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

ADMIT TO DEFENCE
Head of the Department

____________ R. Odarchenko
"_____"____________2022

DIPLOMA WORK

(EXPLANATORY NOTE)

BACHELOR'S DEGREE GRADUATE
BY SPECIALITY "TELECOMMUNICATIONS AND RADIO ENGINEERING"

Topic: «Telecommunication technologies for the VANET networks functioning»

Performer:______________________________________ A. Frolkov
(signature)

Supervisor:______________________________________ I. Terentieva
(signature)

N-controller:______________________________________ D. Bakhtiiarov
(signature)

Kyiv 2022

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications .
Department of telecommunication and radio engineering systems .
Speciality: 172 "Telecommunications and radio engineering" .
Educational professional program: Telecommunication systems and networks .

ADMIT TO DEFENCE
Head of the Department

_________ R. Odarchenko
“_____”__________2022

TASK
for execution of bachelor diploma work

Frolkov Artem
(full name)

1.Topic of diploma work: «Telecommunication technologies for the VANET networks functioning» approved by the order of the rector from « 25» April 2022 №_433 / ст.

2. The term of the work: from 25 April 2022 to 10 June 2022.

3. Initial work data: parameters of a VANET network, road distance < 21km, number of subscribers > 100, rate, QoS.

4. Explanatory note content: Introduction. Analysis of the principles of construction of modern automobile networks. Parameters of the vanet system Development and calculation of the VANET system in Kyiv region.

5. List of required illustrative material: figures, tables, formulas, schemes.

6. Work schedule

№ n/p	Task	Term implementation	Performance note
1.	Approval of the topic of the bachelor's thesis	25.05.2022	Done
2.	Introduction	25.05.2022	Done
3.	Analysis of the principles of construction of modern automobile networks	25.05.2022-29.05.2022	Done
4.	Parameters of the VANET system	30.05.2022-01.06.2022	Done
5.	Development and calculation of the VANET system in Kyiv region	02.06.2022-04.06.2022	Done
6.	Elimination of shortcomings of the thesis	04.06.2022-05.06.2022	Done
7.	Electronic version of the report, illustrative material of the report		Done

7. Date of issue of the assignment: “20” May 2022.

Supervisor __________________ I. Terentieva
(signature) (full name)

Accepted task for execution ___________________ A. Frolkov
(signature) (full name)

ABSTRACT

Thesis "Telecommunication technologies for the VANET networks functioning" contains 52 pages, 14 figures, 2 tables, 9 sources used .

TELECOMUNICATION NETWORK, AUTOMOTIVE NETWORK, VANET TECHNOLOGY,

The object of research is the telecomunication network VANET.

The subject of research is modern methods of planning and designing the telecommunication system of VANET.

The purpose of the thesis is to study the possibilities and methods of modernization of telecommunication system in Kyiv region on the use of modernized base stations.

To achieve the goals in the work it is necessary to perform the following tasks:

- Do an analysis of modern telecommunications automotive networks;
- Calculate cases of critical messages VANET;
- Calculate the coverage area of the VANET network in the Kyiv region;
- Make a critical message distribution model;
- To make a conclusion.

Thesis materials are recommended for use in laboratory work in the educational process and in the practice of specialists in the field of telecommunications, radio and mobile communications.

CONTENT

LIST OF ABBREVIATIONS

QoS - Quality of Service

SDN - Software-Defined Networks

FCC - Federal Communications Commission

WSN - Wireless Sensor Networks

GPRS - General Packet Radio Service

OBU - On 8 Board Unit

WAVE - Wireless Access in Vehicular Environment

IEEE - Institute of Electrical and Electronics Engineers

FANET - Flying Ad Hoc Network

WSMP - WAVE Short Message Protocol

INTRODUCTION

Today, 4.66 billion people use the World Wide Web, which is 58 percent of the people on Earth. The volume of Internet traffic is also growing strongly, which is associated with an increase in the number of users, the digitalization of all sectors of the global economy and an increase in demand for “heavy content”. According to CISCO research, on average, traffic will increase by 26% every year. The number of devices connected to the Internet is also increasing, the number of which by 2022, according to CISCO, will be 28 billion. And of course, the potential of the Internet is far from being unlocked.

Currently, various concepts of smart home, smart city, smart enterprise, tactile interaction via the Internet are being developed and discussed. The basis of these concepts is the idea of global interaction of everything and everyone through the Internet - the ability to connect everything that can somehow benefit from being connected to the global network.

The increase in the number of mobile network devices around the world has provoked intensive research on various aspects of the interaction of these devices. Among the large number of foreign and domestic works in this area, several main areas of research can be distinguished, which cover the technologies of self organizing networks of mobile devices (MANET), wireless sensor networks (WSN), self organizing networks of unmanned aerial vehicles (FANET), self organizing intelligent transport system networks (VANET), etc. Thus, a wide range of civil and military equipment can be networked using a network architecture of wireless dynamically organized decentralized networks.

One of the concepts that will be possible to translate into reality through the interaction of 5G services and the VANET system is the application of unmanned vehicles. It's not a secret for anyone that at present there are big shortcomings in the automobile and transport sector. There are a huge number of accidents, the issues of distribution of road traffic on the roads have not yet been resolved. Safety problems are associated with a great dependence on the human factor, and problems with road traffic are associated with imperfect traffic load distribution algorithms.

The purpose of the bachelor's thesis is studying the possibilities to improve the automotive network VANET functioning.

The object of research is the automotive network VANET.

The subject of research is modern methods of analysis and prevention of road accidents.

The subject of research is modern telecommunication technologies for the automotive networks functioning.

Research methods. To achieve the goals in the work used:

-Calculate cases of critical messages VANET;

-Conduct an analysis of telecommunications automotive networks;

-Calculate the coverage area of the VANET network in the Kyiv region;

-Make a critical message distribution model;

-To make a conclusion.

CHAPTER 1
ANALYSIS OF THE PRINCIPLES OF CONSTRUCTION OF MODERN AUTOMOBILE NETWORKS

1.1. Automotive network data

What is transport in the automotive network of the future? In this network, vehicles will exchange between themselves (V2V) and with external infrastructure (V2I) a huge amount of data. This is data collected from GPS, cameras, radars, leaders that keep track of the state of the road, transport, driver, etc. To interact with the network, vehicles will be equipped with devices that support wireless communication (3GPP, IEE 802.11p, Bluetooth, etc.).

1.1.1. The essence of the network to support unmanned vehicles

There are two types of vehicular communications in such a network: V2V and V2I. Vehicles, roadside infrastructure can collect environmental information for processing and sharing (within reach). V2V means direct connection between vehicles. Such a message allows the exchange of information between vehicles regardless of the infrastructure. Such a connection is useful for extending the communication range of an automobile network.

In this case, the following types of interactions are distinguished:

- Vehicle - Vehicle (V 2 V) – machine-machine interaction, used for information exchange between traffic-related applications [1];
- Vehicle - Roadside (V 2 R) – vehicle-base station interaction, used to unload the network by declaring a part of the functionality for relaying, stationary base stations;
- Vehicle - Infrastructure (V 2 I) is a subtype of interaction V 2 R, when mobile nodes are provided with access to an external network (Internet) through a connection to a base station.

- Infrastructure - Infrastructure / Roadside - Roadside (I 2 I / R 2 R) - used to connect fixed stations into a single network, in order to plan the infrastructure for the tasks of any services.

1.1.2. Vehicular network communications V2V

V2V allows the exchange of information between vehicles and roadside devices when they are not in range of each other. Throughout this process, other vehicles act as intermediaries; they receive the information and route it for entry into the RSU's coverage area. But, nevertheless, V2V communication belongs to a limited range. V2Vs are used for traffic accident applications or street parking applications.

1.1.3. Vehicular network communications V2I

But communication between cars is indispensable, communication with the outside world is needed. Therefore, V2I communication is organized. Because vehicles have limited processing and storage capabilities, some applications use the infrastructure as a platform or middleware. In some cases, V2I communication is expected to provide access to global information. Similarly, some applications can retrieve weather and traffic information via V2I communication. It should be said that the current network architecture and infrastructure does not allow deploying applications that implement such services. The current network has huge shortcomings in terms of QoS. Self-driving car applications require minimal network delays, the fastest possible processing of heavy traffic, and the interaction of a huge number of network units. Therefore, an architecture is proposed that implements the idea of MEC edge computing and SDN software-defined networks. Currently, almost all data is processed in the clouds, which causes huge delays.

Data centers are located quite far from end devices. Therefore, the idea came up to bring computing power from the clouds to Fog and Edge to geographically distributed computing devices. The idea is that we will process delay-sensitive data at the edge, and process heavier traffic data with minimal QoS requirements and data requiring cloud storage in the cloud. The Foga layer processes data that goes beyond the computational capabilities of the frontier. SDN, on the other hand, will separate the management functions and physical transmission functions from routers, switches, removing additional load from them. SDN will also make the network easily manageable and software-configurable, since the entire management function of the entire network will be implemented on the central controller. Thus, SDN builds the optimal route for traffic. Thus, with the help of SDN, MEC and FOG, it will be possible to build a network with ultra low latency.

