electronics

MDPI

Article

Dual-Network Layered Network: A Method to Improve Reliability, Security, and Network Efficiency in Distributed Heterogeneous Network Transmission

Shengyuan Qi [1,2,3,*], Lin Yang [1,2,3,*], Linru Ma [2], Shanqing Jiang [1,2,3] and Guang Cheng [1,3,*]

[1] School of Cyber Science and Engineering, Southeast University, Nanjing 211102, China; sqjiang@njnet.edu.cn
[2] National Key Laboratory of Science and Technology on Information System Security, Institute of System Engineering, PLA Academy of Military Science, Beijing 210002, China; malinru@163.com
[3] Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, Nanjing 100071, China
* Correspondence: syqi@seu.edu.cn (S.Q.); yanglin61s@126.com (L.Y.); chengguang@seu.edu.cn (G.C.)

Abstract: This article delves into the routing architecture and reliable transmission service framework of dual-network layered networks, with a focus on analyzing their core design ideas and implementation strategies. In the context of increasing network complexity today, traditional single-network architectures are unable to meet diverse application needs. Therefore, dual-network layered networks, as an innovative solution, are gradually receiving attention from both academia and industry. This article first analyzes the key technical elements in the dual-network layered network architecture, including the optimization of routing algorithms, distributed consensus, reliability assurance mechanisms for packet transmission, and dynamic allocation strategies for network resources. Through in-depth research on these technologies, this article elaborates on the important role of dual-network layered networks in building efficient and stable transmission environments, providing important theoretical foundations and technical support for the construction and optimization of future network systems.

Keywords: heterogeneous network; distributed optimization; control over networks; reliable transmission; overlay network

check for updates

Citation: Qi, S.; Yang, L.; Ma, L.; Jiang, S.; Cheng, G. Dual-Network Layered Network: A Method to Improve Reliability, Security, and Network Efficiency in Distributed Heterogeneous Network Transmission. *Electronics* **2024**, *13*, 4749. https://doi.org/10.3390/electronics13234749

Academic Editors: Aryya Gangopadhyay, Byung-Seo Kim, Kyu-Tae Lee and Hyunsik Ahn

Received: 23 October 2024
Revised: 21 November 2024
Accepted: 29 November 2024
Published: 30 November 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the progression of society and the advances in science and technology, communication methods have become increasingly convenient and diversified, effectively transcending the traditional constraints of space and time. The conventional single-network architecture model has become increasingly inadequate to meet the increasing demands for communication [1]. To address this challenge, heterogeneous networks have emerged as a promising solution. As shown in Figure 1, with the development of networks, a variety of heterogeneous network resources are now available, including satellite communications [2,3], mobile networks [4,5], wired infrastructures [6,7], and self-organizing drone networks [8,9] as shown in Figure 1. Each of these distributed resources has unique advantages in its respective field, and combining these heterogeneous resources can provide better services. For example, satellite communications offer extensive geographical coverage [10], mobile networks provide flexible and ubiquitous access [11], and wired infrastructures are known for their stability and high bandwidth [12]. By effectively integrating these heterogeneous networks, researchers can develop comprehensive communication systems capable of operating in diverse environments, thereby delivering more flexible, efficient, and reliable communication services. This research focuses on the effective integration of disparate distributed communication resources to optimize the performance of heterogeneous networks, ultimately delivering more reliable and efficient communication services across a wide range of application scenarios.

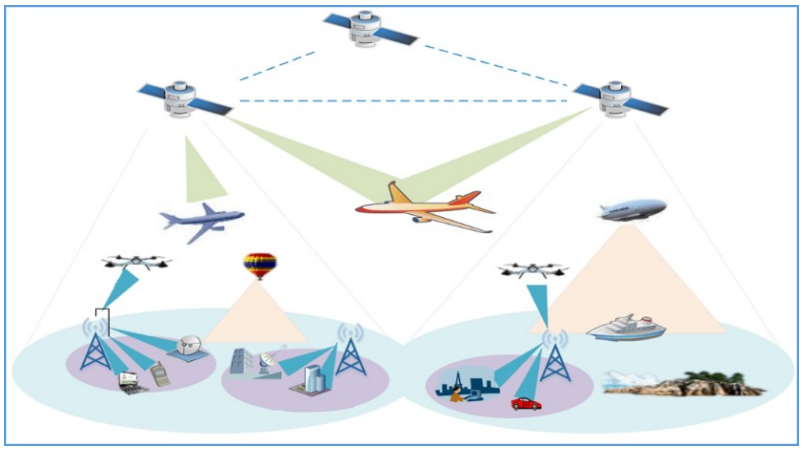


Figure 1. Various distributed heterogeneous network resources.

A recent case study on the October 2023 Israeli–Palestinian conflict exemplifies this dynamic [13]. Israel's targeted airstrikes on the Gaza Strip resulted in the destruction of approximately 70% of the region's transmission and distribution networks, severely impairing communication services. The compounded effects of the destruction of network nodes and energy supply shortages led to a complete blackout of communication services in mid-October, exacerbated the challenges of coordinating humanitarian aid and collecting accurate casualty reports. The UN Emergency Relief Coordinator highlighted that the lack of communication infrastructure rendered the data on casualties inaccessible for more than five days.

This pattern is not isolated. During the 2022 Russian–Ukrainian conflict [14], Russian forces systematically attacked Ukraine's critical communication infrastructure through cyberattacks, blocking satellite internet, terrestrial broadband, and mobile networks. In response, Ukraine deployed SpaceX's Starlink technology, which provided satellite-based internet via 20,000 receiving antennas and routers. This response highlights the creation of a heterogeneous network that integrates multiple communication modalities, which proved essential to maintain command and control capabilities, particularly for military operations such as UAV coordination.

In large-scale network attacks, such as those occurring during wartime, critical nodes are often targeted and destroyed first. As a result, the remaining network resources become fragmented and cannot independently form a cohesive network, leaving only some scattered distributed communication resources, making it challenging for traditional communication methods to ensure reliable information delivery. However, by optimally interconnecting these distributed heterogeneous network resources, it is possible to improve resilience against various disasters or attacks, thereby ensuring sustained communication capabilities. Therefore, studying reliable transmission techniques in distributed heterogeneous networks holds significant practical and research value.

In response to these challenges, this paper proposes a dual-layer network architecture designed to integrate more effectively diverse network resources and provide reliable transmission services to users. This study represents a significant advancement in the field of reliable transmission within distributed heterogeneous networks by exploring cross-subnet user connectivity schemes, with a particular focus on the reliability and security of data transmission.

The following section delves into the characteristics and design strategies of layered architecture of dual networks. Subsequent chapters review relevant research and outline the advantages and disadvantages of various network architectures. The final section provides a comprehensive summary of the paper.

2. Related Work

As the number of network services continues to grow, traditional network architectures have encountered numerous challenges. Due to the inherent limitations of traditional network designs, researchers have proposed various alternative network architectures that offer greater scalability and adaptability to diverse application scenarios. In parallel, distributed optimization control techniques have been increasingly integrated into modern network architectures to enhance performance, security, and reliability. These techniques enable the network to dynamically adjust routing, resource allocation, and traffic management across distributed nodes or network devices in a coordinated fashion. The traditional TCP/IP stack remains the most widely used network architecture [15,16]. However, alternative solutions such as Software-Defined Networking (SDN) [17,18] and information-centric networking (ICN) [19,20] have been developed to address specific data dissemination needs and other network challenges. Current network security models are predominantly host-centric, focusing on securing the communication channels between hosts through encryption protocols, such as Transport Layer Security (TLS) [21,22], and relying on server authentication for trust. However, the decentralized nature of distributed control also calls for more sophisticated security models that secure both data and control channels. In this context, securing the optimization process itself, ensuring data integrity, and preventing malicious nodes from corrupting the consensus are key challenges. Consequently, clients cannot fully trust data received from untrusted locations, even if the data themselves are authentic. To mitigate this issue, workarounds such as publishing separate data fingerprints (e.g., MD5 hashes [23]) are sometimes employed, but these techniques must evolve in distributed environments where data verification and trust are more complex. The integration of distributed optimization control into network architectures thus promises not only enhanced scalability and efficiency but also new challenges in security, trust management, and system resilience.

