020.

[85] M. Fatima and A. Khursheed, "Heterogeneous ad-hoc network management: An overview," *Cloud Computing Enabled Big-Data Analytics in Wireless Ad-hoc Networks,* ISBN 9781003206453, pp. 103–123, Mar. 2022.

[86] F. M. Awaysheh, M. Alazab, S. Garg, D. Niyato and C. Verikoukis, "Big data resource management & networks: Taxonomy, survey, and future directions," *IEEE Communications Surveys & Tutorials,* vol. 23, no. 4, pp. 2098–2130, 4th Quart. 2021.

[87] S. A. Sharifi and S. M. Babamir, "The clustering algorithm for efficient energy management in mobile ad-hoc networks," *Computer networks,* vol. 166, pp. 106983–107008, Jan. 2020.

[88] S. Zahid, K. Ullah, A. Waheed, S. Basar, M. Zareei and R. R. Biswal, "Fault tolerant DHT-based routing in MANET," *Sensors,* vol. 22, no. 11, pp. 4280–4304, Jun. 2022.

[89] P. Novotny, B. J. Ko and A. L. Wolf, "Locating faults in MANET-hosted software systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 15, no. 3, pp. 452–465, May-Jun. 2018.

[90] A. M. Eltahlawy, H. K. Aslan, E. G. Abdallah, M. S. Elsayed, A. D. Jurcut and M. A. Azer, "A survey on parameters affecting manet performance," *Electronics,* vol. 12, no. 9, pp. 1956–1984, Apr. 2023.

[91] D. Kanellopoulos and V. K. Sharma, "Survey on power-aware optimization solutions for MANETs," *Electronics,* vol. 9, no. 7, pp. 1129–1193, Jul. 2020.

[92] P. Chitra and T. Ranganayaki, "A study on manet: Applications, challenges and issues," *International Journal of Engineering Research & Technology (IJERT),* vol. 8, no. 3, pp. 1–4, 2020.

[93] S. Kuang, J. Zhang and A. Mohajer, "Reliable information delivery and dynamic link utilization in MANET cloud using deep reinforcement learning," *Transactions on Emerging Telecommunications Technologies,* vol. 35, no. 9, pp. 5028–5052, Sep. 2024.

[94] S. Rabia, S. I. I, G. Lilia and K. Benjamin, "SDMANET: Enhancing MANETs with hybrid protocols through SDN integration," *International Conference on Artificial Intelligence, Computer, Data Sciences and*

Applications (ACDSA), Victoria, Seychelles, Feb. 2024.

[95] S. S. Priya, S. S and S. P, "Routing optimization for mobile ad hoc networks (MANETs) in urban environments," *International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS),* Erode, India, Oct. 2023.

[96] S. Pamarthi and R. Narmadha, "Literature review on network security in wireless mobile ad-hoc network for IoT applications: Network attacks and detection mechanisms," *International Journal of Intelligent Unmanned Systems,* vol. 10, no. 4, pp. 482–506, Nov. 2022.

[97] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT),* Amman, Jordan, Apr. 2019.

[98] M. Mahamat, G. Jaber and A. Bouabdallah, "Achieving efficient energy-aware security in IoT networks: A survey of recent solutions and research challenges," *Wireless Networks,* vol. 29, no. 2, pp. 787–808, Nov. 2022.

[99] M. A. Karabulut, A. F. M. S. Shah, H. Ilhan, A. S. K. Pathan and M. Atiquzzaman, "Inspecting VANET with various critical aspects-a systematic review," *Ad Hoc Networks,* vol. 150, pp. 103281–103299, Nov. 2023.

[100] S. Kudva, S. Badsha, S. Sengupta, H. La and I. Khalil and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing,* vol. 152, pp. 144–156, Jun. 2021.

[101] A. Guerna, S. Bitam and C. T. Calafate, "AC-RDV: a novel ant colony system for roadside units deployment in vehicular ad hoc networks," *Peer-to-Peer Networking and Applications,* vol. 14, pp. 627–643, Oct. 2020.

[102] A. Srivastava, S. Verma, Kavita, N. Z. Jhanjhi, M. N. Talib and A. Malhotra, "Analysis of quality of service in VANET," *IOP Conference Series: Materials Science and Engineering,* vol. 993, no. 1, pp. 12061–12081, 2020.

[103] S. Gajare, P. Deore and S. Wagh, "Traffic management in VANET using clustering," *International Journal of Engineering and Technical Research (IJETR),* vol. 2, no. 5, pp. 175–180, May 2014.

[104] C. Gao, G. Wang, W. Shi, Z. Wang and Y. Chen, "Autonomous driving security: State of the art and challenges," *IEEE Internet of Things Journal,* vol. 9, no. 10, pp. 7572–7595, May 2022.

[105] S. Sheela, K. R. Nataraj and S. Mallikarjunaswamy, "A comprehensive exploration of resource allocation strategies within vehicle ad-hoc networks," *Mechatronics and Intelligent Transportation Systems,* vol. 2, no. 3, pp. 169–190, Sep. 2023.

[106] S. Panda, I. S. Samanta, P. K. Rout, B. K. Sahu, M. Bajaj, V. Blazek, L. Prokop and S. Misak, "Priority-based scheduling in residential energy management systems integrated with renewable sources using adaptive salp swarm algorithm," *Results in Engineering,* vol. 23, pp. 102643–102659, Sep. 2024.

