

MINISTRY OF SCIENCE AND EDUCATION OF THE REPUBLIC OF
KAZAKHSTAN

Non-Profit Joint Stock Company
ALMATY UNIVERSITY OF POWER ENGINEERING AND
TELECOMMUNICATIONS

Department _____ Telecommunication networks and systems _____

«Admitted»

Head of the Department Baykenov A.S.
d.t.s., professor

(Surname and initials, degree, rank)

« _____ » 20 ____ y.
(sign)

DIPLOMA PROJECT

Theme: The model and strategy for building
software-defined networking SDN

Specialty: 5B071900 Radio engineering electronics and telecommunications

Implemented by: Shynbolatova D ICTe 14-9
(Student's surname and initials) group

Scientific Supervisor: Chezhimbayeva K.S.
(Surname and initials, degree, rank)
« 30 » 05 20 18 y.
(sign)

Advisors:
of Economy section: Turebayev B.I. docent
(Surname and initials, degree, rank)
« 30 » 05 20 18 y.
(sign)

of Life activity safety section: Beginbetova A.S. senior lecturer
(Surname and initials, degree, rank)
« 6 » June 20 18 y.
(sign)

of Computer Science section: Chezhimbayeva K.S.
(Surname and initials, degree, rank)
« 30 » 05 20 18 y.
(sign)

Standards compliance controller: Chezhimbayeva K.S.
(Surname and initials, degree, rank)
« 30 » 05 20 18 y.
(sign)

Reviewer: _____
(Surname and initials, degree, rank)
« _____ » 20 ____ y.
(sign)

Almaty 2018 y.

MINISTRY OF SCIENCE AND EDUCATION OF THE REPUBLIC OF
KAZAKHSTAN

Non-Profit Joint Stock Company
ALMATY UNIVERSITY OF POWER ENGINEERING AND
TELECOMMUNICATIONS

Institute of Space Engineering and Telecommunications (ISET)
Specialty: 5B071900 – Radio engineering electronics and telecommunications
Department: Telecommunication systems and networks

ASSIGNMENT

For diploma project implementation

Student: Shynbolatova Dinara Talgatovna
(name, patronymic and surname)

Theme: The model and strategy for building software-defined networking SDN

Approved by Rector order № 155 of « 23 » 10 20 17 y.

Deadline of completed project: « 25 » 05 20 18 y.

Initial data for project, required parameters of designing result, object initial data:

In this transport networks VANET, identified their main shortcomings. SDN VANET architecture has been developed for security purposes. The gain of the transmitter -15 dBm, Cable loss - 0,23 dB/m. Receiving antenna gain -24 dB, Receiver sensitivity - -85 dBm

List of questions for development in diploma project or brief content:

Introduction
Research of existing VANET Networks
The construction of the VANET with SDN
Simulation of VANET SDN
Calculation of capacity balance

SCHEDULE

of diploma project implementation

[illegible]

Assignment issue date « 3 » October 2018 y.

Head of Department: _____ Baykenov A.S
(sign) (Surname and initials)

Scientific Supervisor:  Chezhibayeva K.S
(sign) (Surname and initials)

Assignment submitted for implementation:

 (sign) Shynbolatova D.T (Surname and initials)






List of illustrations (with exact specifying of mandatory drawing):

Traditional VANET architecture
 Noise in VANET network
 Inefficient routing in VANET
 Architecture with central control
 Architecture with partial decentralization
 Hierarchical architecture
 Diagram of the SDN based on OpenFlow
 Model of the road network
 Comparison of protocols by data rate

Recommended main references:

1. ONF Solution Brief. OpenFlow - Enabled Mobile and Wireless Networks.
2. Software-Defined Networking: The New Norm for Networks.
3. Diego Kreutz, Fernando Ramos and Paulo Verissimo. Towards secure and dependable SDN
4. M. Mendonca, K. Obraczka, T. Turletti. The Case for SDN.

Project adviser with corresponding sections specifying:

Section	Advisor	Dates	Sign
Main part	Cherzhimbayeva K.S	12.01.18 - 30.05.18	
life safety	Begimbetova A.S	2.04 - 6.06.18	
Economic part	Tuzelbayev B.I		
Application of c.t	Cherzhimbayeva K.S	15.05 - 30.05.18	
Standard's comp. conf	Cherzhimbayeva K.S	15.05 - 30.05.18	

Аңдатпа

Бұл дипломдық жобада қазіргі қолданыстағы VANET транспорттық желілеріне талдау жүргізілді, олардың басты кемшіліктері анықталды. Қауіпсіздікті қамтамасыз ету мақсатында балама ретінде SDN VANET архитектурасы құрастырылды. SDN VANET жұмыс режимі ұсынылып, сондай-ақ, олардың артықшылықтары анықталды. VANET желілерінің симуляторы арқылы хаттамалардың маршруттау тиімділігін бағалау үшін модельдеу жүргізілді. Кең масштабты VANET желісі үшін ұсынылған архитектура нысаны жүзеге асырылды.

Жобаның техникалық-экономикалық негіздеулері жүргізілген және өмір қауіпсіздігінің қамтамасыз ету сұрақтары қарастырылған.

Аннотация

В данной дипломной работе проведен анализ существующих транспортных сетей VANET, выявлены их основные недостатки. В качестве альтернативы разработана архитектура SDN VANET в целях обеспечения безопасности. Предложены режимы работы сетей SDN VANET, а также выявлены их преимущества и предложены новые сервисы для них. Проведено моделирование в симуляторе VANET сетей для оценки эффективности протоколов маршрутизации. Реализованы предложенные варианты архитектуры для крупномасштабной VANET сети.

Предоставлено технико-экономическое обоснование и рассмотрены вопросы обеспечения безопасности жизнедеятельности.

Annotation

In this thesis the analysis of existing transport networks VANET, identified their main shortcomings. Alternatively, the SDN VANET architecture has been developed for security purposes. The modes of operation of SDN VANET networks are proposed, as well as their advantages are revealed and new services for them are offered. Simulation in the VANET network simulator to assess the effectiveness of routing protocols is carried out. The proposed architecture options for a large-scale VANET network are implemented.

Provided a feasibility study and considered the issues of life safety.

Content

Introduction	7
1 Research of Existing VANET Networks	8

1.1 The Classical Architecture of VANET	8
1.2 VANET routing protocols	9
1.3 Disadvantages of VANET networks	12
1.4 Simulation of networks of vehicles VANET	15
2 The construction of the VANET networking with SDN technology	21
2.1 Architecture of SDN VANET networks	21
2.2 SDN VANET Networks using OpenFlow Protocol	24
2.3 Advantages and New Services of SDN VANET Networks	31
2.4 Addressing the Issues Identified	32
3 Simulation of VANET networks	33
3.1 Comparison of VANET Routing Protocols	33
3.2 Comparison of VANET architectures, SDN	35
3.3 SDN VANET security	37
3.4 Organization of SDN VANET security policy	39
3.5 Network When Loss of Connectivity with the SDN Controller	39
3.6 Adaptive Transmission Distance	40
4 Calculation part	41
4.1 Calculation of losses in microwave communication system	41
4.2 Calculation of capacity balance	43
4.3 Calculation of Frenel zone	44
4.4 Coverage area calculation for the LTE	46
5 Life safety	49
5.1 Analysis of the company's environmental impact	49
5.2 Maximum permissible levels of human exposure to EMR	50
5.3 Analysis of the working conditions of technical staff	53
5.4 The choice of the lighting system of workplaces	55
5.5 Calculation of natural lighting	56
6 Business plan	57
6.1 Summary	57
6.2 Description of services	58
6.3 Analysis of sales market.	59
6.4 Management	59
6.5 Marketing Strategy	59
6.6 Financial plan	62
6.7 Labour intensity	64
6.8 Depreciation allocation	66
Definitions, symbols and abbreviations	67
Conclusion	68
List of references	69

Introduction

To date, most terrestrial mobile wireless networks have fixed infrastructure and are connected with different, as a rule, wired or wireless data transmission channels. Recently, close attention is paid to the development of dynamic radio networks that do not have a fixed infrastructure – a network of stationary (Ad Hoc) and mobile subscribers (MANET). Such networks are called self-organizing, as their nodes provide not only end user terminals, but also are 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. For example, MANET networks are useful in search and rescue operations, at the theater of military operations at the tactical level, in places of large gatherings of people (for example, to serve conference participants), and where there is no telecommunication infrastructure (for example, in expeditions to remote regions from "civilization"), VANET networks are in turn used to build automobile networks. There is a possibility that these networks in the future may in many cases become an alternative to mass mobile networks. Unlike networks with a hierarchical structure and centralized management, peer-to-peer networks without infrastructure consist of similar nodes, where each node has a set of software and hardware that allow you to organize the transfer of data from source to destination directly in the physical presence of such a path. Thus, the load on the network is distributed and the total network bandwidth is increased. Data transfer from one subscriber to another can occur even if these nodes are out of the direct radio visibility zone. In such cases, subscriber data packets are relayed by other network nodes that communicate with the corresponding subscribers. Network with multiple retransmissions are referred to as multi-span or multi-jump (multihop). When developing such networks, the main problems are routing packets from the source node to the destination node, network scalability, addressing of end devices, maintaining connectivity in variable topology [1].

This work is relevant, as there is a need to create transport networks in order to improve the safety and comfort of motorists, while the known solutions are not effective. The novelty of the work is due to the fact that the VANET network of vehicles is little studied in the domestic science, and the paper proposes a new way to control the network of this type. The field of application of the study – communication systems of vehicles and similar moving networks.