1.2. FANET features

FANET (Flying Ad Hoc Network), similar to mobile peer-to-peer networks MANET and vehicular peer-to-peer networks VANET, represents a special type of peer-to-peer ad hoc network based on UAVs. Such a network has the ability to selforganize and adapt and is characterized by a dynamic changing topology. Special routing algorithms developed due to their specific features are need to organize FANET. The article gives a short overview of the existing FANET algorithms, as well as of the algorithms based on the swarm intelligence algorithms such as ant colony optimization. The experimental analysis was conducted, that proved the possibility of efficient application of ant colony optimization algorithm. The analysis was performed with the AntHocNet protocol simulating the behavior of ants in wildlife to solve the routing problems in FANETs.

1.2.1. Interaction with Fanet networks

FANETs provide a wide range of options for civil applications. The organization of this type of communication is necessary not only to perform surveillance and monitoring tasks, but also, for example, to effectively coordinate the movement of vehicles, increase the level of security (for example, as a means of preventing collisions), etc. FANETs are characterized by high mobility nodes, dynamically changing topology and movement in 3D space, which creates many additional difficulties in organizing communication in the network and requires the use of specialized protocols. The interaction of the nodes is limited by the allocated frequency resources, the power consumption of the nodes, the propagation conditions of the radio signal, etc. The interaction between the sending node and the receiving node is carried out randomly through a chain of intermediate nodes. Thus, the network nodes not only receive data, but also act as a router, ensuring the delivery of data to intermediate nodes.

1.3. Destination MANET

MANET (Mobile Ad hoc NETworks) networks are radio networks with random mobile subscribers that implement completely decentralized control in the absence of base stations or reference nodes. Topology - rapidly changing with random connection of nodes.

To this we must add WSN (Wireless Sensor Networks) - wireless sensor (telemetry) networks, consisting of small-sized sensor nodes with integrated functions for monitoring certain environmental parameters, processing and transmitting data over radio channels. They can, depending on the task, be built as mesh, ad hoc and MANET topologies; automotive networks VANET (Vehicle Ad hoc NETworks) - communication networks of vehicles; and all sorts of hybrids of the above.

1.3.1. Benefits of MANET

Today, the vast majority of terrestrial mobile wireless communication networks have a fixed infrastructure and are interconnected using various, usually wired or microwave, data transmission channels. In the last decade, much attention has been paid to the creation of mobile packet radio networks that do not have a fixed infrastructure - networks of fixed (Ad Hoc) and mobile subscribers (MANET).

Such networks are self-organizing, since their nodes are not only end user terminals, but also relay routers, relaying packets of other subscribers and participating in finding routes to them, therefore, these networks are capable of self-organization. Such networks can consist of tens, hundreds or even thousands of nodes. The scope of such networks is quite wide. Thus, MANET networks are useful in search and rescue operations, in a theater of military operations at a tactical level, in crowded places (for example, to serve conference participants), and where there is no telecommunications infrastructure (for example, on expeditions to regions remote from "civilization"). It is possible that these networks in many cases can become an alternative to mass mobile networks.

Unlike networks with a hierarchical structure and centralized management, peer-to-peer networks without infrastructure consist of nodes of the same type, where each node has a set of software and hardware tools that allow organizing data transfer from source to recipient directly if such a path is physically available and thereby distribute the load on the network and increase the overall network throughput. Data transmission from one subscriber to another can occur even if these nodes are out of direct radio visibility. In these cases, the data packets of these subscribers are relayed by other network nodes that have a connection with the corresponding subscribers. Networks with multiple relays are called multi-hop or multi-hop networks. When developing such networks, the main problems are the routing of packets from the source node to the destination node, network scalability, endpoint addressing, and maintaining connectivity in a variable topology.

Thus, the practical benefit from the implementation of such networks would be really huge. Starting from free calls within such a network, to restoring communications in areas destroyed by the elements.

Table 1.1

Comparison of FANET, VANET and MANET networks

Criteria	Types of Ad Hoc Networks		
	FANET	VANET	MANET
Node mobility	High	Medium	Low
Network node movement model	Usually predefined, special models are used	Medium	Arbitrary
Node Density	Low	Medium	High
Changing the topology	Extremely high	The average	Slow

End of table 1.1

Propagation of radio waves	High above the ground, line of sight is available in most cases	Close to the ground	Very close to the ground
Power consumption and network lifetime	Critical for a mini UAV	Not critical	Use of energy efficient protocols
Computing resources	High	Medium	Limited
Location determination	GPS, AGPS, DGPS, IMU	GPS, AGPS, DGPS	GPS

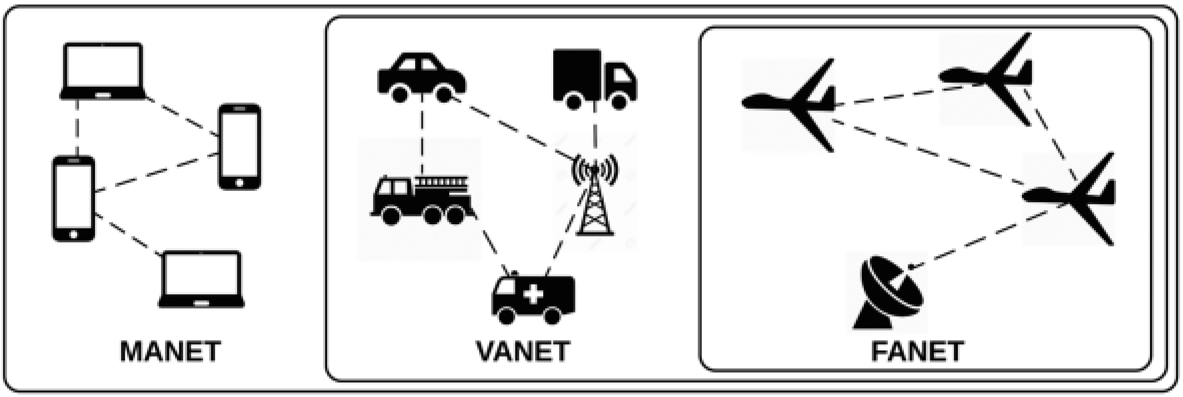

Fig. 1.1. MANET, VANET and FANET

1.4. The difference between networks and VANET

VANET differs from other wireless networks in the following features:

1) Dynamic topology: In VANET, nodes move at a relatively high speed, can change direction in an unpredictable way, resulting in the network topology often changing.

2) Uneven density of knots: as a rule, the density of vehicles on the route is uneven, depending on both time and terrain. For example, traffic density is lower at night than during the day; in remote sparsely populated areas, there are significantly fewer vehicles than in cities.

3) Traffic restrictions: it can be considered that the movement of cars is limited to highways and the territory adjacent to them.

4) The presence of obstacles (buildings, structures, etc.): in VANET, the movement of nodes is carried out along the carriageway, which is usually surrounded by high-rise buildings, trees (in cities), which creates an obstacle to the propagation of radio waves.

5) Lack of a single center of command and control over the topology: VANETs are decentralized networks that unite nodes in large areas of several tens or hundreds of square kilometers. At the same time, it is impossible to single out a single center (base station), with the help of which it would be possible to organize and maintain the topology, security protocols (exchange of cryptographic keys and certificates for authentication), device synchronization. Obviously, the protocols and applications running on the VANET must be adaptive, self-organizing, adding new devices and removing old ones.

6) Irregularity of communication traffic and problems of ensuring quality of service and security: since the traffic flow is not uniform, the volumes of transmitted information can also change over time. Modern entertainment applications, Internet TV, online games, etc. may cause a network denial of service. It should be taken into account that different services have different requirements for quality of service and security. Information is transmitted over an open radio channel, so interference, unintentional and targeted attacks on individual services and the network as a whole by users, hackers, hooligans, etc. are expected.

1.5. Information security in VANET

Security is an issue that requires careful assessment and consideration when developing automotive communication networks. Here are the typical types of violators that can cause information security threats in the VANET network:

Unscrupulous drivers. While we believe that most drivers on VANET members will be respectful and will abide by the rules for interacting safely with other members of the network, some drivers may seek to maximize their personal gain. For example, there may be situations where a driver may send false information in order to divert traffic to a different route and clear their way.

Scammers using wiretapping. The goal of these attackers is to collect information about drivers and use this information to analyze driver behavior and traffic flows.

Insiders. This type of attacker includes car company employees who install and configure the modules used to build the VANET.

Criminals. These intruders have great financial resources to create tools for implementing information security threats in VANET networks.

There is no unified classification of information security threats in VANET, therefore, after analyzing the article, it was found that the authors over the past 5 years have identified the following groups of classification features:

a) MonitoringAttack - listening to the network and identifying in it not only the movement of vehicles, but also listening to conversations between vehicles of the police (law enforcement agencies);

b) SocialAttack - a psychological attack on a person. . The authors represent the network as a kind of chat in which subscribers can exchange messages, and by sending a broadcast “freak” message, provoke the driver to violate traffic rules;

c) TimingAttack - an attack on the network in order to increase the delay in routing messages by physically "holding" them on the attacker's vehicle;

d) ApplicationAttack - an attack on a mobile application in order to change the messages sent to the network;

e) NetworkAttack - an attack on network equipment such as DoS, Sybil, NodeImpersonation.

Other authors propose to classify threats as attacks on availability, attacks on confidentiality, attacks on integrity and data trust, attacks on non repudiation/accountability, authentication and identification. (attacks on authenticity and identification).