Content Distribution Networks (CDNs) [24,25] are primarily designed to manage explicitly created copies of data and are unable to fully leverage the distributed nature of all available data resources. This limitation restricts their functionality to being supplementary components of the Internet, aimed at addressing a specific set of common problems for targeted user groups. To overcome these limitations, Christian et al. [26] proposed a novel information-centric network (ICN) architecture that simplifies the service process. This architecture enables an information-centric network capable of routing requests for named data objects and efficiently transmitting the corresponding data across various technical and administrative domains. The architecture supports flexible object retrieval through a hybrid approach that combines name-based routing with name resolution. This adaptable object retrieval method allows the architecture to efficiently operate in diverse network environments while providing effective caching mechanisms and scalability with emerging network technologies.

The Named Data Networking (NDN) [27] project similarly adopts a name-based routing approach to facilitate object retrieval. The name-based routing mechanism in the NDN architecture relies on routing state tables within network routers to support efficient data transmission during the computation process. Additionally, the hierarchical namespace in NDN allows for customization and requires Public Key Infrastructure (PKI) to verify the integrity of named data [28]. The NDN architecture significantly reduces the transmission of duplicate data by caching small data chunks within each router, thereby improving network bandwidth utilization. In an NDN network, routers not only forward packets but also cache them, enabling subsequent requests to retrieve data directly from the cache without needing to access the original data source. This caching mechanism significantly enhances both the efficiency and responsiveness of the network.

Delay-tolerant networking (DTN) [29] is a research domain closely related to information-centric networking (ICN), specifically developed to facilitate data communication in environments characterized by high latency and unreliable connectivity. DTN is particularly suited for scenarios where conventional networks are ineffective or inefficient,

such as space communication, emergency communications in disaster-stricken areas, and networks in rural or remote regions. DTN employs a hop-by-hop, store-and-forward data transmission method, which is capable of tolerating high latency. The DTN architecture utilizes a bundling protocol that allows packets to traverse interruptions and recoveries during transmission [30]. Additionally, it employs a neighbor discovery protocol to manage neighboring nodes, ensuring smooth data forwarding once the next hop is identified, thereby enabling a "store, carry, and forward" mechanism. This architecture offers a robust solution for ensuring Internet communication in challenging and harsh environments.

At present, researchers are mostly combining new technologies such as DTN and 5G for research. However, there are still many issues that need to be addressed, including routing, performance, and architecture. To address these issues, Agussalim et al. [31] applied DTN to the field of smart cities and proposed a protocol called Spray and Hop Distance (SNHD), which combined a large number of IoT devices as DTN network nodes to construct the Surabaya Smart City Plan scenario. Dhabliya et al. [32] addressed the issue of network interruptions by constructing a new topology based on DTN and sensors, and using robots as relays to continue supporting information transmission in the network Noah et al. [33] addressed the issues of long round-trip times, connection interruptions, and asymmetric link data rates in the high-speed delay-tolerant network developed by NASA. They proposed an encoding method using fountain codes to segment, distribute, and reassemble data (in bundled form) from multiple nodes (i.e., satellites) to any number of receivers (i.e., ground stations), and experimentally verified the effectiveness of the proposed method.

Kindervag et al. [34] highlighted that the traditional perimeter-based network protection model is no longer sufficient to address the demands of modern technology. The zero-trust network model has garnered widespread attention as a modern security paradigm. Its core principle, "never trust, always verify," dictates that every access request, whether originating from within or outside the network, must undergo rigorous authentication before gaining access to resources. He et al. [35] emphasize strong authentication, stringent access control, and continuous trust assessment.

Despite the existence of layered network technologies such as SDN and NFV, which have significant flexibility and scalability, there are still many challenges in their implementation and practical operation. For example, in terms of resource intensity, layered networks require efficient integration of heterogeneous resources, which often consumes a large amount of computing, storage, and bandwidth resources. Especially in resource-limited environments such as disaster relief scenarios or post-war communication recovery, this resource intensity may result in the system being unable to achieve expected performance.

Researchers found that by combining distributed computing and edge computing technology, resource utilization efficiency can be significantly improved. For example, the caching and computing power of edge nodes are integrated into the network resource layer to share the load of the core network [36]. Meanwhile, dynamic resource allocation algorithms (such as reinforcement learning-based algorithms) have also been used to optimize resource allocation, thereby reducing computational and transmission overhead [37].

The compatibility issue between heterogeneous networks also needs to be considered, requiring compatibility and interoperability of the underlying network. However, differences in protocols, resource management methods, and hardware characteristics across different networks may lead to a decline in overall system performance [38]. To address this issue, protocol-independent transport control (PITC) technology has received widespread attention. PITC constructs a unified transmission control interface by abstracting the common characteristics of network protocols, thereby achieving seamless access to various heterogeneous network resources [39,40].

In practical deployment, layered networks also encounter different problems. For example, information transmission interruption caused by node failure [41], a significant increase in routing jitter or transmission delay caused by link failure [42], and system vulnerability to attacks due to the complexity of network integration [43].

To address the potential issues mentioned above, researchers have proposed various mitigation measures and improvement strategies. Fu et al. introduced an automated node management system in the transmission control layer, which can sense node status in real time and dynamically adjust network topology when nodes fail [44]. Meanwhile, studies have shown that dynamic routing algorithms based on Deep Reinforcement Learning (DRL) can significantly reduce the impact of link failures on system performance [45]. This algorithm can select the optimal path based on the real-time status of the link (such as delay, bandwidth, etc.) while retaining alternative paths to cope with potential link failures. Awan et al. [46] developed a blockchain-based distributed trust management system to enhance the security of virtual nodes and links. Blockchain technology ensures that the identity of nodes in the transmission control layer cannot be tampered with, and dynamic access control is achieved through smart contracts.

Despite the strengths of these network architectures, ensuring reliable communication of distributed residual communication resources in harsh or post-conflict environments remains a significant challenge. The dual-layer network architecture proposed in this paper addresses these challenges by integrating its inherent advantages with distributed heterogeneous network resources. This integration not only adapts to complex and evolving network environments but also offers enhanced flexibility and scalability across various application scenarios. This system enables efficient resource utilization while delivering more reliable data transmission to users.

3. Methodology

3.1. Design Ideas

The core function of a network architecture is to effectively coordinate various network resources and deliver the necessary functionality to users. However, malicious actors exploit various attack vectors that pose significant threats to the reliability and security of networks. For instance, single points of failure [47,48] and denial-of-service (DoS) [49,50] attacks can disrupt or interfere with the normal operation of network control systems, leading to service interruptions or performance degradation. Traditional defense mechanisms rely heavily on perimeter protection, which seeks to delay and block attacks by minimizing the attack surface of the control system [51]. However, as information transmission and user interaction continue, achieving a completely secure and isolated network environment through this approach is nearly impossible. Additionally, the inherent limitations of traditional network architectures and hardware facilities make it challenging to address unpredictable network environments and emerging threats.

To enhance a network architecture's ability to cope with unknown risks, we introduce the concept of "system resilience", which integrates risk management strategies from the outset of the design process. System resilience refers to a system's capacity to sustain the continuous operation of its core functions and return to a stable state through ongoing adaptation when exposed to uncertainties, such as disruptions, failures, or threats [52]. This concept, originally rooted in physics research, has since been widely adopted in the field of systems engineering. Unlike traditional security mechanisms, resilient security emphasizes the system's inherent capabilities, functioning as an intrinsic security mechanism [53]. A well-designed resilient system can continuously adapt its structure to environmental changes in complex network environments, offering adaptive functions and strategies that maximize the system's security and its ability to control and maintain network integrity.