[107] X. Jiang, F. R. Yu, T. Song and V. C. M. Leung, "Resource allocation of video streaming over vehicular networks: A survey, some research issues and challenges," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 7, pp. 5955–5975, Jul. 2022.

[108] S. Sharma, A. Kaul, S. Ahmed and S. Sharma, "A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions," *International Journal of Communication Systems,* vol. 34, no. 14, pp. 4905–4972, Aug. 2021.

[109] M. F. Tuysuz and R. Trestian, "From serendipity to sustainable green IoT: Technical, industrial and political perspective," *Computer Networks,* vol. 182, pp. 107469–107498, Dec. 2020.

[110] D. Gura, V. Rukhlinskiy, V. Sharov and A. Bogoyavlenskiy, "Automated system for dispatching the movement of unmanned aerial vehicles with a distributed survey of flight tasks," *Journal of Intelligent Systems,* vol. 30, no. 1, pp. 728–738, May 2021.

[111] I. Chandran and K. Vipin, "Multi-UAV networks for disaster monitoring: Challenges and opportunities from a network perspective," *Drone Systems and Applications,* vol. 12, pp. 1–28, Apr. 2024.

[112] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones,* vol. 6, no, 6, pp. 147–174, Apr. 2022.

[113] T. Li, C. Yang and L. Yang, "Intent-driven QoS-aware routing management for flying ad hoc networks," *International Wireless Communications and Mobile Computing (IWCMC),* Dubrovnik, Croatia, May 2022.

[114] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access,* vol. 8, pp. 56371–56378, Mar. 2020.

[115] B. Mohammed, "AI-empowered flying ad-hoc networks for dynamic connectivity," *International Journal of Computing and Digital Systems,* vol. 15, no. 1, pp. 167–177, Jan. 2024.

[116] S. O. Ajakwe, D. S. Kim and J. M. Lee, "Drone transportation system: systematic review of security dynamics for smart mobility," *IEEE Internet of Things Journal,* vol. 10, no. 16, pp. 14462–14482, Aug. 2023.

[117] A. S. Nair and S. M. Thampi, "Flying ad hoc networks: security, authentication protocols, and future directions," *Internet of Things and Secure Smart Environments,* Chapman and Hall/CRC, pp. 223–272, 2020.

[118] M. A. Khan, I. Ullah, N. Kumar, O. S. Oubbati, I. M. Qureshi, F. Noor and F. U. Khanzada, "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 5, pp. 4839–4851, May 2021.

[119] Y. Tan, J. Liu and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Transactions on Industrial Informatics,* vol. 17, no. 11, pp. 7629–7638, Nov. 2021.

[120] H. Xie, J. Zheng, T. He, S. Wei and C. Hu, "A blockchain-based ubiquitous entity authentication and management scheme with homomorphic encryption for FANET," *Peer-to-Peer Networking and Applications,* vol. 17, no. 2, pp. 569–584, Feb. 2024.

[121] B. Xiao and S. Yin, "A deep learning based data-driven thruster fault diagnosis approach for satellite attitude control system," *IEEE Transactions on Industrial Electronics,* vol. 68, no. 10, pp. 10162–10170, Oct. 2020.

[122] S. K. Ibrahim, A. Ahmed, M. A. E. Zeidan and I. E. Ziedan, "Machine learning techniques for satellite fault diagnosis," *Ain Shams Engineering Journal,* vol. 11, no. 1, pp. 45–56, Mar. 2020.

[123] X. Liu, T. Ma, Z. Tang, X. Qin, H. Zhou and X. S. Shen, "Ultrastar: A lightweight simulator of ultra-dense LEO satellite constellation networking for 6G," *IEEE/CAA Journal of Automatica Sinica,* vol. 10, no. 3, pp. 632–645, Mar. 2023.

[124] N. A. Ochuba, D. O. Olutimehin, O. G. Odunaiya and O. T. Soyombo, "Sustainable business models in satellite telecommunications," *Engineering Science & Technology Journal,* vol. 5, no. 3, pp. 1047–1059, Mar. 2024.

[125] G. M. Cappello, G. Colajanni, P. Daniele, L. Galluccio, C. Grasso, G. Schembra and L. Scrimali, "Optimizing FANET lifetime for 5G softwarized network provisioning," *IEEE Transactions on Network and Service Management,* vol. 19, no. 4, pp. 4629–4649, Dec. 2022.

[126] A. Mekrache, A. Ksentini and C. Verikoukis, "Machine reasoning in FCAPS: Towards enhanced beyond 5G network management," *IEEE Communications Surveys & Tutorials,* vol. 26, no. 4, pp. 2769-2797, 4th Quart 2024.

[127] K. Guo, K. An, B. Zhang, Y. Huang, X. Tang, G. Zheng and T. A. Tsiftsis, "Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 5, pp. 5129–5141, May 2020.

[128] A. Diro, S. Kaisar, A. V. Vasilakos, A. Anwar, A. Nasirian and G. Olani, "Anomaly detection for space information networks: A survey of challenges, techniques, and future directions," *Computers & Security,* vol. 139, pp. 103705–103737, Apr. 2024.

[129] S. M. Mohammed, A. Al-Barrak and N. T. Mahmood, "Enabling technologies for ultra-low latency and high-reliability communication in 6G networks," *Ingénierie des Systèmes d'Information,* vol. 29, no. 3, pp. 1195–1208, Jun. 2024.