In, it is proposed to divide threats into active and passive, and the latter - in accordance with the model of interaction of open systems by levels, highlighting the following: physical (for example, Jamming), network (Sybil), transport (Man in the Middle), applied (Repudiation) and, apparently, a separate group contains attacks that affect several levels (DDoS).

In, an analytical review of the 10 most popular threats to information security in VANET was made. In this article, "popular" threats were studied according to the scheme: attack - vulnerability - damage - countermeasures:

1) Sybil - destruction of the network's reputation by cloning false identifiers.

2) Node impersonation - substitution of the identification of a road user.

3) Man in the middle - interception and modification of messages between cars and access points.

4) GPS-spoofing / Hidden vehicle (position faking) - substitution of the node location coordinates.

5) Traffic analysis - determination of the network topology, routing.

6) Key and / or certificate replication - unauthorized identification in the system.

7) DoS (Denial of Service) - denial of service.

8)Routing: blackhole, greyhole, wormhole, tunneling etc. – unauthorized access to confidential information, violation of the data route.

9) Tracking - unauthorized access to identification information about the node.

10)Messagetampering / suppression / fabrication - attacks on transmitted messages. After the analysis, it was concluded that despite the abundance of threats presented in the analyzed sources, almost all of them are typical for any wireless network; Specific threats specifically for VANET include, perhaps, only GPS-spoofing / Position faking.

1.6. ITS Architecture

Despite the tremendous amount of standardization done around the world, it is not possible to form a detailed picture of a universal system architecture. This is due to the fact that the practical implementation of the systems is closely tied to the goals and objectives of each region separately. The list of technologies chosen in this case is also determined by local factors, such as the availability of devices and sensors, as well as the availability of competencies in the field of implementation. As a result, the already complex nature of ITS acquires a heterogeneous structure globally. However, even taking into account these differences, the key direction of development remains the integration of regional subsystems in order to create a global ITS.

The main prerequisite for this is the nature of the control objects, which consists in the high mobility of the vehicle. Taking into account the ability of the TS to move between regions, it is obvious that despite the private implementation of the infrastructure part, the ITS should not lose its functionality globally. This means that the I2V (Infrastructure to Vehicle) and I2I (Infrastructure to Infrastructure) interfaces must be implemented in accordance with international standards. As a result, in modern standards, instead of attempts to describe the general architecture of ITS, there are models of interaction of both individual objects and entire subsystems that meet the requirements of generally accepted technical regulations. A generalized model of the interaction of objects within the transport system, described in the ETSI EN 302 665 standard, is shown in Figure 1.2 .

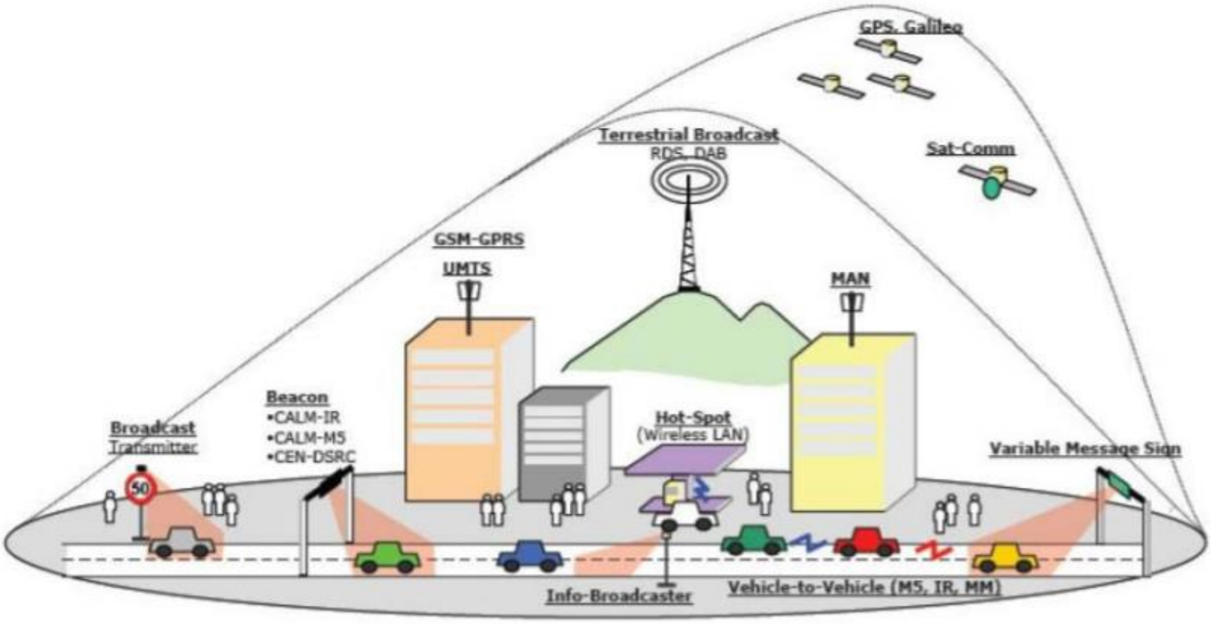

Fig. 1.2. Generalized interaction model for ITS

Taking into account the specifics of transport systems, a wide range of technologies used and differences in regional requirements, in the course of developing interaction standards and forming uniform architectural approaches to building ITS, it is necessary to take into account the following significant aspects:

– mobility of network nodes, leading to high dynamics of topology change;

– potential possibility of supporting any types of communication technologies;

– potential support of any kind of applications, including such as :

• developed specifically for ITS;

• using the ITS infrastructure as a transparent tunnel for the purpose of transiting their own data;

• stations using ITS exclusively for organizing internal interaction between connected devices.

– the ability to quickly and flexibly adapt to the needs of users in terms of bandwidth, availability of a communication channel, reliability of 28 connections, security of communication channels and cost (in the case of using commercial services);

– availability of effective prioritization mechanisms for different classes of applications;

– the potential to support the compatibility of applications and communication technologies, taking into account differences in the requirements for ITS functionality in different regions;

– support for the modular principle of construction with the possibility of increasing the functionality of ITS stations by installing additional expansion cards;

– support for service profiling;

– global applicability and scalability.

Taking into account the list of aspects of the implementation of the most flexible architecture formed during the evolution of ITS, the ETSI EN 302 636-3 standard provides the basic principles for building an architecture at the subsystem level. It presents a network model of interaction of ITS stations with each other, as well as ITS stations and external subsystems. Standardization at the level of individual ITS stations is made in the form of a generalized reference architecture of nodes, represented by interconnected functional blocks, with a description of their main purpose.

1.7. Network components

The main components of the ITS architecture are communication stations (ITS-S). They perform two basic roles:

– they are nodes of a composite network, working as initiators or receivers of connections;

– are transit nodes since the ITS network can operate in ad-hoc mode.

Network structures formed on the basis of various ITS stations are differentiated according to their functional characteristics into internal and external networks. External networks are responsible for the interaction of stations with each other and for connecting to other external networks. Among them, the following classes of networks are distinguished:

– ITS ad hoc network;

– access network;

– core network.

The task of internal networks is to organize the interaction of the internal components of the ITS stations. Each network structure formed from the ITS of stations carries the goal of implementing support for applications related to solving at least one of the basic tasks. These tasks include the organization of road safety, the effectiveness of traffic management, the provision of infotainment content, and the maintenance of business applications. However, interaction within a single network cannot provide the full range of ITS functionality. In this regard, individual networks are combined into a complex network architecture, as shown in Figure 1.3.

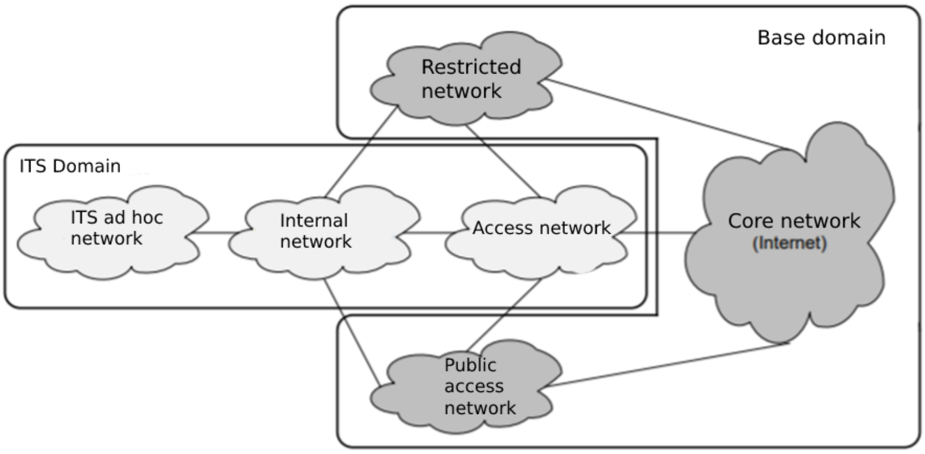

Fig.1.3. Top-level network architecture of ITS

ITS ad hoc network allows TS to interact with each other, as well as with RSU and personal mobile devices. This interaction is carried out using wireless communication technologies and allows nodes to form their own arbitrary network topology without the need for control from the infrastructure. The ITSG5 described in EN 302 663 or WAVE (Wireless Access in Vehicular Environments) based on the IEEE 1609 series of standards can be used as wireless technologies to form such networks.