Future network architecture design will necessitate the incorporation of system resilience as a fundamental component. Integrating resilience into design thinking enables more effective responses to evolving and unpredictable network threats. This approach facilitates rapid network recovery and the maintenance of essential functions in the event of an attack or failure [54]. As network threats become increasingly complex and diverse, resilient design not only strengthens the network's defensive capabilities but also enhances its adaptability and robustness, ensuring reliable operation across various environments.

Integrating this security concept will lay a strong foundation for future network architecture development and drive the continued advancement of network technology.

Figure 2 illustrates the process of system resilience, with the green solid line representing the resilient system and the red dashed line representing the normal system. Initially, both systems function optimally. T1 is the first occurrence of threat event S, and after a short period of destruction, time arrives at T2. T2 is the time when the system experiences losses and begins to implement response measures. Different systems use different measures and produce different response effects. T3 is the time after the first event S stabilizes. After a new period of time, T4 is the event where the system encountered the second event S.

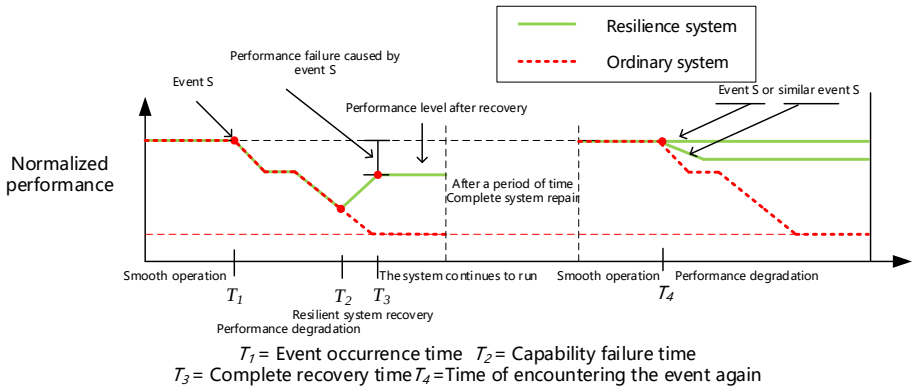


Figure 2. System resilience measurement curve.

However, at time T1, they encounter a risk event, labeled as S. This event causes a continuous decline in system performance from T2 to T3. The normal system exhibits only passive resilience, allowing it to withstand some degradation until it reaches its lowest performance point at T3. In contrast, a resilient system, designed with appropriate measures, can minimize losses and partially restore performance or services by dynamically sensing the system's real-time state and adjusting strategies within the allowed failure time. Despite operating below normal performance levels, the resilient system still maintains functional capability.

After some time, engineers identify the issue and restore the system's performance to normal by repairing or replacing the faulty components. At this point, the performance curves of both the resilient system and the normal system return to their initial state. At time T4, the system encounters the S event, or a similar event, once again. By this time, the resilient system has accumulated a corpus of defensive data through self-learning, enabling it to mount an effective defense against the attack. As a result, the system's performance is either minimally affected or remains nearly unaffected. In contrast, the normal system, having not learned from the previous event, once again experiences significant performance degradation when the event recurs.

Consequently, the dual-network layered transmission control network system is designed with resilience at its core, incorporating a resilient transmission control architecture from the outset. This architectural approach ensures the uninterrupted operation of the system's critical services in the event of an attack or other hostile incidents [55,56]. It leverages the remaining distributed components to reorganize the network and sustain reliable transmission services. As network attacks become increasingly sophisticated, the concept of resilient systems will become an indispensable element in network architecture design.

3.2. Design Principles

Given the complex demands on network components and the challenges of ensuring secure data transmission, it is crucial to design a resilient and dependable distributed heterogeneous network architecture. The following principles should be rigorously adhered to throughout the design process.

Heterogeneity

The rapid evolution of diverse network types and the widespread adoption of services have made heterogeneity in equipment, networks, and technologies a critical design consideration [57]. Addressing these heterogeneities in the design process is essential to prevent network asynchrony, compatibility issues, and the operational complexities that may arise.

Security

To effectively defend against potential network attacks, the design must incorporate intrusion detection, data encryption, firewalls, and other multi-layered defense strategies [58]. The dual-network layered architecture further mitigates attack impacts by distributing network load and reducing the attack surface, thereby enhancing overall network protection.

Resilience

Enhancing the uptime and resistance of the network architecture is paramount. The network must have the capacity to learn and adapt, quickly adjusting to ensure the uninterrupted operation of essential services following an attack or failure [59]. A resilient design not only allows the system to recover rapidly from unexpected events but also strengthens overall risk resistance through continuous learning and optimization.

Real-time data.

Monitoring and analysis of network status are critical for formulating effective system strategies in an ever-changing network environment [60]. By acquiring and processing real-time data, the system can dynamically adjust its strategies to ensure optimal service and security under varying network conditions.

Functional

To meet the diverse needs of users and provide personalized services, the system must be equipped with enhanced functional modules [61]. This includes expanding service capabilities, facilitating diverse application scenarios, and ensuring an optimized user experience.

Scalability

The network architecture must exhibit robust scalability, allowing the system to adapt to evolving technological advancements and accommodate expanding business requirements [62]. The design should anticipate future hardware upgrades, software updates, and new business needs to ensure flexible expansion and sustained efficient operation. The complexity of heterogeneous networks requires robust management capabilities.

Manageability

The design should integrate comprehensive monitoring, control, and maintenance mechanisms that enable straightforward system status monitoring, troubleshooting, and configuration optimization for administrators. These measures will enhance the network's operational efficiency and reduce maintenance costs.

Adhering to these design principles will enable the dual-network layered transmission and control network architecture to deliver efficient, reliable, and secure communication services in complex and evolving network environments.

3.3. Network Architecture

In light of the aforementioned design principles, this paper presents a comprehensive analysis and deconstruction of the proposed dual-network layered transmission control architecture, examining it from both logical and physical perspectives. As illustrated in Figure 3, the system comprises three fundamental elements: structure, policy, and function.

The "structure" refers to the system's components and their interrelationships. In the context of the dual-network hierarchical transmission control architecture, this includes each input/output device entity and its connectivity. Collectively, these elements form the skeleton of the system architecture, analogous to the torso of the human body.

The "Policy" refers to the strategies or plans that the system develops to achieve various objectives. In the dual-network hierarchical transmission control architecture, policy is analogous to the decisions made by the system in response to mission requirements

and environmental changes. This is akin to the human brain, which directs the activities of the body.

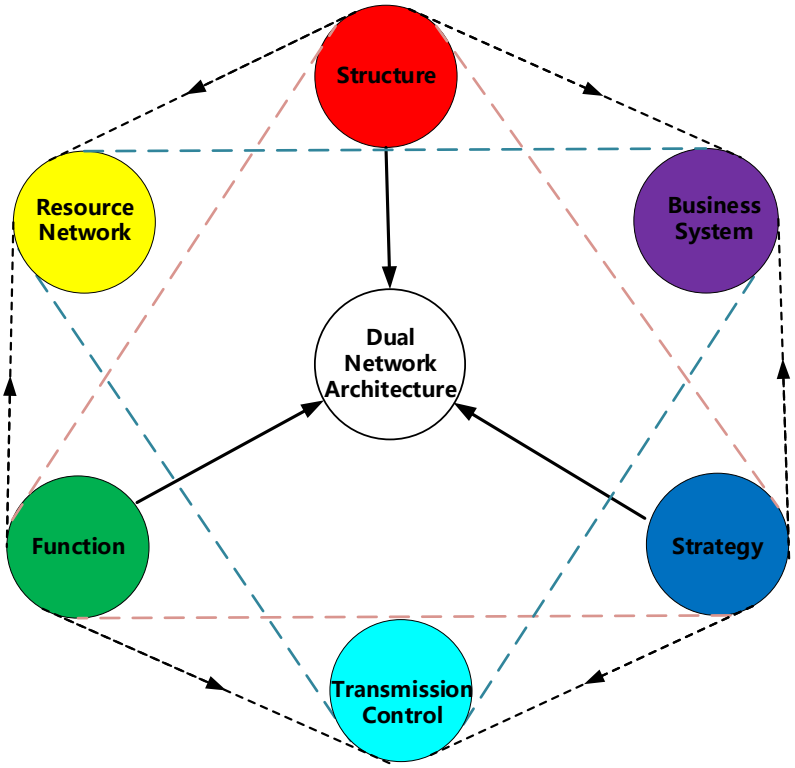


Figure 3. Conceptual diagram of dual-network layered architecture.