Goal – to improve the security of the networks of vehicles with technology SDN. To achieve this goal in the work following tasks are solved:

- study of the existing VANET networking;
- architecture development SDN VANET;
- implementation of SDN control in VANET network, providing improved network throughput, fault tolerance, and implementation of security policies;

- implementation of P2P connections, including with your own home through the road network and NGN network. Useful information can also be from the roadside network of hotels, gas stations, menus in restaurants and so on.

1 Research of Existing VANET Networks

VANET (Vehicular Ad hoc Network) networks are radio networks with random mobile subscribers that implement fully decentralized management in the absence of base stations or support nodes. Topology-rapidly changing with a random connection of nodes. The objective of VANET's transport networks is to create a network interface in the vehicle that would allow support for four groups of connections: vehicle — to — vehicle (V2V), vehicle — to — infrastructure network (V2I), vehicle-to-housing, infrastructure network-to-housing (I2H). At the same time, there are two groups of services: security and comfort services. The architecture of the VANET network implies the interaction of the car with other cars and with the road network [3].

In the field of safety, the following three groups of services can be identified:

- assistance to the driver (navigation, detour of mass collisions, change of road markings);
- information support of the driver (speed mode, information on road works);
- Warning alarm (emergency situations, obstacles or events, adverse road conditions).

In terms of navigation, VANET networks can provide information not only about the location of their vehicle, using GPS / GLONASS, but also any other vehicle, as well as about traffic jams, including their numerical estimates.

In the area affecting the provision of increased comfort, the following services can be identified: the creation of groups of interest POI (Points of Interest) in local traffic jams, obtaining information about the current traffic on the roads, the weather, the availability of the possibility of receiving messages and so on. It is also possible to implement P2P connections, including with your own home through the road network and NGN network. Useful information can also be from the roadside network of hotels, gas stations, menus in restaurants and so on.

1.1 The Classical Architecture of VANET

VANET (Vehicular Ad hoc Network) — wireless decentralized self-organizing networks consisting of transport devices. Each such device can move independently in any direction, and, as a result, often break and establish connections with neighbors. This diagram (figure 1) shows the traditional architecture of VANET networks:

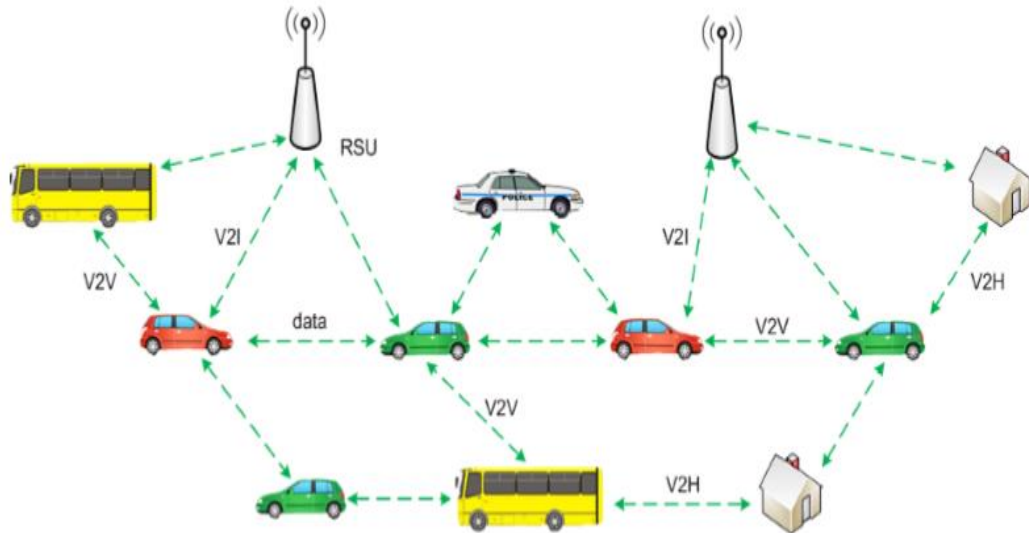


Figure 1-traditional VANET network architecture

An important feature of VANET networks is maximum decentralization, when there is no dedicated server in the network, and the entire infrastructure is distributed among communication nodes. This feature provokes the emergence of a large number of significant shortcomings that prevent the introduction of this technology.

1.2 VANET routing protocols

Feature dynamic topology makes the design of efficient routing protocols for VANET challenging. Existing VANET routing protocols can be divided into two categories: routing topology and geolocation-based routing protocols.

Proactive or tabular (eng. proactive, table-driven) protocols periodically send service messages over the network with information about all changes in the topology. As a result, each node of the network based on this information builds routes to all nodes and stores them in the routing table, where they are then read if necessary to send a message to any recipient.

Reactive or on-demand protocols-nodes do not store the necessary routing information all the time. The node initiates routing on demand, at the time of the request for data transfer. This route-building mechanism is based on a flood algorithm, the node simply passes the first packet to all its neighbors, and the intermediate nodes forward it further to their neighbors. These recurring actions allow you to deliver a package to its destination.

Typically, when a packet passes, it remembers the route (for example, as a list of nodes involved) and then, when subsequent packets are sent, this information is used to select the direction.

The classification of VANET routing protocols is shown in figure 2:

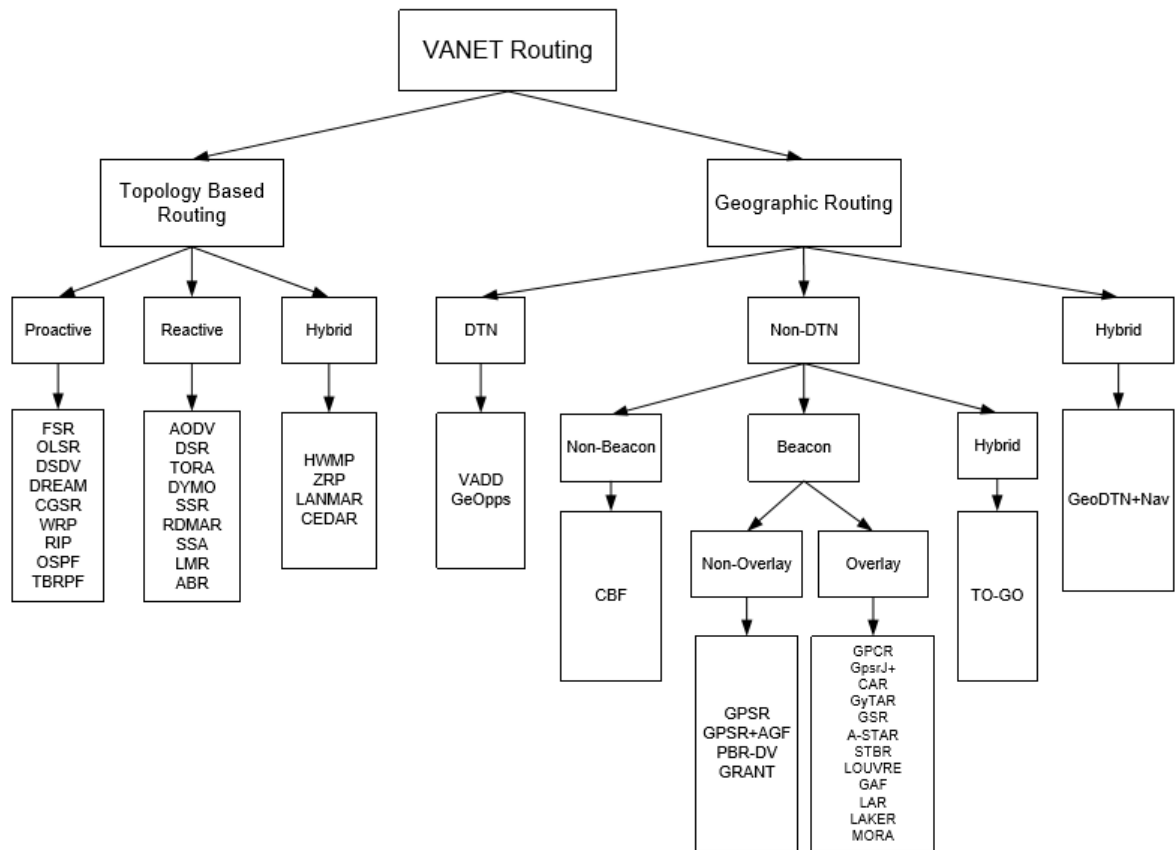


Figure 2-classification of VANET routing protocols

Hybrid protocols are a combination of reactive and proactive approaches. They take advantage of these two protocols and, as a result, work quite effectively in individual cases. As a rule, they divide the network into many subnets, within which a proactive Protocol operates, and the interaction between them is carried out by reactive methods. In large networks, this can reduce the size of the routing tables that are driven by the network nodes, because they need to know the exact routes only for the subnet nodes to which they belong. Geographic protocols use data on the geographical location of nodes, usually obtained through satellite navigation, to predict the possibility or impossibility of communication between individual nodes and possible routes in the network. Table 1 shows the routing comparison in the VANET network:

Table 1-comparison of routing approaches

Characteristic	Reactive	Proactive	Hybrid
Route structure	Flat	Flat / hierarchical	Hierarchical
Routing overhead	Low	High	Average
Delay	High	Low	Inside the area low
Scalability	Designed for a small network, up to 100 nodes	More than 100 nodes	Designed for large network, >1000 nodes