[130] M. N. A. Siddiky, M. E. Rahman and M. S. Uzzal, "Beyond 5G: A comprehensive exploration of 6G wireless communication technologies," *Preprints,* May 2024, doi: 10.20944/preprints202405.0715.v1.

[131] C. Serôdio, J. Cunha, G. Candela, S. Rodriguez, X. R. Sousa and F. Branco, "The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges," *Future Internet,* vol. 15, no. 11, pp. 348–380, Oct. 2023.

[132] Q. Duan, J. Huang, S. Hu, R. Deng, Z. Lu and S. Yu, "Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: Challenges, recent advances, and future directions," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 4, pp. 2892–2950, 4th Quart. 2023.

[133] V. L. Nguyen, P. C. Lin, B. C. Cheng, R. H. Hwang and Y. D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials,* vol. 23, no. 4, pp. 2384–2428, 4th Quart. 2021.

[134] A. Bhattarai, "AI-enhanced cloud computing: A comprehensive review of techniques, challenges, and future directions in resource manage-

ment, fault tolerance, and security automation," *Emerging Trends in Machine Intelligence and Big Data,* vol. 15, pp. 39–50, Jul. 2023.

[135] S. Prasanna, M. R. Lenka and A. R. Swain , "A survey on routing protocols for disaster management," *SN Computer Science,* vol. 5, no. 2, pp. 216–236, Jan. 2024.

[136] S. Islam, Z. A. Atallah, A. K. Budati, M. K. Hasan, R. Kolandaisamy and S. Nurhizam, "Mobile networks toward 5G/6G: Network architecture, opportunities and challenges in smart city," *IEEE Open Journal of the Communications Society,* Jun. 2024, doi: 10.1109/OJCOMS.2024.3419791.

[137] L. P. Rachakonda, M. Siddula and V. Sathya, "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)," *High-Confidence Computing,* vol. 4, no. 2, pp. 100220–100237, Jun. 2024.

[138] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad and H. V. Poor, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proceedings of the IEEE,* vol. 110, no. 6, pp. 712–734, Jun. 2022.

[139] P. P. Ray, "A review on 6G for space-air-ground integrated network: Key enablers, open challenges, and future direction," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 9, pp. 6949–6976, Oct. 2022.

[140] R. Jaganathan and K. Rajendran, "Peregrine falcon optimization routing protocol (PFORP) for achieving ultra-low latency and boosted efficiency in 6G drone ad-hoc networks (DANET)," *International Journal of Computing and Digital Systems,* vol. 16, no. 1, pp. 1–31, Aug. 2024.

[141] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs," *Journal of Network and Computer Applications,* vol. 213, pp. 103607–103633, Apr. 2023.

[142] M. A. B. S. Abir, M. Z. Chowdhury and Y. M. Jang, "Software-defined UAV networks for 6G systems: Requirements, opportunities, emerging techniques, challenges, and research directions," *IEEE Open Journal of the Communications Society,* vol. 4, pp. 2487–2547, Oct. 2023.

[143] P. Yue, J. An, J. Zhang, J. Ye, G. Pan and S. Wang, "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 3, pp. 1604–1652, 3rd Quart. 2023.

[144] S. Mahboob and L. Liu, "Revolutionizing future connectivity: A contemporary survey on AI-empowered satellite-based non-terrestrial networks in 6G," *IEEE Communications Surveys & Tutorials,* vol. 26, no. 2, pp. 1279–1321, 2nd Quart. 2024.

[145] R. Matteo, "Adaptive monitoring, detection, and response for agile digital service chains," *Computers & Security,* vol. 132, pp. 103343–103361, Sep. 2023.

[146] M. Kang, S. Park and Y. Lee, "A survey on satellite communication system security," *Sensors,* vol. 24, no. 9, pp. 2897–2942, May 2024.

[147] Ł. Lemieszewski, P. Borkowski, A. Radomska-Zalas, L. Dobryakova and E. Ochin, "Cybersecurity of the unmanned marine vehicles in the conditions of partial or complete interruption multi-GNSS signals by jamming and/or spoofing," *European Conference on Artificial Intelligence,* Springer, Cham, pp. 83–94, Aug. 2024.

[148] A. A. Aremo, "SNMP's MIB support and future of network management," *Campbellsville University,* Apr. 2023.

[149] A. Basu, R. Singh, C. Yu, A. Prasad and K. Banerjee, "Designing, developing and deploying an enterprise scale network monitoring system," *Proceedings of the 15th Innovations in Software Engineering Conference,* New York, United States, Feb. 2022.

[150] M. Aboubakar, M. Kellil and P. Roux, "A review of IoT network management: current status and perspectives," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 7, pp. 4163–4176, Jul. 2022.

[151] A. Neumann, L. Wisniewski and P. Rost, "About integrating 5G into profinet as a switch function," *Kommunikation in der Automation,* Magdeburg, Germany, Nov. 2019.

[152] W. Zhang, M. Dong, K. Ota, J. Li, W. Yang and J. Wu, "A big data management architecture for standardized IoT based on smart scalable SNMP," *IEEE International Conference on Communications (ICC),* Dublin, Ireland, Oct. 2020.

[153] A. Giorgetti, A. Sgambelluri, R. Casellas, R. Morro, A. Campanella and P. Castoldi, "Control of open and disaggregated transport networks using the open network operating system (ONOS)," *Journal of Optical Communications and Networking,* vol. 12, no. 2, pp. 171–181, Dec. 2019.