The "Functions" are the operations or activities that the system can perform. In the dual-network layered transmission control architecture, this refers to the functional service modules of the system, analogous to the behavioral capabilities of the human body.

The system formulates policies in response to changes in the network environment and delegates these policies to structural entities within the system, enabling the realization of functions. This is analogous to the brain sending commands to the body in response to external stimuli, directing it to perform various actions. The logical hierarchical design of the dual-network layered transmission control architecture allows it to adapt dynamically to complex and evolving network environments, ensuring the system's efficient and reliable operation across a variety of scenarios.

Subsequently, the network architecture is translated from the logical to the physical level. The dual-network layered architecture in the physical domain consists of three distinct layers: the business system layer, the transmission control layer, and the resource network layer. These layers are depicted as inverted triangles in Figure 3.

The business system layer encompasses the structure and policies defined at the logical level and is positioned at the topmost layer of the network architecture, functioning as the endpoint for various tasks. This layer is user-oriented, offering capabilities such as control, transmission, and operation and maintenance.

The transmission control layer, derived from the functions and policies at the logical level, is situated within the virtual network layer of the network architecture. This layer comprises various functional modules responsible for specific tasks, including formulating transmission paths, executing covert transmissions, and performing resource sensing.

The resource network layer, also derived from the structures and functions at the logical level, includes a variety of distributed heterogeneous network resources, such as traditional Internet, satellite networks, mobile communication networks, and self-organized UAV networks. This relationship can be expressed as follows:

$$\begin{aligned} N &= H(structure, function, strategy) \\ &= F_{reso}(X, Y) + F_{tran}(X, Y) + F_{buss}(X, Y) \end{aligned} \tag{1}$$

As shown in Equation (1), the network system z can be represented by a logical function $H()$ or generated by a physical function $F()$. In the logical domain, a network consists of structure, methods, and policies, and different $F()$ represent different layers of the system in the physical scene, including the business layer, control layer, and resource layer (will be introduced later). Among them, X, Y are the node and link states of the network, respectively. Meanwhile, the process of formulating transmission strategies for network systems can be seen as the derivative process of Equation (1), so the transmission strategy can be expressed as:

$$dz = f_{reso}(X, Y)dt + f_{tran}(X, Y)dt + f_{buss}(X, Y)dt \tag{2}$$

where dz represents the decision generated by the system, there are independent variables X, Y to decide, $X = (x_1, x_2, \ldots, x_n)$ is the state of the node, and $Y = (y_1, y_2, \ldots, y_n)$ is the state of the link, so the decision dz that is X, Y in the dt moment of the full derivative, and the state of the independent variables X, Y will also affect the decision making. When the simpler the independent variable X is, the simpler the decision is, for example $x \in [0, 1]$; when X has only two states 0 and 1 indicating that the link is on or off, then dz can only give a simple shortest path. Conversely, when the information of the independent variables is more careful, the more detailed decisions are made by the system, e.g., when x is a vector with multiple dimensions, $x \in [state, bandwith, reliability, effectiveness, delay, neighor]$, the system can select the optimal transmission path based on multiple objective requirements and states, after screening and optimization. Through such mapping, the dual-network layered architecture of the physical layer can effectively realize the design goals of the logical layer and ensure that the system can operate flexibly and efficiently in different network environments.

As illustrated in Figure 4, the network architecture proposed in this paper adopts a layered decoupling design, which allows for the independent separation of the transmission control layer from the resource network layer. This approach leads to the creation of a flexible dual-network architecture, consisting of the transmission control network and the resource network. This layered design enhances system flexibility and provides robust support for navigating complex network environments. The structural and logical differences between the two layers are as follows: The resource layer, situated at the lowest level of the architectural framework, is primarily concerned with providing a stable and reliable infrastructure. The network is designed with elastic scalability and flexible programmable forwarding capabilities, ensuring the availability of redundant heterogeneous physical transmission paths.The resource network layer provides a stable and efficient foundation for supporting the upper transmission control layer, ensuring reliable data transmission even in complex and volatile network environments. In contrast, the transmission control layer focuses on ensuring reliable information transmission. To achieve this, it employs technologies like delay-tolerant networking (DTN), enabling flexible responses to diverse information transmission needs. Additionally, the transmission control layer establishes a logically independent overlay network. Within this network, virtual nodes are generated by the transmission control system, with virtual links corresponding to the heterogeneous access networks in the resource network layer. This design ensures reliable transmission between neighboring nodes through multiple virtual links. The logical isolation at this level allows the system to achieve efficient data transmission and resource scheduling without being constrained by the underlying physical network, thereby enhancing the system's resilience and adaptability. The subsequent sections outline the functions assigned to each layer of the system architecture and the key technologies employed.

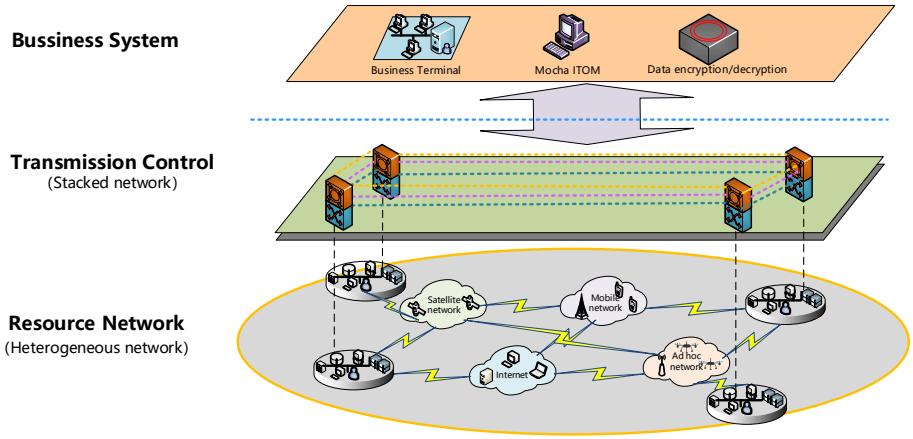


Figure 4. Layered dual-network transmission control architecture.

When the user terminal of the application layer sends information, the system will command the transmission control layer to develop a multi-path transmission algorithm across heterogeneous networks based on the real-time status information of the current network, in order to achieve fast and reliable transmission of information. The transmission control layer obtains the status, link conditions, and other information of nodes in heterogeneous networks through the resource awareness module and summarizes it into a unified resource status table for the entire network. Based on this state table, the system conducts multidimensional attribute analysis on potential transmission paths, including path reliability, latency, load conditions, and security risks, providing comprehensive support for path selection. In multi-path transmission, the system adopts a shared transmission method, dividing data into multiple segments and allocating them to multiple paths for parallel transmission. This strategy not only improves transmission efficiency, but also enhances fault tolerance for path failures or congestion. When a certain path fails, the transmission control layer can adjust the transmission strategy in real time, quickly switch to alternative paths, and ensure the continuity and stability of the transmission process. At the same time, the path selection strategy of the system also combines cross-layer collaboration mechanisms, comprehensively considering the business requirements and service priorities of the application layer. In summary, the system not only achieves efficient information transmission through multi-path transmission algorithms across heterogeneous networks, but also significantly enhances the security, reliability, and flexibility of the transmission process, providing strong technical support for dealing with complex and changing network environments.

