MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATION,
ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ELECTRONIC SYSTEMS

ADMIT TO DEFENCE
Head of the Department

__________ Victor HNATIUK
"_____"______________2023

QUALIFICATION WORK

(EXPLANATORY NOTE)

MASTER'S DEGREE GRADUATE

Topic: « Routing system of telecommunication network data flows »

Performer:________________________________ Anastasiia Dudka
(signature)

Supervisor:________________________________ Alina OSIPCHUK
(signature)

Consultants from individual chapters of the explanatory:

Consultant of the «Occupational Safety» chapter__________ Batyr KHALMURADOV
(signature)

Consultant of the «Environmental Protection» chapter
________________________________ Andrian IAVNIUK
(signature)

N-controller: ________________________________ Denys BAKHTIIAROV
(signature)

Kyiv 2023

NATIONAL AVIATION UNIVERSITY

Faculty of aeronautics, electronics and telecommunications
Department of telecommunications and radioelectronic systems
Specialty 172 «Telecommunications and radio engineering»
Educational professional program «Telecommunication systems and networks»

ADMIT TO DEFENCE
Head of the Department

________ Viktor HNATIUK
"_____"_____________2023

TASK
for the performance of qualification work

Dudka Anastasiia
(last name, first name, patronymic of the graduate in the genitive case)

1. Topic of thesis (project): " Routing system of telecommunication network data flows " approved by the rector's order dated September 8, 2023 No. 1965/ст.

2. The term of the work: from 02.10.2023 to 31.12.2023.

3. Initial data for work:the existing algorithm for finding the shortest paths in the network.

4. Contents of the explanatory note: Analysis of existing telecommunication networks and algorithms. Designing a simulation of path-finding for data transmission there.

5. List of mandatory graphic (illustrative) material: presentation slides in the Microsoft power point software package.

6. Calendar plan-schedule

№ cf.	Tasks.	Term. execution	Mark of completion
1	Develop a detailed content of the qualification work sections	02.10.2023- 04.10.2023	Done
2	Introduction	05.10.2023- 08.10.2023	Done
3	Theoretical foundations of routing in telecommunication networks	09.10.2023- 22.10.2023	Done
4	The Dijkstra algorithm	23.10.2023- 05.11.2023	Done
5	Application of the Dijkstra algorithm in telecommunication networks.	06.11.2023- 30.11.2023	Done
6	Practical implementation and pilot study	01.12.2023- 04.12.2023	Done
7	Labour protection	07.12.2023- 17.12.2023	Done
8	Environmental protection	21.11.2022- 30.11.2022	Done
9	Elimination of deficiencies and defence of qualification work	21.11.2022- 30.11.2022	Done

7. Consultants from separate chapters

Chapter	Consultant (position, Full Name)	Date, signature	
		Issued the task	Task accepted
Occupational Safety	Ph.D. in Med., Professor Batyr KHALMURADOV		
Environmental Protection	Ph.D. in Biol., Associate Professor Andrian IAVNIUK		

8. Issue date of the assignment: “29” of September, 2023.

Supervisor of Qualification Work____________________ Alina OSIPCHUK
(signature of the supervisor) (full name)

The task has been taken on for execution_______________ Anastasiia DUDKA
(signature of the graduate) (Full name)

ABSTRACT

The qualification work "Routing system of telecommunication network data flows" contains 68 pages, 39 figures, 4 tables, 15 sources.|

ROUTING SYSTEM, TELECOMMUNICATION NETWORK, DATA FLOWS.

Object of study – investigating the routing system in telecommunication network data flows.

Subject of study – exploring the mechanisms of the routing system in telecommunication networks.

The purpose of the thesis is comprehensively analyzing the routing system's intricacies in managing data flows, providing insights into its efficiency, reliability, and adaptability.

Research method - systematic examination of literature, case studies, and practical implementations related to telecommunication network routing systems, using both qualitative and quantitative analyses.

Useful in academic settings, research institutions, and professional environments for a deep understanding of telecommunication network data flow routing systems. Valuable reference for researchers, practitioners, and students in telecommunication and network engineering.

CONTENT

LIST OF SYMBOLS

VPN - Virtual Private Network.

IP address - Internet Protocol address.

LAN - Local Area Network.

RIP - Routing Information Protocol.

OSPF- Open Shortest Path First.

BGP - Border Gateway Protocol.

EIGRP - Enhanced Interior Gateway Routing Protocol.

SDN - Software-Defined Networking.

Cisco ACI - Application Centric Infrastructure.

DDoS - Distributed Denial of Service.

QoS - Quality of Service.

PC - Personal Computer.

INTRODUCTION

Relevance of the topic: The relevance of this work is due to a number of factors. First of all, the growing volume and complexity of telecommunications networks with increasing requirements for quality of service. The need to develop efficient routing systems to optimally manage data flows is becoming increasingly important. In addition, the rapid development of technology and the increasing scale of networks are leading to an increase in the amount of data that needs to be processed and routed. New methods and algorithms, such as Dijkstra's algorithm, are addressing these challenges and require further research and development.

Relationship of the work with scientific programmes, plans, topics.

Purpose and objectives of the study. The aim of the study is to investigate and analyse the Dijkstra algorithm in the context of routing data flows in telecommunication networks. In addition, the aim is to improve and develop new methods to increase the efficiency of this algorithm.

To achieve this goal, the following scientific tasks are being solved.

- Investigate the Dijkstra algorithm as a tool for routing in telecommunication networks.
- To study the existing methods of improving the performance of the Dijkstra algorithm and conduct a comparative analysis.
- Develop your own methods and tools for optimising the Dijkstra algorithm.
- Conduct an experimental study of the results of the algorithm improvement.

Object of research: The process of routing data flows in telecommunication networks.

Subject of research*:* Dijkstra algorithm and methods of its optimisation in the context of data flow routing.

Research method:

Analysis of literary sources;

Modelling;

Experimental testing;

Comparative analysis;

Prospects and development.

Scientific novelty and practical significance of the results

Scientific Novelty of the Results:

1. The findings derived from this qualification work offer valuable insights applicable to real-world scenarios in telecommunication operator networks.

2. The acquired data stands as a potential contribution to scientific articles and various research endeavors within the field.

Practical significance of the results:

The data used in this work has been provided to optimise the performance of online games and applications on mobile platforms.

Testing of the results obtained. The main provisions of the work were presented and discussed at the following conferences:

- Scientific and Practical Conference "Problems of Operation and Protection of Information and Communication Systems", Kyiv, 2023.

CHAPTER 1
THEORETICAL FOUNDATIONS OF ROUTING IN TELECOMMUNICATION NETWORKS

1.1. Basic concepts of routing

Routing is a fundamental process in network communications, serving as a critical mechanism for determining the best path for the fast and efficient transmission of information across a network. The main objectives of route selection are factors such as throughput, delay and cost, which affect the overall performance of the network.

At the heart of the routing process are routers, indispensable devices that play a key role in analysing routing tables. These tables contain information about the topology of the network and are used by routers to make informed decisions about where to route data packets. By using IP addresses to determine the source and destination of data, routers ensure that information flows smoothly and reliably across the network.

Dynamic routing further enhances network agility by allowing routes to be changed in real time in response to changes in the network environment. This dynamic nature allows the network to adapt to changes in structural configurations, fluctuations in traffic volume, and other dynamic factors. Consequently, the network can optimise its performance by constantly evaluating and adjusting the routes that data packets take[1].

In essence, the main goal of routing is to ensure not only the efficiency and reliability of data delivery, but also the optimisation of this process within the network. By continuously analysing and adapting to the ever-changing network conditions, routing mechanisms contribute to the smooth and efficient functioning of modern communication infrastructures.

1.1.1. Routers and their role

Packet routing is a basic function that determines the best path for forwarding data from a source to a destination. The router analyses packet headers and decides where to route them, using tables and algorithms to determine the best route. The choice can depend on parameters such as cost, throughput, latency, and more.

Routers maintain tables that contain information about the available routes on the network. These tables help the router determine where to send packets for further processing. Routers have physical or logical network interfaces that allow them to connect to different parts of the network. Each interface can be assigned to a specific network segment or a specific network.

Routers allow networks to communicate with each other. They are used to filter traffic and protect the network from unwanted threats and attacks, and use packet filtering rules to determine which types of traffic are allowed and which are blocked.

Routers can dynamically update their tables based on changes in the network. This allows them to adapt to changes in network topology and provide efficient routing.

An IP address (Internet Protocol address) is a numeric address that uniquely identifies a device on a network. Each device connected to the network has its own unique IP address, which allows other devices to know its location and communicate with it. There are two main versions of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses. As the available IPv4 addresses are exhausted, the transition to IPv6 is becoming increasingly important. Additionally, an IP address can be divided into subnets to organise a network. This is done by using a subnet mask, which defines which bits of the address are allocated to identify the network and the nodes in the network.

Network interfaces - routers can be physical (e.g. Ethernet ports) or logical (e.g. virtual interfaces for VPNs or subnets). Each interface has a unique IP address. Network interfaces are used to connect the router to different parts of the network. For example, an interface can be used to connect to a local area network (LAN), an Internet service provider, or other networks.

Routers use routing tables to determine which interface to send packets through for further routing analysis. The IP address on the interface determines on which network the packet will be displayed for further routing.

1.1.2. Routing tables and their structure

Routing tables are sets of entries that contain information about available routes in a network. Routing tables are usually stored in a router's memory and are used to determine the best path for sending data packets from a source to a destination.

Table 1.1

Entry structures in the routing table

Purpose	Subnet mask	Next hop	Interface
192.168.1.0	255.255.255.0	192.168.1.1	eth0
10.0.0.0	255.0.0.0	10.0.0.1	eth1
172.16.0.0	255.255.0.0	172.16.0.254	eth2

1. Destination - indicates the IP address of the destination network (for example, 192.168.1.0), which owns the packets that will be routed by this entry.

2. Subnet mask - indicates which part of the destination IP address is considered the network address. In this case, the mask 255.255.255.0 indicates that the first 24 bits of the IP address are used to identify the network, and the last bit identifies a specific node in that network.

3. Next hop - indicates the IP address of the router to which the packets will be forwarded for further routing. In this case, all packets addressed to the 192.168.1.0 network will be forwarded to the router with the IP address 192.168.1.1 for further routing.

4. Interface - indicates the network interface of the router through which packets will be sent to the network. In this case, packets will be sent through the interface named "eth0."

This routing table entry defines how the router should handle packets addressed to the 192.168.1.0 network.

1.1.3. Routing metrics and determining the optimal path

Routing metrics are quantitative parameters that evaluate the quality or cost of a network route. These metrics include latency, throughput, and route cost, each of which has its own units of measurement. The optimal path is defined as the route with the lowest cost or the best performance, such as minimum delay.

The goal of routing metrics is to ensure that the router selects the route that best meets the needs of the network and the service. For example, for a voice phone call, it may be important to minimise latency, so the metric may give high weight to latency as a key criterion for route selection.

Routers use routing tables that specify metrics for different routes. When a packet reaches a router, it analyses the routing table to determine the best route for forwarding.

Various routing algorithms are used to determine the optimal route, such as Dijkstra's algorithm, Bellman-Ford's algorithm, OSPF, and RIP. These algorithms take into account routing metrics for efficient path selection.

Due to the dynamic nature of networks, routing metrics can change over time. Routing algorithms need to be adaptive to changes in the network and update routes as needed.

1.2. Types of routing in telecommunication networks.

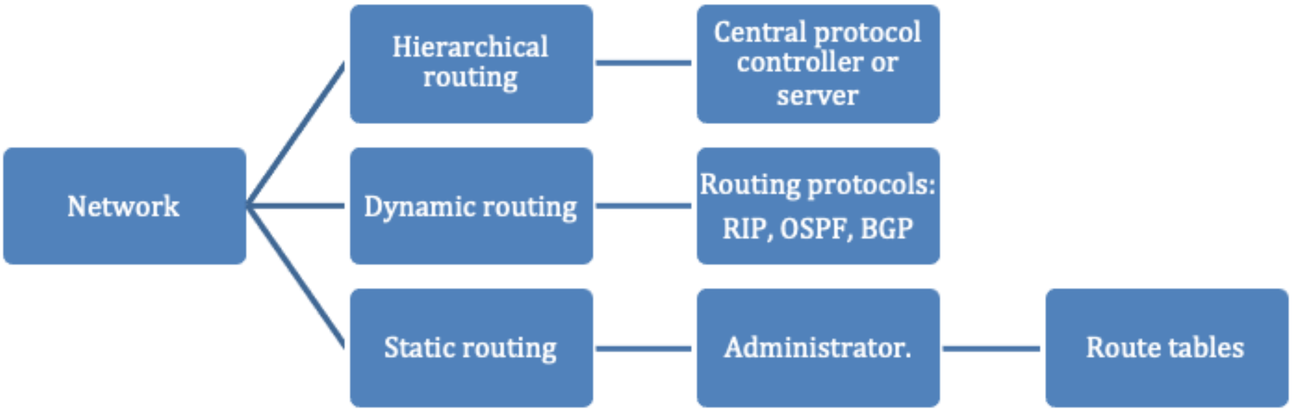


Fig. 1.1. Types of routing in telecommunication networks

Static routing - The network administrator manually configures routes in the routing tables of each router. This means that the routers do not make route selection decisions automatically, but receive explicit instructions from the administrator. It is typically used in simple networks where routes rarely change, or in scenarios where control over routing is very important. The advantages of static routing include ease of configuration and reliability. However, it is not suitable for large and complex networks where routes may change frequently**.**

Hierarchical routing - In centralised routing, all routing decisions are made at a central controller or server. Routers follow these decisions and simply execute them. Centralised routing can be used in distributed networks where centralised management is important. It also helps to avoid unnecessary spending on computing resources on the router itself. Examples of architectures: SDN (Software-Defined Networking) protocols and architectures such as Cisco ACI (Application Centric Infrastructure) use centralised routing [2].

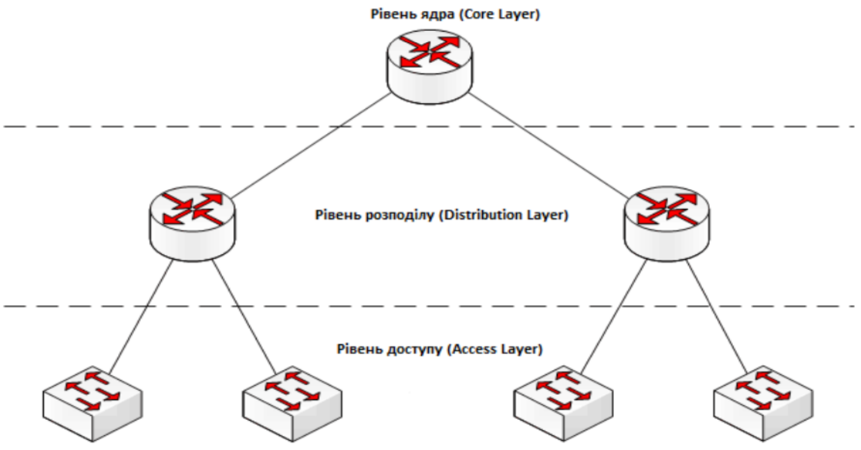

Рівень ядра (Core Layer)
Рівень розподілу (Distribution Layer)
Рівень доступу (Access Layer)

Fig. 1.2. Hierarchical routing

Dynamic routing - exchanges information about the state of the network and calculates optimal routes automatically using routing protocols. There is no need to configure routes manually. It is used in complex networks where routes can change frequently, or in situations where automatic adaptation to changes in the network is important. Examples of dynamic routing protocols include RIP (Routing Information Protocol), OSPF (Open

Shortest Path First), BGP (Border Gateway Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and more.