Table 1 continue

Characteristic	Reactive	Proactive	Hybrid
Periodic update	NO	Yes	Inside the zone, Yes
Mobility support	Route maintenance	Periodic update	Combination of both
Availability of information	Available if necessary	Always available	Combination of both
Traffic control	Low	High	Very low
Storage requirements	Low	High	Depending on the size of the zone

Since it is not correct to compare geographical routing with other types of routing, the most common protocols of geographical routing are placed separately in table 2:

Table 2 – Comparison of geographical routing protocols

Characteristic	GPSR	GSR	A-STAR
Ratio of delivered packets	Low	High	Average
Scenario	Highway	City	Adjacent

There are many VANET routing protocols. Most of them are designed to operate under certain conditions or to solve a specific problem, that is, today there is no universal routing Protocol. Preference to one or another type of protocols can be given only taking into account the situation and the speed of the subscribers. For example, the use of reactive protocols will be most effective in small automotive networks (up to 100 nodes) with high mobility due to the absence of constant flooding of the network with beacons. Among the protocols of reactive routing, the most universal can be considered the protocols AODV and DSR, both protocols are characterized by a low load on the network, but with high mobility, the performance of the Protocol DSR deteriorates. The rest of the reactive routing protocols are either modifications of AODV and DSR or developed for a specific scenario of urban traffic. Proactive protocols are characterized by minimal time delays, nodes constantly exchange messages among themselves, because of this, the network is flooded with service information, reduced bandwidth. OLSR and DSDV have the best performance among proactive protocols, when they are used, the number of retransmissions of packets is significantly reduced, the connection delay is reduced, there is no need to open the route. The implementation of loop protection also makes the use of these protocols appropriate in large and dense networks with low mobility. Proactive protocols FSR, DREAM, RIP, etc. have a lower speed compared

to the previously discussed and require more bandwidth. WRP is superior to DSDV in many ways, but the complexity of maintaining multiple tables requires more memory and more computing power from the nodes, and limited scalability makes it inefficient in large networks. Hybrid protocols HWMP and ZRP use proactive and reactive routing and are designed for large urban networks, which are divided into zones. In the development of these protocols were taken into account all the advantages of reactive and proactive protocols. This reduced the amount of service information sent over the network, as the main part of it is distributed only within subnets, which was a serious problem in the protocols of practical routing. However, there are still shortcomings inherited from the reactive protocols, for example, when the route goes beyond the zone of the initiating packet, time delays significantly increase. In addition, it should be noted that the size of the zone in these protocols is fixed, and after implementation can not change. Geographical protocols based on the knowledge of the location of the nodes can be used in networks with high mobility. The DTN-based VADD Protocol demonstrates a high percentage of packet delivery even with a large number of transit sections, but it is sensitive to changes in network density that result in increased time delays. The GPSR Protocol, which uses periodic hello messaging, is effective in highway conditions where nodes move in the same direction. An overlay network that uses the GSR Protocol is useful in an urban network with dense traffic, where there are enough nodes to send packets. The GSR packet delivery rate is better than AODV and DSR, and GSR is better scalable. The main drawback of the protocols based on geographical routing is the dependence on GPS navigation, so when moving in the tunnel, the implementation of package delivery significantly worsens. Thus, there is a problem of the General capacity of networks and efficiency of the applied routing methods.

1.3 Disadvantages of VANET networks

Traditional VANET networks are characterized by maximum decentralization, when there is no dedicated server in the network, and the entire infrastructure is distributed among the communication nodes. This feature provokes the following disadvantages:

- low mobilization capacity;
- long reaction time of the system to external influences.

Today, VANETs supports a large number of new services and protocols. However, there are still a number of problems that prevent the full implementation of this technology in life.

1.3.1 The problem of noise immunity. For transport networks VANET peculiar to a large number of different types of noise. The maximum reduction of interference can be achieved by selecting the optimal channel frequency or by regulating the power of receivers and transmitters in the network, but in classical VANET networks this problem remains unresolved and has a significant impact on the functioning of the network. Figure 3 shows the VANET network, the red

rectangle indicates the relationship between the nodes, on the way experiencing interference:

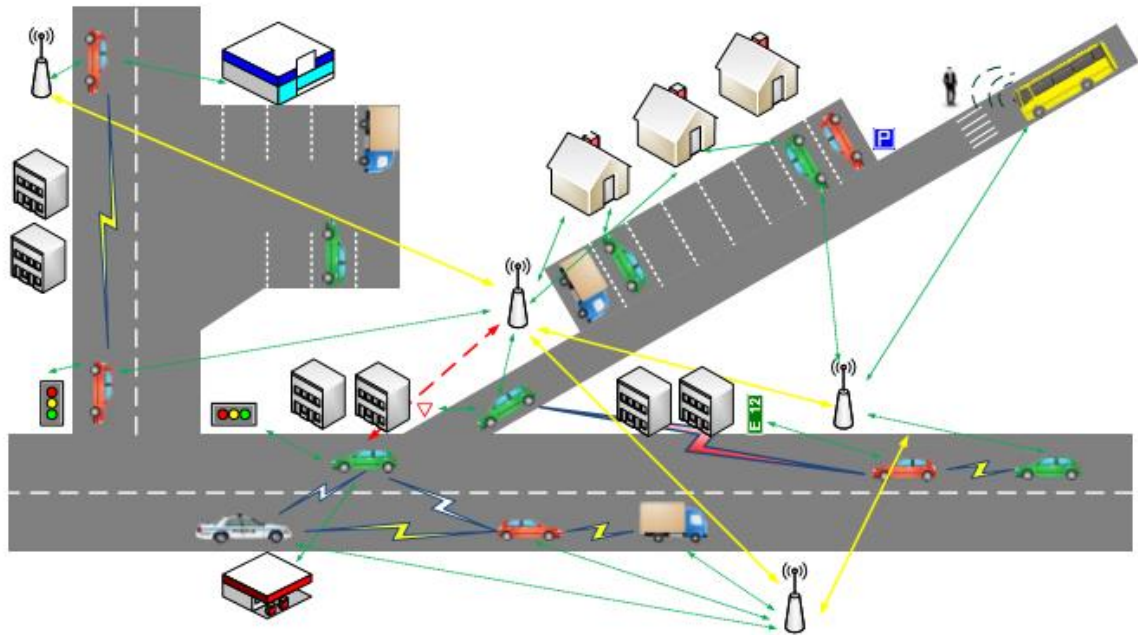


Figure 3 - Noise In VANET networks

1.3.2 Problem of security of transmitted data. The causes of problems related to information security of VANET transport networks are:

- lack of tools to protect nodes from intruders;
- ability to listen to channels and message spoofing due to the General availability of the transmission medium;
- impossibility to use the classical security system due to the features of the classical architecture of VANET networks; * the need to use complex routing algorithms that take into account the probability of incorrect information from compromised nodes as a result of changes in the network topology;
- any node within the range of the signal source that knows the transmission frequency and other physical parameters (modulation, encoding algorithm) can potentially intercept and decode the signal. In this case, neither the source nor the receiver will know about it;
- impossibility to implement the security policy due to the features of the classical architecture of VANET networks, such as the lack of a fixed topology and Central nodes;

Thus, it can be noted that self-organizing VANET networks are vulnerable to the classic types of attacks inherent in most wireless networks, and have their own distinctive vulnerabilities. Since wireless self-organizing networks do not have a fixed topology, Central nodes, broadband channel, stable power sources, constant communication of nodes, the implementation of a successful attack by an attacker

becomes easily feasible. Attacks in VANET transport networks can be divided into passive and active.

In passive attacks, an attacker is usually hidden and connects to communication lines to collect certain data. Passive attacks can be divided into two classes:

- interception (sniffing);
- traffic analysis.

In case of active attacks, the attacker has a direct impact on the operation of the system occurring in the attacked network. The obvious difference between active and passive impact is the principal possibility of its detection, as a result of its implementation in the system there are some changes. Active attacks can be classified into the following groups:

- physical;
- falsification (spoofing), replay, and modify messages;
- denial of service.

As an example, figure 4 shows the Man-on-the-Middle attack on the VANET network. Two cars exchange messages. An attacker on the same network wants to intercept messages between these nodes. During an ARP-spoofing attack, an attacker sends two ARP responses (without prompting) to the cars. As the car spontaneous ARP support, then, after receiving an ARP response, they alter your ARP tables. Thus, the ARP-spoofing attack is executed, and now all packets between cars pass through the malefactor.

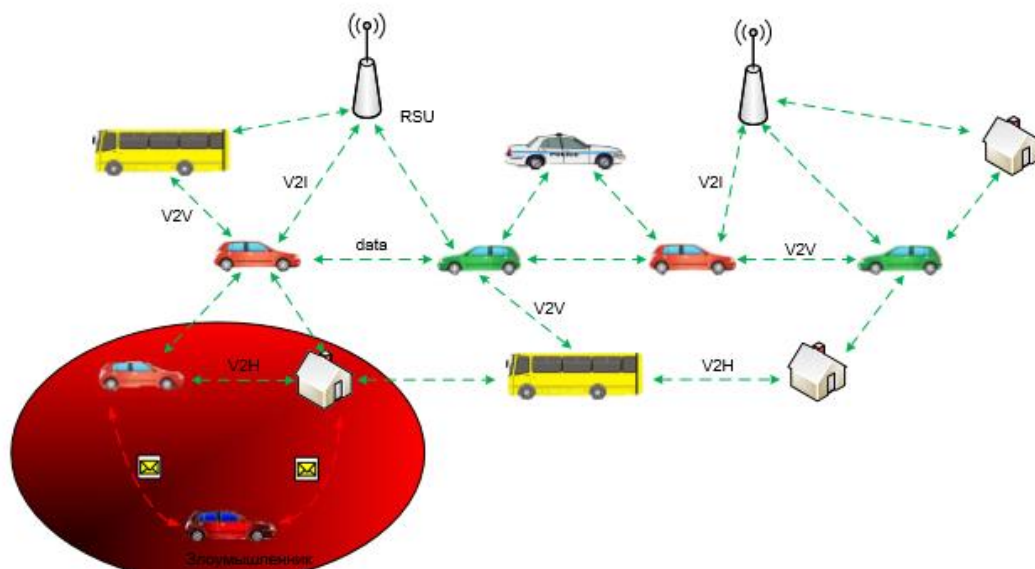


Figure 4-Man-on-the-Middle Attack on VANET network

1.3.3 The Problem of efficient routing. In VANET networks, the problem of bandwidth is most acute when a large amount of video information is transmitted at the same time. The situation is exacerbated by the inefficiency of routing methods when the network is overflowing with broadcast requests or a "bottleneck" is formed.