At the resource network level, to address the distributed heterogeneity and mobility characteristics of distributed physical transmission network resources, the system employs overlay network technology. This approach involves constructing an information transmission control overlay network for the transmission control system, implemented across multiple heterogeneous network resources. This technology effectively mitigates discrepancies inherent in underlying heterogeneous network transmission resources, establishing an efficient, secure, and distributed identification and forwarding network through a centerless identification system and a secure transmission mechanism. This design not only improves system compatibility but also enhances adaptability in changing network environments. Additionally, disparate connection methodologies are employed between managed terminals, ensuring the establishment of at least two autonomous transmission conduits along the transmission route. The multi-path design significantly enhances the resilience of the transmission control network, ensuring the maintenance of highly reliable communication services in the event of single-path failures or network attacks.

The transmission control layer connects disparate heterogeneous network resources through controlled terminals, facilitating automatic access and dynamic networking capabilities. This approach not only facilitates physical information transmission across

heterogeneous networks, but also establishes a comprehensive transmission control layer that spans the entire network, ensuring seamless data transmission across diverse network environments. A lightweight consensus algorithm is employed between transmission control systems to establish a network-wide consistent node resource and link-state information sharing table. Based on this shared table, the system can perform redundant dynamic link computation and path control strategies using identifiers, ensuring reliable information transmission. This lightweight algorithm not only enhances system efficiency but also reduces computing resource consumption, further improving overall system performance.

The business system layer is primarily responsible for interacting with end users and providing a range of application-layer services, including business terminals, operational and maintenance management, and data encryption and decryption. This layer's objective is to provide personalized business support while ensuring the security and privacy of user data. The business system layer also aims to optimize the user experience, ensuring that the system meets diverse business needs while providing comprehensive security at the application level.

At the same time, we modularize different service applications in the transmission control layer, including the development of a new multi-attribute path selection algorithm that can dynamically adjust path selection strategies based on multidimensional attributes such as latency, bandwidth, node stability, etc., thereby significantly improving transmission efficiency. The transmission control software based on cross-layer design achieves deep collaboration between the resource layer and the control layer, enabling real-time adjustment of network resource allocation to meet dynamic business requirements. These functional modules achieve resource sharing and policy control through a service-oriented architecture (SOA). At the network resource layer, efficient management of heterogeneous resources is the focus of research. In order to better control nodes, the Edge Resource Management System (ERMS) can run lightweight software agents on edge devices, monitor resource status in real time, and assist upper level decision making. Simultaneously running lightweight consensus algorithms improves the overall efficiency of the system.

Figure 5 illustrates the functional structure of the dual-network transmission control service, which is based on the proposed layered design concept and dual-network architecture. The structure primarily consists of two components: the switching bearer service and the transmission service. This layered design clearly delineates the system's functional modules, enhancing its manageability and scalability. From bottom to top, the gray areas represent Network Infrastructure, including Satellite Network, Mobile Network, Internet, and Ad hoc Network. The blue part is the Exchange Bearer layer, which includes Heterogeneous resource scheduling, Node link evaluation module, Cross-layer protocol automatic conversion, Identification parsing and mapping, Protocol-independent controlled exchange. The green part is the Transport Service layer, which includes control services such as Resource perception and aggregation, Multi-path concatenation control, etc.

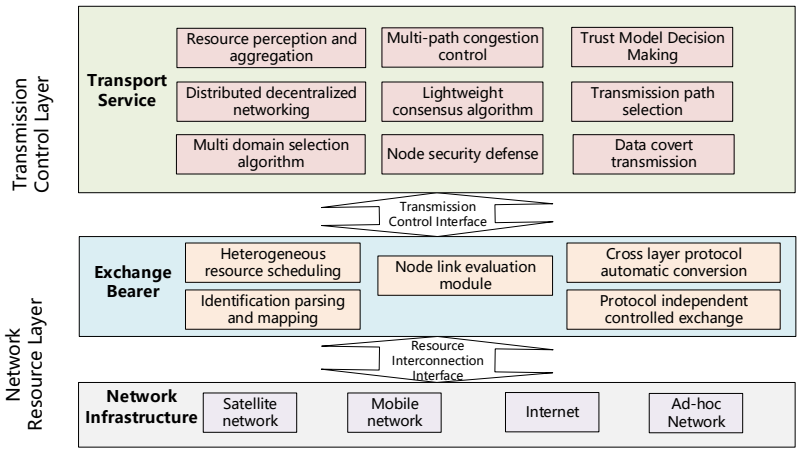


Figure 5. Functional diagram of the transmission control service.

The transmission service layer ensures reliable information transmission within the network through functional modules such as resource sensing, node consensus, transmission path selection, and covert access. Services at this layer focus not only on optimizing information transmission paths but also on enhancing the security and confidentiality of the network. The distributed heterogeneous transmission resource sensing software performs real-time sensing and monitoring of connectivity status between nodes, forming a consistent network-wide resource status information table through a consensus broadcasting mechanism. This sensing and consensus mechanism ensures the system maintains a global view of the network state, enabling it to adapt effectively to dynamic network environments. The multi-attribute transmission path calculation software comprehensively evaluates multiple factors, including network resource status, node transmission capacity, and connectivity. By dynamically calculating transmission paths and generating routes, the software selects the optimal path for information transmission, maximizing efficiency and reliability. The covert access module allows nodes to access the network using virtual identities, supported by automatic logo updates and remote switching. This enhances information concealment and encryption. This covert access mechanism not only enhances system security but also provides a robust safeguard for transmitting sensitive information. By encapsulating transmission-related functions in a service-oriented manner, the system creates multiple independent transmission control service entities. These entities interact through a unified and common interface within a service-oriented architecture (SOA). This service-oriented design enhances system modularity, allowing functional modules to be extended and maintained with greater flexibility. The transmission and control layer consists of functional services responsible for essential tasks, including resource collection and synchronization, path policy control, and information transmission control via the transmission and control interface. This interface design streamlines module interactions, facilitates efficient data transmission, and ensures timely implementation of control policies.

The switching bearer service layer offers capabilities such as heterogeneous resource scheduling, node link evaluation, automatic cross-layer protocol conversion, and protocol-independent controlled switching services for the network system. These services enable effective coordination of heterogeneous resources, facilitating efficient data exchange and protocol conversion across different layers. The multi-resource protocol-independent controlled exchange system features automatic conversion of heterogeneous network communication protocols, controlled information transfer across heterogeneous resources, and support for in-depth information detection and controlled exchange. The system supports dynamic node deployment and flexible application, ensuring network operability in complex environments. The system automates heterogeneous access protocol conversion through an identification system, creating a unified resource state table for the entire network via consensus broadcasting among nodes. The transmission control interface facilitates access to underlying network resources for the upper-layer transmission control service while implementing policy control and transmission path scheduling. This design ensures reliable and secure information transmission, providing robust support for complex and evolving network environments.

Compared with traditional architectures, this architecture significantly enhances the compatibility and flexibility of heterogeneous network resources by building logically independent overlay networks. The various functional modules in the service framework achieve resource sharing and policy control through a service-oriented architecture (SOA). The multi-path transmission algorithm not only enhances the security and reliability of the system, but also provides technical support for the stable operation of the service framework.

4. Experiment

In this section, we experimentally validate the above network system model by replaying the traffic and executing the attack.