The ITS access network is a dedicated network that provides access to specific applications or services that can be implemented and managed by local network operators or road services. The tasks of this network include connecting individual RSUs to each other in order to ensure interaction between them, as well as between OBUs connected to these RSUs. The ITS access network can also be used to connect RSUs distributed along the road network to a central ITS station. The formation of such a network architecture allows organizing data translation between OBUs through the local infrastructure, and not directly in ad hoc mode. However, if short distance communication technologies are used to connect to the RSU, the data exchange session with the services becomes intermittent.

The Public Access Network provides access to public, public networks. For example, this network can provide access to the Internet for the OBU and personal mobile devices connected to the OBU.

A restricted access network, unlike a public access network, is designed to serve limited groups of people by providing them with secure connection services. For example, these services can be used to provide access to closed corporate segments of a private company network.

1.8. The structure of a typical station ITS

Any ITS subsystem is built on the basis of interconnected ITS stations. In turn, each station consists of a set of components that communicate with each other through an internal network, as shown in Figure 1.4.

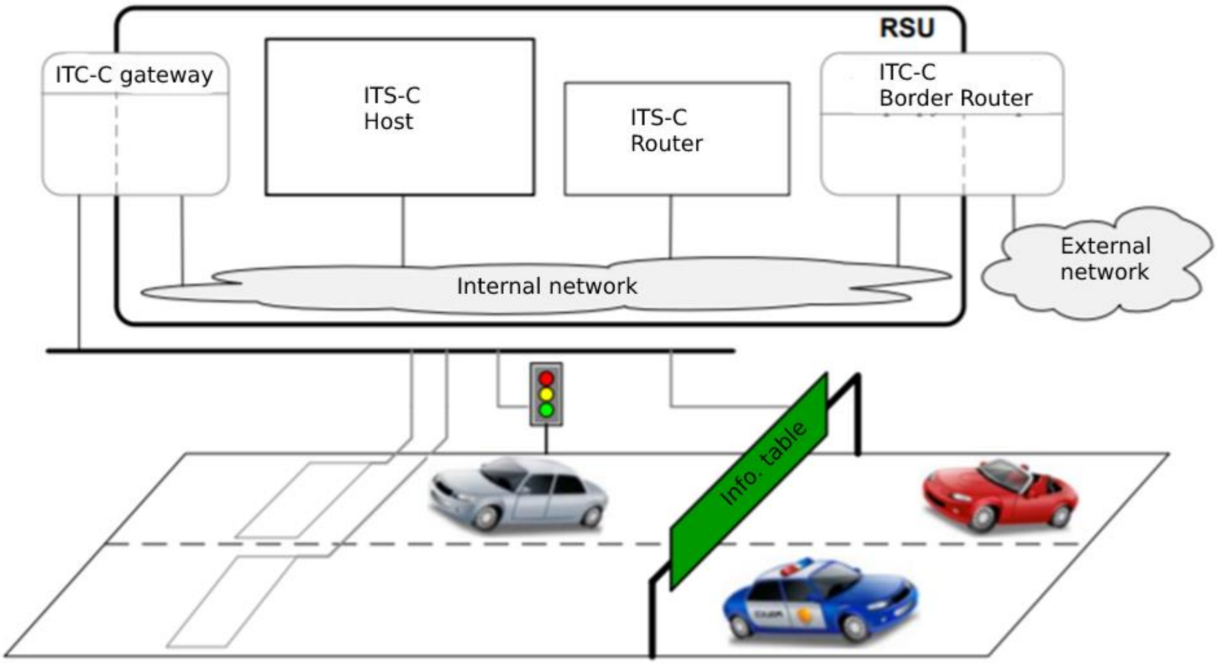

Fig. 1.4. Component composition of RSU

According to the EN 302 636-3 standard, the total mass of components is differentiated according to the functional feature into:

– hosts;

– gateways;

– routers;

– edge routers.

ITS-C hosts implement the minimum required functionality to support the underlying applications [4].

The tasks of ITS gateways include the implementation of support for the normal interaction of various protocol stacks at the levels of the OSI model from the 5th to the 7th. This requires a protocol conversion mechanism.

ITS-C routers provide cross-protocol communication functionality at the 3rd layer of the OSI model. Moreover, one of the interaction protocols must necessarily belong to the standard ITS stack of the station.

By analogy with routers, edge routers implement cross-protocol communication functions at the 3rd layer of the OSI model. However, their key difference is the provision of interaction with external networks, which can use mechanisms of control interactions and security that are different from the standard ITS stations.

1.9. Protocol stack of a typical ITS station.

Figure 1.5 shows the internal structure of a typical plant in the form of a single reference architectural model, described in the ETSI EN 302 665 standard.

This model, extended in the interests of transport systems, explains the functionality of the ITS station as part of the overall ITS subsystem. It obeys the basic principles of building the OSI model, defined in the ISO / IEC 7498-1 standard, where the total mass of protocols is distributed over seven levels of interaction.

As can be seen in Figure 1.5, in contrast to the ISO/OSI base model, the ITS reference model has three horizontal protocol layers and two vertical ones. The upper level of applications interacts with the ITS protocol stack through specialized programming interfaces - APIs [3].

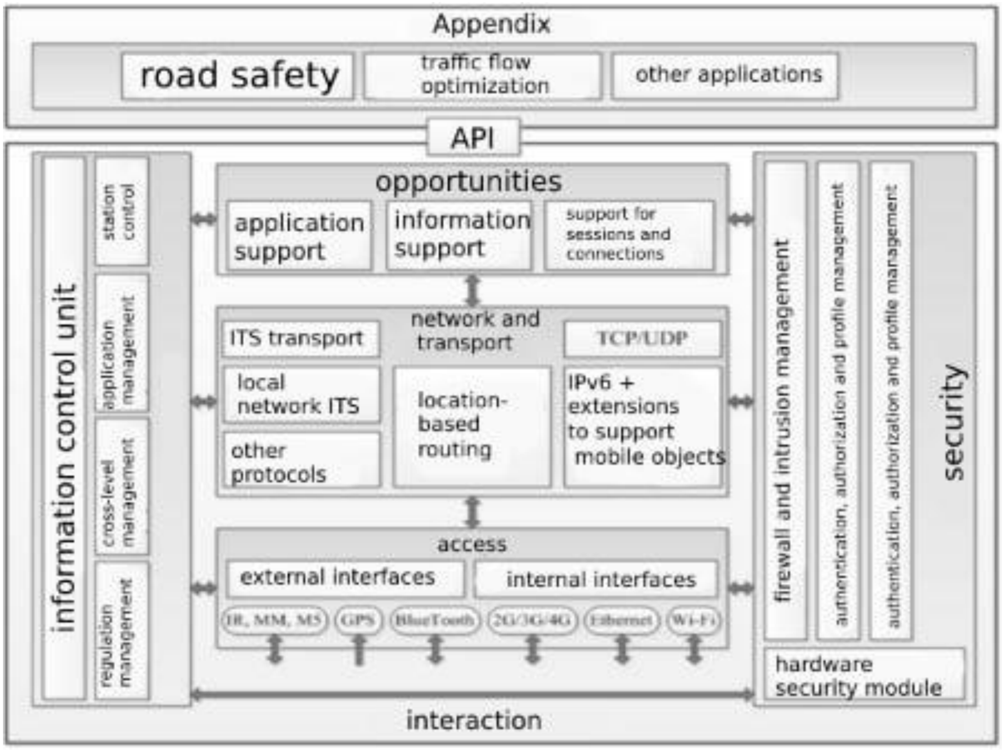

Fig. 1.5. Station ITS reference model

Despite external differences, from a functional point of view, all levels of the ISO/OSI model interaction protocol stack are present in full and are combined at three horizontal levels of the ITS reference model, which include:

- access level covering a wide range of interaction methods. This layer includes a group of communication technologies and protocols operating at the physical and data link layers of the ISO/OSI base model. The technologies included in it are not limited to any specific types of distribution medium, however, taking into account the specifics of ITS, preference is given to wireless methods of interaction. The technologies presented at the 34th access level are used both for organizing external and internal types of interaction. Moreover, for organizing external interaction, independent, not specific to ITS, communication systems, such as GPRS, UMTS, WiMAX, can be used. In this case, from the point of view of the ITS, the connection is established in the form of a transparent logical tunnel, using third-party systems as a medium for transiting their own data:

– combined network and transport layer. It contains protocols responsible for the delivery of data both between individual station components and between stations and other infrastructure objects of the ITS. Protocols related to the problem of networking perform the functions of routing data, ensuring the efficiency of their distribution within a certain geographical area. The group of transport protocols organizes data delivery on an end-to-end basis, while providing, depending on the requirements of applications or ITS services, functions such as reliability assurance, flow control and overload protection. In particular, this layer uses the IPv6 protocol, which allows using all its capabilities when transmitting packets through the ITS network[4];

– level of capability. Contains a collection of functions to support ITS applications. This level provides means of representing, aggregating and storing data structures of various types and from various sources. In order to provide ITS-specific methods for processing messages, as well as establishing and configuring sessions, several addressing methods are supported at this layer. An equally important functionality of this layer is the service management mechanism. Within the framework of this mechanism, there is the possibility of discovering new services, as well as expanding the existing list of services by downloading and installing special software modules [5].