An example of inefficient routing is shown in figure 5 when all traffic passes through a single node:

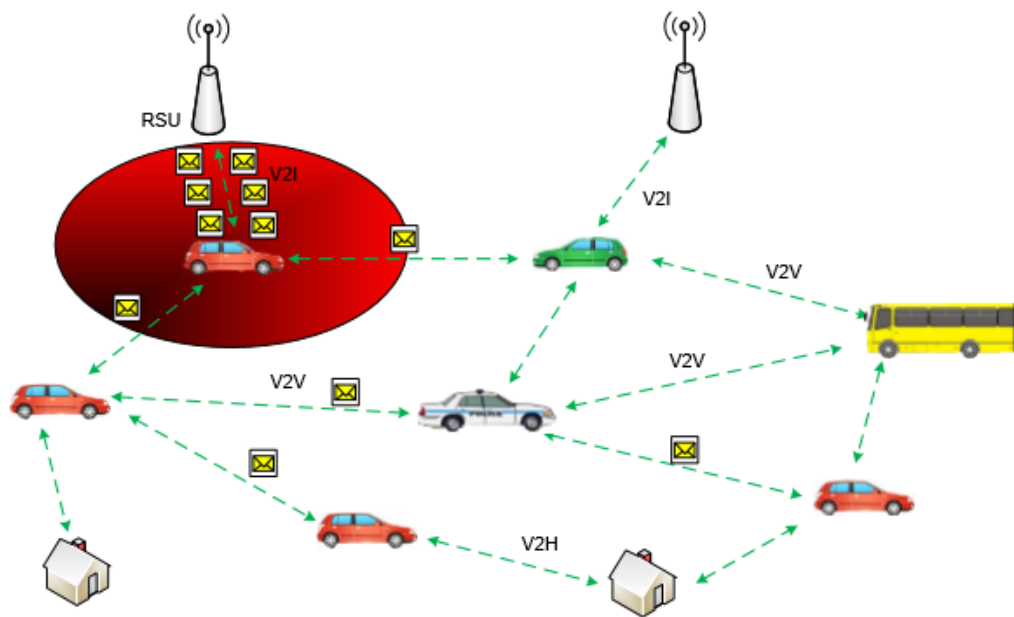


Figure 5-Inefficient routing in a VANET network

1.4 Simulation of networks of vehicles VANET

VANET deployment and testing involves a high cost. Therefore, simulation is a good alternative to actual implementation. VANET modeling is often associated with large and heterogeneous scenarios. Compared to MANET networks, some specific characteristics found in the automotive environment should be considered when modeling VANET. In addition, mobility models can have a significant impact on simulation results. For the results to be useful, it is important that the modelled model be as close to reality as possible. Model for MANETs, the random waypoint is the most popular mobility model, however, the transport network nodes (vehicles) can only move through the streets, which leads to the necessity of using a road model. Another important aspect in VANET is that the nodes do not move independently, they move in accordance with the established models of vehicles. Moreover, the speed of these nodes is different: in MANET networks, the speed of nodes ranges from 0 to 5 meters per second, while in VANET networks the speed ranges from 0 to 40 meters per second.

1.4.1 Requirements for the simulator. The VANET network simulator must meet all of the following requirements:

- realistic movement of vehicles must be simulated
- it should be possible to set your own city map (either from a file or build manually);
- must be visualizing the movement of vehicles throughout the simulation;
- it should be possible to add base stations and roadside network nodes;

- radius of data transmission should be displayed for cars, base stations, roadside units;
- it should be possible to change the speed of data transmission in cars;
- the packet rate and the percentage of packets delivered should be displayed;
- it should be possible to establish a safety policy for road users (access differentiation, priority setting).);
- vehicle traffic and data rates should be linked.

1.4.2 Comparison of VANET simulators. This section covers the public VANET simulators that are currently in use and whose source code is publicly available. Figure 6 shows the classification of VANET modeling software. The software was divided into 3 categories:

- vehicle traffic generators;
- network simulators;
- VANET simulators.

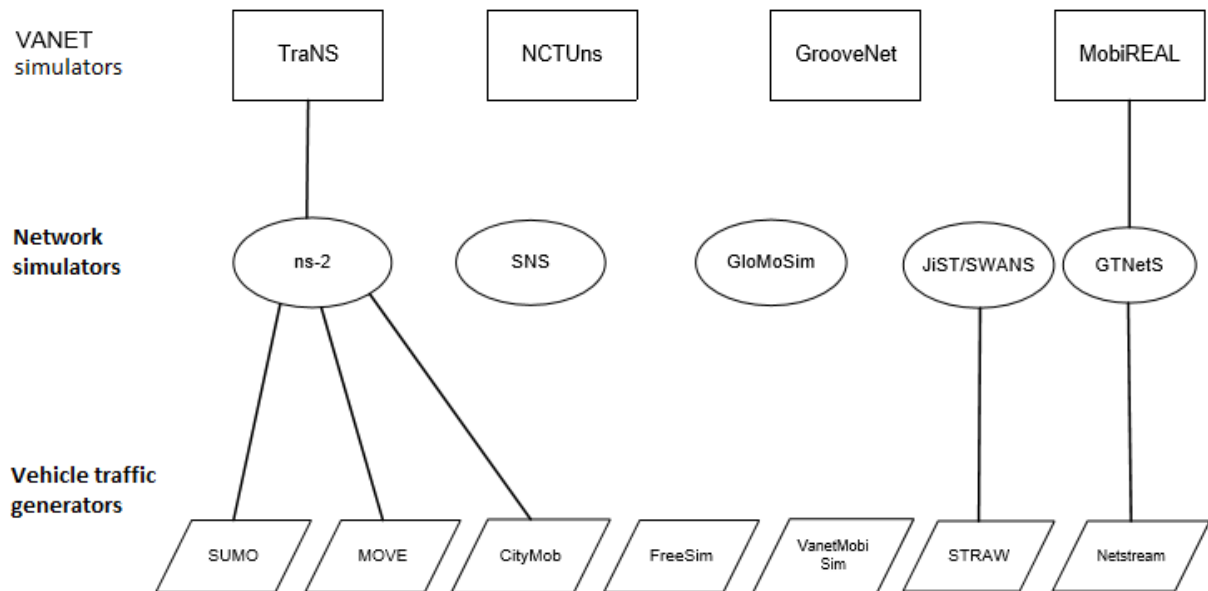


Figure 6– Classification of software

Vehicle motion generators are needed to increase the level of realism in VANET network modeling. They create realistic car traffic that can be used at the entrance of the network simulator. The input data of the vehicle traffic generators are the road model, the scenario parameters (i.e. the maximum speed of the vehicles, the direction of their movement).

The output is information about the exact location of each vehicle at each time during the entire simulation period, as well as profiles of vehicle mobility. Network simulators allow detailed modeling at the data package level. The output of the network simulators are receiving the sender and receiver addresses, sending and receiving data packets, information about the background load, routes, connections, and channels. Most existing network simulators are designed for

MANET networks and therefore require VANET expansion before they can be used to simulate automotive networks, so they are used in conjunction with vehicle traffic generators.

VANET simulators provide both simulation of traffic flows and simulation at the data package level. Can be a combination of existing vehicle traffic generators and network simulators. Table 3 shows a comparison of simulators, the main function of which is the generation of vehicle traffic:

Table 3 - Comparison of traffic simulators

	VanetSim	SUMO	MOVE	STRAW	FreeSim	CityMob
SOFTWARE						
Portability	+	+	+	+	+	+
Free	+	+	+	+	+	+
Open Ref. code	+	+	+	+	+	+
Console	+	+	+	-	-	+
GUI	+	+	+	+	+	+
Available examples	+	+	+	-	+	-
Further development	-	+	-	-	-	+
Complexity of installation	medium	medium	easy	medium	easy	easy
Complexity of use	medium	hard	medium	medium	easy	easy
Maps						
Real	+	+	+	+	+	-
User-defined	+	+	+	-	-	-
Random	+	+	+	-	-	+
Traffic						
Random arrangement	+	+	+	-	-	+
Multi-lane roads	+	+	+	+	-	+
The choice of type of road	+	+	+	+	-	+
The choice of the direction of movement	+	+	+	+	-	+
Speed limit	+	+	+	+	+	+
Road sign	+	+	+	+	-	+
Traffic lights	+	+	+	-	-	-
Overtaking conditions	+	-	-	-	-	-