4.1. Dataset

To substantiate the validity and applicability of the proposed method, we select the ChinaNet network from the Topology Zoo as the focal point of this experiment [62]. The Topology Zoo encompasses 261 authentic network topologies from around the globe, serving as a valuable resource for network-related research and experiments. It is particularly well-suited for diverse network simulations. Moreover, to enhance the realism of our experiment, we employ traffic data from the WIDE Project. This initiative, managed by MAWI Labs in a collaboration between Japan and the United States, maintains a repository of network traffic. The project gathers data from a specific backbone network spanning Japan to the U.S. at various time intervals (e.g., a specific minute of the day, monthly). This data collection has been ongoing since the year 2000. Importantly, the network traffic is subjected to desensitization procedures, ensuring that IP addresses are processed to retain solely IP packet header information. This approach safeguards privacy while facilitating meaningful analyses of network performance.

In our experimental design, careful attention was given to node connectivity within the topology and the operational feasibility of the experiments. As a result, we selected ONOS version 2.4.1 in conjunction with Mininet to establish our test environment. Mininet provided the flexibility needed to configure network topologies according to our specific experimental requirements, while the ONOS controller automated the deployment of flow tables and managed node interconnections. This setup offered significant benefits for subsequent attack simulations, making it easier to identify and target specific nodes.

We conducted the experiment on the Ubuntu 18.04 system server, and we replicated the ChinaNet network using Mininet, carefully configuring parameters such as IP addresses, MAC addresses, and bandwidth to closely resemble the real network's attributes. To ensure that the traffic in our experiments matched the constructed network environment, we conducted preprocessing on packet data from the WIDE Project. Since the project's dataset included a wide variety of irrelevant information, we filtered it to focus specifically on the 42 primary data flows corresponding to the 42 nodes in the ChinaNet network. We then generated a new pcap file and adjusted relevant parameters using the tcpreplay tool. For effective reinjection of this modified traffic into our constructed network, the file was replayed at the edge nodes, allowing us to measure the number of packets sent and received for each node and link. The resulting traffic data and topology metrics were then integrated into our evaluation algorithm in real time, leading to the outcomes presented in our study. This detailed approach ensured both the accuracy and relevance of our experimental findings.

As shown in Figure 6, based on the actual network configuration, we divided the network topology into different heterogeneous sub-networks according to a ratio of 2:3:1:4. Since nodes in different sub-networks exhibit varying information transmission performance, we define the common transmission delay of different heterogeneous networks as different unit times, i.e., the time it takes for data to traverse a link of length 1 in the topology, based on data from Google. The node types and their corresponding transmission unit delays are defined as follows: Dark blue nodes represent wired interconnection networks with a unit delay of 20 ms. Light blue nodes represent the mobile Internet with a unit delay of 5 ms. Yellow nodes represent satellite networks with a unit delay of 100 ms. Orange nodes represent drone self-organizing networks with a unit delay of 5 ms. To achieve efficient transmission across different heterogeneous networks, we must address the protocol conversion problem. When transmitting data across heterogeneous networks, the protocol fields of packets need to be converted to meet the requirements of the destination network. Traditional protocol conversion methods typically rely on complex protocol cross-reference tables, requiring each network node to refer to the table when transmitting data. This approach not only increases computational overhead but also introduces potential conversion errors and transmission delays.

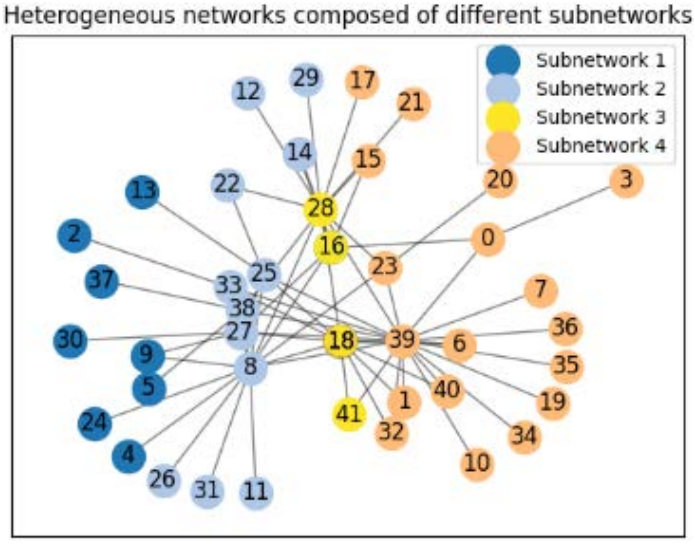


Figure 6. Heterogeneous network composition of ChinaNet network topology.

As illustrated in Figure 6, we segmented the network topology into distinct heterogeneous sub-networks according to a 2:3:1:4 ratio, based on the real-world network setup. Given that nodes in various sub-networks demonstrate diverse information transmission characteristics, we assigned unique unit transmission times for different heterogeneous networks. This unit time is defined by the duration required for data to traverse a link of length 1 in the topology, using data sourced from Google as a reference. The types of nodes and their respective transmission delays are defined as follows: dark blue nodes correspond to wired interconnection networks with a unit delay of 20 ms, light blue nodes represent mobile Internet nodes with a 5 ms unit delay, yellow nodes signify satellite networks with a delay of 100 ms, and orange nodes stand for drone-based self-organizing networks, each with a unit delay of 5 ms.

We evaluate the performance of the network system by examining the traffic and node states at different times. Among them, we measure the traffic and topology information of the network using effectiveness and importance indicators, respectively.

$$NIP_T = F(NEC_T, NIC_T, LEC_T, LIC_T, NRC_T, w_T) \tag{3}$$

where LEC denotes link effectiveness capability, NEC is node effectiveness capability, LIC represents link importance capability, NIC stands for node importance capability, and NRC signifies network reliability capability. Among them, both traffic and node information can be captured through the system, and each specific indicator is uniformly calculated using commonly recognized methods. The parameter w denotes the weight assigned to each capability, which is calculated by the entropy method, not defined by oneself, which will be more objective.

4.2. Result

This experiment is designed to evaluate how network attribute values dynamically shift under attack scenarios. During each attack round, specific nodes are targeted, and fresh traffic replay is initiated, allowing us to monitor various attribute metrics of the affected nodes, links, and the overall network performance at that moment. To maintain fairness across experiments, any traffic involving the attacked nodes, either as source or destination, is filtered out post-attack. The adjusted traffic is then reinjected into the network topology after the attack. Each trial focuses on attacking a single node. Given the experiment's extended duration and the volume of data produced, we measure the decline rate in overall network performance after each attack, comparing it to the pre-attack state.

This decline rate serves as a clear metric, illustrating how quickly the network can stabilize and recover after an incident.

Figure 7 illustrates a comparison between the overall performance of our system and a static resilient network during attack scenarios. The red curve represents our system's performance under attack, initially showing a slower degradation due to the system's reliance on situational awareness, redundancy, and alternative routing paths to cushion the impact on network stability. However, when critical nodes are compromised, the performance drop becomes sharper. As the system undergoes subsequent attacks, optimization measures are applied, flattening the performance decline and mitigating further damage. In contrast, the blue curve illustrates the performance of a rigid, non-dynamic heterogeneous network when facing attacks. The initial impact of an attack is most pronounced, significantly affecting the network's overall stability. As the attack sequence progresses, conventional methods prove insufficient to counteract the effects, causing critical nodes to fail, which results in a more fragmented topology and an increase in isolated nodes. Consequently, the negative impact slows down with subsequent attacks. The experimental setup includes a topology of 42 nodes, which, by the 40th attack, was reduced to a linear two-node configuration. The 41st attack left only one active node, causing the network to become non-functional, reducing the comprehensive performance value to zero.