The application layer sits on top of the protocol stack layers of the station ITS reference model. It consists of blocks that implement the logic of the services related to traffic safety, the efficiency of traffic flows, as well as entertainment and business applications.

The two vertical levels are represented by controls and security. The control level is responsible for various functions of configuring the station's ITS, as well as for inter-level data exchange. The security layer provides security services such as message encryption at various layers of the protocol stack, identity and credential management, and other security aspects such as firewall, secure gateway, and tamper-proof features.

CONCLUSIONS TO CHAPTER 1

In the first chapter the types of networks were considered. One of the decisive criteria was range and energy consumption.The use of the proposed methodology will allow to develop the problems of mobile networks of vehicles in domestic science and technology. The most effective system was VANET. The structure of a typical ITS station was developed.

The problem of the vehicle can be extended by extending it to the mobile network (MU SS), because, in addition to the vehicle, the network can unite users equipped with communicators or similar laptops that need communication in the absence of an external network. Thus, the problem and possible options for further modernization and change of mobile transport networks were considered.

CHAPTER 2
PARAMETERS OF THE VANET SYSTEM

2.1 VANET classification

VANET is divided into two classes . The first class is represented by vehicles with specialized OBU (On 8 Board Unit) communication modules installed. The second class refers to the elements of the fixed infrastructure RSU (Road Side Unit), installed on the principle of base stations serving the geographical segment of the network[2].

2.1.1. VANET network standard

Features and tasks of VANET Vehicle communication networks VANET use the vehicles themselves (cars, trains, etc.) as devices that form the network. As a result of many years of consultations and work of groups of specialists under the auspices of the international Institute of Electrical and Electronics Engineers (Institute of Electrical and Electronics Engineers, IEEE), the VANET IEEE 802.11p communication standard has been published. This standard uses the IEEE 1609 protocol family. The combination of these protocols is called IEEE 802.11p / WAVE (Wireless Access in Vehicular Environment, wireless access in the transport environment).

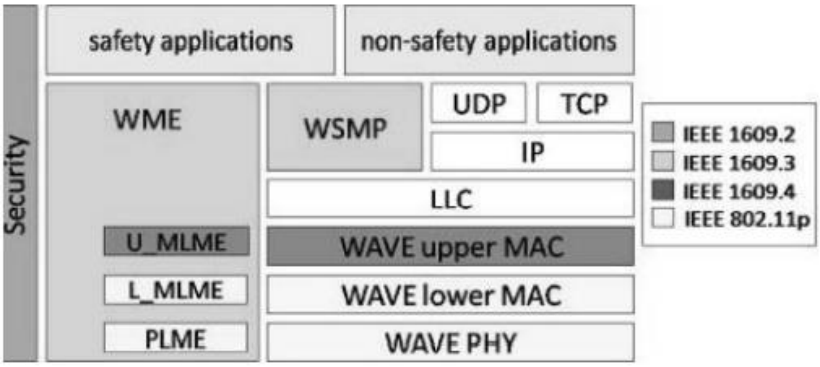

Fig. 2.1. IEEE 802.11p/WAVE protocol stack

As can be seen from Figure 1, the 802.11p protocol supports both the standard TCP/UDP/IP protocol stack used to organize data transmission for non-security user applications, such as Internet access, and the WSMP (WAVE Short Message Protocol) protocol. , intended for the exchange of short messages containing security application information or status information. It is important to note that the exchange of WSMP protocol messages occurs directly between devices implementing the WAVE protocol, without involving IP. The 802.11p / WAVE protocol provides for the use of one control channel (CCH, Control Channel), designed to control the network and transmit messages related to security, and up to six service channels (SCH, Service Channel), which are used to transmit other traffic (for example, custom IP traffic). With regard to the introduction of technology, the current situation is as follows. In the US, the FCC (Federal Communications Commission) has already allocated a 75 MHz bandwidth for VANET between 5.850 GHz and 5.925 GHz. The frequency region around 5 GHz was chosen due to the fact that at these frequencies it is possible to carry out data transmission at a high speed and low dependence on weather conditions. This frequency band is divided into a control channel (10 MHz), 6 service channels (10 MHz each) and a reserve channel (5 MHz).

2.1.2 Frequency allocation

The European Telecommunications Standards Institute proposes to use the frequency range 5.855-5.925 GHz, while the spectrum will be divided as follows: 2 channels of 10 MHz - for high priority safety-related messages, mainly transmitted between vehicles; 30 MHz for the transmission of safety and road control messages, transmitted mainly between vehicles and road infrastructure; finally, 20 MHz for the transmission of non-safety messages. In this case, the control channel will be located in the frequency region of 5.880 GHz, which will make the European and American systems compatible. In Japan, due to the fact that a number of the above frequencies are already occupied, it is planned to place VANET channels in the 5.900 GHz frequency region.

But of course, in addition to the advantages, the implementation of this architecture generates many problems:

- Load distribution. Network devices in edge computing networks have poor processing power. Therefore, there are tasks that require calculations and load balancing in accordance with the bandwidth of the equipment of edge networks.
- Security and privacy, end devices are more vulnerable to attacks than centralized devices, as cloud providers are able to provide better data protection. The cloud operator organizes and guarantees encryption, disaster recovery and high-quality protection against attacks.
- Routing and forwarding. Vehicles are constantly moving at incredible speeds, so it is difficult to predict which particular vehicle will receive its services from any of the base stations or edge servers. It is necessary to develop algorithms for predicting the location of transport.
- Price. Huge monetary investments for deployment of such networks.
- Deployment. Since the deployment of network equipment is expensive, it is important to optimally install the appropriate number of network elements. It is necessary to deploy equipment so that the traffic path passes through fewer devices, while still satisfying all the needs of transport in network performance.

2.2. Telecommunication networks

A key role in our study is played by a vehicle(V), which, being equipped with - telecommunications devices (TKU), forms local networks inside vehicles, which we will designate as autonomous telecommunication networks (ATNs). TS, together with the TCU located in it, connected in ATCS, we will also designate as a hardware-software complex (HSC).

Under the communication network (CN) of vehicles (V) we mean a communication system between hardware and software complexes (HSC) created on the basis of vehicles and equipped with telecommunication devices. If such a network is self-organizing, then we denote it as “ad hoc” network of vehicles, which is analogous to the term VANET – vehicular ad hoc network.

Among the features of the SS TS is the absence of a fixed backbone network, since the scope of such networks can be very diverse (tundra, taiga, swamps, steppe, desert, extreme north, the Arctic, Antarctica, air and outer space, etc., where it may not be technically possible to locate base stations of cellular operators for many kilometers). And even if the backbone is present, the CC can function without it, using “ad hoc” routing.

We also note that despite the possibility of the presence of dedicated vehicles, in general, communication clients, and base stations, and servers providing communication services in this case are the hardware and software systems themselves, created on the basis of the vehicles used in the network.

2.3.1 Organization of communication networks

Let us now consider options for organizing communication networks for vehicles.

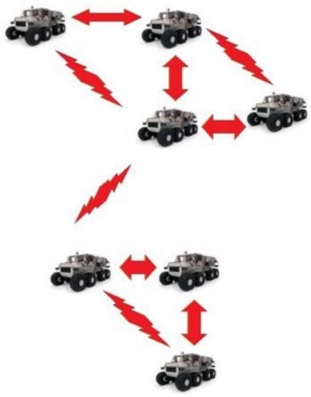

Fig. 2.2. Example of VANET – Vehicular Ad Hoc Network

If self-tuning tools are not provided, then such networks have limited capabilities due to the fact that in such networks it becomes impossible for new users to work, users cannot be transferred from one vehicle to another while maintaining its operability in the network (and this is possible, for example, in case of loss or destruction of the vehicle).

2.3.2. Self organizing network

Consider a variant of a self organizing network using “ad hoc” routing (for example, AODV). If the algorithms “ad hoc” routing (such as AODV), then the network is formally self-organizing (for example, the ping and traceroute utilities of the Linux operating system or ping and tracert Windows will diagnose the full connectivity of the network when moving its nodes). That is, each node will be formally available. But if self-organization is implemented only at the IP level, then, despite the technical availability, the network of users (but not devices) cannot be considered a self-organizing network!

So, such networks of telecommunication devices, when changing due to routing algorithms ad hoc 120 (for example AODV) retain connectivity, but the subscribers of such networks do not retain network connectivity when moving the latter, we will denote it as ad hoc layer 1 vehicle network”. Their self-organization is implemented only at the network level, only IP addresses are routed. (see Fig. 1.3).