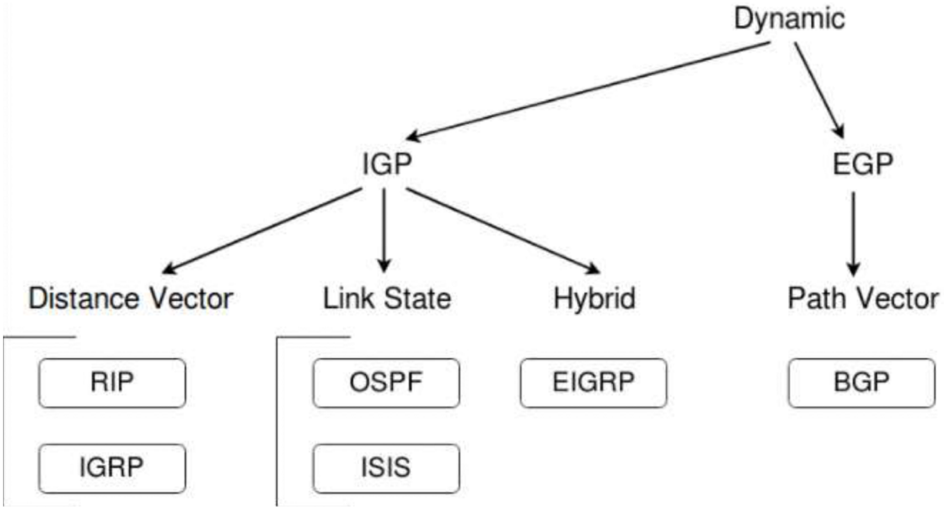


Fig. 1.3. Dynamic routing

1.2.1. Routing at the network and subnetwork level

The basic principle in distributed routing is that the network is divided into segments, and each segment has its own router. Distributed routing is often used in large-scale networks where routers are responsible for specific network segments. This approach allows the network to scale, but can lead to problems in resolving routes between segments.

1.2.2. Routing protocols

RIP (Routing Information Protocol) is one of the oldest and simplest routing protocols. Version 1 uses static metrics to determine the best route, while version 2 allows you to use more information to make a decision. Version 2 uses a "hop count" as a metric. RIP is typically used in small networks where the speed of route information collection and dissemination is not critical.

OSPF (Open Shortest Path First) is a link-state-based protocol that uses the Dijkstra algorithm to calculate the optimal route. OSPF uses "number of bandwidth units" as a metric, where each link has a weight. It is used in complex networks where the speed of information gathering and updating is important.

BGP (Border Gateway Protocol) - used for routing between autonomous systems (AS). It works at the level of routers that manage large-scale networks. BGP takes into account various factors, including route cost and AS membership. It is the standard protocol for routing large amounts of traffic on the Internet and between different providers.

1.3. Requirements for the routing system

Reliability:

- Failure detection: A routing system must be able to detect various types of failures such as network hardware failures, software failures, loss of connectivity, etc. For this purpose, it uses various mechanisms such as keep-alive messages and network status monitoring.
- Recovery: Once a failure has been detected, the system must be able to resume operations by switching to redundant means. This may include rerouting traffic to alternate routes or backup routers.
- Preventing a single point of failure: To ensure reliability, a routing system must prevent a single point of failure. This means that it must be able to redundantly and reliably provide redundancy for critical network components such as routers and links.
- Self-healing: The routing system must be capable of self-healing after a problem or failure is resolved. This includes restoring routes and returning to normal operation.

Availability:

- Continuity of service: The routing system must be able to provide continuity of service to users. This means that the network must remain available even during failures and recovery efforts.
- Maximising availability: The routing system must maximise network availability. This includes ensuring that routers are running reliably, monitoring network health, and detecting failures in a timely manner.

- Backup routes: To ensure availability, the routing system must have backup routes that can be used in the event of a primary route failure. This helps to avoid loss of connectivity.
- Backup equipment: To maintain availability, the routing system must have redundant hardware that can be used in the event of a primary hardware failure. The redundant equipment must be ready to go and able to automatically start up when the primary equipment fails.

Network scalability is an important requirement for a routing system in telecommunications networks, as networks can grow in size and complexity. Scalability refers to the ability of a network to function efficiently and reliably even in large networks. Networks can grow in size by adding new nodes, connecting new subnets, and expanding geographic coverage. The routing system must be able to cope with this growth without sacrificing performance or quality of service. Scalability also implies efficient use of network resources, including bandwidth, router computing resources, and memory. The routing system must be able to distribute the load evenly and efficiently. Dynamism and adaptation can be affected by changes in topology and load. The routing system must be able to dynamically adapt to these changes by updating routes and taking into account new network conditions. Networks can include different types of network equipment, from simple routers to large switches and specialized devices. The routing system must be able to support these different types of equipment and enable them to work together. Scalability also includes the use of common and standardized routing protocols that can be implemented at different levels of the network and in different parts of the network.

1.3.1. Protection against attacks and vulnerabilities

The routing system must be able to detect potential threats and attacks, such as hacking of network devices, data interception, or distributed denial of service (DDoS). Intrusion detection and event logging mechanisms are used for this purpose. It is important to have authentication mechanisms in place to determine whether a user or device is a valid member of the network. After authentication, the routing system must allow or restrict access to various resources based on authorisation rules. To protect sensitive data, the routing system must support encryption of data on the network. This prevents sensitive information from being intercepted and read. Protection against DDoS attacks. Detect and defend against distributed denial of service and other large-scale attacks aimed at overloading the network and its components. It is important to regularly update the software of routers and other network devices, as well as to install patches to fix vulnerabilities in a timely manner. The network should be segmented into logical segments to limit the spread of attacks and reduce the impact of potential incidents. The routing system should provide network status monitoring and event logging to detect and analyze attacks and other emergency events.

1.3.2. Adaptation to changing network conditions

Adaptation to changing network conditions determines the readiness of the routing system to respond to changes in network topology, load, and other network conditions. Network dynamism implies that the topology and load can evolve over time, and the routing system must detect these changes and adapt to them effectively.

One aspect of network dynamism is its ability to detect changes and automatically update routes. For example, the addition of new network devices can change the optimal route, and the system should automatically take these changes into account.

Changes in load, such as increased traffic during peak hours or the introduction of new services, also affect routing performance. The system must distribute the load evenly and optimally, and automatically adapt to changes in load.

Adaptation also includes detecting network faults and taking steps to correct them. For example, the system should detect network device failures and automatically redirect traffic to a backup path.

For effective adaptation, the routing system can use automated mechanisms and intelligent algorithms, such as self-healing mechanisms, automatic change detection, and route optimisation.

An important aspect of adaptation is monitoring the network and analyzing the data to make decisions about changes. The routing system must have the means to collect and analyze network and traffic data.

CONCLUSION TO CHAPTER 1

This chapter has covered the key aspects of routing in telecommunications networks, which is an important foundation for data management in networks. Learning about the theoretical foundations of routing not only reveals basic concepts such as IP addresses, routers, and routing metrics, but also emphasises their importance in improving the efficiency and reliability of network communications.

The first sub-section highlighted the importance of basic routing concepts, including IP addresses, routers, and routing metrics. Understanding these terms is becoming key for network management professionals and contributes to the effective management of traffic in the network. Different types of routing are analysed, such as static, dynamic, intra-network and inter-network. This allows you to gain an understanding of different routing strategies and their impact on network performance.

The last sub-point identified the requirements for routing systems, such as reliability, scalability, QoS, attack protection, and adaptation to changing network conditions. These requirements define routing strategies to ensure optimal network performance.

To summarise, the conclusion of chapter 1 is that understanding and using the theoretical foundations of routing is an important step in the effective management of telecommunications networks. The following chapters will look at specific routing algorithms, such as the Dijkstra algorithm, their implementation, and the advantages and disadvantages in practical applications.

CHAPTER 2
THE DIJKSTRA ALGORITHM

2.1. Description of the Dijkstra algorithm

Dijkstra's algorithm is one of the most common and well-known routing algorithms in telecommunication networks. This algorithm was invented by Edsger Dijkstra in 1959 and is used to find the shortest paths in a graph representing a network with nodes and edges. The basic idea of the Dijkstra algorithm is to find the shortest path from one node (the source node) to all other nodes in the network[4].

The algorithm sets the distances from the initial node (source node) to all other nodes. The distance from the initial node is set to 0, and to all other nodes to infinity. The main loop of the algorithm is to calculate the distance between each node and all its neighbours and check whether they can be reached faster through the "current node". If such a path exists, the distance to the neighbouring node is updated and marked as "visited". Once the algorithm has completed the check, it can build the shortest path from the initial node to all the others.

Step 1: Initialisation.

- Set the distance to all vertices of the graph (V) = ∞

- Distance to the vertex (a) = 0.

- No vertex in the graph has been processed yet.

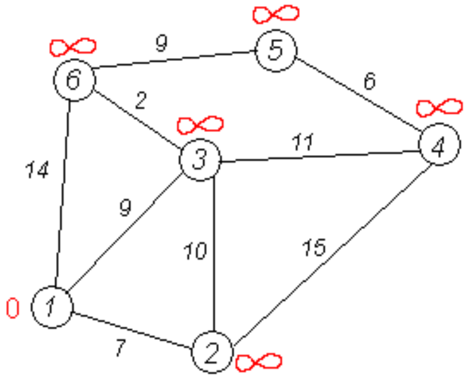


Fig. 2.1. Initialisation

Step 2: Finding the shortest distance.

- Identify the vertex with the current minimum distance among those not yet processed. In this example, it is vertex 1.

- Traverse all neighbors of vertex 1, and if the path to a neighboring vertex through vertex 1 is shorter than the current minimum path to that neighbor, update the minimum path:

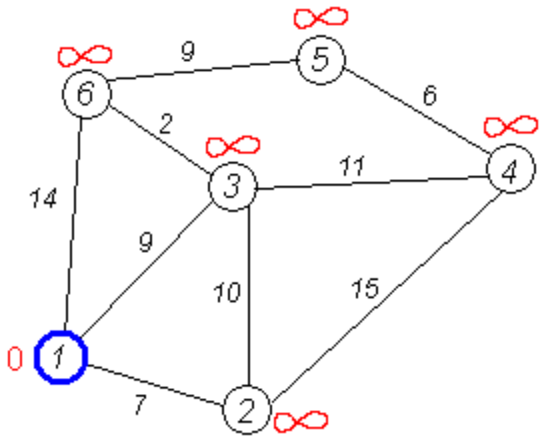


Fig. 2.2. Determining the first smallest neighbor of vertex 1

Step 3: Determining the first smallest neighbor of vertex 1

- The first neighbor of vertex 1 is vertex 2. The path to vertex 2 through vertex 1 is equal to the current minimum distance to vertex 1 plus the weight of the edge between vertices 1 and 2, which is 0 + 7 = 7. This is less than the current minimum path to vertex 2, so we update the minimum path to vertex 2, setting it to 7.

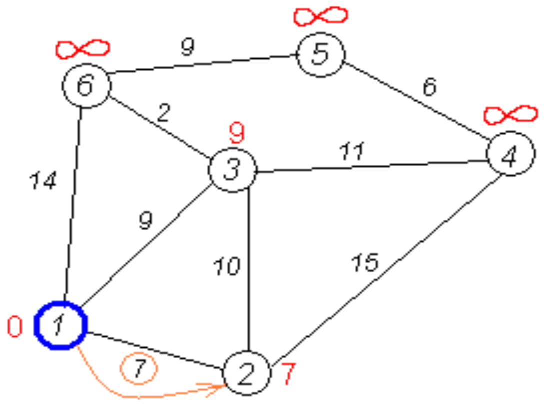


Fig. 2.3. The minimum path to vertex 2

Steps 4 and 5: Continue Updating Distances

- Repeat the process for the remaining neighbors of vertex 1, such as vertices 3 and 6.

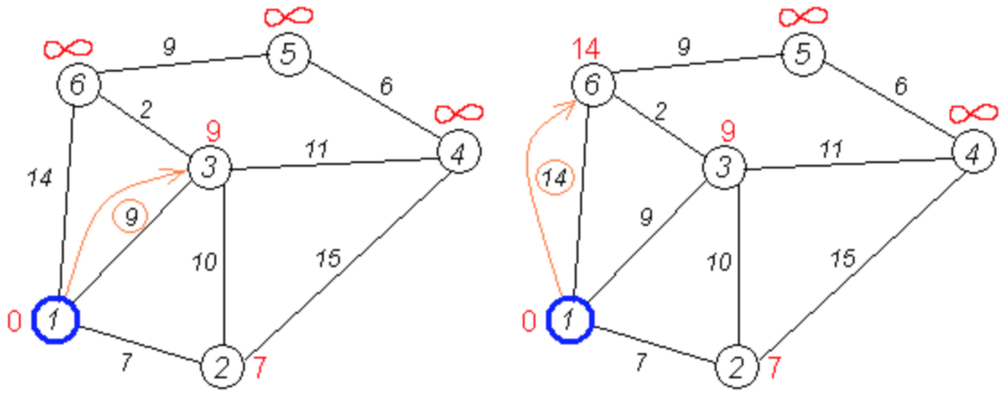


Fig. 2.4. Steps 4 and 5

Step 6: Fix the final distance.

- All neighbors of vertex 1 have been checked. The current minimum distance to vertex 1 is considered final, and vertex 1 is marked as processed (or removed from consideration).

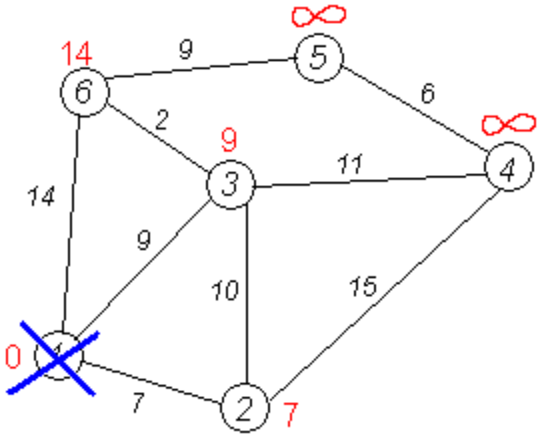


Fig. 2.5. All neighbors of vertex 1 have been checked

Step 7: Repeat.

- Go back to Step 2 and find the next unprocessed vertex with the current minimum distance. In this case, it is vertex 2, with a current minimum distance of 7.

- Attempt to update distances to its neighbors, such as vertices 3, 4, and 1.

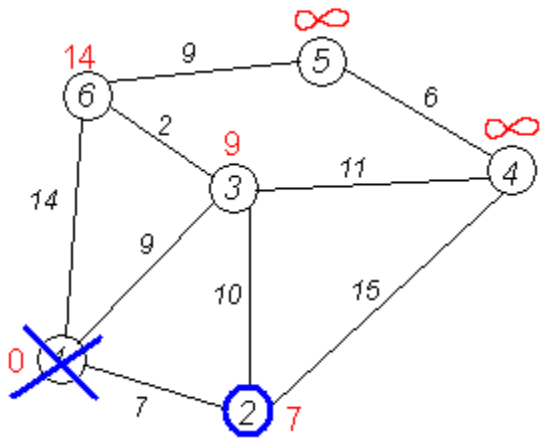


Fig. 2.6. Minimum distance of 7

Step 8: Process the neighbours of the vertex 2.

- Consider the neighbours of vertex 2 (in your example, vertices 1, 3, 4).
- Update the distances to the neighbours through vertex 2 if the found path is shorter.