[154] A. Clemm, M. F. Zhani and R. Boutaba, "Network management 2030: Operations and control of network 2030 services," *Journal of Network and Systems Management,* vol. 28, no. 4, pp. 721–750, Mar. 2020.

[155] D. R. Cacciagrano, F. Corradini, R. Culmone, N. Gorogiannis, L. Mostarda, F. Raimondi and C. Vannucchi, "Analysis and verification of ECA rules in intelligent environments," *Journal of Ambient Intelligence and Smart Environments,* vol. 10, no. 3, pp. 261–273, Jan. 2018.

[156] A. Yichiet, J. K. Y. Min, G. M. Lee and L. J. Sheng, "Intent-based network policy to solution architecting recommendations," *International Journal of Business Data Communications and Networking (IJBDCN),* vol. 17, no. 1, pp. 55–74, Jan. 2021.

[157] M. Abdullahi and N. Othman, "Bridging the gap between policy intent and implementation," *Journal of Science, Technology and Innovation Policy,* vol. 6, no. 1, pp. 24–33, Jun. 2020.

[158] A. I. Rana and B. Jennings, "Semantic aware processing of user defined inference rules to manage home networks," *Journal of Network and Computer Applications,* vol. 79, pp. 68–87, Feb. 2017.

[159] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello and A. Coen-Porisini, "Security policy enforcement for networked smart objects," *Computer Networks,* vol. 108, pp. 133–147, Oct. 2016.

[160] Y. Ouyang, C. Yang, Y. Song, X. Mi and M. Guizani, "A brief survey and implementation on refinement for intent-driven networking," *IEEE Network,* vol. 35, no. 6, pp. 75–83, Nov/Dec. 2021.

[161] A. Leivadeas and M. Falkner, "A survey on intent-based networking," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 1, pp. 625–655, 1st Quart. 2023.

[162] M. H. Bashi, L. De Tommasi, A. Le Cam, L. S. Relaño, P. Lyons, J. Mundó, I. Pandelieva-Dimova, H. Schapp, K. Loth-Babut, C. Egger, M. Camps, B. Cassidy, G. Angelov and C. E. Stancioff, "A review and mapping exercise of energy community regulatory challenges in European member states based on a survey of collective energy actors," *Renewable and Sustainable Energy Reviews,* vol. 172, pp. 113055, Feb. 2023.

[163] A. Clemm, L. Ciavaglia, L. Z. Granville and J. Tantsura "Rfc 9315: intent-based networking-concepts and definitions," Oct. 2022.

[164] H. Guo, W. Li, M. Nejad and C. C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," *IEEE international conference on blockchain (Blockchain),* Atlanta, GA, USA, Jul. 2019.

[165] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *Journal of Network and Computer Applications,* vol. 156, pp. 102563–102591, Apr. 2020.

[166] K. C. Serdaroglu and S. Baydere, "An efficient multipriority data packet traffic scheduling approach for fog of things," *IEEE Internet of Things Journal,* vol. 9, no. 1, pp. 525–534, Jan. 2021.

[167] P. Kamboj and S. Pal, "A policy based framework for quality of service management in software defined networks," *Telecommunication Systems,* vol. 78, no. 3, pp. 331–349, Aug. 2021.

[168] J. C. Nobre, C. Melchiors, C. C. Marquezan, L. M. R. Tarouco and L. Z. Granville, "A survey on the use of P2P technology for network management," *Journal of Network and Systems Management,* vol. 26, pp. 189–221, Jan. 2018.

[169] E. J. Scheid, D. Lakic, B. B. Rodrigues and B. Stiller, "PleBeuS: A policy-based blockchain selection framework," *IEEE/IFIP Network Operations and Management Symposium,* Budapest, Hungary, Apr. 2020.

[170] W. Zhang, P. Sun, Y. Tian and H. Xu, "A policy-based network management architecture for satellites networks," *International Conference on Information Management and Engineering,* Chengdu, China, Apr. 2010.

[171] E. Chen, Y. Zhu, Z. Zhou, S. Y. Lee, W. E. Wong and W. C. C. Chu, "Policychain: A decentralized authorization service with script-driven policy on blockchain for internet of things," *IEEE Internet of Things Journal,* vol. 9, no. 7, pp. 5391–5409, Apr. 2022.

[172] H. Sato, S. Tanimoto, T. Kobayashi and A. Kanai, "Adaptive policy evaluation framework for flexible service provision," *IEEE Symposium on Service-Oriented System Engineering (SOSE),* Bamberg, Germany, Mar. 2018.

[173] K. Odagiri, S. Shimizu, N. Ishii and M. Takizawa, "Suggestion of the cloud type virtual policy based network management scheme for the common use between plural organizations," *International Conference on Network-Based Information Systems,* Taipei, Taiwan, Sep. 2015.

[174] G. Katsikogiannis, S. Mitropoulos and C. Douligeris, "Optimizing SLA-driven adaptive routing," *IEEE Symposium on Computers and Communication (ISCC),* Messina, Italy, Jun. 2016.

[175] C. C. Machado, J. A. Wickboldt, L. Z. Granville and A. Schaeffer-Filho, "Arkham: An advanced refinement toolkit for handling service level agreements in software-defined networking," *Journal of Network*

and Computer Applications, vol. 90, pp. 1–16, Jul. 2017.