Table 3 continue

	VanetSim	SUMO	MOVE	STRAW	FreeSim	CityMob
Different types of vehicles	-	+	+	-	-	+
Different types of connections	+	+	+	-	-	-
Route calculation	+	+	+	+	+	-
Trace						
Ns-3 support	-	+	+	-	-	+
GloMoSim Support	+	-	+	-	-	-
QualNet Support	+	-	+	-	-	-
Support SWANS	-	-	-	+	-	-
Support for XML-based	+	-	-	-	-	-
Import various formats	+	+	+	-	-	-

Table 4 shows a comparison of network simulators that allow detailed simulation at the data package level:

Table 4 - Comparison of network simulators

	ns-3	GloMoSim	JiST/SWANS	SNS
SOFTWARE				
Console	+	+	+	+
GUI	+	+	+	+
Available examples	+	+	+	+
Further development	+	-	+	-
Large network	-	+	+	+
Scalability	Low	High	High	High
Complexity of installation	Low	Medium	High	Low
Complexity of use	High	High	High	High

Table 5 shows a comparison of the previously considered VANET simulators:

Table 5 - Comparison of VANET simulators

	TraNS	GrooveNet	NTCUns	MobiReal
Vehicle traffic generator	SUMO	GrooveNet	NTCUns	MobiReal
Network simulation	ns-3	-	-	-
Motion models	Random and user-defined routes	Random route points and specified in the format: start point-destination point	Random and user-defined routes	Based on established rules
Speed simulation	Streets at a given speed	Uniform, street speed	Random	Streets at a given speed
Traffic simulation	Using the DUA approach	Following the car	Following the car	Following the car
Road topology	Any	Any	User selectable	Any
Traffic lights	Added manually	Added manually	Automatically added to each intersection	Added manually
Simulation of intersections	The car on the right has the advantage	Regulated by traffic lights	Regulated by traffic lights	The car on the right has the advantage or Regulated by traffic lights
Route modeling	Random or manually selected	Dijkstra's algorithm is used	Random or manually selected	Random or manually selected
Support for VANET	802.11 p two ready-to-use VANET applications: road hazard warning and dynamic route change	Support for V2V and V2i communication of several types of messages	802.11 p, supports multiple interfaces, agents monitor driving behavior	-

Table 5 continue

	TraNS	GrooveNet	NTCUns	MobiReal
Topology	Google maps, with the ability to zoom	with the ability to scale	with the ability to scale	with the ability to scale
Input parameter	File with a map of the streets, a script file of the movement, graphical input	File with a map of the streets, a script file of the movement, graphical input	A file with the topology, a graphical input	File with a map of the streets, the model of motion, file with the traffic density and routes graphical input
Output parameter	ns-3 trace,.kmz file (Google Maps)	Simulation file and simulation animation	Simulation file and simulation animation	Simulation file and simulation animation
Comments	Combines the car motion generator and network simulator. The exchange of information in communication protocols can affect the behavior of the vehicle on the road	Capable of supporting hybrid simulation (i.e. communication between simulated vehicles and real vehicles on the road)	Supports the integration of simulation and modeling. This requires a minimum of 9 operating systems.	Simulates realistic movement of people and cars, and their behavior can be changed depending on the application context

After reviewing all the available VANET simulators, it can be concluded that today there is no such simulator that would meet all the requirements. Depending on the purpose of the simulation, you can choose one or the other SOFTWARE. If it is necessary to simulate the most realistic and visual movement of cars, it is most advisable to use SUMO, if necessary, to simulate the process of data transmission when moving nodes, use NS-3.

2 The construction of the VANET networking with SDN technology

To solve the problems of traditional VANET networks discussed in the previous Chapter, it was proposed to use the SDN technology.

The flexibility of SDN makes THIS approach attractive to meet the requirements of building an efficient VANET network. Application of SDN principles will bring programmability and flexibility, which are not enough in modern transport networks. Also, the use of SDN will allow to achieve simultaneous simplification of network management and provision of new V2V and V2I services. In addition, the use of software-defined network allows you to increase the level of security.

2.1 Architecture of SDN VANET networks

Was developed 3 options for the architecture of VANET networks using the technology of SDN: 1) Architecture c Central management server critical security tasks (figure 7):

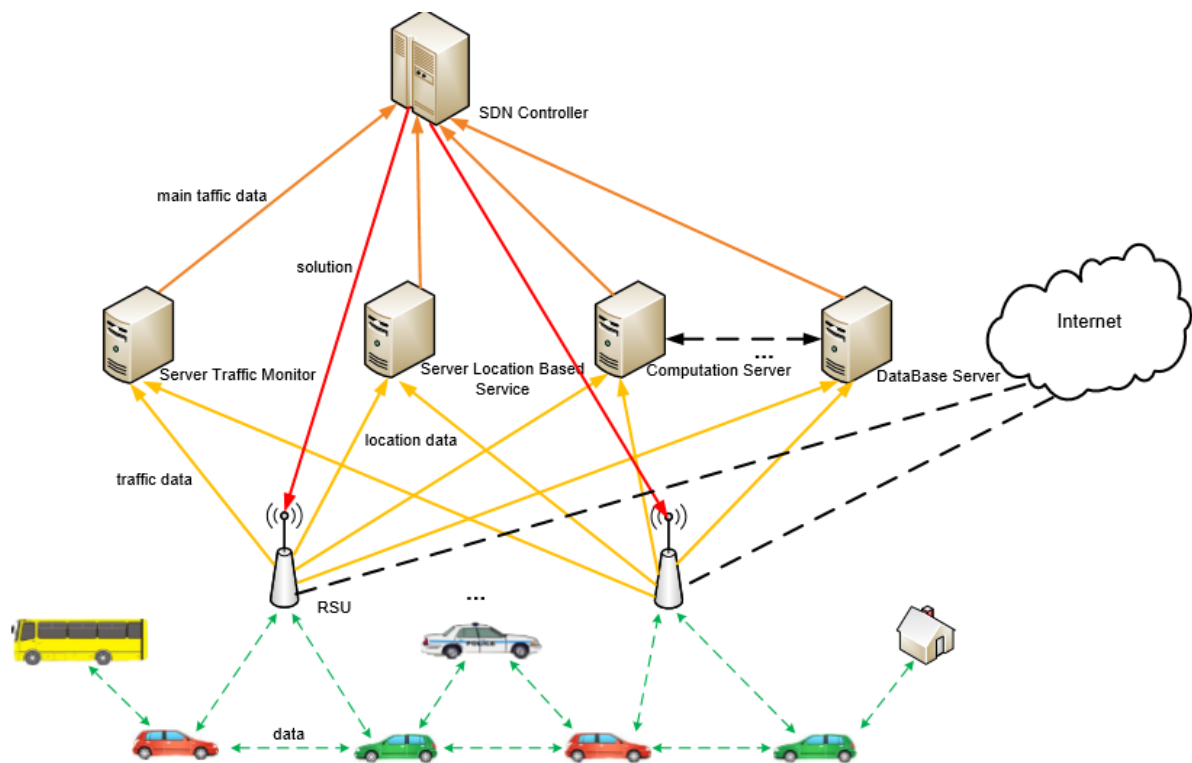


Figure 7-Architecture with Central control and servers

The architecture consists of:

- software-defined controller (SDN Controller): the logical Central intelligence SDN that controls the network behavior of the entire VANET system. The controller gets processed by the server information, and based on the data sets

the rules, defines the routing related parameters, decides on the increase or decrease in the power of the transmitters to specific nodes in the network, etc.;

- server: the device that performs the collection of certain information about the network, performing an analysis of the information received. The results of the analysis are processed and then sent to the software-configured controller. The servers may contain various traffic analyzers, services responsible for processing the geolocation of end users, databases containing information about the traffic situation, cars and their owners. In addition, there is a calculation server that calculates the speed of the car, the distance, the assessment of the road situation. In this VANET architecture, the server networks can be linked. For example, a calculation server is associated with a database that is constantly updated and uses the knowledge stored in the database to perform subsequent calculations;

- roadside network node (RSU): devices deployed along the road connecting end-users, road users, with servers and a software-defined controller, also providing access to the Internet. The node can be a router, bridge, access point and the client;

- end users of the VANET network, road users and the infrastructure of the city: cars, smart home, DPS.