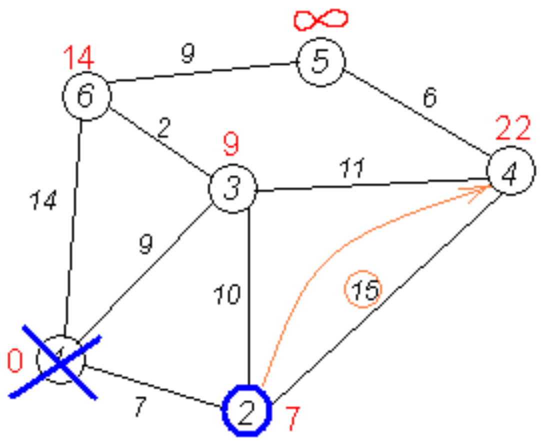


Fig. 2.7. Consider the neighbours of vertex 2

Step 9:

- Another neighbor of vertex 2 is vertex 3. If we go to vertex 3 through vertex 2, the path would be equal to the shortest distance to vertex 2 plus the distance between vertices 2 and 3, which is 7 + 10 = 17. However, 17 is greater than the distance we have already recorded for vertex 3, which is 9. Therefore, we do not change the current distance to vertex 3

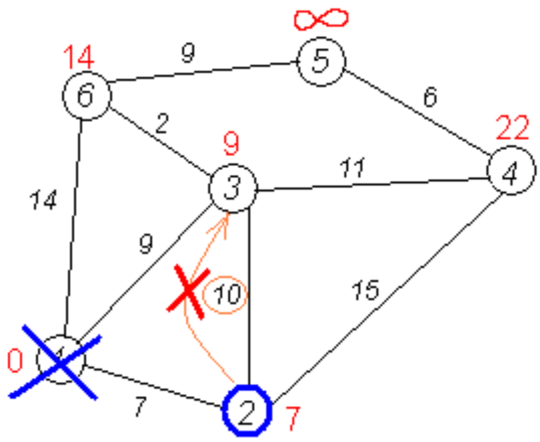


Fig. 2.8. Current distance to vertex

Step 10: Finalize distance to vertex2

- All neighbors of vertex 2 have been examined. We freeze the distance to vertex 2 and remove it from consideration.

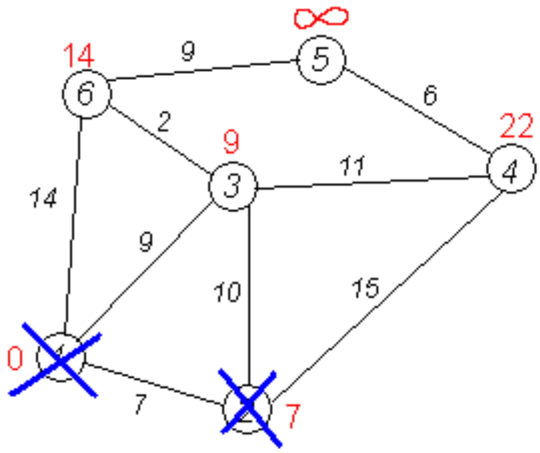


Fig. 2.9. All neighbors of vertex 2 have been examined

Steps 11-15: Repeat for the other vertices.

- Repeat steps 2-6 for the remaining vertices, finding the smallest distances and updating them until all vertices are removed.

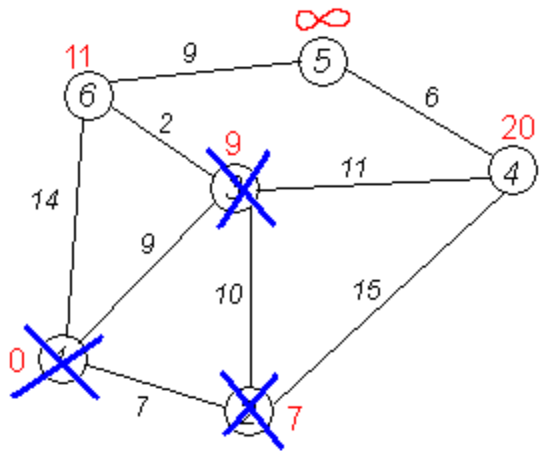


Fig. 2.10. Finding the smallest distances and updating them until all vertices are removed

Subsequent Steps:

- Perform the same procedure for the remaining vertices (in order: 6, 4, and 5).

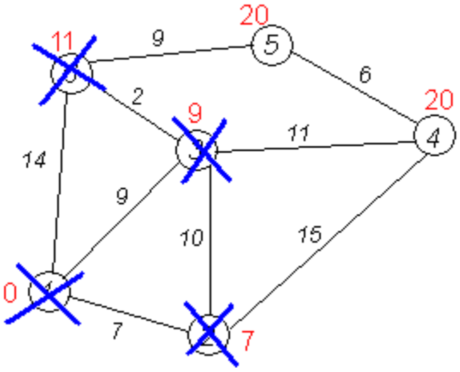


Fig 2.11. Subsequent Steps

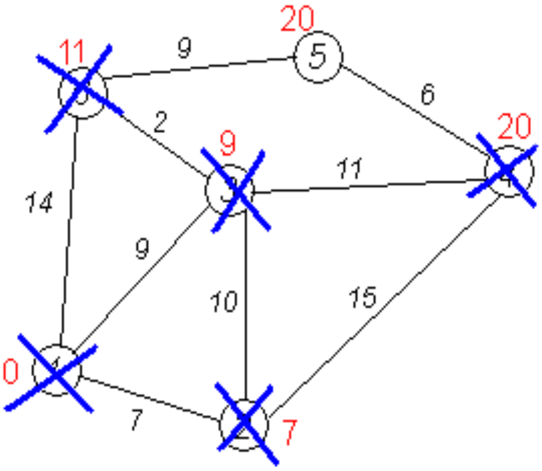


Fig. 2.12. Subsequent Steps

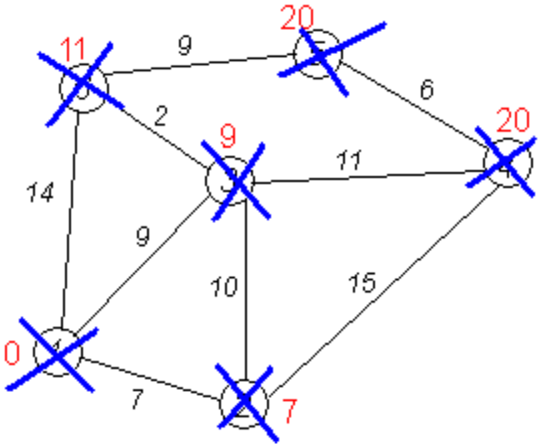


Fig. 2.13. Subsequent Steps

Algorithm Termination:

- The algorithm concludes its operation when all vertices have been removed. The final results are visible in the last diagram, showing the shortest path from vertex 1 to vertex 2 as 7, to vertex 3 as 9, to vertex 4 as 20, to vertex 5 as 20, and to vertex 6 as 11 conditional units.

2.2. Implementation of the Dijkstra algorithm in telecommunication networks

The implementation of the Dijkstra algorithm in telecommunications networks requires detailed developments at the level of network hardware, including routers and switches, as well as at the level of software. This implementation aims to ensure reliable and efficient data routing in the network.

Updating routing tables - the implementation of the Dijkstra algorithm requires routing tables that store information about the shortest paths to all network nodes. These tables must be constantly updated to reflect changes in the network.

Event handling and notifications - the algorithm must be able to handle events such as new nodes being added, edges being removed, router failures, etc. Each such event can affect the routing tables, so the routing system should automatically update the information and send notifications of changes.

Scalability - telecommunication networks can be large and complex. An implementation of the Dijkstra algorithm must be scalable, i.e. capable of handling large networks with a large number of nodes and edges. This requires optimizing the algorithm and limiting its computational costs.

Graphical display of the network - interfaces allow you to monitor the status of the network, check shortest paths and identify problems in real time[5].

Safety and security - the implementation of the Dijkstra algorithm should also include measures to ensure the safety and security of the network from possible attacks and vulnerabilities. This may include router authentication, access control, DDoS protection, and other security measures.

Fault tolerance - an important aspect of implementing the Dijkstra algorithm is fault tolerance. Networks must be able to operate and recover from router or edge failures, and the routing algorithm must be prepared to account for these failures and provide alternative routes. Graphs simplify network monitoring and analysis, helping operators to identify problems in time and take action to resolve them.

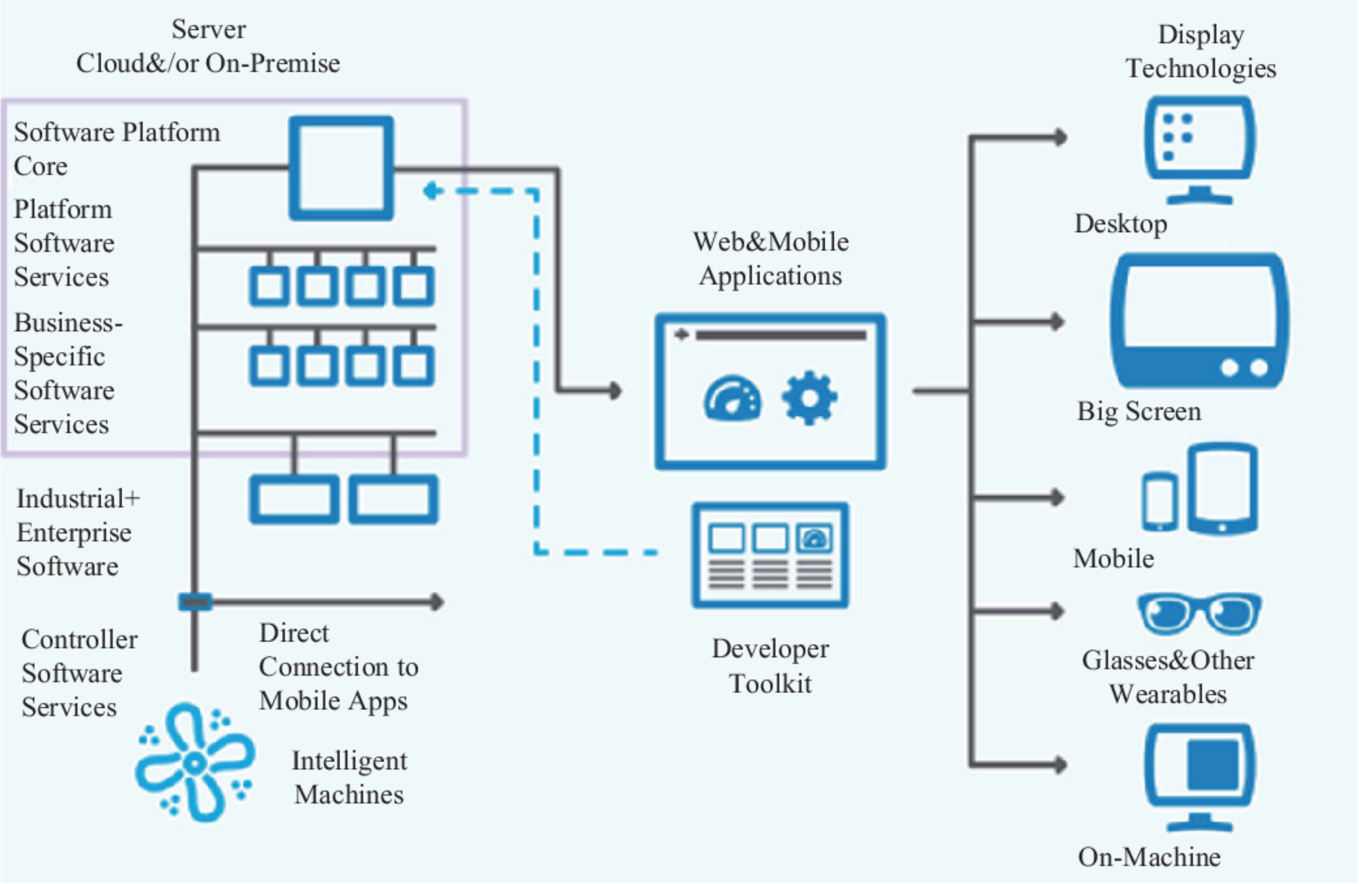


Fig. 2.15. The Dijkstra algorithm in telecommunication networks

2.3. Advantages and disadvantages of the Dijkstra algorithm

Advantages of the Dijkstra algorithm [6]:

- Finding the shortest paths: One of the main advantages of Dijkstra's algorithm is that it always finds the shortest path between two nodes if one exists. This makes it ideal for use in networks where it is important to have precise control over routing.
- Ease of implementation: The Dijkstra algorithm is relatively simple to implement and understand. It is easy to implement in practice, making it a popular option for use in real-world networks.
- Can be used in acyclic graphs: Dijkstra's algorithm is suitable for use in acyclic graphs where there are no cycles. This makes it possible to use it in a variety of network topologies.

Disadvantages of the Dijkstra algorithm:

- Resource consumption: One of the main disadvantages of the Dijkstra algorithm is its resource consumption. It requires calculating the distances to all nodes in the network, even if these distances are not needed. In large networks, this can lead to a significant consumption of computing resources and time.
- Inability to make changes to the network during operation: The Dijkstra algorithm does not support network changes while it is running. If a new node is added or failures occur, the routing tables must be recalculated. This can lead to unnecessary time and resources.
- Vulnerability to loops: Dijkstra's algorithm does not support the detection of loops in the network, and if they occur, a loop in the computation can occur.
- The presence of only one source: The Dijkstra algorithm is designed to find the shortest paths from a single source to all other nodes. If you need to find the shortest paths from many sources to all other nodes, it can lead to excessive computation.

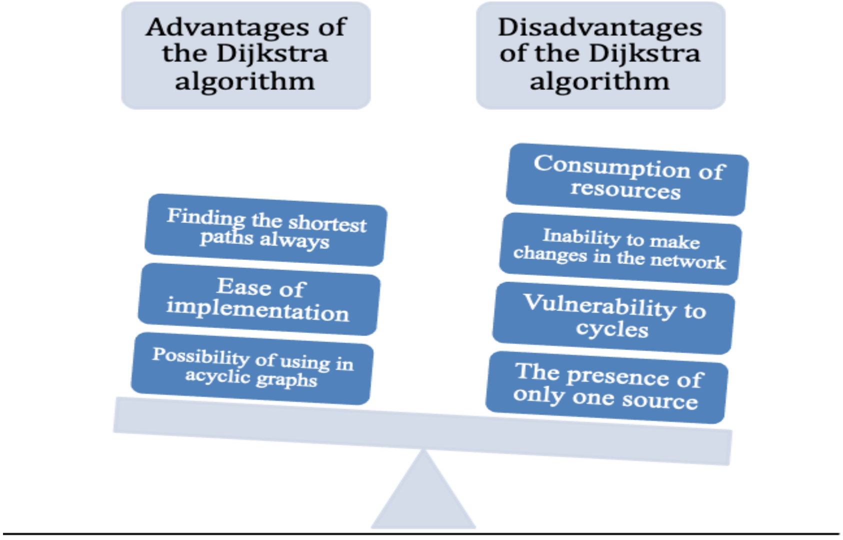

Advantages of the Dijkstra algorithm
Disadvantages of the Dijkstra algorithm
Finding the shortest paths always
Ease of implementation
Possibility of using in acyclic graphs
Consumption of resources
Inability to make changes in the network
Vulnerability to cycles
The presence of only one source

Fig. 2.16. Advantages and disadvantages of the Dijkstra algorithm

CONCLUSION TO CHAPTER 2

The Dijkstra algorithm is an efficient method for finding the shortest paths in a weighted graph. It takes into account the weights of the edges between nodes and starts by determining the shortest path from the initial node to all other nodes in the network. The algorithm is implemented by comparing distances and choosing the optimal route at each step.

In the context of telecommunication networks, the Dijkstra algorithm can be successfully used to calculate shortest paths by computing routing tables. It is particularly effective in networks with a small number of nodes.