[176] K. Dzeparoska, A. Tizghadam and A. Leon-Garcia, "Emergence: An intent fulfillment system," *IEEE Communications Magazine,* vol. 62, no. 6, pp. 36–41, Jun. 2024.

[177] M. Kiran, E. Pouyoul, A. Mercian, B. Tierney, C. Guok and I. Monga, "Enabling intent to configure scientific networks for high performance demands," *Future Generation Computer Systems,* vol. 79, pp. 205–214, Feb. 2018.

[178] R. Soulé, S. Basu, P. J. Marandi, F. Pedone, R. Kleinberg, E. G. Sirer and N. Foster "Merlin: A language for managing network resources," *IEEE/ACM Transactions on Networking,* vol. 26, no. 5, pp. 2188–2201, Oct. 2018.

[179] C. Prakash, J. Lee, Y. Turner, J. M. Kang, A. Akella, S. Banerjee, C. Clark, Y. Ma, P. Sharma and Y. Zhang, "Pga: Using graphs to express and automatically reconcile network policies," *ACM SIGCOMM Computer Communication Review,* vol. 45, no. 4, pp. 29–42, Aug. 2015.

[180] A. Abhashkumar, J. M. Kang, S. Banerjee, A. Akella, Y. Zhang and W. Wu, "Supporting diverse dynamic intent-based policies using janus," *International Conference on emerging Networking Experiments and Technologies,* Incheon Republic of Korea , Nov. 2017.

[181] M. Riftadi and F. Kuipers, "P4I/O: Intent-based networking with P4," *IEEE Conference on Network Softwarization (NetSoft),* Paris, France, Jun. 2019.

[182] Y. Elkhatib, G. Coulson and G. Tyson, "Charting an intent driven network," *International Conference on Network and Service Management (CNSM),* Tokyo, Japan, Nov. 2017.

[183] A. S. Jacobs, R. J. Pfitscher, R. A. Ferreira and L. Z. Granville, "Refining network intents for self-driving networks," *Self-Driving Networks,* Budapest Hungary, Aug. 2018.

[184] D Lenrow, "Intent: don't tell me what to do!(tell me what you want)," 2015. [Online]. Available: https://www.sdxcentral.com/articles/contributed/network-intent-summit-perspective-david-lenrow/2015/02/

[185] B. K. Saha, D. Tandur, L. Haab and L. Podleski, "Intent-based networks: an industrial perspective," *International Workshop on Future Industrial Communication Networks,* New Delhi India, Oct. 2018.

[186] T. Szigeti, D. Zacks, M. Falkner and S. Arena, "Cisco digital network architecture: intent-based networking for the enterprise," *Cisco Press, Indianapolis, IN,* 2018.

[187] A. Clemm and T. Eckert, "Combining autonomic and intent-based networking," *IEEE/IFIP Network Operations and Management Symposium,* Miami, FL, USA, May 2023.

[188] D. A. Tamburri, W. J. Van den Heuvel, C. Lauwers, P. Lipton, D. Palma and M. Rutkowski, "TOSCA-based intent modelling: Goal-modelling for infrastructure-as-code," *Sics software-Intensive cyber-Physical systems,* vol. 34, pp. 163–172, Feb. 2019.

[189] K. Mehmood, K. Kralevska and D. Palma, "Intent-driven autonomous network and service management in future cellular networks: A structured literature review," *Computer Networks,* vol. 220, pp. 109477–109496, Jan. 2023.

[190] J. Huang, C. Yang, S. Kou and Y. Song, "A brief survey and implementation on AI for intent-driven network," *Asia Pacific Conference on Communications (APCC),* Jeju Island, South Korea, Oct. 2022.

[191] L. Pang, C. Yang, D. Chen, Y. Song and M. Guizani, "A survey on intent-driven networks," *IEEE Access,* vol. 8, pp. 22862–22873, Jan. 2020.

[192] A. S. Jacobs, R. J. Pfitscher, R. H. Ribeiro, R. A. Ferreira, L. Z. Granville, W. Willinger and S. G. Rao, "Hey, lumi! using natural language for intent-based network management," *USENIX Annual Technical Conference (USENIX ATC 21),* Jul. 2021.

[193] V. Heorhiadi, S. Chandrasekaran, M. K. Reiter and V. Sekar, "Intent-driven composition of resource-management SDN applications," *International Conference on Emerging Networking Experiments and Technologies,* Heraklion Greece, Dec. 2018.

[194] X. Chang, C. Yang, H. Wang, Y. Ouyang, R. Dong, J. Guo, Z. Ji and X. Liu, "KID: Knowledge graph-enabled intent-driven network with digital twin," *Asia Pacific Conference on Communications (APCC),* Jeju Island, South Korea, Oct. 2022.

[195] J. Zhang, J. Guo, C. Yang, X. Mi, L. Jiao, X. Zhu, L. Cao and R. Li, "A conflict resolution scheme in intent-driven network," *IEEE/CIC International Conference on Communications in China (ICCC),* Xiamen, China, Jul. 2021.

[196] L. Velasco, S. Barzegar, F. Tabatabaeimehr and M. Ruiz, "Intent-based networking and its application to optical networks," *Journal of Optical Communications and Networking,* vol. 14, no. 1, pp. A11–A22, Jan. 2022.