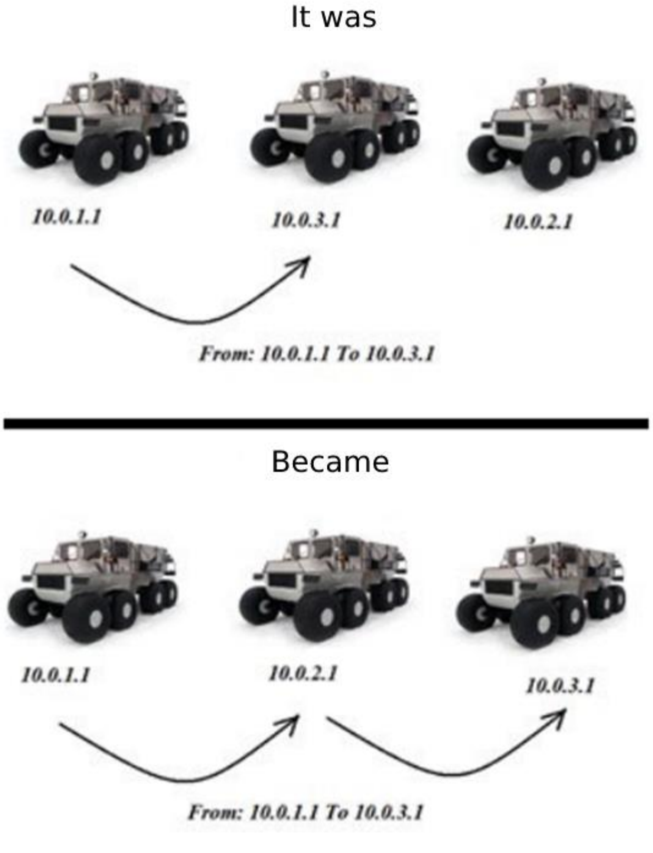

Fig. 2.3. Ad hoc networks of the first level

Possible areas of application of self-organizing radio networks are described in table 2.1.

Table 2.1

Possible areas of application of self-organizing radio networks

Sphere	Appointment
Tactical measures	Military networks
Emergency measures	Search and rescue operations. Replacement of fixed networks in case of natural disasters (earthquake, hurricane, etc.)
Commercial facilities	Electronic commerce, business: dynamic access of the correspondent to the base, mobile office. Service when moving on a transport facility.
Home and enterprise networks	Rootless home screens for various programs Personal screens
Learning networks	Virtual classrooms, conferences
Entertainment networks	Multiplayer games, homework, external Internet access
Position service	Information services: automatic call forwarding, gas station coordinates, etc.
Sensor networks	Domestic, industrial and military applications designed to monitor the environment: movement of animals; chemical, biological analysis of plants; dynamics of weather conditions

2.3.3. Disadvantages of self-organizing networks

The main problems of radio measurement that self-organize Among the main problems of radio measurement with self-organization can be seen:

1. The problem of efficient use of radio resources and increasing the speed of information transmission in these networks at the physical level of the EMVVS. One of the modern areas of solution is the use of ultra-wideband signals.
2. The problem of "fair" distribution and collective use of radio resources at the channel level of the EMVVS.
3. The problem of efficient routing in terms of the dynamics of the network topology (network layer EMVVS) and different requirements for the maintenance of certain types of traffic.
4. The problem of creating effective methods (algorithms) of management at different levels of the EMVVS for a particular MSC. The emergence of new technologies (directional antennas, positioning systems, ultra-wideband signals, etc.), various areas of application of MCP require the creation of new methods of managing these networks, including the use of artificial intelligence methods.
5. The problem of efficient use of node resources (most MCP nodes can be portable and, accordingly, limited in their resources: CPU performance, memory capacity and battery power, etc.)
6. The problem of providing a given quality of service for different types of traffic. Characteristics of radio channels and network topology are subject to rapid change. The solution of this problem requires intellectualization and integration of levels of the reference model of interaction of open systems.
7. The problem of scalability and organization of large networks. In leading networks, the amount of service traffic is proportional to the number of nodes and channels of the network. In MSR, nodes are mobile, wave packet distribution is very often used - so a significant amount of office traffic. The intensity of service traffic increases quadratically N2v, where N is the set of network nodes and v is the intensity of topological changes.

8. The problem of security in the conditions of decentralized management and broadcasting of the radio channel.

CONCLUSIONS TO CHAPTER 2

Thus, the analysis of open sources showed that VANET technology is a progressive and convenient platform for further development in the field of automotive safety.

The organization of network communication was developed and presented. The disadvantages of self-organized networks are also given.

The main advantages of the VANET network are self-organizing networks that connect cars without additional transmitters. The development of such a system will provide pedestrians and drivers with greater safety on public roads.

The main purpose of modernizing the existing system is to provide certain data and open access to the internal structure, calculate the coverage area and possible subscriber area for a particular base station.

CHAPTER 3
DEVELOPMENT AND CALCULATION OF THE VANET SYSTEM IN KYIV REGION

3.1. Epidemic theory

One of the approaches to studying the process of message transmission through an ad hoc network is the theory of epidemics based on the Poya model. The original goal of this theory was to study the characteristics of the spread of an infectious disease in a group of individuals susceptible to infection. Subsequently, drawing analogies with the composition and reaction of ad hoc networks to a transmitted broadcast message, this theory began to be applied to analyze the principles of involving network nodes in the process of distributing this message. According to this theory, the virus spreads from an infected subject to a susceptible subject through direct contact between them. Thereafter, susceptible subjects become infected and can further spread the virus. After a certain period of time, infected subjects may recover, becoming immune to further infection. This behavior is typical for the SIR(Susceptible-Infective-Recovered) model. Or become susceptible to infection again, which is typical for the SIS (Susceptible-Infective Susceptible) model [6].

3.1.1. Basic analytical model

The description of the transition process of node states in the theory of epidemics is carried out by compiling the mass balance equation. To do this, we denote the relative proportion of susceptible S, infected I and recovered nodes R. Moreover, since the transition process takes place within a closed population, it is obvious that: S+I+R =1.

Then, the basic system of differential equations describing the mass balance for the SIR model, known from the theory of epidemics , can be written as follows:

$$\begin{cases} \frac{d\tilde{S}}{dt} = -\beta\tilde{I}\tilde{S}, \\ \frac{d\tilde{I}}{dt} = \beta\tilde{I}\tilde{S} - \gamma\tilde{I}, \\ \frac{d\tilde{R}}{dt} = \gamma\tilde{I}, \end{cases} \tag{3.1}$$

where β is a probability coefficient characterizing the volume infection of susceptible nodes upon contact with the infected; t is a time; γ is a probabilistic coefficient characterizing the volume of node recovery after infection.

Let us consider the possibility of applying this system of equations to the case of transmission of security messages through the VANET network. To do this, we introduce a quantitative estimate into the existing system (3.21). Taking into account the previously introduced restrictions on the number of retransmissions in three steps and the fact that the speed of signal propagation is many times higher than the speed of vehicles, we can assume that during the propagation of a message over the network, the relative position of vehicles practically does not change [7]. This assumption allows us to consider the total number of vehicles requiring information to be unchanged and equal to:

$$N = S(t)+I(t)+R(t) \tag{3.2}$$

As a result of message translation, only a part of the total number of nodes N is infected. In the context of time t, this part can be defined as S(t)/N. Further, to estimate the absolute value of the number of susceptible nodes, it is necessary to introduce several assumptions. So, we will assume that the nodes of the network are distributed uniformly with a certain density ρ. Then, taking into account the use of omnidirectional antennas, the number of nodes with which an infected node can contact when transmitting a message can be found as $\rho\pi r_0^2$. In real conditions, the location of network nodes is limited by the boundaries of the carriageway. These restrictions can be represented as a truncated circle, shown in Figure 3.1[8]. What should be reflected in the analysis by entering a special shape factor α, depending on the geometric shape of the roadway.

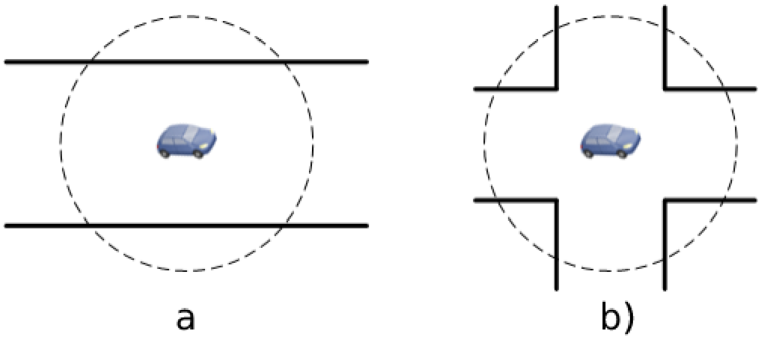

Figure 3.1. Examples of coverage areas for various forms of the carriageway:
a) a straight section of the road; b) an intersection.

Thus, the basic system of differential equations (3.1), for the case of transmission of critical messages over the VANET network, can be written as:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta\gamma I(t)\frac{\alpha\rho\pi r_0^2}{N}S(t), \\ \frac{dI(t)}{dt} = \beta I(t)\frac{\alpha\rho\pi r_0^2}{N}S(t) - \gamma I(t), \\ \frac{dR(t)}{dt} = \gamma I(t). \end{cases} \tag{3.3}$$

3.2. Model with SINR-Based Limiting Algorithm

As noted earlier, in order to limit the overhead consumption of channel resources by duplicate messages that occurs in the case of broadcast message distribution in multihop mode, it is necessary to use specialized limiting algorithms. Also, it must be taken into account that the main task of sending security messages in VANET networks is to provide reliable information coverage of all neighboring nodes located at a distance sufficient to take the necessary preventive measures[9]. This effect can only be achieved by minimizing the number of relay nodes while maintaining the infection volume. Obviously, the use of specialized algorithms should ensure the transition of most of the nodes from state I to state R without relaying the message. It is for these purposes that a signal propagation algorithm was developed based on the value of the signal-to-noise ratio + SINR interference. Let us compare the process of functioning of this algorithm with the basic principles set forth in the theory of epidemics.