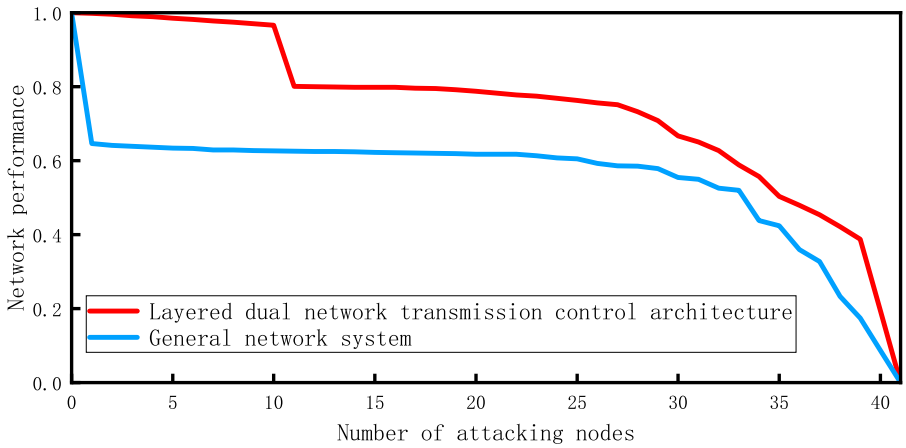


Figure 7. The change in the rate of decrease of the comprehensive network performance curve after an attack on the network.

5. Conclusions

The threat of war poses a substantial risk to the cybersecurity of critical infrastructure globally, causing the remaining network communication resources to exist in a distributed form, particularly affecting systems that depend on traditional, single-channel communication methods. Such disruptions can lead to the paralysis of critical infrastructure and a loss of connectivity between individuals, further exacerbating communication challenges during a crisis. To address these challenges and ensure the safe and reliable transmission of information, we propose implementing a dual-network architecture. This architectural approach involves separating the transmission control layer from the resource network layer, coordinating distributed heterogeneous network resources to enhance the system's flexibility and resilience. This design not only improves the network's resilience to attacks but also creates a more secure environment for information transmission in complex and hostile contexts. Furthermore, our dual-network architecture integrates advanced technologies, including cross-layer protocol encapsulation and multi-path redundant transmission. Integrating these technologies enhances the resilience of information transmission against interference, ensuring secure and complete delivery to the receiver, even in the event of network attacks or path failures. This multi-level, multi-path safeguard significantly enhances the overall reliability and security of the network.

Author Contributions: Conceptualization, L.Y.; Methodology, S.Q. and S.J.; Formal analysis, L.M. and G.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data available in a publicly accessible repository. The data presented in this study are openly available in [topology-zoo] at [http://www.topology-zoo.org/], reference number [62].

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Haji, S.H.; Zeebaree, S.R.; Saeed, R.H.; Ameen, S.Y.; Shukur, H.M.; Omar, N.; Sadeeq, M.A.; Ageed, Z.S.; Ibrahim, I.M.; Yasin, H.M. Comparison of software defined networking with traditional networking. *Asian J. Res. Comput. Sci.* **2021**, *9*, 1–18. [CrossRef]
2. De Sanctis, M.; Cianca, E.; Araniti, G.; Bisio, I.; Prasad, R. Satellite communications supporting internet of remote things. *IEEE Internet Things J.* **2015**, *3*, 113–123. [CrossRef]
3. Su, Y.; Liu, Y.; Zhou, Y.; Yuan, J.; Cao, H.; Shi, J. Broadband LEO satellite communications: Architectures and key technologies. *IEEE Wirel. Commun.* **2019**, *26*, 55–61. [CrossRef]
4. Xiao, M.; Mumtaz, S.; Huang, Y.; Dai, L.; Li, Y.; Matthaiou, M.; Karagiannidis, G.K.; Björnson, E.; Yang, K.; Chih-Lin, I.; et al. Millimeter wave communications for future mobile networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1909–1935. [CrossRef]
5. Guo, J.; Liu, Z.; Tian, S.; Huang, F.; Li, J.; Li, X.; Igorevich, K.K.; Ma, J. TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 3548–3560. [CrossRef]
6. Hesmondhalgh, D.; Valverde, R.C.; Kaye, D.B.V.; Li, Z. Digital platforms and infrastructure in the realm of culture. *Media Commun.* **2023**, *11*, 296–306. [CrossRef]
7. Bar, F.; Galperin, H. Building the wireless Internet infrastructure: From cordless Ethernet archipelagos to wireless grids. *Commun. Strateg.* **2004**, *1*, 45–70.
8. Aydın, E.E.; Kara, O.; Cakir, F.; Cansiz, B.S.; Secinti, G.; Canberk, B. Enabling self-organizing tdma scheduling for aerial swarms. In Proceedings of the Eighth Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, Portland, OR, USA, 1 July 2022; pp. 13–18.
9. Guan, Z.; Cen, N.; Melodia, T.; Pudlewski, S. Self-organizing flying drones with massive MIMO networking. In Proceedings of the 2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Capri, Italy, 20–22 June 2018; pp. 1–8.
10. Wang, P.; Zhang, J.; Zhang, X.; Yan, Z.; Evans, B.G.; Wang, W. Convergence of satellite and terrestrial networks: A comprehensive survey. *IEEE Access* **2019**, *8*, 5550–5588. [CrossRef]
11. Wang, X.; Qu, D.; Li, K.; Cheng, H.; Das, S.K.; Huang, M.; Wang, R.; Chen, S. A flexible and generalized framework for access network selection in heterogeneous wireless networks. *Pervasive Mob. Comput.* **2017**, *40*, 556–576. [CrossRef]
12. Bria, A.; Gessler, F.; Queseth, O.; Stridh, R.; Unbehaun, M.; Wu, J.; Zander, J.; Flament, M. 4th-generation wireless infrastructures: Scenarios and research challenges. *IEEE Pers. Commun.* **2001**, *8*, 25–31. [CrossRef]
13. Tekin, E. Assessing Artificial Intelligence's Military Application in Urban War: A Study of the Israel Defense Forces Operations Since 2021. Master's Thesis, The George Washington University, Washington, DC, USA, 2024.
14. Aviv, I.; Ferri, U. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *Int. J. Crit. Infrastruct. Prot.* **2023**, *43*, 100637. [CrossRef]
15. Dunkels, A. Full TCP/IP for 8-bit architectures. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003; pp. 85–98.
16. Sidler, D.; Alonso, G.; Blott, M.; Karras, K.; Vissers, K.; Carley, R. Scalable 10Gbps TCP/IP stack architecture for reconfigurable hardware. In Proceedings of the 2015 IEEE 23rd Annual International Symposium on Field-Programmable Custom Computing Machines, Vancouver, BC, Canada, 2–6 May 2015; pp. 36–43.
17. Carrascal, D.; Rojas, E.; Arco, J.M.; Lopez-Pajares, D.; Alvarez-Horcajo, J.; Carral, J.A. A comprehensive survey of in-band control in sdn: Challenges and opportunities. *Electronics* **2023**, *12*, 1265. [CrossRef]
18. Javeed, D.; Saeed, M.S.; Ahmad, I.; Kumar, P.; Jolfaei, A.; Tahir, M. An intelligent intrusion detection system for smart consumer electronics network. *IEEE Trans. Consum. Electron.* **2023**, *69*, 906–913. [CrossRef]
19. Koide, M.; Matsumoto, N.; Matsuzawa, T. Caching Method for Information-Centric Ad Hoc Networks Based on Content Popularity and Node Centrality. *Electronics* **2024**, *13*, 2416. [CrossRef]
20. Pruthvi, C.; Vimala, H.; Shreyas, J. A systematic survey on content caching in ICN and ICN-IoT: Challenges, approaches and strategies. *Comput. Netw.* **2023**, *233*, 109896.
21. Ohwo, O.B.; Ayankoya, F.Y.; Ajayi, O.F.; Alao, D.O. Advancing DNS Performance Through an Adaptive Transport Layer Security Model (ad-TLSM). *Ingénierie Des Systèmes D'Information* **2023**, *28*, 1777. [CrossRef]
22. de Carné de Carnavalet, X.; van Oorschot, P.C. A Survey and Analysis of TLS Interception Mechanisms and Motivations: Exploring how end-to-end TLS is made "end-to-me" for web traffic. *ACM Comput. Surv.* **2023**, *55*, 1–40. [CrossRef]
23. Renklier, A.; Öztürk, S. Image authentication and recovery: Sudoku puzzle and MD5 hash algorithm based self-embedding fragile image watermarking method. *Multimed. Tools Appl.* **2024**, *83*, 13929–13951. [CrossRef]