[197] K. Abbas, T. A. Khan, M. Afaq and W. C. Song, "Network slice lifecycle management for 5G mobile networks: An intent-based networking approach," *IEEE Access,* vol. 9, pp. 80128–80146, May 2021.

[198] Y. Song, C. Yang, J. Zhang, X. Mi and D. Niyato, "Full-life cycle intent-driven network verification: Challenges and approaches," *IEEE Network,* vol. 37, no. 5, pp. 145–153, Sep. 2022.

[199] W. Chen, N. Jain and S. Singh, "ANMP: Ad hoc network management protocol," *IEEE Journal on Selected Areas in Communications,* vol. 17, no. 8, pp. 1506–1531, Aug. 1999.

[200] M. B. Channappagoudar, "An efficient network management system using agents for MANETs," *PhD thesis, Indian Institute of Science,* 2018.

[201] A. V. Gavrilov and M. V. Kavalerov, "Mobile ad hoc network management and routing efficiency," *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus),* Saint Petersburg, Russian Federation, Jan. 2022.

[202] A. Habboush, "Ant colony optimization (ACO) based MANET routing protocols: A comprehensive review," *Computer and Information Science,* vol. 12, no. 1, pp. 82–92, Jan. 2019.

[203] M. Al Qurashi, C. M. Angelopoulos and V. Katos, "An architecture for resilient intrusion detection in ad-hoc networks," *Journal of Information Security and Applications,* vol. 53, pp. 102530–102542, Aug. 2020.

[204] H. Bakht and S. Eding, "Policy-based approach for securing message dissemination in mobile ad hoc networks," *IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech),* Athens, Greece, Aug. 2018.

[205] F. Hamad and O. Adwan, "Policy based approach for information transfer over mobile ad hoc network using messages privacy control," *Modern Applied Science,* vol. 12, no. 5, pp. 22–35, Apr. 2018.

[206] A. Tajalli-Yazdi, H. Lutfiyya and D. Kidston, "MANET security through a distributed policy-based evaluation of node behaviour," *International Wireless Communications and Mobile Computing Conference (IWCMC),* Dubrovnik, Croatia, Aug. 2015.

[207] J. Wang, H. Zhang, F. Xu, N. Xu, Z. Wang, X. Zhou, C. Li and Z. Shen, "A novel colored time petri net model for policy management and context awareness procedure in MANET," *International Conference on Soft Computing in Information Communication Technology,* Atlantis Press, May 2014.

[208] M. Salmanian and M. Li, "Enabling secure and reliable policy-based routing in MANETs," *IEEE Military Communications Conference,* Orlando, FL, USA, Nov. 2012.

[209] M. Kumar, R. Bhandari, A. Rupani and J. H. Ansari, "Trust-based performance evaluation of routing protocol design with security and QoS over MANET," *International Conference on Advances in Computing and Communication Engineering (ICACCE-2018),* Paris, France, Jun. 2018

[210] Y. Singh, K. Deep and S. Niranjan, "Clustering approach in route selection using mobile agent in mobile ad-hoc network," *International Journal of Engineering Research and Development,* vol. 5, no. 11, pp. 63–73, Feb. 2013.

[211] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban and N. D. Han, "A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks," *Wireless Personal Communications,* vol. 120, no. 1, pp. 49–62, Apr. 2021.

[212] S. LaMar, J. J. Gosselin, I. Caceres, S. Kapple and A. Jayasumana, "Congestion aware intent-based routing using graph neural networks for improved quality of experience in heterogeneous networks," *IEEE Military Communications Conference (MILCOM),* San Diego, CA, Nov. 2021.

[213] M. M. Karthikeyan and G. M. A Christy, "Proposed hybrid congestion control algorithm (HCCA) using mobile adhoc network," *Partners Universal International Research Journal,* vol. 2, no. 1, pp. 35–46, Mar. 2023.

[214] B. F. Ferreira, J. N. Isento, J. A. Dias, J. J. P. C. Rodrigues and L. Zhou, "An SNMP-based solution for vehicular delay-tolerant network management," *IEEE Global Communications Conference (GLOBECOM),* Anaheim, CA, Dec. 2012.

[215] J. B. C. B. de Freitas, "SNMP agent for on-board-units in vehicular systems," *PhD thesis, Universidade do Minho (Portugal),* 2022.

[216] S. Sousa, A. Santos, A. Costa, B. Dias, B. Ribeiro, F. Gonçalves, J. Macedo, M. J. Nicolau and Ó. Gama, "A new approach on communications architectures for intelligent transportation systems," *Procedia Computer Science,* vol. 110, pp. 320–327, Jul. 2017.

[217] A. D. Al-Ani and J. Seitz, "QoS-aware routing in multi-rate ad hoc networks based on ant colony optimization," *Network Protocols and*

Algorithms, vol. 7, no. 4, pp. 1–25, Dec. 2015.

[218] Y. Xia, X. Liu, J. Ou and W. Chen, "A policy enforcement framework for secure data dissemination in vehicular ad hoc network," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 12, pp. 13304–13314, Dec. 2021.

[219] P. K. Pandey, V. Kansal and A. Swaroop, "Security challenges and solutions for next-generation VANETs: An exploratory study," *Role of Data-Intensive Distributed Computing Systems in Designing Data Solutions, Springer,* pp. 183–201, Jan. 2023.

[220] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," *Journal of information security and applications,* vol. 46, pp. 193–209, Jun. 2019.