2) Architecture with partial decentralization (figure 8):

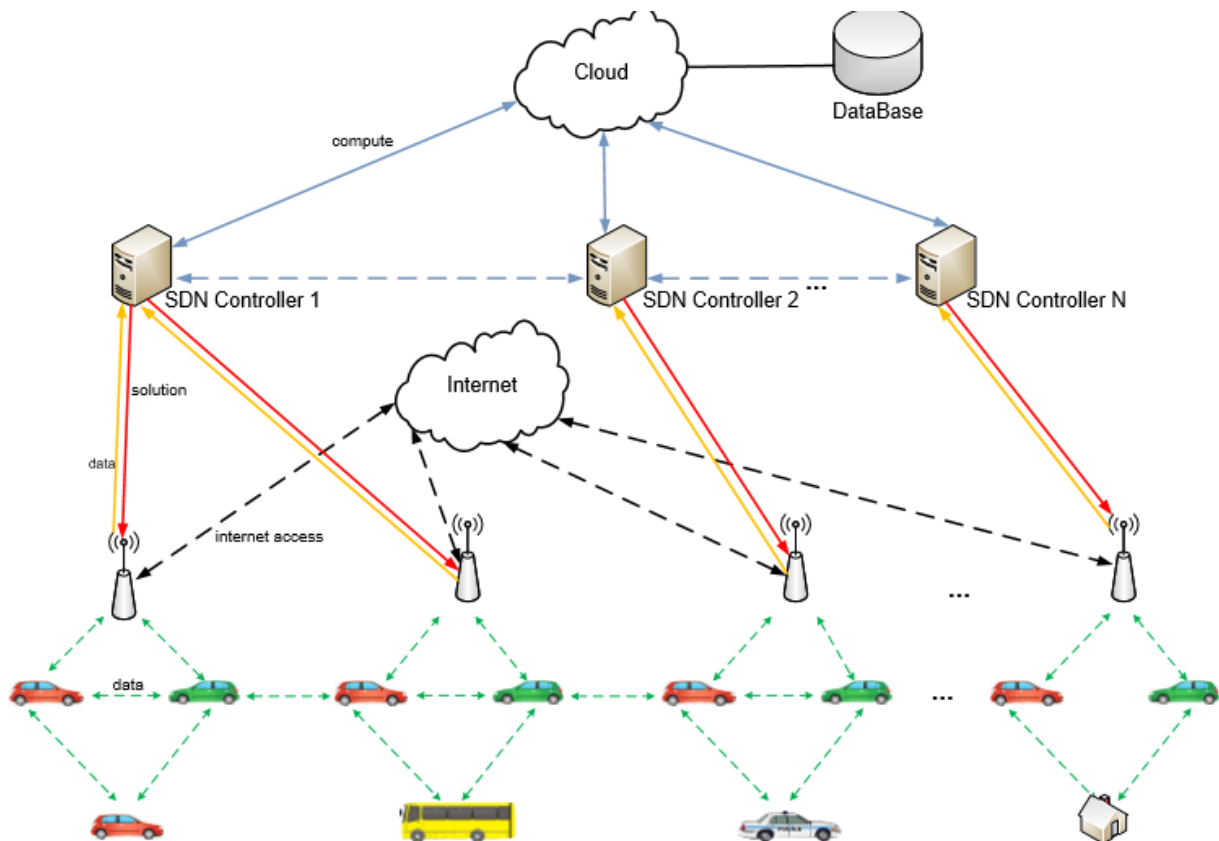


Figure 8-Architecture with partial decentralization

The structure of the architecture includes:

- cloud: there are various calculations such as the calculation of the speed of the car, the distance, the assessment of the road situation. Cloud computing is connected to a database that is constantly updated, and uses the knowledge stored in the database to perform calculations;
- database: a database that stores information about the traffic situation, cars and their owners;
- software-configurable controller (SDN Controller): logical Central intelligence SDN, managing the behavior of a single part of the VANET network. Each controller collects network information and analyzes the data. Controllers can exchange the received data among themselves, and use the cloud to perform calculations. Based on the processed information, the controllers establish the necessary security policy rules, determine the routing parameters within their area of responsibility in the VANET network;
- roadside network node (RSU): devices deployed along the road connecting end-users, road users, with software-configurable controllers, also providing access to the Internet. The node can be a router, bridge, access point and the client;
- end users of the VANET network, road users and the infrastructure of the city: cars, smart home, DPS.

3) Hierarchical architecture (figure 9):

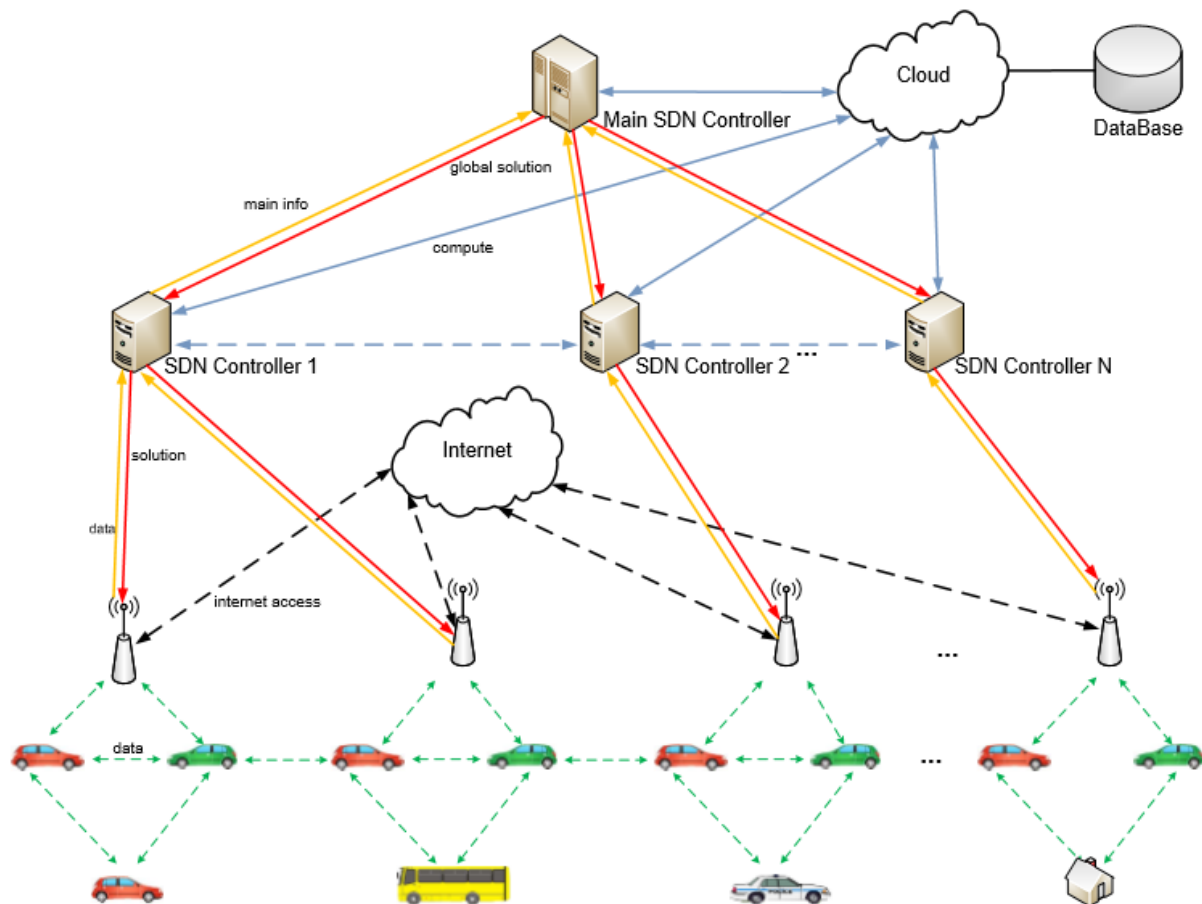


Figure 9-Hierarchical architecture

A part of the architecture includes:

- Central software-defined controller (Main Controller SDN): the Central controller sends policy rules to the controllers carries out the division of the VANET network on the area of responsibility. Thus, the Central controller SDN has a complete picture of the state of the entire VANET network, which allows it to instruct controllers, for example, to launch a specific routing Protocol with certain parameters;
- cloud: various calculations such as the calculation of the speed of the car, the distance, the assessment of the road situation. Cloud computing connected to a database that is constantly updated and uses the knowledge stored in the database to perform calculations;
- database: a database that stores information about the road situation, cars and their owners;
- software-configured controller (SDN Controller): the logical intelligence SDN, which controls the behavior of a single part of the VANET network. Each controller collects network information and analyzes the data. Controllers can exchange the received data among themselves, and use the cloud to perform calculations. Based on the processed information, the controller installs the appropriate rules of the security policy, determines the parameters of the routing within its area of responsibility in the network VANET;
- roadside network unit (PSU) deployed along the road device that connects end-user, road users, with software-defined controllers, also allowing access nodes to the Internet. The NMC can be a router, a bridge, an access point, and a client;
- end users of the VANET network, road users and the infrastructure of the city: cars, smart home, DPS.

2.2 SDN VANET Networks using OpenFlow Protocol

The OpenFlow Protocol was born in 2008, as a result of the collective scientific work of professors and their research teams from different universities in the United States. The birth of the Protocol occurred almost simultaneously with the birth of the SDN paradigm. In describing the principles of OpenFlow, it is assumed that all modern switches use switching tables built on the basis of CAM-tables to transmit packets at the speed of the environment. The same principle is used in the construction of tables for most other network technologies, such as NAT, QoS, various firewalls, etc. the work of the OpenFlow switch is entirely based on the principle described above. The use of OpenFlow Protocol makes it possible to program flow tables (switching) on a large number of different devices. OpenFlow implements the concept of separation of data transfer control planes (OpenFlow-controller) and directly the transmission itself (Openflow switch)[2]. Figure 10 shows a set of hardware and software tools that support or can participate in building an SDN network using OpenFlow. The main roles are assigned to OpenFlow switches and controllers. To help developers and researchers are also

available already written applications that implement a particular functionality of the network, and tools for debugging and monitoring.