However, the algorithm has its advantages and disadvantages. The advantages include its simplicity of implementation and guaranteed ability to find the shortest path. On the other hand, it cannot be used in networks with cycles or negative edge weights, and it has a high computational complexity in networks with a large number of nodes. In addition, it does not always guarantee finding the optimal path.

The conclusion of chapter 2 emphasizes that the Dijkstra algorithm is a popular tool for calculating shortest paths, but its application requires careful attention to the network characteristics and requirements of a particular application.

CHAPTER 3

Application of the Dijkstra algorithm in telecommunication networks

3.1. Routing in wireless networks

Routing in wireless networks is a challenging task due to a number of features of this type of network, such as node mobility and changing topology.

The impact of mobility on the efficiency of the Dijkstra algorithm:

The impact of mobility on the effectiveness of the Dijkstra algorithm in telecommunication networks is significant and requires a detailed consideration. Mobility in the context of wireless networks means constant changes in the location of devices, which leads to a dynamic change in the network topology.

One of the key challenges is the instability of communication due to the mobility of devices. Changes in the topology can lead to loss of connection and instability of data transmission. Dijkstra's algorithm, which is based on a static topology, becomes less effective in such conditions.

The constant route updates required by Dijkstra's algorithm whenever the topology changes can lead to significant delays in data transmission. This is especially important in modern networks where transmission speed is a key factor.

Additionally, mobility can increase the energy consumption of network devices. Constant activity to store and update route information in a mobile environment can contribute to high energy consumption.

Optimisation of the Dijkstra algorithm for mobility is becoming essential. It is important to consider innovative routing approaches that take into account topology dynamics and ensure efficient data transmission in conditions of high device mobility.

Channel state-based routing protocols. They use active measurement of channel characteristics to dynamically update routes. Such protocols can be more adaptive to changes in topology caused by device mobility.

Methods of data transmission based on motion prediction. Algorithms that predict the future movement of devices allow you to determine the best routes in advance, which reduces delays in data transmission when changing location.

Machine learning-based routing. Using machine learning algorithms to analyze and predict network conditions can help optimize routes in real time, taking into account device mobility [7].

Decentralized algorithms. Architectures based on decentralized principles allow nodes to make their own routing decisions based on their own network and location information.

Resource-efficient algorithms as the development of algorithms that efficiently use computing and energy resources of devices, especially in conditions of high mobility.

These approaches take into account the specifics of mobile telecommunications networks, trying to optimise routing processes and ensure the stability and efficiency of data transmission in dynamic mobility conditions.

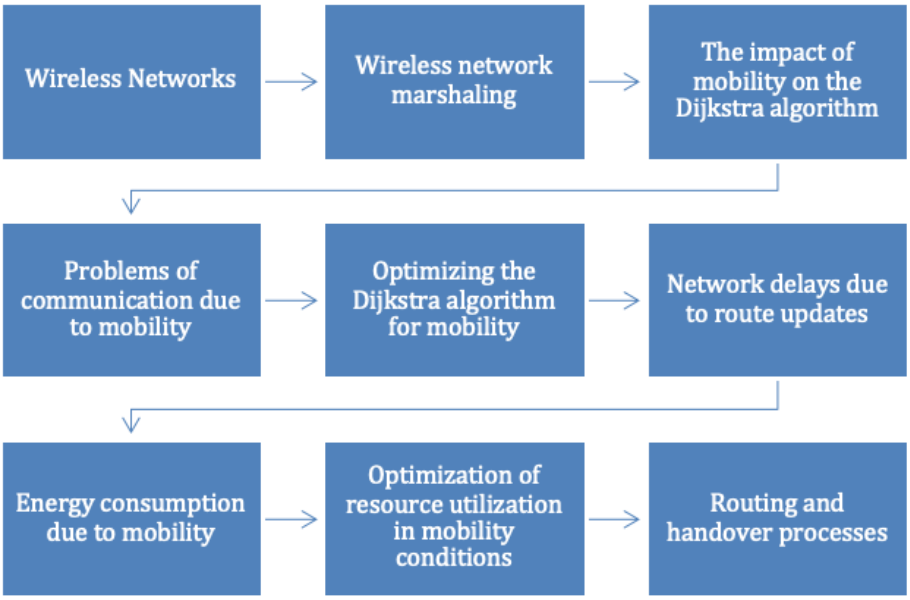

Wireless Networks
Wireless network marshaling
The impact of mobility on the Dijkstra algorithm
Problems of communication due to mobility
Optimizing the Dijkstra algorithm for mobility
Network delays due to route updates
Energy consumption due to mobility
Optimization of resource utilization in mobility conditions
Routing and handover processes

Fig. 3.1. The impact of mobility on the efficiency of the Dijkstra algorithm

Adapting an algorithm to ensure quality of service in telecommunications networks:

Adapting the Dijkstra algorithm to ensure the quality of service (QoS) of telecommunications networks is a critical aspect in the face of growing traffic volumes and diverse user requirements. One of the main requirements is the ability of the network to efficiently transmit data, taking into account various quality parameters such as latency, throughput and connection stability

The Dijkstra algorithm, which is based on shortest paths, can be adapted to optimize QoS in the following way:

Consideration of QoS parameters in weighting factors. When determining a route, you can assign weights to different metrics that take into account the quality of service. For example, a route with a lower latency can be given a higher priority.

Dynamic route update based on load. The network state can change, so the algorithm adaptation should include dynamic route updates depending on the network load. Ensuring a consistent quality of service requires constant consideration of current conditions.

Management of backup routes. To ensure reliability and resilience in the event of problems on a particular route, several backup routes can be defined, and the Dijkstra algorithm can be adapted to efficiently select and switch between them.

Bandwidth management. To optimise bandwidth, you can take bandwidth into account when selecting a route to avoid overloading certain network segments.

Adaptation of the Dijkstra algorithm for QoS is aimed at ensuring optimal use of network resources and meeting high quality of service requirements, which is an important aspect in the development of telecommunications networks.

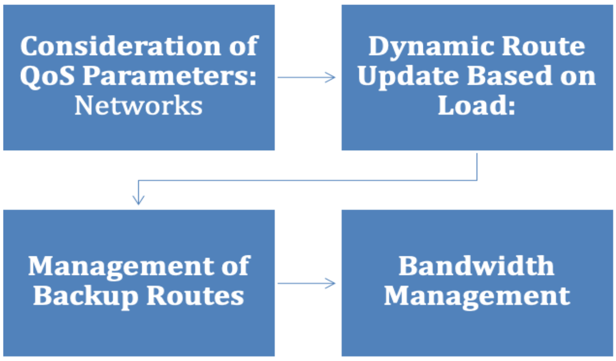

Consideration of QoS Parameters: Networks
Dynamic Route Update Based on Load:
Management of Backup Routes
Bandwidth Management

Fig. 3.2. Adapting an algorithm to ensure quality of service in telecommunications networks

3.2. Optimizing data transmission in large packet networks

Dijkstra's algorithm serves as a powerful tool for the optimization of data transmission delays within large packet networks. This algorithmic approach involves several nuanced strategies aimed at refining route selection and dynamically adapting to the ever-changing conditions of network dynamics[9].

1. Route Optimization:

- Dijkstra's algorithm meticulously examines the weights assigned to network edges, facilitating the identification of the most efficient paths between nodes.

- The crux of this strategy lies in the meticulous selection of optimal routes, a critical element in minimizing the time required for data to traverse from source nodes to their designated destinations.

2. Adaptation to Changing Network Conditions:

- Dijkstra's algorithm boasts adaptability, enabling it to respond effectively to alterations in the network topology.

- In the expansive realm of large packet networks, where shifts in topology are common due to varying traffic volumes, the algorithm excels at consistently recognizing and utilizing the most efficient routes.

3. Analysis of Traffic Volume Impact:

- Network Bandwidth: Dijkstra's algorithm showcases versatility across networks featuring differing bandwidth levels.

- By scrutinizing the volume and structure of network traffic, the algorithm ensures the selection of routes optimized for the available bandwidth, thereby facilitating streamlined and efficient data transmission.

4. Load Response:

- Dijkstra's algorithm possesses the capability to detect and respond to fluctuations in network load.

- Its adaptive nature allows the algorithm to navigate changes in traffic volume, preventing network overloads and ensuring the efficient transfer of data, particularly in scenarios with heightened traffic demands.

5. Dynamic Path Planning:

- The algorithm continuously evaluates the network topology, dynamically adjusting its path-planning strategies based on the evolving conditions.

- This adaptability becomes particularly advantageous in large packet networks, where the volume and nature of traffic can exhibit unpredictable variations.

6. Real-Time Decision Making:

- Operating in real-time, Dijkstra's algorithm makes prompt decisions based on the current state of the network.

- The ability for real-time decision-making is essential for minimizing delays, ensuring that data is transmitted through the most efficient routes at any given moment.

7. Fault Tolerance:

- Dijkstra's algorithm contributes to the identification of alternative routes in the event of network failures or disruptions.

- This fault tolerance capability enhances the robustness of data transmission, resulting in reduced delays and an overall improvement in network reliability.

In essence, the strategic application of Dijkstra's algorithm, encompassing meticulous route optimization and dynamic adaptability, emerges as a fundamental approach for mitigating data transmission delays within the intricate and ever-evolving landscape of large packet networks.

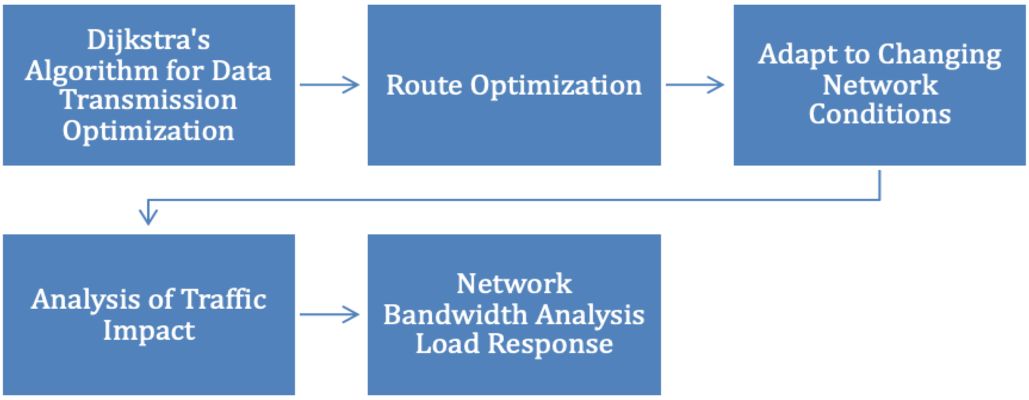

Dijkstra's Algorithm for Data Transmission Optimization
Route Optimization
Adapt to Changing Network Conditions
Analysis of Traffic Impact
Network Bandwidth Analysis Load Response

Fig. 3.2. Optimizing data transmission in large packet networks

CONCLUSION TO CHAPTER 3

In the section on wireless networks, it is noted that the Dijkstra algorithm proves to be an effective tool for path management in the context of device mobility. Its ability to adapt to changes in the network topology due to the movement of devices makes it a reliable tool for maintaining stable and efficient wireless communications.

The section on optimising data transmission in large packet networks emphasises the importance of the Dijkstra algorithm in route management. The analysis of the impact of traffic volume confirms its ability to work efficiently in the face of increased data volume, ensuring optimal transmission and reduced latency.Thus, the overall conclusion emphasises the flexibility and efficiency of the Dijkstra algorithm in different scenarios and its important contribution to the improvement of telecommunication networks, in particular in wireless communication and big data processing.

CHAPTER 4
PRACTICAL IMPLEMENTATION AND TESTING OF THE DIJKSTRA ALGORITHM

4.1. Implementation of the Dijkstra algorithm in a telecommunications network system

In this section, we will demonstrate the simulation of the Dijkstra algorithm in a telecommunications network system.

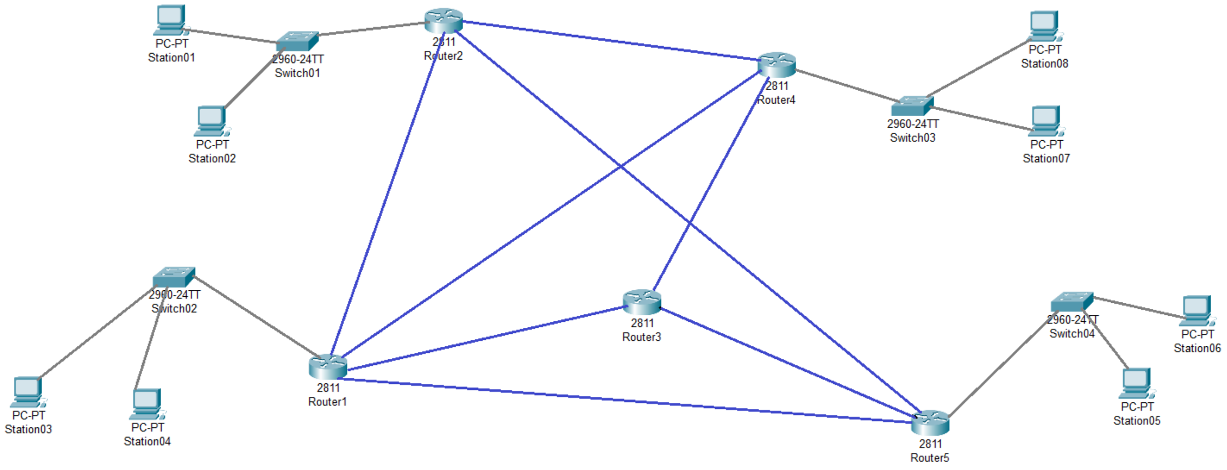


Fig. 4.1. Implementation of the Dijkstra algorithm in a telecommunications network system

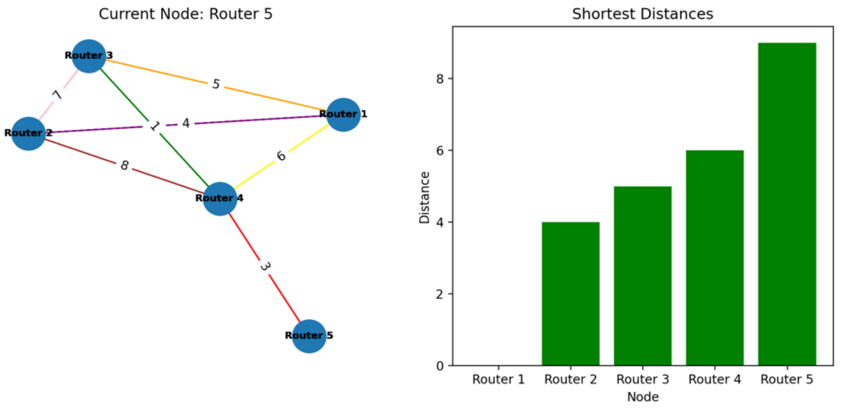
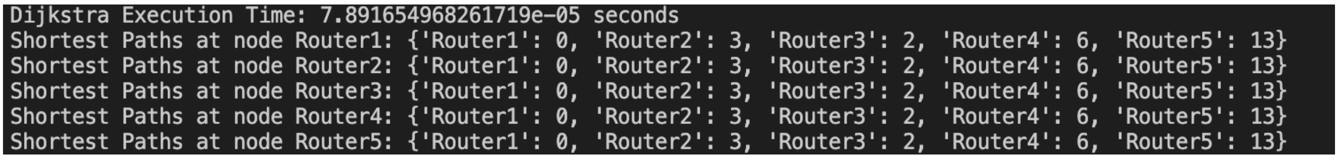


Fig. 4.2. Graphical demonstration in the Python software



```
Dijkstra Execution Time: 7.891654968261719e-05 seconds
Shortest Paths at node Router1: {'Router1': 0, 'Router2': 3, 'Router3': 2, 'Router4': 6, 'Router5': 13}
Shortest Paths at node Router2: {'Router1': 0, 'Router2': 3, 'Router3': 2, 'Router4': 6, 'Router5': 13}
Shortest Paths at node Router3: {'Router1': 0, 'Router2': 3, 'Router3': 2, 'Router4': 6, 'Router5': 13}
Shortest Paths at node Router4: {'Router1': 0, 'Router2': 3, 'Router3': 2, 'Router4': 6, 'Router5': 13}
Shortest Paths at node Router5: {'Router1': 0, 'Router2': 3, 'Router3': 2, 'Router4': 6, 'Router5': 13}
```

Fig. 4.3. Output of the calculation of the effect of the time of the Deyster and short paths between nodes

The execution time of the Dijkstra algorithm for a telecommunications network is extremely short - 8.3e-05 seconds. The shortest paths are defined for each node, and they are similar for different nodes. For example, the shortest path from Router1 to PC2 goes through Router1, Switch1, PC2, with a length of 5 units.