[221] A. Kchaou, R. Abassi, S. Ayed and S. G. El Fatmi, "A distributed resource management for VANET using smart contract," *International Wireless Communications and Mobile Computing (IWCMC),* Harbin City, China, Aug. 2021.

[222] B. Alaya, R. Khan, T. Moulahi and S. E. Khediri, "Study on QoS management for video streaming in vehicular ad hoc network (VANET)," *Wireless Personal Communications,* vol. 118, no. 4, pp. 2175–2207, Feb. 2021.

[223] K. Mershad, "SURFER: A secure SDN-based routing protocol for internet of vehicles," *IEEE Internet of Things Journal,* vol. 8, no. 9, pp. 7407–7422, May 2021.

[224] S. R. Pokhrel, "Software defined internet of vehicles for automation and orchestration," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 6, pp. 3890–3899, Jun. 2021.

[225] S. Safavat and D. B. Rawat, "On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based internet of vehicles for smart cities," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 8, pp. 5050–5059, Aug.2021.

[226] Y. Wang, Z. Tian, Y. Sun, X. Du and N. Guizani, "LocJury: An IBN-based location privacy preserving scheme for IoCV," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 8, pp. 5028–5037, Aug. 2021.

[227] H. Liao, Z. Zhou, W. Kong, Y. Chen, X. Wang, Z. Wang and S. A. Otaibi, "Learning-based intent-aware task offloading for air-ground integrated vehicular edge computing," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 8, pp. 5127–5139, Aug. 2020.

[228] A. Singh, G. S. Aujla and R. S. Bali, "Intent-based network for data dissemination in software-defined vehicular edge computing," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 8, pp. 5310–5318, Aug. 2020.

[229] P. A. D. S. N. Wijesekara and S. Gunawardena, "A comprehensive survey on knowledge-defined networking," *Telecom, MDPI,* vol. 4, no. 3, pp. 477–596, Aug. 2023.

[230] A. Laghari, A. Khan and H. Hui, "Quality of experience (QoE) and quality of service (QoS) in UAV systems," *Imaging and Sensing for Unmanned Aircraft Systems,* vol. 2, Feb. 2019.

[231] P. Cumino, K. Maciel, T. Tavares, H. Oliveira, D. Rosário and E. Cerqueira, "Cluster-based control plane messages management in software-defined flying ad-hoc network," *Sensors,* vol. 20, no. 1, pp. 67–85, Dec. 2019.

[232] M. H. Eiza, T. Owens and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Transactions on Dependable and Secure Computing,* vol. 13, no. 1, pp. 32–45, Jan-Feb. 2016.

[233] M. Kolisnyk and O. Piskachov, "Analysis and systematization of vulnerabilities of drone subsystems," *International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications,* Ivano-Frankivsk, Ukraine, Sep. 2023.

[234] N. Hu, Z. Tian, Y. Sun, L. Yin, B. Zhao, X. Du and N. Guizani, "Building agile and resilient UAV networks based on SDN and blockchain," *IEEE Network,* vol. 35, no. 1, pp. 57–63, Jan/Feb. 2021.

[235] F. Wiedner, J. Andre, P. Mendes and G. Carle, "Policy-based routing for flying adhoc networks," *Micro Aerial Vehicle Networks, Systems, and Applications,* Portland, OR, Jul. 2022.

[236] M. Bada, D. E. Boubiche, N. Lagraa, C. A. Kerrache, M. Imran and M. Shoaib, "A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs," *Transportation Research Part A: Policy and Practice,* vol. 149, pp. 300–318, Jul. 2021.

[237] A. F. Tarhan, E. Koyuncu, M. Hasanzade, U. Ozdemir and G. Inalhan, "Formal intent based flight management system design for unmanned aerial vehicles," *International Conference on Unmanned Aircraft Systems (ICUAS),* Orlando, FL, May 2014.

[238] L. Yang, P. Tao, T. Li, C. Yang, X. Mi, Y. Ouyang, D. Wei and Q. Wang, "Reservation and traffic intent-aware dynamic resource allocation for FANET," *International Conference on Communication Technology (ICCT),* Tianjin, China, Oct. 2021.

[239] T. Ling, L. Shen, X. Wang, L. Wu, Z. Hui, Y. Fei, G. Wu, H. Hu, L. Liu and C. Zheng, "Research on a management control system in space-terrestrial integrated network," *Wireless and Satellite Systems: 11th EAI International Conference,* Nanjing, China, Feb. 2021.

[240] H. Li, "Design and implementation of spacecraft network monitoring system based on SNMP," *IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC),* Chongqing, China, Oct. 2019.

[241] P. Hu, "Closing the management gap for satellite-integrated community networks: a hierarchical approach to self-maintenance," *IEEE Communications Magazine,* vol. 59, no. 12, pp. 43–49, Dec. 2021.

[242] Y. Qu, F. Pu, J. Yin, L. Liu and X. Xu, "Dynamic traffic detection and modeling for beidou satellite networks," *Journal of Sensors,* vol. 2020, pp. 1–11, Jan. 2020.

[243] T. Ma, B. Qian, X. Qin, X. Liu, H. Zhou and L. Zhao, "Satellite-terrestrial integrated 6G: An ultra-dense LEO networking management architecture," *IEEE Wireless Communications,* vol. 31, no. 1, pp. 62–69, Feb. 2024.