The main difference between the network operation in the case of applying the mentioned algorithm is the limitation of the number of relay nodes out of the total number of infected ones. Thus, I(t) can be represented as the sum of nodes with a high probability of retransmitting, and nodes with a high probability of passing into a recovered state without retransmission $I^a(t) + I^p(t)$. Accordingly, the radius r_0 can be divided into two segments r_0^a and r_0^p, $r_0^a << r_0^p$. The model for distributing a message from a RTS-related application is shown in Figure 3.2.

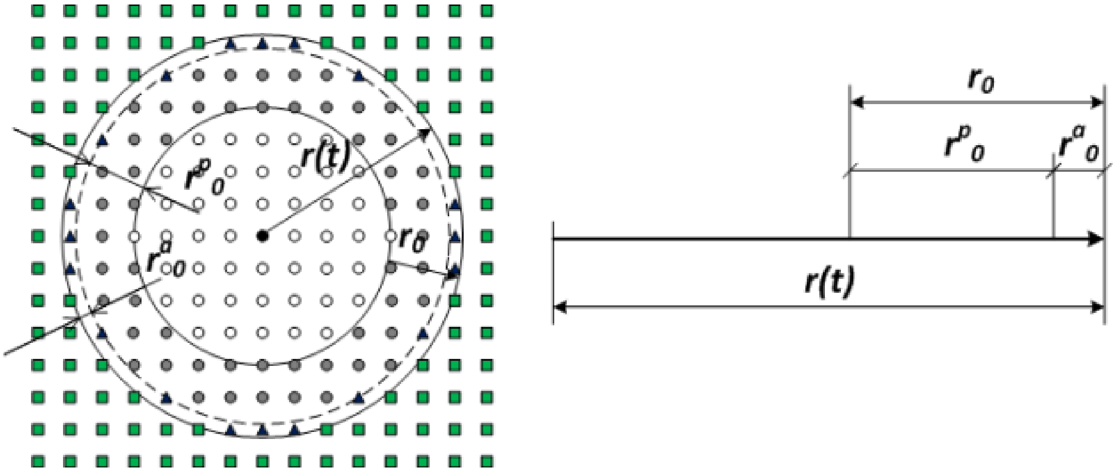

Fig. 3.2. Critical message distribution model over VANET using SINR-based algorithm [3]

Taking into account the above clarifications, the system of differential equations (3.3) should be reduced to the form:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta I(t)\dfrac{\alpha\rho\pi r_0^2}{N}S(t), \\ \dfrac{dI(t)}{dt} = \beta(I^a(t)(r_0^a)^2 + I^p(t)(r_0^p)^2)\dfrac{\alpha\rho\pi}{N}S(t) - \gamma I(t), \\ \dfrac{dR(t)}{dt} = \gamma I(t). \end{cases} \qquad (3.4)$$

Taking into account that each transmission of a message is an independent event, within which at the primary stage there is only one infected node, we can write the initial values of the number of each type of node as:

$$\left\{\begin{array}{c} S(t)=N-1, \\ I(t)=1, \\ R(t)=0, \end{array}\right|$$

(3.5)

To estimate the abundance of each type of nodes at t>0, one should refer to Figure 3.2. It can be seen from the figure that, taking into account the peculiarities of the algorithm, the driving force of the external front of infection is the value of active infected nodes I (t). Thus, first of all, it is necessary to determine the relationship between the volumes of susceptible nodes and active infected ones:

$$\begin{cases} S(t)=N-\alpha\rho\pi r(t)^2, \\ I^a(t)=\alpha\rho\pi r(t)^2-\alpha\rho\pi(r(t)-r_0^a)^2-\gamma I^a(t). \end{cases}$$

(3.6)

From the system of equations (3.5), taking into account the fact that $r^{a}_{0}<<r(t)$, we obtain

$$I^a(t)\simeq\frac{2\alpha\rho\pi r_0^a r(t)}{1+\gamma}$$

(3.7)

Expressing r(t) in terms of S(t) and substituting into (3.6), we obtain

$$I^a(t)\simeq\frac{2r_0^a\sqrt{\alpha\rho\pi}}{1+\gamma}\sqrt{N-S(t)}.$$

(3.8)

Next, we substitute expression (3.8) into the differential equation for S(t) from the system of equations (3.4). For the resulting equation, a general solution can be found:

$$S(t)=N-N\left(\frac{2}{1+e^{-At+C}}-1\right)^2, \tag{3.9}$$

Taking into account the initial values (3.5), we find a particular solution:

$$S(t)=N-N\left(\frac{2}{1+Be^{-At}}-1\right)^2, \tag{3.10}$$

Let us turn again to the system of differential equations (3.4). It can be seen from it that the transition from state S to state R occurs sequentially through state I. Thus, at first glance, a direct relationship between these two states is not observed. However, if we turn to Figure 3.2, it becomes clear that the number of recovered nodes at time t depends on the number of receptive nodes at the time of the previous relay. This observation can be written as R(t)=(N-S(t-τ)), where τ is the time interval spent on one retransmission. From here we can write down the system of equations describing the transient processes between states I and R as:

$$\begin{cases} R(t)=\begin{cases} 0, \text{при } t=0, \\ N-S(t-\tau), \text{при } t>0, \end{cases} \\ I(t)=S(t)-R(t). \end{cases} \tag{3.11}$$

Using the expression (3.10) obtained earlier for S(t), we can define R(t) for t > 0 as:

$$R(t)=N-S(t-\tau)=N\left(\frac{2}{1+Be^{-A(t-\tau)}}-1\right)^2. \tag{3.12}$$

Further, based on (3.11) and (3.12), we obtain the equation for I(t):

$$I(t) = N - N\left(\frac{2}{1+Be^{-At}} - 1\right)^2 - N\left(\frac{2}{1+Be^{-A(t-\tau)}} - 1\right)^2 . \tag{3.13}$$

3.3. Double beam model

Two-Rays Ground (TRG) radio signal propagation model with two beams. This is a radio propagation model in which the gap loss between the transmitting antenna and the receiving antenna is predicted based on a two-component signal. The transmitting and receiving sides are in the line of sight. As a rule, each of the two antennas has a different height.

The TRG model belongs to the class of deterministic ones, since, like, for example, the well-known Frieze formula, it determines the power of the received signal as a deterministic function of the distance between the transmitting and receiving sides. For this model, such concepts as the Carrier Sense Range (CS) are widely used, this is the radius of the zone within which the sending of a message can be detected by neighboring nodes, and the communication range (Communication Range - CR), this is the radius of the zone within which a sent message can be successfully received if there are no interfering signals, as shown in Figure 3.3.

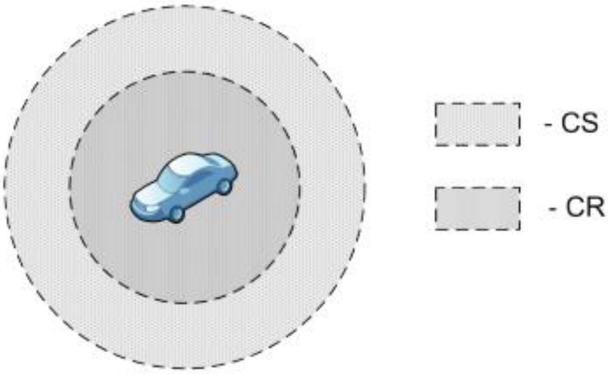

Figure 3.3. Signal propagation by two beams

The possibility of using these concepts is determined by the constancy of the signal power at a fixed distance from the transmitter. With the help of them, the distance at which the interaction of network nodes is carried out is described, and as a result, the signal power level necessary to reach the given radii of the interaction zones is estimated. The model sets the principle of signal propagation, which is close to reality for the study of wireless communication systems in open spaces. According to this model, the power of the received signal at a distance D from the transmitter can be determined by the formula:

$$P_r(D) = \frac{P_t G_t G_r h_t^2 h_r^2}{D^4 L}$$

where h_t, h_r are the heights of the transmitting and receiving antennas;

P_t is the transmitted signal power;

G_t, G_r – antenna gain;

L - system losses.

In particular, there are many works in which a model study of the characteristics of VANET networks for long-distance sections of routes was carried out using a two-beam signal propagation model.

3.4 P-01 highway safety

Official statistics are an order of magnitude more modest compared to the real ones due to the specifics of data collection at the Ministry of Internal Affairs, since the dead are recorded only at the site of a road incident, the authors of the investigation clarify.

Experts say that the problem is also due to excessively high traffic, which the transport infrastructure in this area is not designed for:

“Despite the fact that the R-01 highway belongs to the second category highways, for which the traffic intensity is provided by the GOS at the level of 3,000 to 10,000 vehicles per day, the actual load of the R-01 from the Atmosfera shopping center in the Kozin village exceeds the limit three times - 28,900 cars on a weekday, ” it is reported with reference to the engineering audit of the Research Institute of Ukravtodor, carried out at the end of 2019.

“With such intensity and density of traffic, in 2010, instead of giving the R-01 road a category of national importance with the corresponding infrastructure improvements, the leadership of the Ukrainian Highway Service in the Kyiv region decided only to redraw the markings, as a result of which four lanes appeared on the pavement, which barely reach the width allowed by state construction standards, and sometimes they do not reach.”