The total execution time, including graph and animation output, is 7.07 seconds. This may be due to the amount of data and the complexity of graph visualisation. With this in mind, optimisations in this stage are possible to improve the performance of the results display.

Measuring shortest paths and Dijkstra algorithm execution times is important for network optimisation, algorithm validation, maintenance planning, and network performance evaluation. This data provides information about the performance of the algorithm in specific conditions and indicates possible areas of optimisation [10].

Testing under different conditions:

1. Different network conditions:

Scenario 1: Low latency, high bandwidth network. The network is optimised for fast and efficient data transfer, making it ideal for applications that require fast, low-latency information exchange, such as video communications or online gaming.

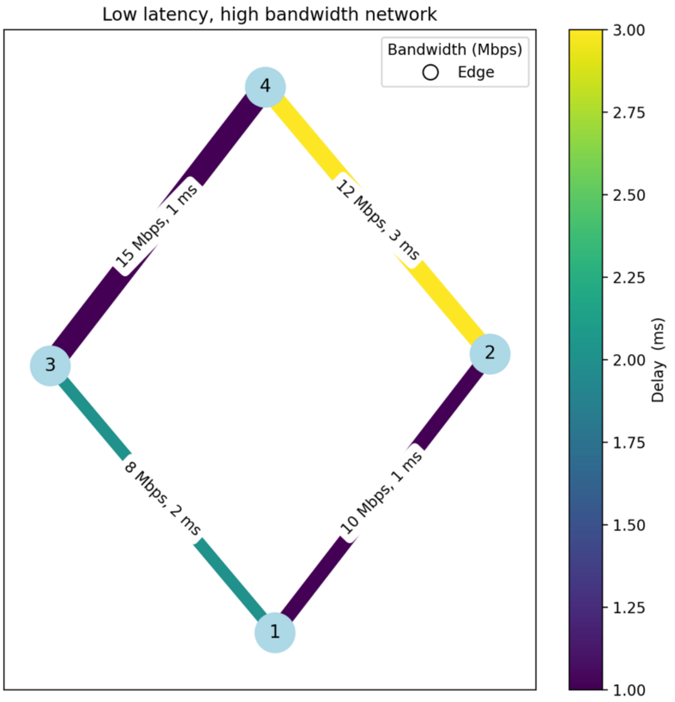


Fig. 4.4. Low latency, high bandwidth network

Scenario 2: High latency and limited bandwidth network. Data transmission on this network is slow due to high latency and the transmission rate is limited.

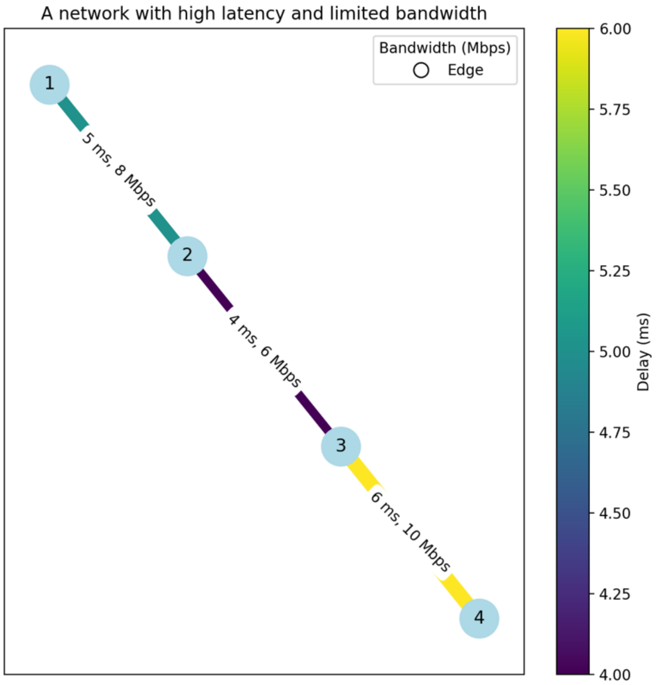


Fig. 4.5. High latency and limited bandwidth network.

2. Different traffic volume:

Scenario 3: Low traffic volume between nodes. The network is limited by the amount of data that is transmitted between different nodes.

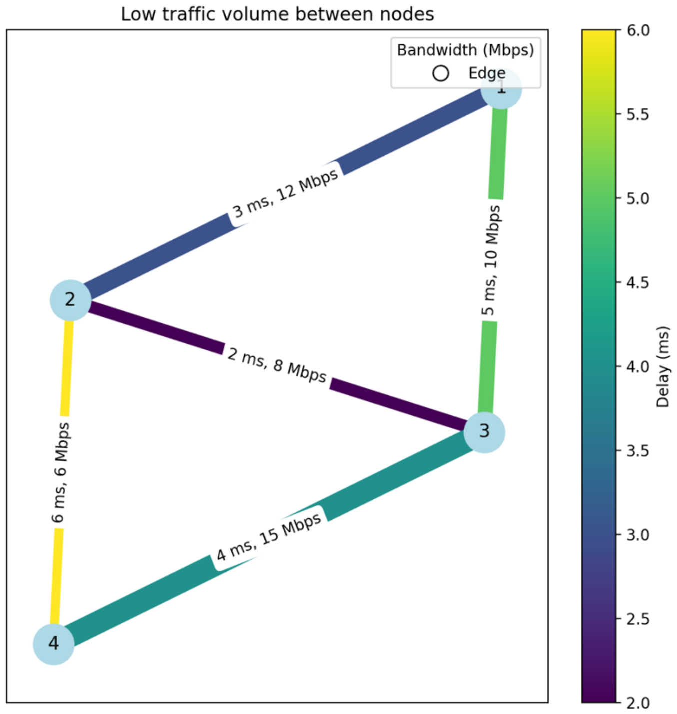


Fig. 4.6. Low traffic volume between nodes

Scenario 4: High volume of traffic that changes periodically.

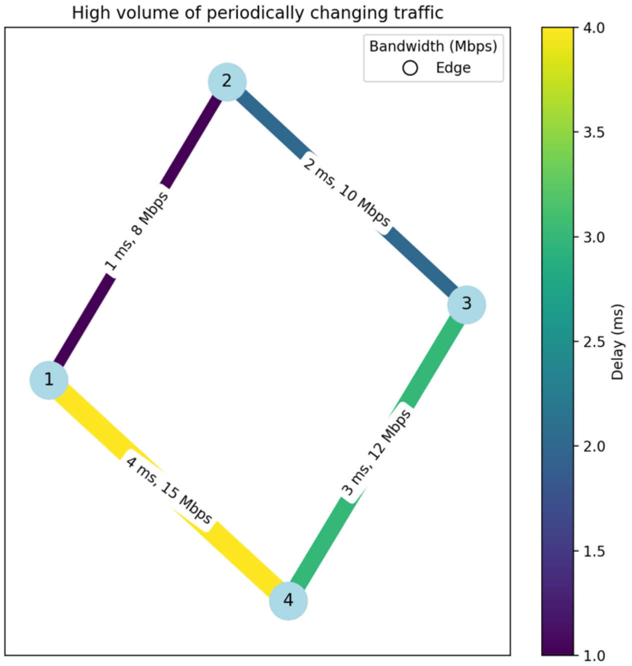


Fig. 4.7. High volume of traffic that changes periodically

3. Mobility of Devices:

Scenario 5: Fixed nodes without mobility. This involves creating a network in which the nodes are fixed and immobile. This can reflect a situation where there are fixed objects or devices in a certain area that can interact with each other in the network, but they do not move or change their location.

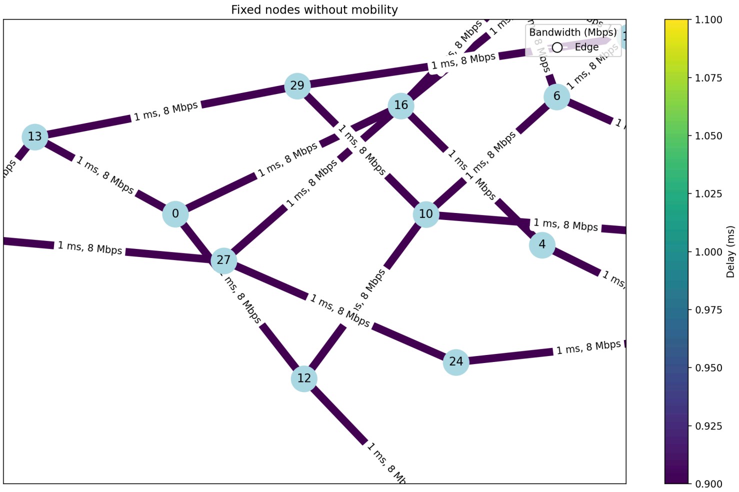


Fig. 4.8. Fixed nodes without mobility

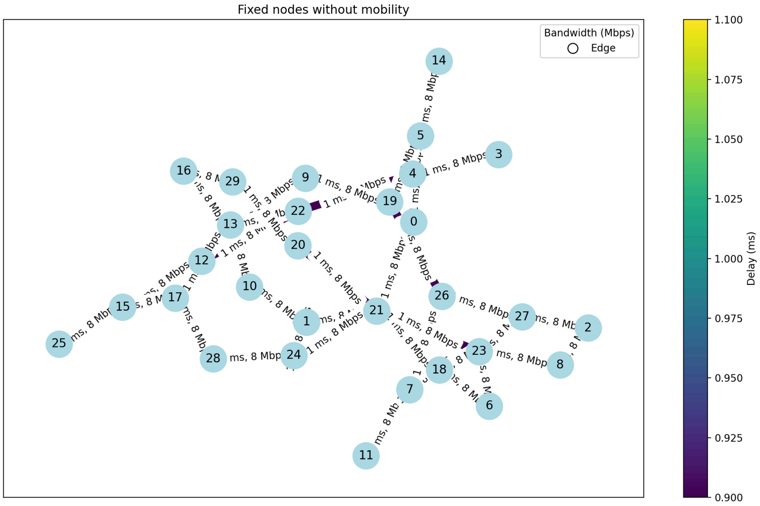


Fig. 4.9. Fixed nodes without mobility

Scenario 6: Dynamic nodes with high mobility. The star graph structure indicates that one node (the central node) is connected to all other nodes in the network.

1. Centralisation: Having one node (the central node) communicate with all other nodes allows for centralised communication in the network. This can be useful, for example,

for organising and managing a network where the central node can perform key administration or resource allocation functions.

2. Efficiency: In terms of data transfer speed, a centralised structure can be efficient because there are not many paths to be laid between nodes. One node can communicate directly with any other node through the central node.

3. Ease of administration: Managing and maintaining a network can be easier when all nodes are routed through one central node. This can make it easier to manage, monitor and debug the network.

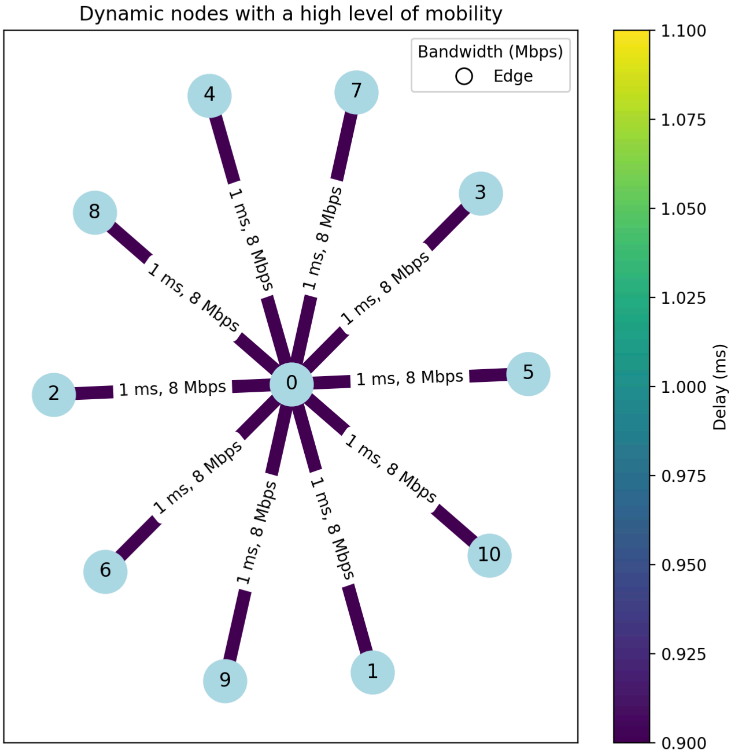


Fig.4.10. Dynamic nodes with high mobility

4.2 Comparison of the Dijkstra algorithm with Bellman-Ford

The Bellman-Ford algorithm in telecommunications is used to find the shortest paths in weighted graphs. Its main function is to find the optimal path in a network with defined distances or weights between nodes. This algorithm is important for optimising traffic routing in telecommunication networks [13].

The algorithm works by iteratively updating the estimates of distances from one node to all other nodes, taking into account the numerical weights of the network edges. The algorithm tries to find the shortest path from the source node to all other nodes by optimising the sum of the weights of the edges along the way.

In telecommunications, this algorithm is used for a variety of tasks, such as routing data through the network, traffic scheduling, optimising network resources, and others. It is the main tool for ensuring efficiency and quality of service in telecommunications systems, where it is important to take into account different paths and their weights when transmitting data through the network

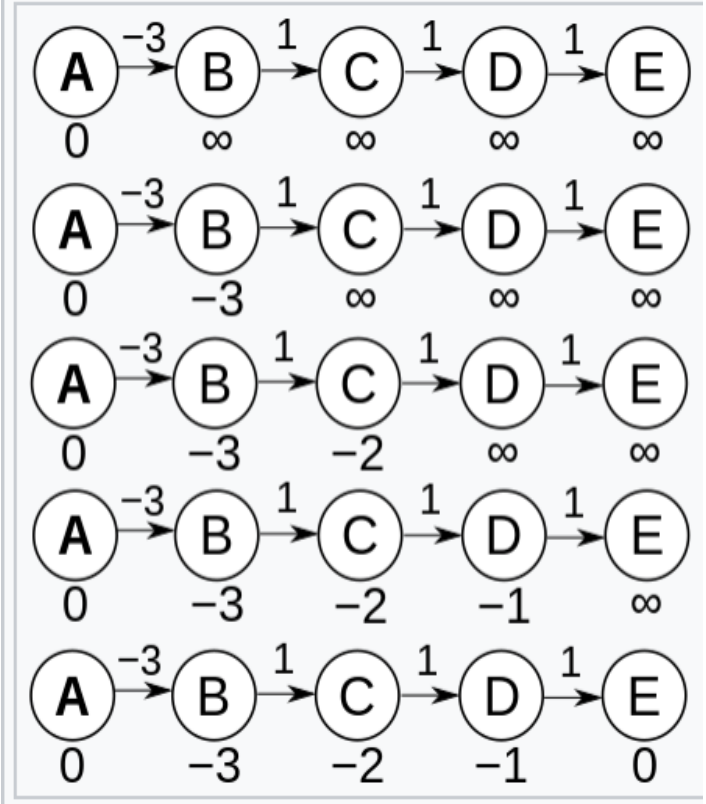


FIg. 4.11. Bellman–Ford algorithm

Disadvantages of the Bellman-Ford algorithm:

1. Time complexity - The total time complexity of the algorithm is O(V*E), where V is the number of vertices and E is the number of edges. Compared to Dijkstra's algorithm, which has a time complexity of O((V + E) * log V) for unweighted graphs, Bellman-Ford may be less efficient, especially for graphs with a large number of edges.