[244] T. Sui, P. Sun, Z. Zhang and Z. Wan, "A management policy applying to integrated satellite information network," *International Conference on Computer Science and Network Technology,* Harbin, China, Dec. 2011.

[245] B. Deng, C. Jiang, H. Yao, S. Guo and S. Zhao, "The next generation heterogeneous satellite communication networks: Integration of resource management and deep reinforcement learning," *IEEE Wireless Communications,* vol. 27, no. 2, pp. 105–111, Apr. 2020.

[246] Y. Ouyang, J. Linz, T. Fengz, C. Yang, L. Zhang, T. Li and Z. Han, "Intent-driven CoX resource management for space-terrestrial networks," *IEEE Wireless Communications,* pp. 1–9, May 2023.

[247] L. Zhang, C. Yang, Y. Ouyang, T. Li and A. Anpalagan, "ISFC: Intent-driven service function chaining for satellite networks," *Asia Pacific Conference on Communications (APCC),* Jeju Island, South Korea, Oct. 2022.

[248] Y. Wang, K. Guo, N. Wang, Z. Qin, X. Zhong and X. Han, "Intent-driven LEO satellite networks resource management," *International Conference on Communication Technology (ICCT),* Nanjing, China, Nov. 2022.

[249] T. Li, Y. Ouyang, L. Zhang, Y. Bai and C. Yang, "Autonomous intent detection for intent-driven satellite network," *International Wireless Communications and Mobile Computing (IWCMC),* Marrakesh, Morocco, Jun. 2023.

[250] R. J. Reifert, S. Roth, A. A. Ahmad and A. Sezgin, "Comeback kid: Resilience for mixed-critical wireless network resource management," *IEEE Transactions on Vehicular Technology,* vol. 72, no. 12, pp. 16177–16194, Dec. 2023.

[251] A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur and H. Al-Bashar, "Dynamic clustering and management of mobile wireless sensor networks," *Computer Networks,* vol. 117, pp. 62–75, Apr. 2017.

[252] J. Miserez, D. Colle, M. Pickavet and W. Tavernier, "Exploiting queue information for scalable delay-constrained routing in deterministic networks," *IEEE Transactions on Network and Service Management,* vol. 21, no. 5, pp. 5260–5272, Oct. 2024.

[253] D. Strzęciwilk, "Timed petri nets for modeling and performance evaluation of a priority queueing system," *Energies,* vol. 16, no. 23, pp. 7690–7719, Nov. 2023.

[254] F. Hussain, S. A. Hassan, R. Hussain and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1251–1275, 2nd Quart. 2020.

[255] B. Dai, Y. Cao, Z. Wu, Z. Dai, R. Yao and Y. Xu, "Routing optimization meets machine intelligence: A perspective for the future network," *Neurocomputing,* vol. 459, pp. 44–58, Oct. 2021.

[256] G. Luo, Q. Yuan, J. Li, S. Wang and F. Yang, "Artificial intelligence powered mobile networks: From cognition to decision," *IEEE Network,* vol. 36, no. 3, pp. 136–144, May/Jun. 2022.

[257] K. Dzeparoska, J. Lin, A. Tizghadam and A. Leon-Garcia, "LLM-based policy generation for intent-based management of applications," *International Conference on Network and Service Management (CNSM),* Nov. 2023.

[258] G. Luo, Q. Yuan, J. Li, S. Wang and F. Yang, "An AI-driven intent-based network architecture," *IEEE Communications Magazine,* Nov. 2024, doi: 10.1109/MCOM.001.2400143.

[259] G. Carvalho, B. Cabral, V. Pereira and J. Bernardino, "Computation offloading in edge computing environments using artificial intelligence techniques," *Engineering Applications of Artificial Intelligence,* vol. 95,

pp. 103840–103859, Oct. 2020.

[260] A. J. Ferrer, J. M. Marquès and J. Jorba, "Towards the decentralised cloud: survey on approaches and challenges for mobile, ad hoc, and edge computing," *ACM Computing Surveys (CSUR),* vol. 51, no. 6, pp. 1–36, Oct. 2019.

[261] M. S. Rahman, M. A. P. Chamikara, I. Khalil and A. Bouras, "Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city," *Journal of Industrial Information Integration,* vol. 30, pp. 100408–100419, Nov. 2022.

[262] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications,* vol. 166, pp. 102693–102731, Sep. 2020.

[263] D. Serghiou, M. Khalily, T. W. C. Brown and R. Tafazolli, "Terahertz channel propagation phenomena, measurement techniques and modeling for 6G wireless communication applications: A survey, open challenges and future research directions," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 4, pp. 1957–1996, 4th Quart. 2022.

[264] H. Sarieddeen, M. -S. Alouini and T. Y. Al-Naffouri, "An overview of signal processing techniques for terahertz communications," *Proceedings of the IEEE,* vol. 109, no. 10, pp. 1628–1665, Oct. 2021.

[265] M. Wang, F. Gao, S. Jin and H. Lin, "An overview of enhanced massive MIMO with array signal processing techniques," *IEEE Journal of Selected Topics in Signal Processing,* vol. 13, no. 5, pp. 886–901, Sept. 2019.

[266] V. G. Ataloglou, S. Taravati and G. V. Eleftheriades, "Metasurfaces: Physics and applications in wireless communications," *National Science Review,* vol. 10, no. 8, pp. 164–180, Jun. 2023.