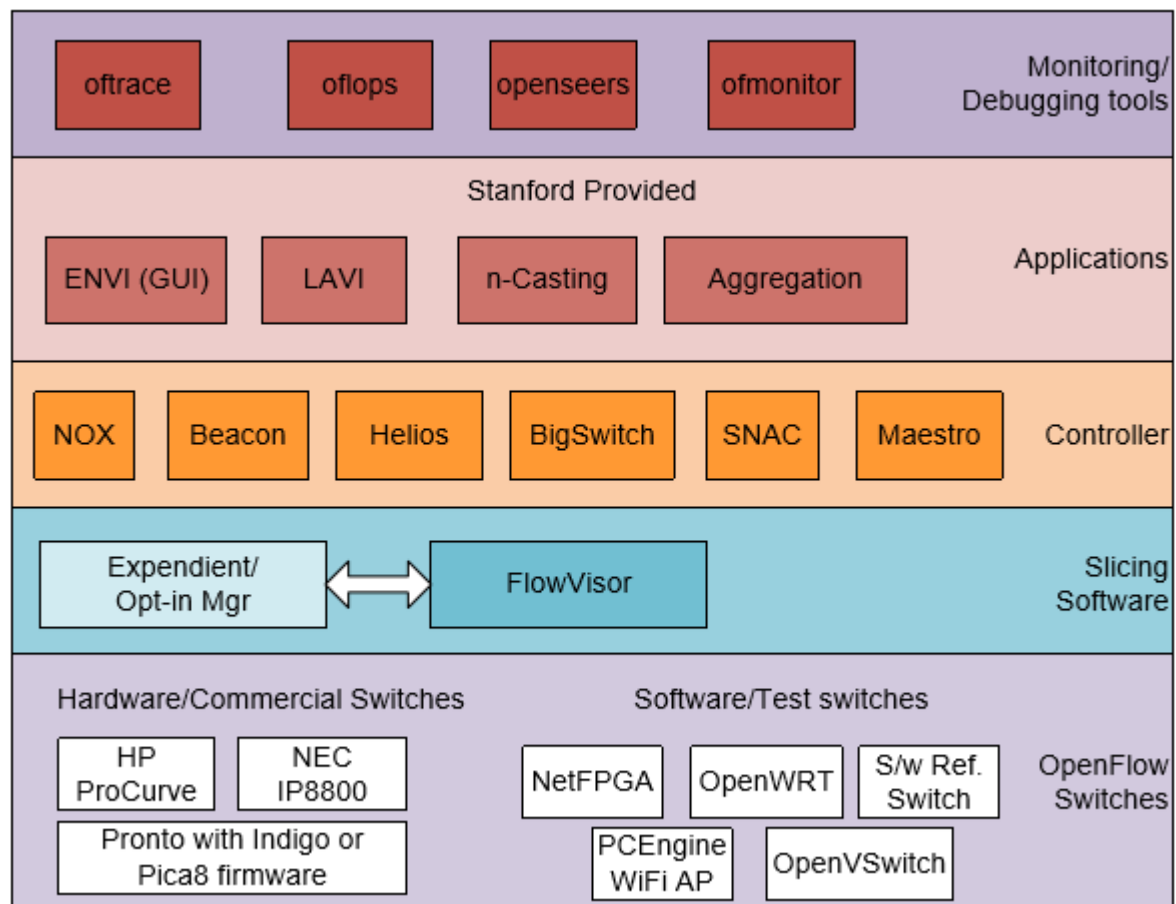


Figure 10 – a Set of hardware and software SDN and OpenFlow

The main components of software-configured networks based on the OpenFlow Protocol are (figure 11):

- OpenFlow switch;
- controller;
- secure channel through which the controller and switch interact. As a rule, TLS is used to protect the transmitted messages, however, it is possible to transfer over standard TCP without encryption.

The network operating system (or controller) within the framework of the OpenFlow concept is the main, Central part of software-defined networks (SDN), in which all the functionality for SDN networks management is concentrated. The operating system does not manage the network itself, but only provides a software interface (API) to manage it. Thus, the actual solution of network management tasks is performed using applications implemented on the basis of the API of the network operating system. It should be noted that the program interface should be General enough to support a sufficiently wide range of applications to solve network management problems. In contrast to the traditional interpretation of the term NOS (Network operating System) as an operating system integrated with a stack of

network protocols, in this case, the NOS is understood as a software system that provides monitoring, access, management, resources of the entire network, and not a specific node. NOS generates data about the status of all network resources and provides access to them for management applications.

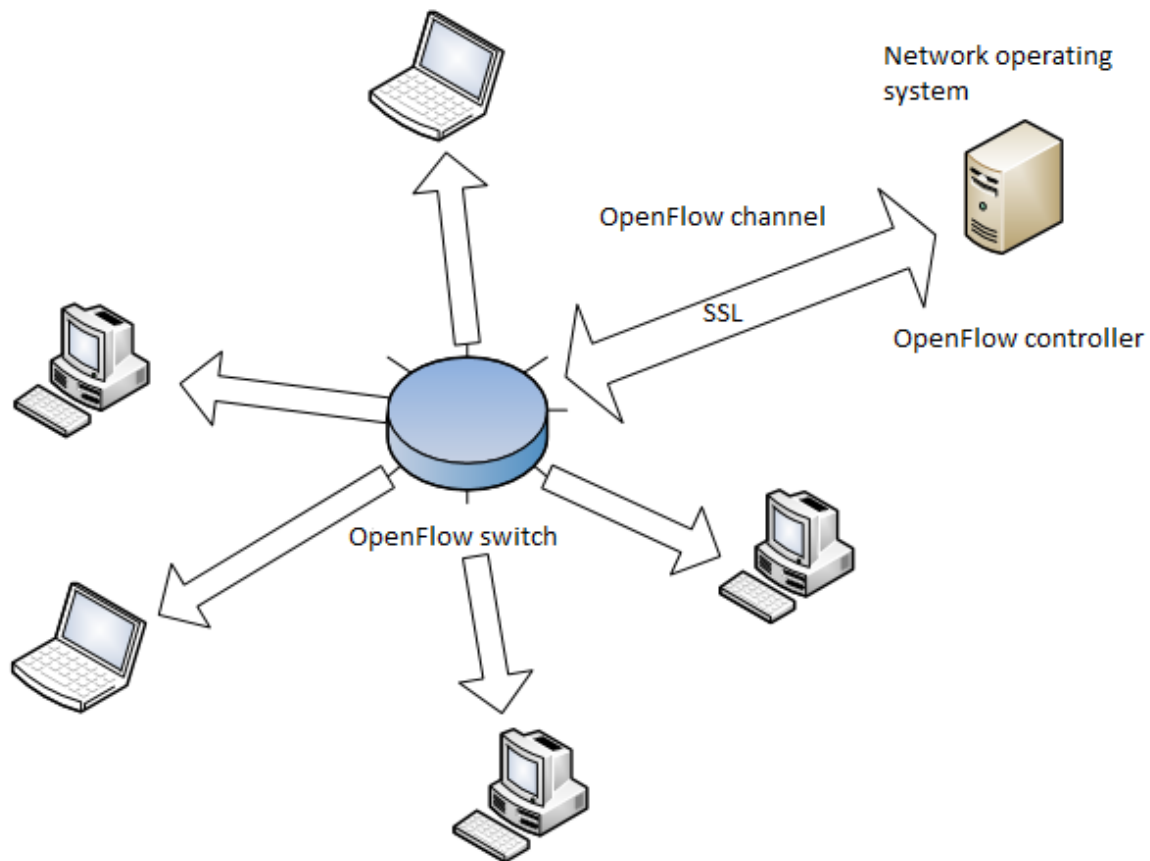


Figure 11 – diagram of the SDN network based on OpenFlow

2.2.1 Architecture of SDN VANET using OpenFlow Protocol. The main elements of the VANET automotive network, built on a software-defined network, using cloud technologies are:

- SDN controller: the logical Central intelligence SDN, which controls the behavior of the network of the entire VANET system. Controller installs rules that is tracking the state of the device, is traffic monitoring and statistics collection;
- switch SDN: is under the control of the SDN controller. The task of the switch is to transmit packets from one port to another without delay, performing some processing in accordance with the rules. When prompted, the switch can inform the controller of its capabilities and configuration, and signal changes in its state, such as a loss of channel or an error. Otherwise, the switch relies entirely on the controller;

- roadside network unit (PSU) deployed along the road device connecting the SDN switches with end users, road users. The dog can be a router, bridge, access point and the client;
- cloud: there are various calculations such as the calculation of the vehicle speed, distance, grade a vehicle;
- database: a database that stores information about the traffic situation, cars and their owners. Also for data transmission over long distances can be used towers with powerful antennas 4G / LTE. The diagram below shows the network structure (figure 12).

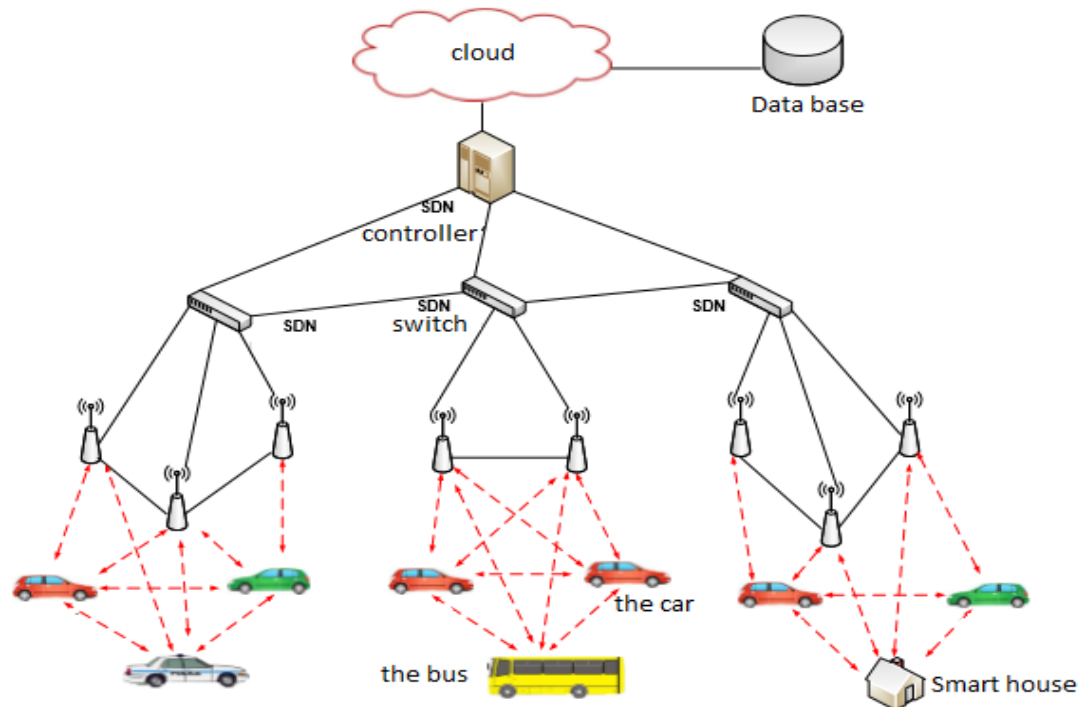


Figure 12-structure of VANET network based on SDN

Figure 13 shows the internal components of the wireless SDN node, which contains all of the functionality of the OpenFlow switch, as well as the additional intelligence to control the different modes of operation in the VANET environment. The number of WiFi interfaces used as a data link depends on the configuration and service that the SDN switch needs to support.