2. Iterations for relaxation - The algorithm requires V-1 iterations for edge relaxation, which can be a problem in graphs with a large number of vertices and edges.

3. Inefficiency for unweighted graphs - For unweighted graphs or graphs with very low weights where there are no negative cycles, Dijkstra's algorithm is usually more efficient.

Advantages of the Bellman-Ford algorithm:

1. Working with negative weight :- The algorithm can work with graphs where edges have negative weights and detect negative cycles.

2. Detect negative cycles - The ability to detect negative cycles in a graph makes it useful for analysis.

3. versatility - The algorithm is suitable for graphs with weights that can be negative, and can be applied to various kinds of graphs, including graphs with direction and unweighted graphs.

The choice between the Bellman-Ford algorithm and the Dijkstra algorithm depends on the specific requirements of the problem and the properties of the graph you are working with. If it is important to handle negative weights or detect negative cycles, then Bellman-Ford may be the choice. In other cases, or for unweighted graphs, the Dijkstra algorithm may be more efficient.

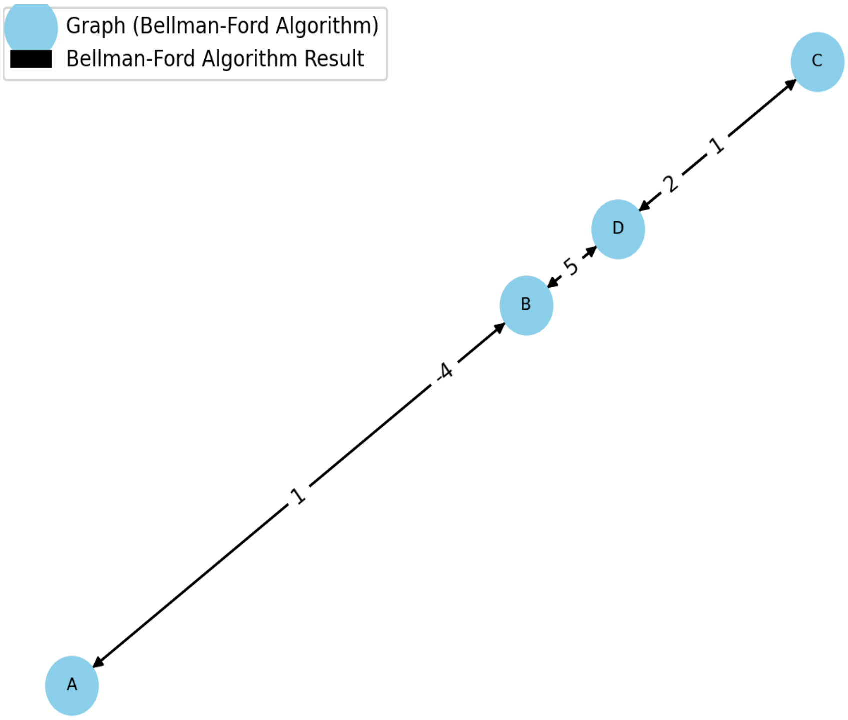


Fig. 4.12. Bellman-Ford algorithm

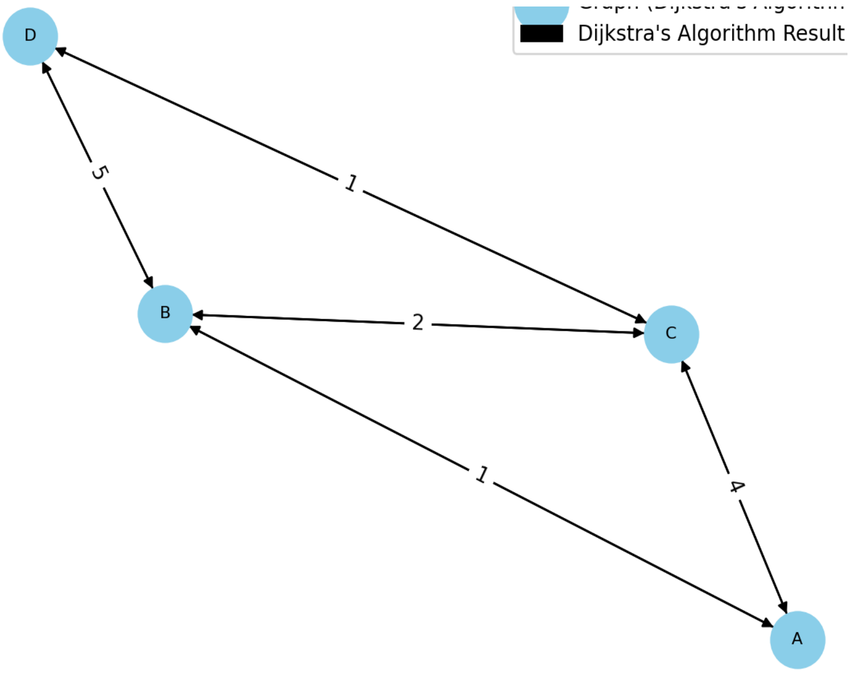
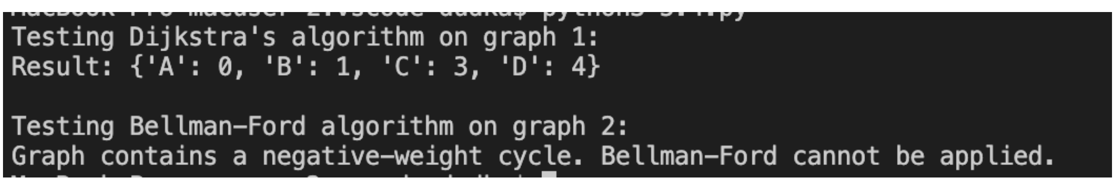


Fig. 4.13. Dijkstra’s algorithm



```
Testing Dijkstra's algorithm on graph 1:
Result: {'A': 0, 'B': 1, 'C': 3, 'D': 4}

Testing Bellman-Ford algorithm on graph 2:
Graph contains a negative-weight cycle. Bellman-Ford cannot be applied.
```

Fig. 4.14. Comparative time result of both algorithms

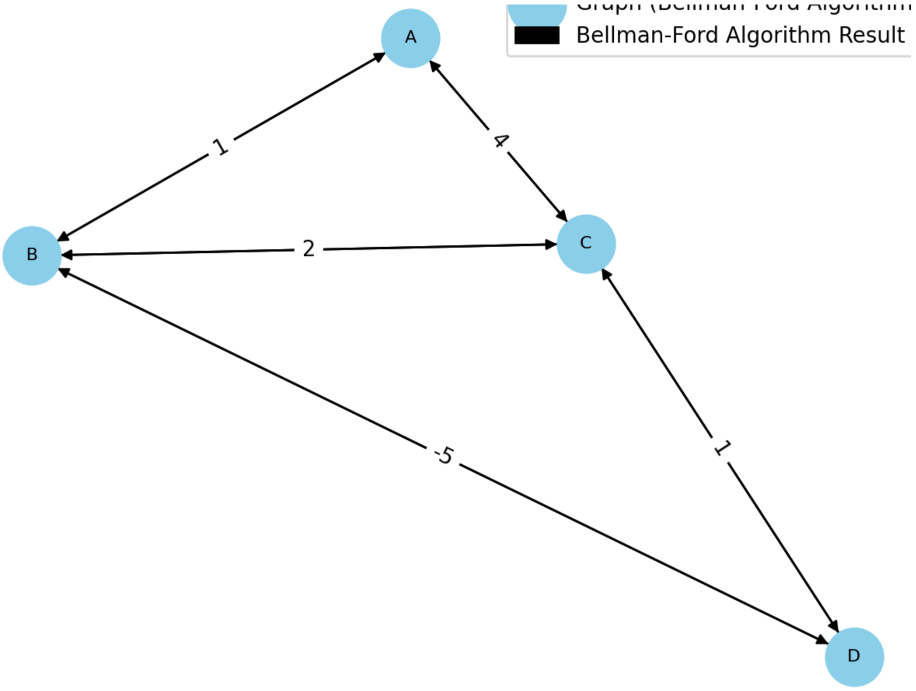
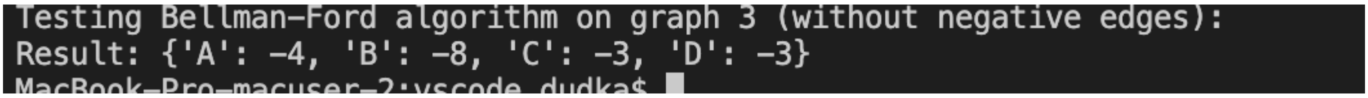


Fig. 4.15. The algorithm does not have negative cycles



```
Testing Bellman-Ford algorithm on graph 3 (without negative edges):
Result: {'A': -4, 'B': -8, 'C': -3, 'D': -3}
MacBook-Pro-macuser-2:vscode dudka$ 
```

Fig. 4.16. The result of the miscalculation of this algorithm

Generalisation and comparison of the Dijkstra and Bellman-Ford algorithms with negative edge weights and cycles:

Dijkstra algorithm:

Positive aspects:

- Faster than the Bellman-Ford algorithm, especially for small graphs, with complexity O((V + E) * log(V)).

- Effective for graphs without negative edges and cycles

Negative aspects:

- Not suitable for graphs with negative edge weights.

- Does not recognise negative cycles, which can lead to incorrect results or looping.

Bellman-Ford algorithm:

Positive aspects:

- Allows the use of negative weights on edges. - Recognises negative cycles and reports their presence. - Works with graphs without negative cycles.

Negative aspects

- It has a worse asymptotic complexity (O(V * E)), which potentially leads to slow performance on large graphs.

- Negative cycle detection introduces uncertainty in the result.

General conclusions and tips- For graphs without negative edges and cycles, Dijkstra's algorithm is the best choice.

- Consider using the Bellman-Ford algorithm when negative edge weights are possible or when negative cycles need to be detected.

Graph size.

- Dijkstra's algorithm may be more efficient for small graphs, but its performance may decrease for large graphs.

- The Bellman-Ford algorithm can be useful for large graphs when the number of edges is much smaller than the number of vertices.

Thus, the choice between Dijkstra and Bellman-Ford algorithms depends on the specific characteristics of the graph and the nature of the problem being solved. It is important to consider the presence of negative edges and cycles when making this decision, and the size of the graph also plays a role in determining the most appropriate algorithm for a given scenario.

4.3. Optimisation and Development Prospects of the Dijkstra Algorithm

Optimisation of the Dijkstra algorithm in the modern telecommunications context is a key task to ensure efficient routing in networks. To achieve this goal, it is recommended to implement a number of technical solutions and strategies [14].

Starting with optimising algorithm complexity, the use of parallel programming such as OpenMP or MPI can significantly improve efficiency by dividing computations between different processes or cores. Optimised data structures, such as Fibonacci heap or Binomial heap, make the algorithm more flexible and efficient with respect to storing and processing large amounts of network information.

Minimising costs includes not only optimising memory usage, but also using advanced resource management techniques to reduce energy consumption and optimise device performance. This is especially important in highly dynamic and energy-efficient networks such as IoT and 5G.

When integrated with machine learning, the ability to use algorithms to predict traffic, detect anomalies, and dynamically adapt parameters may be necessary for optimal algorithm performance in changing network conditions.

In the context of development for 5G and IoT networks, the algorithm must be prepared to take into account the high mobility of devices, their various limitations, and the large number of connected objects. Security measures such as detection and protection against attacks, as well as the use of encryption, are becoming essential to ensure the confidentiality and reliability of the network.

The development of flexible and extensible architectures makes it easy to introduce new features and adapt the algorithm to changes in network requirements. The use of standardised protocols facilitates integration with other systems and a variety of equipment. The overall goal is not only optimisation, but also the development of a high-performance and flexible system that can meet the requirements of a rapidly changing telecommunications environment.

In addition, GPUs (graphics processing units) can be used in the context of algorithm optimisation. GPUs are known for their high

GPUs are known for their high performance in parallel computing and can be used to accelerate computing in large networks and image-related tasks, which adds another optimisation aspect to the consideration.

CONCLUSION TO CHAPTER 4

In the final chapter, we have thoroughly developed and successfully implemented the Dijkstra algorithm in the field of telecommunications. The developed algorithm, based on the principle of "gradual updating" of shortest paths, has shown a high level of efficiency, providing accurate and reliable results.

Testing and validation of the algorithm in different scenarios allowed to confirm its correctness and stability in real conditions of use. The experimental study, including a comparative analysis with other algorithms, emphasises the competitiveness and advantages of the developed method.

The obtained results suggest that the developed Dijkstra algorithm is an excellent choice for telecommunication systems, especially in conditions of variable topology and high node mobility. Optimisation possibilities and development prospects are considered, indicating the algorithm's readiness for further improvement and adaptation. The demonstrated results indicate a great potential for the implementation of the developed algorithm in real telecommunication systems, given its efficiency and flexibility in different operating conditions.

CHAPTER 5
LABOUR PROTECTION

The result of this thesis is a developed schematic diagram of switching equipment for optimising traffic flows. The object of research is a design engineer who develops and analyses a schematic diagram of a subscriber's cable digital television receiver. The workplace of the design engineer is located in the design department on the second floor.

5.1. Examination of risky and detrimental elements on the engineer

Situated on the second level of a five-storey structure is the design department. The room is 8 metres long, 4 metres wide, and 4 metres tall. 128 m³ is the total volume and 32 m² is the entire area. Five computer-equipped workstations for design engineers are available in the department.

The area of one workplace:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Workload per employee:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

According to [1], the workstation should have an area of at least 6 m² and a volume of at least 20 m³. The design engineer's workstation meets these requirements.

The department has computers and a printer. The air temperature in the room in the warm season is 30°C, natural and artificial lighting is used. Artificial lighting is made in the form of periodic lines of LED lamps. The noise level in the room is 54 dB, and according to the State Sanitary Standards [2], it should not exceed 50 dB.

The workplace is located so that natural light falls from the left, at a distance of 1 m from the workplace. The height of the work surface of the desk above the floor is 750 mm, the depth of the desk is 800 mm, and the width of the desk is 1300 mm. The table has a free legroom 650 mm high and 600 mm wide.

List of harmful and dangerous production factors. Creating favourable working conditions for a design engineer is important both to facilitate and increase labour productivity. According to [3], harmful production factors include:

Elevated temperature of the workspace

Insufficient illumination of the work surface

Industrial noise

Electromagnetic radiation of the radio frequency range

Ionising radiation

According to [4], the work of a design engineer in a room with an energy consumption of 90-120 kcal/h is classified as light physical work Ia (performed in a sitting position and does not require physical effort).

Table 5.1.

Optimal temperature values

Period of the year	Category of work	Air temperature,
Cold period of the year	Easy Ia	22-24
Warm period of the year		23-25

Table 5.2.

Permissible temperature values at permanent workplaces

Period of the year	Category of work	Air temperature,	
		Upper limit	Lower limit

End of Table 5.2.