3.5 Equipment

When carrying out calculations, the necessary parameters for base stations were determined, in the sector where there is not enough power from the rest.

When choosing equipment, attention was paid not only to the output parameters of the base station, but also to cost, durability and maintainability.

Cambium cnPilot Outdoor E501S

Fig. 3.4. Cambium cnPilot Outdoor E501S

-supports high transmitter output power up to 29 dBm, which, together with the built-in sector antenna with a gain of 10.5 dBi at 2.4 GHz and 13 dBi at 5 GHz, provides a high range of subscriber service.

- Supports secure authentication 802.1x / WPA2-Enterprise.

-supports Hotspot Captive Portal functionality.

- Provides service for up to 256 clients with the Band steering function of transferring a dual band client from 2.4 GHz to 5 GHz.

-provides standard 802.11 seamless roaming: Pre-Authentication, Opportunistic Key Caching (PKM Caching), 802.11r/k without using an external controller.

- interacts with 3G Offload mobile access networks according to the Passpoint 2.0 (HotSpot 2.0) standard.

- Supports Multi-Hop mesh, Airtime Fairness and other premium AP functionality;

-industrial version with enclosure protection class IP-67 with operation of the device at an ambient temperature of -30+60 °C.

- provides lightning protection of power supply and data transmission circuits and protection against out-of-band interference of 3G stations by using frequency filters;

-heating of the device at start in conditions of low temperature - "cold start".

-monitoring and management of network management (NMS) through the cloud Cloud or corporate (on-Premises) access controller cnMaestro.

Cambium cnPilot Outdoor E700

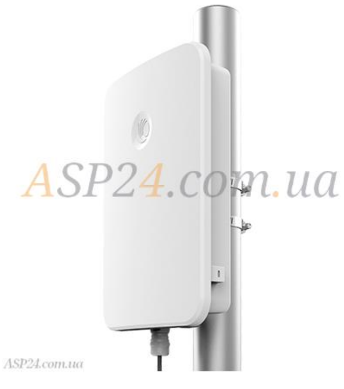

Fig. 3.5. Cambium cnPilot Outdoor E700

- Omnidirectional (OMNI) antenna, MU-MIMO 4x4 in the 5 GHz band.

-802.11ac, support 512 clients, 16 SSIDs.

- Wall brackets included.

-RF filters for collaboration with LTE-equipment.

-Guest access, customizable welcome pages, vouchers, Google and Facebook social media logins.

- Automatic parameter setting.

- Tracking and inventory of equipment.

-Location on the map.

-Monitoring of critical data and accidents.

-Massive software update on devices.

-Built-in troubleshooting tools for access points, client hardware and Cambium client modules.

-Use cloud or local virtual controller.

The technical characteristics of base stations are described above, with suitable parameters. The price of the first BS is 20948 hryvnia, which is 7245 hryvnia cheaper than the newer model. But the main parameter is not only the price, but also technical data, CAMBIUM E700 has better technical data, which allows reducing the number of stations themselves and simplifying maintenance and connection.

The length of the route is almost 21 km. In order to provide full coverage of the network, approximately 40 base stations are needed. This is not quite a small amount, since 40 base stations at a price of 28,000 UAH will eventually turn out to be 1,120,000 hryvnia. But due to the fact that BS of cellular operators have already been installed along the route, this reduces the cost of the project.

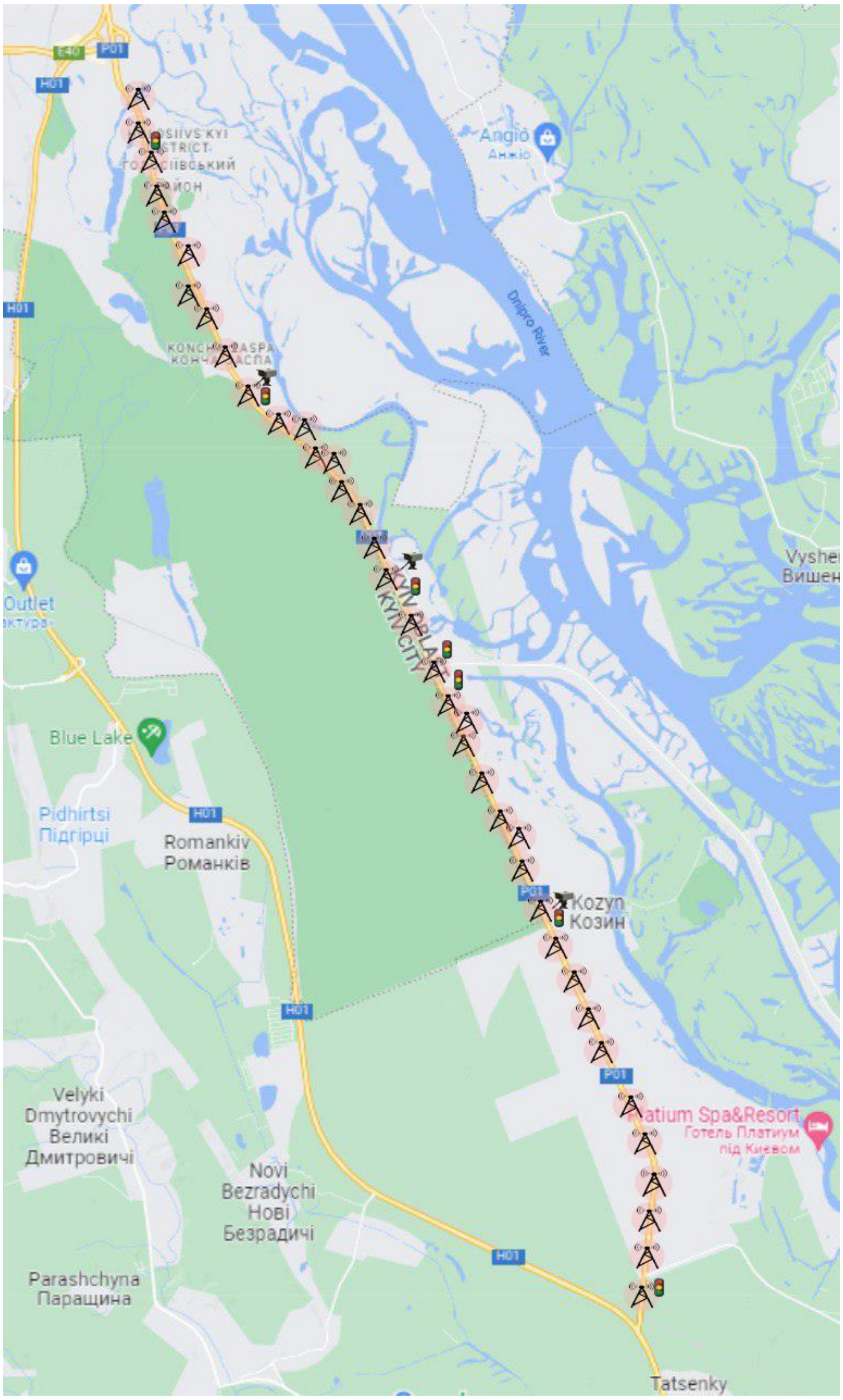

Figure 3.6. Territorial distribution and radius of base stations

CONCLUSIONS TO CHAPTER 3

In the third chapter, a model of the VANET network node was developed in the form of a queuing system for the cases of using the mode of simple broadcast distribution of messages over the network. The interaction model of VANET nodes can be represented as an open network of queuing systems, the aggregate flow in which obeys the Poisson distribution, provided that the network is stationary. It is shown that the stream entering the main buffer of the network node, obtained by the method of stochastic sieving in the filtering subsystem, is the simplest.

In addition, a method has also been developed for estimating the probabilistic characteristics of the transient distribution of broadcast messages over the VANET network.

CONCLUSIONS

In this diploma project one of the options for the organization of the automobile system VANET in Kyiv region was proposed. The general description and basic parameters of VANET technology are given.

A brief technical analysis of VANET network planning is presented, during which the optimal network design option was selected. A brief analysis of the location of base stations for full network coverage was also conducted.

The comparison of network systems with similar parameters is made, and the most optimal one for the required tasks is chosen. After comparing the three types, the VANET system was chosen for the area with a high building density.

The area covered by the base station of the three-sector site was calculated and the frequency-territorial division and situational location of eNB base stations for all types of terrain were depicted.

The Cambium cnPilot Outdoor E700 base station was selected and the approximate number of base stations on the P01 highway was calculated. The main purpose of the study was to ensure the safety of the road and the provision of other VANET services.

REFERENCES

1. https://ru.wikipedia.org/wiki/Сети_VANET
2. https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network
3. https://www.psuti.ru/sites/default/files/field/attachments/2018/10/yartsev_sv_diss.pdf
4. https://www.iec.ch/about/
5. Project COMeSafety. - http://www.ecomoveproject.eu/links/comesafety
6. Routing Protocol (OLSR) RFC 3626. Available: https://www.ietf.org/rfc/rfc3626.txt.
7. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. Available: http://www.rfc-base.org/rfc-4728.html.
8. The Network Simulator – ns-2. Available: http://www.isi.edu/nsnam/ns/
9. Anylogic - http://www.anylogic.ru.