24. Yadav, P.; Kar, S. Efficient Content Distribution in Fog-Based CDN: A Joint Optimization Algorithm for Fog-Node Placement and Content Delivery. *IEEE Internet Things J.* **2024**, *9*, 16578–16590. [CrossRef]
25. Gao, L.; Zhu, X. ICN-Based Enhanced Content Delivery for CDN. *Future Internet* **2023**, *15*, 390. [CrossRef]
26. Dannewitz, C.; Kutscher, D.; Ohlman, B.; Farrell, S.; Ahlgren, B.; Karl, H. Network of information (netinf)—An information-centric networking architecture. *Comput. Commun.* **2013**, *36*, 721–735. [CrossRef]
27. Zhang, L.; Afanasyev, A.; Burke, J.; Jacobson, V.; Claffy, K.; Crowley, P.; Papadopoulos, C.; Wang, L.; Zhang, B. Named Data Networking. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *44*, 66–77.
28. Aboodi, A.; Wan, T.C.; Sodhy, G.C. Survey on the Incorporation of NDN/CCN in IoT. *IEEE Access* **2019**, *7*, 71827–71858. [CrossRef]
29. Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K.; Weiss, H. *Delay-Tolerant Networking Architecture*; Technical Report; RFC Editor: Marina del Rey, CA, USA, 2007.
30. Lokmic-Tomkins, Z.; Bhandari, D.; Bain, C.; Borda, A.; Kariotis, T.C.; Reser, D. Lessons learned from natural disasters around digital health technologies and delivering quality healthcare. *Int. J. Environ. Res. Public Health* **2023**, *20*, 4542. [CrossRef]
31. Tsuru, M.; Cahyo, W.N.; Brastama, P.A. Performance of delay tolerant network protocol in Smart City scenario. *Proc. J. Phys. Conf. Ser.* **2020**, *1569*, 022056.
32. Dhabliya, D. Delay-tolerant sensor network (DTN) implementation in cloud computing. *Proc. J. Phys. Conf. Ser.* **2021**, *1979*, 012031. [CrossRef]
33. Douglass, N.P.; Langel, J.; Moore, W.J.; Ng, L.; Dudukovich, R.M.; Mal-Sarkar, S. Application of fountain code to high-rate delay tolerant networks. *IEEE Access* **2023**, *11*, 10845–10855. [CrossRef]
34. Kindervag, J. Build security into your network's dna: The zero trust network architecture. *Forrester Res. Inc.* **2010**, *27*, 1–16.
35. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
36. Kourtit, K.; Nijkamp, P.; Suzuki, S. The principle of cascadic prosilience—Assessment of territorial recovery strategies after disrupted regional infrastructure systems in Iraq. *J. Infrastruct. Policy Dev.* **2024**, *8*, 2924. [CrossRef]
37. Gupta, D.; Rani, S.; Ahmed, S.H. ICN-edge caching scheme for handling multimedia big data traffic in smart cities. *Multimed. Tools Appl.* **2023**, *82*, 39697–39717. [CrossRef]
38. Khani, M.; Sadr, M.M.; Jamali, S. Deep reinforcement learning-based resource allocation in multi-access edge computing. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e7995. [CrossRef]
39. Tyagi, V.; Singh, S. Network resource management mechanisms in SDN enabled WSNs: A comprehensive review. *Comput. Sci. Rev.* **2023**, *49*, 100569. [CrossRef]
40. Park, K.; Sung, S.; Kim, H.; Jung, J.i. Technology trends and challenges in SDN and service assurance for end-to-end network slicing. *Comput. Netw.* **2023**, *1*, 109908. [CrossRef]
41. Fu, X.; Li, Q.; Li, W. Modeling and analysis of industrial IoT reliability to cascade failures: An information-service coupling perspective. *Reliab. Eng. Syst. Saf.* **2023**, *239*, 109517. [CrossRef]
42. Shahid, K.; Ahmad, S.N.; Rizvi, S.T.H. Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems. *Future Internet* **2024**, *16*, 339. [CrossRef]
43. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
44. Fu, R.; Wang, L. Research on control and management of smart grid optical network based on optical transmission control Protocol (OTN) technology. *Therm. Sci. Eng. Prog.* **2024**, *53*, 102763. [CrossRef]
45. Rao, Z.; Xu, Y.; Yao, Y.; Meng, W. DAR-DRL: A Dynamic Adaptive Routing Method based on Deep Reinforcement Learning. *Comput. Commun.* **2024**, *228*, 107983. [CrossRef]
46. Awan, K.A.; Din, I.U.; Almogren, A.; Seo-Kim, B. Blockchain-Based Trust Management for Virtual Entities in the Metaverse: A Model for Avatar and Virtual Organization Interactions. *IEEE Access* **2023**, *11*, 136370–136394. [CrossRef]
47. Noveck, B.S. The single point of failure. In *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 77–99.
48. Mirnia, M.J.; Shamsari, M. Numerical prediction of failure in single point incremental forming using a phenomenological ductile fracture criterion. *J. Mater. Process. Technol.* **2017**, *244*, 17–43. [CrossRef]
49. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
50. Mirkin, M.; Ji, Y.; Pang, J.; Klages-Mundt, A.; Eyal, I.; Juels, A. Bdos: Blockchain denial-of-service. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020; pp. 601–619.
51. Sengupta, S.; Chowdhary, A.; Sabur, A.; Alshamrani, A.; Huang, D.; Kambhampati, S. A survey of moving target defenses for network security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1909–1941. [CrossRef]
52. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A review of definitions and measures of system resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]
53. Liu, X.; Wang, H.; Li, C. A Review of Endogenous Security Research. *Electronics* **2024**, *13*, 2185. [CrossRef]
54. Bie, Z.; Lin, Y.; Li, G.; Li, F. Battling the extreme: A study on the power system resilience. *Proc. IEEE* **2017**, *105*, 1253–1266. [CrossRef]
55. Serôdio, C.; Cunha, J.; Candela, G.; Rodriguez, S.; Sousa, X.R.; Branco, F. The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges. *Future Internet* **2023**, *15*, 348. [CrossRef]

56. Yilmaz, A.; Gunes, A. *A Model to Protect Disaster Recovery Centers from Cyber Threats with Multi-Layered Network Security Architecture*; Springer Science, Business Media, LLC: Berlin/Heidelberg, Germany, 2024.
57. Stocchero, J.M. A Network Centric Architecture for Military Command and Control Systems. Doctoral Dissertation, Institute of Informatics, Federal University of Rio Grande do Sul., Porte Alegre, Brazil, 2023.
58. Hussein Ali, M. Dynamic Fast Convergence Improvement using Predictive Network Analysis. *Int. J. Comput. Digit. Syst.* **2024**, *16*, 1–16.
59. Di Napoli, C.; Ercolano, G.; Rossi, S. Personalized home-care support for the elderly: A field experience with a social robot at home. *User Model.-User-Adapt. Interact.* **2023**, *33*, 405–440. [CrossRef]
60. Allioui, H.; Mourdi, Y. Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors* **2023**, *23*, 8015. [CrossRef]
61. Yuan, C.; Zhang, W.; Ma, T.; Yue, M.; Wang, P.P. Design and implementation of accelerator control monitoring system. *Nucl. Sci. Tech.* **2023**, *34*, 56. [CrossRef]
62. Knight, S.; Nguyen, H.X.; Falkner, N.; Bowden, R.; Roughan, M. The internet topology zoo. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 1765–1775. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.