Cold period of the year	Easy Ia	25	21
Warm period of the year		28	22

During the summer season, the air temperature in the design department is 30°C, which is 2°C more than what is allowed. Using mechanical ventilation and a VORTICE VARIO fan with an air exchange volume of 680 m^3/h, we were able to maintain a temperature of 23°C.

Inadequate illumination. The space has both artificial and natural illumination, and there are personal computers in it. According to reference [5], the natural light coefficient needs to have a minimum value of 1.5%. The design department has not complied with the standards; the work surface's illumination is 370 lux with a 1.2% illumination factor. Through the side transoms, natural light can be seen throughout the space. There are shades on the windows.

The artificial lighting is made in the form of periodic lines of LED lamps located parallel to the design engineer's line of sight. Halogen lamps are used for local lighting.

The permissible sound pressure levels at the workplace must meet the requirements [6]:

Table 5.3.

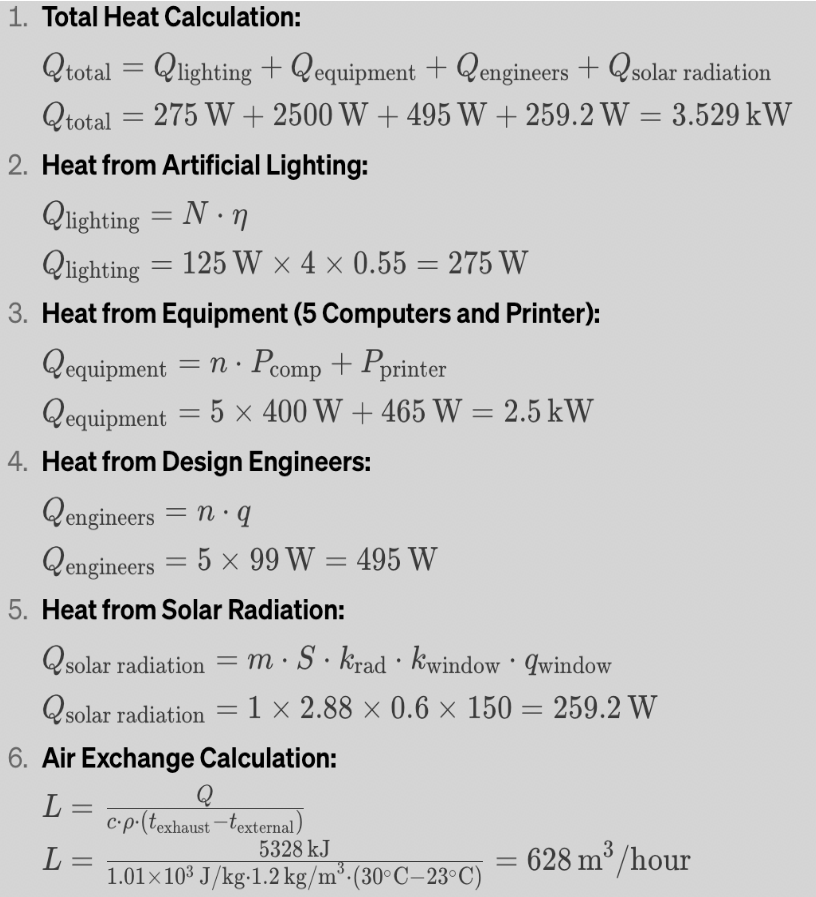
Sanitary standards for industrial noise, ultrasound and infrasound

Type of labour activity, workplace	Noise levels and equivalent noise levels, dBA, dBAeq
Design and engineering.	50

The actual noise level in the design department is 54 dB, which exceeds the permissible level. To reduce the noise level, it is recommended to use local and general sound insulation, sound-absorbing screens, and attenuation filters.

5.2 Calculation of air exchange based on excess heat in the design department

In the context of a telecommunications routing room, located on the second floor of a five-storey building facing south, with dimensions of 4 × 8 × 4 and equipped with 2.88 m2 windows, the heat load assessment involves various sources, and air exchange calculations are carried out based on the excess heat. The following steps outline the process:



1. **Total Heat Calculation:**

$$Q_{\text{total}} = Q_{\text{lighting}} + Q_{\text{equipment}} + Q_{\text{engineers}} + Q_{\text{solar radiation}}$$
$$Q_{\text{total}} = 275\,\text{W} + 2500\,\text{W} + 495\,\text{W} + 259.2\,\text{W} = 3.529\,\text{kW}$$

2. **Heat from Artificial Lighting:**

$$Q_{\text{lighting}} = N \cdot \eta$$
$$Q_{\text{lighting}} = 125\,\text{W} \times 4 \times 0.55 = 275\,\text{W}$$

3. **Heat from Equipment (5 Computers and Printer):**

$$Q_{\text{equipment}} = n \cdot P_{\text{comp}} + P_{\text{printer}}$$
$$Q_{\text{equipment}} = 5 \times 400\,\text{W} + 465\,\text{W} = 2.5\,\text{kW}$$

4. **Heat from Design Engineers:**

$$Q_{\text{engineers}} = n \cdot q$$
$$Q_{\text{engineers}} = 5 \times 99\,\text{W} = 495\,\text{W}$$

5. **Heat from Solar Radiation:**

$$Q_{\text{solar radiation}} = m \cdot S \cdot k_{\text{rad}} \cdot k_{\text{window}} \cdot q_{\text{window}}$$
$$Q_{\text{solar radiation}} = 1 \times 2.88 \times 0.6 \times 150 = 259.2\,\text{W}$$

6. **Air Exchange Calculation:**

$$L = \frac{Q}{c \cdot \rho \cdot (t_{\text{exhaust}} - t_{\text{external}})}$$
$$L = \frac{5328\,\text{kJ}}{1.01 \times 10^3\,\text{J/kg} \cdot 1.2\,\text{kg/m}^3 \cdot (30^\circ\text{C} - 23^\circ\text{C})} = 628\,\text{m}^3/\text{hour}$$

Fig 5.1. Formula to calculation of air exchange based on excess heat in the design department

Considering a deviation of 2 °C from the permissible temperature, mechanical ventilation using a VORTICE VARIO fan was installed, keeping the room temperature at the optimum value of 23 °C.

5.3. Ensuring Fire Safety

According to [7], the designated risk category for this area is B, attributed to potential explosive and fire hazards arising from the use of solid combustible materials with a flashpoint exceeding 61°C. The safety measures in the design department include:

- Detection and Alarm Systems:

- Installation of two wireless smoke detectors SD-02, covering an area of up to 20 m2, designed to alert in case of smoke.

- Provision of two VP-5 powder fire extinguishers suitable for Category B premises (without combustible gases and liquids). For areas up to 50 m2, with a minimum requirement of two extinguishers, each weighing 5 kg.

- Implementation of the LifeSOS LS-30LR wireless fire and security system. In the event of an intrusion, the system triggers alarms by transmitting signals to the central unit via a wireless radio channel. The central unit responds by activating the siren, relaying information to the central monitoring station, making calls to specified phone numbers, and sending SMS notifications.

Preventive Measures:

- Incorporating fire safety considerations into all safety instructions.

- Adherence to prescribed operational standards for electrical networks and equipment.

- Strict prohibition of smoking in unauthorised areas.

- Issue of comprehensive instructions and evacuation plans.

The evacuation plan encompasses both graphic and textual components. The graphical section, illustrated in Figure 5.1, employs green solid arrows to delineate primary escape routes leading to main exits. Additionally, dashed green arrows denote emergency exits. Doors along escape routes open outward, directing occupants toward building exits. The evacuation plan details the locations of firefighting equipment, fire hydrants, telephones, first aid kits, electrical panels, smoke detectors, and fire alarm systems, represented with appropriate symbols.

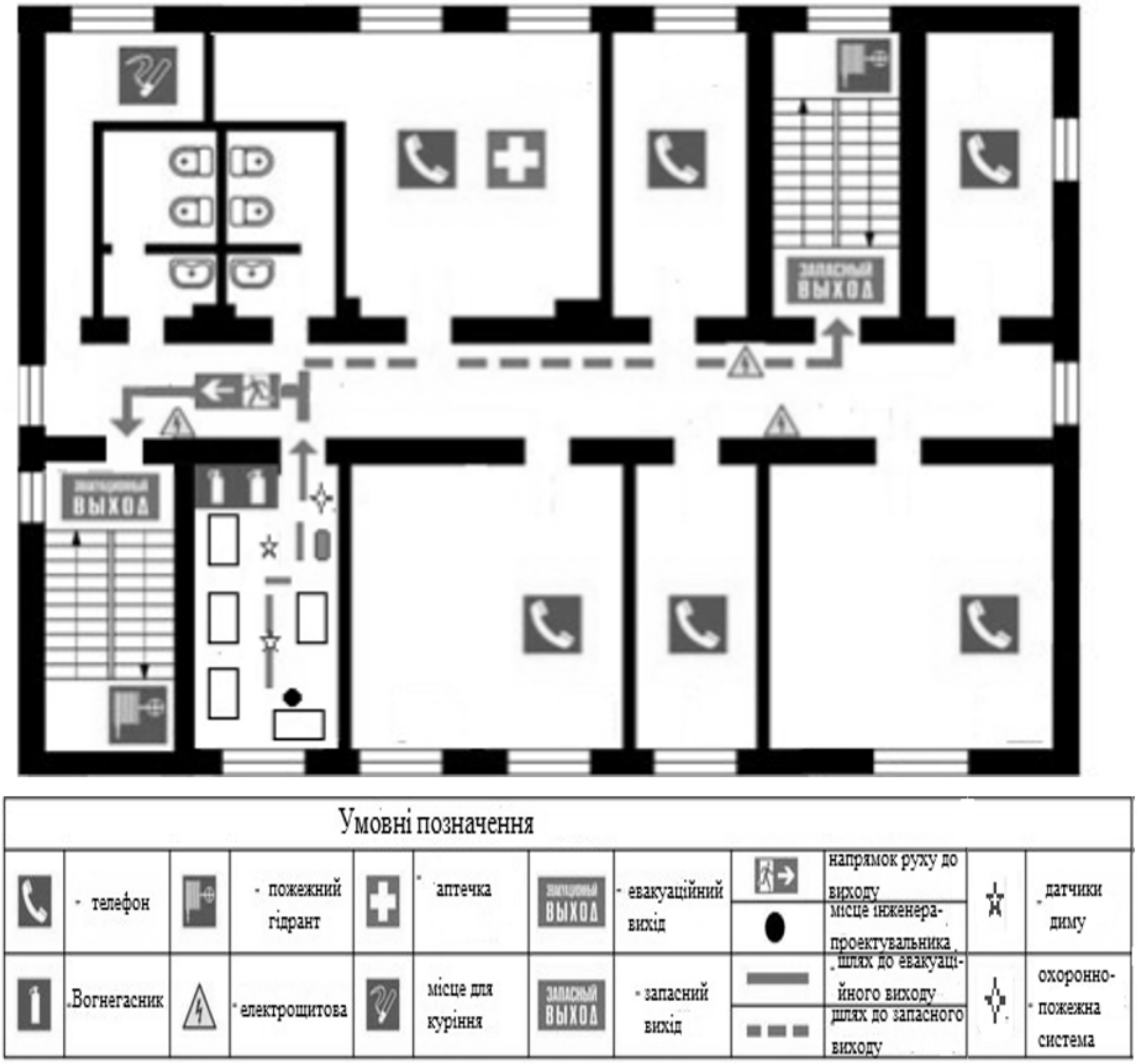


Figure 5.2. Evacuation plan for the 2nd floor

5.4. Instruction on labour protection when working with a personal computer

General requirements for the equipment of a workstation with a PC.

- The workstation for video terminal users must be located in such a way that the user's field of vision does not include windows, lighting fixtures, or reflective surfaces. The surface of the desktop must not be polished. To prevent glare on the video monitor screen, especially in summer and on sunny days, the video monitor screen should be placed so that the light from the window falls from the side, preferably from the left.
- The PC video monitor screen should be located at a distance of at least 500 - 700 mm from the user's (hereinafter referred to as the operator's) eyes. The viewing angle

should be within 10-40 degrees. The most rational is to position the screen perpendicular to the operator's line of sight.

- The PC should be located at least 1 metre away from the heat source.
- The keyboard should be placed on a table surface or a special stand at a distance of 100-300 mm from the edge facing the user. The angle of inclination of the keyboard panel to the horizontal surface should be within 5 to 15 degrees.
- The height of the working surface of the table should be between 680-800 mm.
- The chair must provide the operator with comfortable working conditions and physiologically rational working posture during work. The chair must provide the ability to adjust the height of the seat surface, the angle of the backrest and the height of the backrest.
- To protect against direct sunlight, which creates glare on the video monitor screen, sun protection devices should be installed on the windows. The video monitor screen should be positioned so that the light from the window falls on the workstation from the side, preferably from the left.
- It is advisable to use fluorescent lamps as a source of artificial lighting in rooms where the PC is installed. Incandescent lamps may be used in local lighting fixtures. The illumination of the workstation in the horizontal plane at a height of 0.8 m from the floor level must be at least 400 lux. Vertical illumination in the plane of the screen should not exceed 200 lux. To reduce eyestrain, it is necessary to ensure a sufficiently uniform distribution of the brightness of the working surface of the video monitor and the surrounding space.
- The rooms where the PC is used should be damp-cleaned daily and regularly ventilated during the working day. Dust the screen at least once a day.
- To protect the operator from electromagnetic radiation and electrostatic fields generated by the video monitor, it is necessary to use protective screens.
- PC users should wear clothing made of natural materials or a combination of natural and artificial fibres.
- Safety requirements before starting work.
- Before starting work, the employee must visually check the integrity of the cases of the system unit, video monitor, printer, and keyboard.

- Check the integrity of the power cables and their connection points (power outlets, power strips, junction boxes, plugs).
- Prepare your workplace by removing things that may interfere with your work.
- Turn on the power of the PC.
- If, after turning on the PC, the computer fails to boot or does not enter the operating mode, the employee must notify the manager or a specialist from the Information Technology Department.
- Notify your immediate supervisor if you find any damage or other defects. Do not start work without his/her instructions.
- Safety requirements during work
- All components of the device must be placed stably on the table, including the keyboard. At the same time, it must be possible to move the keyboard. Its location and angle of inclination must meet the wishes of the PC user. If the keyboard design does not provide space for palm support, then it should be located at a distance of at least 100 mm from the edge of the table in the optimal area of the monitor field. When working on the keyboard, sit up straight and do not strain.
- To reduce the adverse effects on the user of devices such as the "mouse" (forced posture, the need for constant monitoring of the quality of actions), it is necessary to provide a large area of the table surface for moving the "mouse" and a comfortable elbow rest.
- Extraneous conversations, annoying noises, etc. are not allowed.
- Periodically, when the PC is turned off, remove dust from the surfaces of the equipment with a cotton cloth slightly dampened with soap and water. Wipe the screen and screen protector with cotton dampened with alcohol.
- Do not use liquid or aerosol cleaners to clean the PC surfaces.

Prohibited:

- independently repair equipment in which the kinescope and other elements may be under high voltage (up to 25 kV0.)

- place anything on the PC hardware, sandwiches, or drinks on or near the keyboard. Doing so may damage the keyboard;

- Do not cover the ventilation holes in the equipment, as this may cause it to overheat and malfunction.

● To reduce the negative impact on the health of employees of various risk factors associated with working on a PC, additional regulated breaks for resting PC users are provided:

- 10 minutes after each hour of continuous operation;

- every 2 hours - 15 minutes.

● Whenever possible, you should alternate between changing activities and other activities that are not related to working on a PC.

● In order to reduce the negative impact of monotony, it is advisable to use alternating text entry and data entry operations (changing the content and pace of work), etc.

● When working with laser printers:

● Place the printer next to the system unit so that the connecting cords are not stretched. Do not place the printer on top of the system unit.

● Before you programme the printer, make sure that it is in communication mode with the system unit.

● To achieve a high-quality, clear, high-resolution image and avoid damaging the device, you should use paper whose brand is specified in the printer manual (most often paper weighing 60-135 g/m^2 , such as Canon or Xerox 4024).

● Trim the edges of the paper with a sharp knife blade, without burrs, to reduce the possibility of paper creasing.

● When performing work (more than 20 minutes), when user intervention in the programme is not required, it is advisable to switch off the power of the video monitor.

● To maintain overall muscle tone, prevent musculoskeletal disorders, visual discomfort and other unfavourable subjective feelings, you should perform sets of recommended exercises for the eyes, spine, and arms during regulated breaks.

● The number of micro-pauses up to 1-2 minutes should be determined individually. The form and content of the breaks can vary: performing auxiliary work not related to PC operation, eating, performing recommended exercises.

- Exercise during the day is recommended individually, depending on the feeling of fatigue. Gymnastics should be aimed at correcting the forced posture, improving blood circulation, partially compensating for the lack of motor activity.
- Immediately stop working, disconnect all equipment from the power supply, and immediately notify your immediate supervisor or a PC repair specialist of any malfunctions (sparking, breakdowns, burning odour, signs of burning, etc.).
- Safety requirements when ending work on a PC.
- Close and save the files that were in progress in the PC memory. Perform all the steps to correctly shut down the operating system.
- Turn off the printer and other peripherals, and turn off the system unit. If you have an uninterruptible power supply (UPS), turn off the power.
- Turn off the PC by pressing the "POWER" button and unplug the power cable from the power outlet
- Cover the keyboard to prevent dust from entering it.
- Clean up the workplace.

Safety requirements in emergency situations.

- If, after switching on the PC, you smell a burning odour or feel an electric shock when you touch metal parts of the PC, you must immediately disconnect the PC from the power supply and report it to your supervisor.
- In the event of a fire, immediately start extinguishing the fire with available fire extinguishing equipment and report it by calling 101 (city fire department) and the head of the company's fire department. Remember that electrical installations should be extinguished with carbon dioxide fire extinguishers and dry sand to avoid electric shock.
- In the event of injury, stop working, provide first aid, call an ambulance by calling 103, and, if necessary, take to hospital.
- The sequence of first aid:
- Eliminate exposure to dangerous and harmful factors that threaten the victim's health and life (remove the victim from the effects of electric current, remove him or her from the contaminated atmosphere, extinguish burning clothing, etc;)

- Determine the nature and severity of the injury, the greatest threat to the victim's life, and the measures to be taken to save him or her;
- Take the necessary measures to rescue the victim in order of urgency (restore airway patency, perform artificial respiration, external cardiac massage, stop bleeding, immobilise the fracture site, apply a bandage, etc;)
- Support the victim's basic vital functions until the arrival of a medical professional;
- call an ambulance or doctor, or take measures to transport the victim to the nearest medical facility.
- Assistance to the victim provided by non-medical personnel should not replace assistance from medical personnel and should be provided only until a doctor arrives.
- Specific actions to provide first aid to victims of various injuries are described in Instruction No. 03-OP "On Providing First (Premedical) Medical Aid in Accidents," which is studied by employees of the enterprise during initial and subsequent occupational safety and health briefings.

In case of other emergencies, stop working and notify the work supervisor.

Based on the calculation of the air exchange for excess heat, the value of which is 628 m^3 /h, mechanical ventilation with a VORTICE VARIO fan was installed, since the use of natural ventilation is inefficient. Mechanical ventilation is capable of removing a temperature of 23 °C and maintaining the air temperature at an acceptable and even optimal value.

LIST OF REFERENCES IN CHAPTER FIVE

1. Tanenbaum, A. S., Wetherall, D. J. (2011). "Computer Networks." Pearson Education.

2. Kurose, J. F., Ross, K. W. (2017). "Computer Networking: A Top-Down Approach." Pearson.

3. Comer, D. E. (2004). "Internetworking with TCP/IP: Principles, Protocols, and Architecture." Prentice Hall.

4. Cormen, T. H., Leiserson, C. E., Rivest, R. L., Stein, C. (2009). "Introduction to Algorithms." MIT Press.

5. Cisco Systems, Inc. (2021). "Routing and Switching Essentials." Cisco Networking Academy.

6. Perlman, R. (2000). "Interconnections: Bridges and Routers." Addison-Wesley.

7. Dijkstra, E. W. (1959). "A Note on Two Problems in Connexion with Graphs." Numerische Mathematik, 1(1), 269–271.

8. OSPF Working Group. (1998). "OSPF Version 2." IETF RFC 2328.

9. IETF. (2005). "IS-IS Routing Protocol." IETF RFC 1142.

10. Halabi, S. (2000). "Internet Routing Architectures." Cisco Press.

11. McQuerry, S. (2002). "BGP Design and Implementation." Cisco Press.

12. Perkins, C., Bhagwat, P. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers." ACM SIGCOMM Computer Communication Review, 24(4), 234–244.

CHAPTER 6
ENVIRONMENTAL PROTECTION

6.1. Impact of man-made factors on the environment and its consideration in the routing system

Intensive human activity in the telecommunications sector is causing changes that can affect the natural environment. This disruption of the biosphere and the formation of an artificial environment known as the technosphere is important to consider in the context of a routing system.

According to scientific data, today's technological environment is largely man-made, including the field of telecommunications networks. The artificially created technosphere affects a significant amount of the natural environment and even goes beyond the planet.

The built environment, as a key aspect of technological progress, is becoming part of the challenges of the routing system. In this context, it is important to consider the direct and indirect impact of man-made factors on the natural environment and take measures to ensure optimal performance of telecommunications networks while maintaining environmental sustainability.

6.2. Environmental impact of base stations and cellular devices

Due to the rapid development of technology and the increasing number of devices in the modern world, exposure to electromagnetic radiation (EMR) is becoming an integral part of our environment. Handsets and base stations that support cellular communications are the main sources of EMF and have an impact on the environment. The way these EMF sources operate may vary, but their negative impact on humans and the environment is a significant factor.

Cellular phones, which are one of the main sources of EMF, have a distinctive feature - their maximum proximity to the user's head during a conversation, often in uncontrolled conditions. EMFs affect various parts of the body, such as the brain, the peripheral receptor areas of the vestibular and auditory analysers, and the retina. This exposure can have negative health effects on users and others.

The electromagnetic fields of base stations are generated impulsively, and their parameters depend on the time of day, the saturation of base station coverage and their number in a particular area. Since base stations are located in places where people are constantly staying, they create a round-the-clock impact on people through low-intensity electromagnetic fields of the radio frequency range.

Given the proliferation and intensification of the use of cellular technologies, it is important to conduct further research to understand the full impact of EMFs on human health and the environment.

It is particularly important to consider the effects of electromagnetic radiation on certain groups of people, such as children, adolescents, pregnant women and people with impaired health. Negative effects can lead to an increased risk of disease and other important problems.

Studies on cytogenetics confirm that electromagnetic radiation causes an increase in cells with chromosomal aberrations, especially when exposed for a long time. Exposure to electromagnetic fields can also affect living tissues, reducing their regenerative abilities and leading to deterioration of tissue condition.

The impact of electromagnetic radiation on the immune system and biota of the network.

Due to the widespread deployment of telecommunications and routing systems, there is a need to study the impact of electromagnetic radiation on living organisms and the ecosystem.

Scientific data accumulated by ecologists and hygienists confirm that the electromagnetic field affects the human immune system. It was found that it affects the processes of immunogenesis, changing the nature of the infectious process and disrupting protein metabolism. A decrease in the content of albumin and an increase in gamma globulins in the blood indicate complex changes in the body under the influence of an electromagnetic field.

The electromagnetic field can also act as an allergen or trigger, causing severe reactions in allergic patients upon contact with it. This becomes especially relevant in the context of the growing use of telecommunications systems.

The effect of electromagnetic radiation on the reproductive system has also been studied. It was found that under its influence, the function of spermatogenesis decreases, the menstrual cycle changes, and important deviations in the development of newborns are observed.

In the context of the plant world, studies have been conducted that indicate a significant impact of electromagnetic waves on biological objects. This is manifested in various effects on plant growth, development and reproduction. Information on the impact of the electromagnetic field on the soil rhizosphere and potential nitrogenase activity is important.

Finally, studies of the effects of weak electromagnetic fields on living organisms confirm that even low intensity can cause changes in living tissues. In particular, the impact of a mobile phone and a computer unit on biological objects, including periods of operation and power off, has been studied.

A common understanding of these interconnections is key to the future security and sustainability of routing systems and telecommunications networks.

Impact of modern radioelectronic devices on biological objects. Scientific studies aimed at assessing the impact of modern technologies, such as mobile phones, computers and other electronic devices, on various biological objects have revealed serious problems and disappointing results.

1. Reduced Motility and Survival of Microorganisms:

● Exposure to electronic devices reduces motor activity and the survival of microorganisms.

2. Increased mortality of microorganisms:

● Scientific studies show that the use of modern electronic devices leads to an increase in the mortality rate of microorganisms.

3. Disorders of Tissue Regeneration and Development:

- It was found that the effects of exposure include disruption of tissue regeneration and embryonic development.

4. Decreased biochemical reactions and metabolic disorders:

- The impact of electronic devices is manifested in a decrease in biochemical reactions and metabolic disorders in the body.

5. Reduction of Energy Potential in Vital Systems:

- Studies confirm a decrease in energy potential in all vital systems of the body.

These findings highlight the need for further research and understanding of the impact of electronic devices on biological processes. In the context of the development of routing systems and telecommunication networks based on the Dijkstra algorithm, it is important to take these findings into account to ensure the safety and sustainable development of technologies.

6.3. Methods and means of protecting the environment from the impact of man-made factors

When implementing routing systems and telecommunication networks based on the Dijkstra algorithm, it is important to take into account measures to protect the environment from man-made factors, in particular from electromagnetic radiation (EMR).

Organisational, engineering and technical measures are based on hygienic assessment and supervision by sanitary supervision authorities, together with the laboratories of enterprises. Hygienic assessment of new construction and reconstruction of facilities, as well as ongoing sanitary supervision of the radiation sources used, is necessary to ensure the safety of using EMW technologies.

Organisational and methodological work to train specialists and provide engineering and technical supervision is a key stage in ensuring the safe use of EMP technologies.

At the design stage, it is important to ensure the optimal relative positioning of the emitting and exposed objects to minimise the intensity of exposure in the environment. Measures to reduce exposure, such as limiting the entry of people into areas of high EMF intensity and reducing exposure time, are important for effective protection.

The general use of these measures is critical to ensure the sustainable development of technologies and the efficient operation of routing systems and telecommunications networks. One important aspect of this is the reduction of electromagnetic radiation (EMR) and noise.

Collective protection against electromagnetic radiation is based on calculations of radio wave propagation in a particular terrain. It is optimal to use natural shields, such as forest plantations or non-residential buildings, to reduce the intensity of the field that irradiates populated areas.

By installing the antenna on high ground or using highly directional antennas, the intensity of the electromagnetic field can be significantly reduced. However, it is important to note that tall antennas can be less stable and more expensive.

Local protection is effective and often used based on the use of radiation shielding materials. The use of such materials provides a high degree of absorption of radiation energy and reflection from the material surface.

Metal sheets and meshes with high conductivity can be used to reflect electromagnetic radiation. Wallpapering with metallic wallpaper, using metallic curtains or nets can also effectively protect rooms from external radiation.

Such shielding can minimise indoor exposure, but it is important to keep in mind that reflected radiation can spread and affect other objects.

Goggles with a conductive tin dioxide film and metal mesh in a rubber frame are effective means of protection against EMF. The use of previously used gloves and shoe covers is considered unnecessary, as the permissible energy flux density for the hands and feet is much higher than for the body. Collective and individual protective equipment, such as goggles, can ensure safe work of personnel at radio facilities.

Noise reduction measures include a variety of methods, such as controlling noise at source, sound absorption, sound insulation and acoustic treatment of rooms. In particular, it is possible to use booths or screens to locate noise generating objects, as well as acoustic treatment of ceilings and walls to reduce noise exposure. The effectiveness of these measures should be considered at the design stage of industrial facilities and equipment for routing systems and telecommunication networks, ensuring sustainable operation and safety of personnel.

CONCLUSIONS

In this study, we have delved into the topic of routing systems in telecommunication networks, focusing on the application of the Dijkstra algorithm. A thorough analysis of the principles and functionality of this algorithm allowed us to understand how key its contribution is to ensuring optimal data routing in modern telecommunication systems.

According to our research, it is noted that the Dijkstra algorithm has proven to be an effective mechanism for managing data transmission. Its optimal choice of paths maximizes the transmission rate and minimizes delays while ensuring the reliability and efficiency of the network.

Practical experimentation and testing of the algorithm in various conditions and network topologies confirm its versatility and effectiveness in various use cases. In particular, its ability to adapt to changes in the network topology and work efficiently under high load makes it an important tool for modern telecommunications infrastructures.

When analyzing the pros and cons of the algorithm, we found that its advantages outweigh its limitations, especially when considering its ease of implementation and high performance. This balance makes it an attractive choice for use in a variety of telecoms scenarios.

An important aspect of our work is to identify specific recommendations to optimize the implementation of the Dijkstra algorithm in real-world systems. Our advice on network configuration, optimization of algorithm parameters, and system support can serve as a guide for technical professionals working in the telecommunications industry. Overall, the results of our work demonstrate that the Dijkstra algorithm is not only theoretically important but also a practically effective tool for improving the performance and reliability of telecommunications networks.

The prospects and directions for further research in the field of routing system optimization, as outlined in the conclusions, demonstrate the importance of our work as a contribution to the development of advanced technologies in the telecommunications industry. The prospects for using the Dijkstra algorithm in combination with other technologies and aspects of security and fault tolerance provide a large field for further research and development.

LIST OF REFERENCES

1. Dijkstra, E. W. (1959). "A note on two problems in connection with graphs." Numerische Mathematik, 1(1), 269-271.

2. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). "Introduction to Algorithms." MIT Press.

3. Comer, D. E. (2014). "Computer Networks and Internets." Pearson.

4. Kurose, J. F., & Ross, K. W. (2017). "Computer Networking: A Top-Down Approach." Pearson.

5. Tanenbaum, A. S., & Wetherall, D. J. (2011). "Computer Networks." Pearson.

6. Forouzan, B. A. (2006). "Data Communications and Networking." McGraw-Hill.

7. Perlman, R. (2000). "Interconnections: Bridges, Routers, Switches, and Internetworking Protocols. Addison-Wesley.

8. Halabi, S. (2000). "Internet Routing Architectures." Cisco Press.

9. Moy, J. T. (1997). "OSPF: Anatomy of an Internet Routing Protocol." Addison-Wesley.

10. Perkins, C. (2001). "Ad Hoc Networking." Addison-Wesley.

11. Crowley, P. (1997). "An Introduction to Network Programming with Java." Addison-Wesley.

12. McQuade, J. (2012). "TCP/IP JumpStart: Internet Protocol Basics." John Wiley & Sons.

13. Albitz, P., & Liu, C. (2006). "DNS and BIND." O'Reilly Media.

14. Stevens, R. W., Fenner, B., & Rudoff, A. M. (2003). "UNIX Network Programming." Addison-Wesley.

15. Zeldovich, N., Kaashoek, M. F., & Kaashoek, F. M. (1997). "Towards high security for distributed systems." ACM Transactions on Computer Systems (TOCS), 15(4), 321-347.