In the composition of each SDN wireless node includes a local agent of the SDN, the functionality of which depends on what features are enabled on the switch SDN. If you lose communication with the SDN controller, the local agent can serve as a backup controller and as the primary intelligent component. Traditional Ad hoc routing protocols (e.g. GPSR, AODV, DSDV, and OLSR) are supported as agents of standby arrangements to allow the SDN network to revert to the Ad hoc network even in the case where the communication with the SDN controller is unavailable. In cases where the connection to the SDN controller is stable and has full control, the SDN agent performs minimal intelligent load.

A distinctive feature of Ad hoc peer-to-peer networks is that nodes act both as hosts (sending/receiving traffic) and as routers (redirecting traffic on behalf of other nodes).

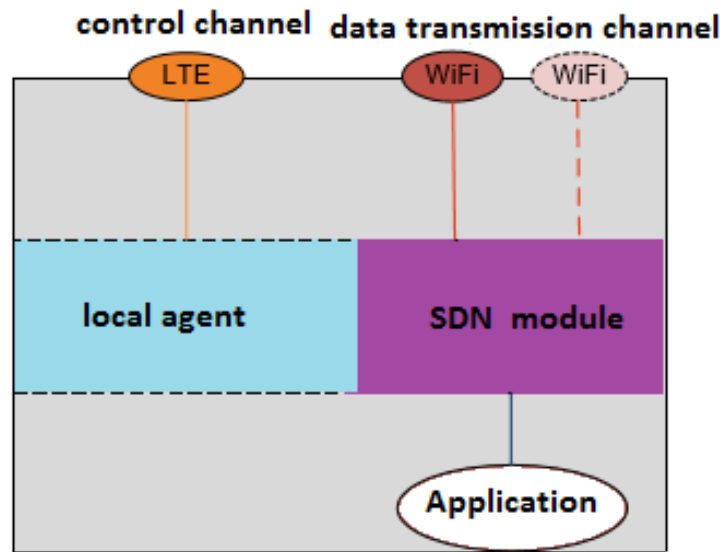


Figure 13 – Components of the switch SDN

Traffic from any wireless host (such as application traffic) will pass through its own SDN module before sending, which allows the SDN controller to determine user traffic access on the network.

2.2.2 Modes of Operation. Although the SDN concept is the separation of control and data plane, there are differences in how the software-defined VANET network can operate based on the degree of control of the SDN controller. For the architectures under consideration, the following three modes can be distinguished:

- Central mode: this is the mode in which the SDN controller controls all actions performed by the SDN switch and the RSU. As shown in figure 14, the SDN controller will pass down the hierarchy all the rules of how to handle traffic.

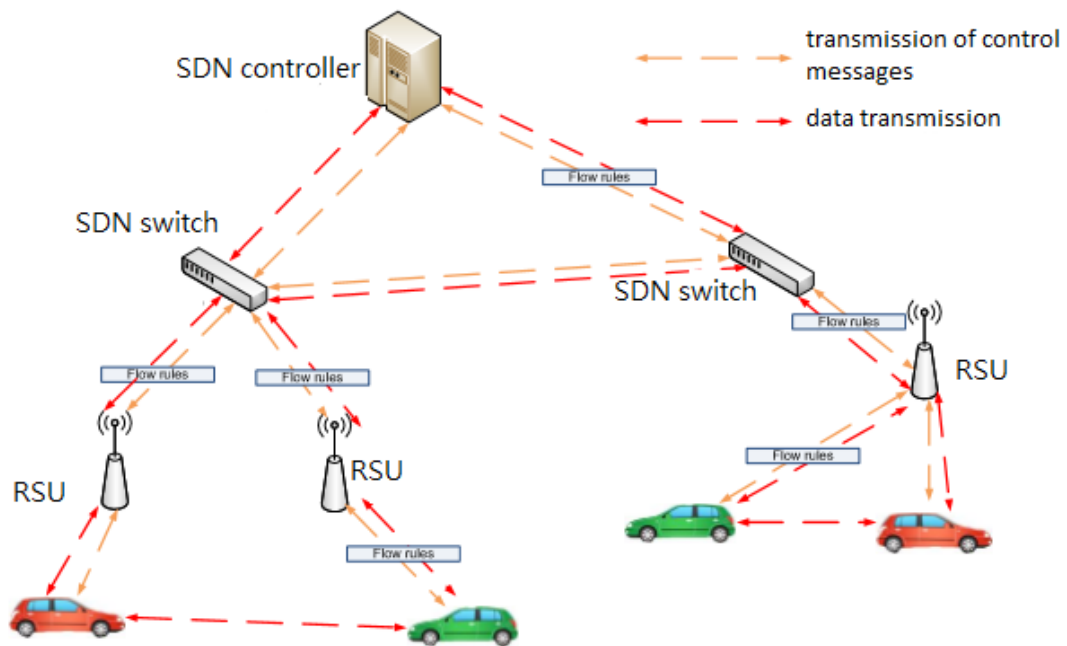


Figure 14-Central network operation

- Distributed mode: this is the mode in which the SDN switches and the NMC do not receive any instructions from the SDN controller when transmitting data packets. This control mode is essentially similar to the original Ad hoc network without any indication of SDN, except that the local agent on each SDN switch controls the behavior of each individual node (such as running GPSr routing), as shown in figure 15.

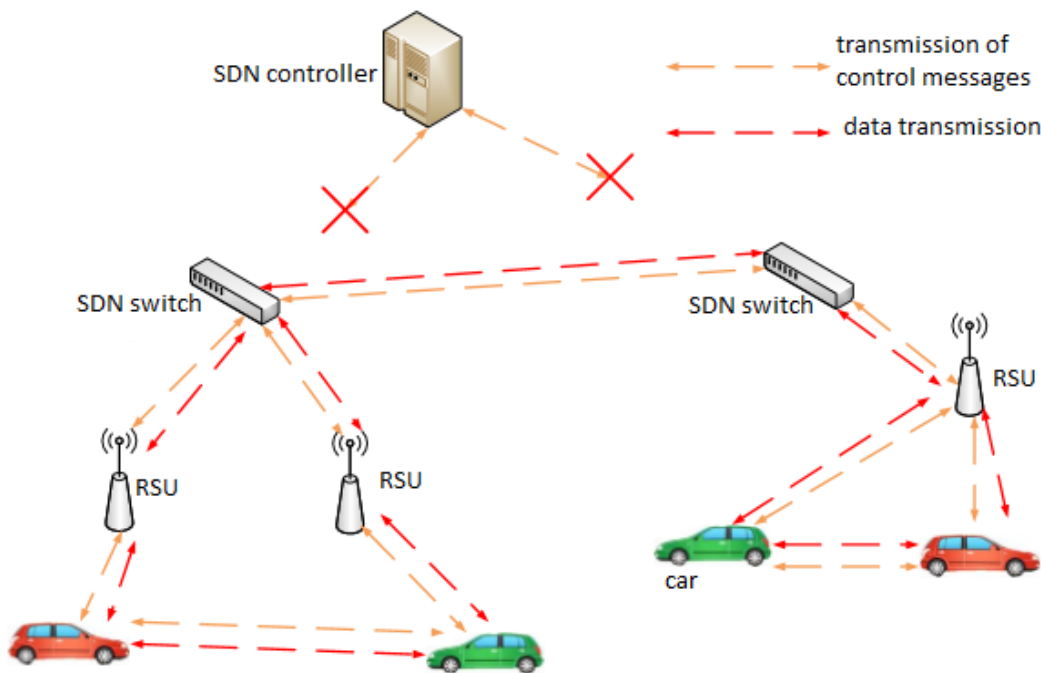


Figure 15-Distributed network operation

- Hybrid mode: this mode includes all operating modes of the system in which the SDN controller controls anywhere between full and zero. Figure 16 shows an example in which there is no full control on the part of the SDN controller, that is, part of the management of packet processing is transferred to local agents. Therefore, managing exchange of traffic is distributed between all elements of the SDN. For example, there may be a situation where instead of sending full flow rules, the SDN controller sends out policy rules that determine behavior, while the SDN switches and the RSU use local intelligence to forward packets and process the flow level. Thus, the SDN controller instructs the SDN switches and the RSU to run a specific routing Protocol with certain parameters.

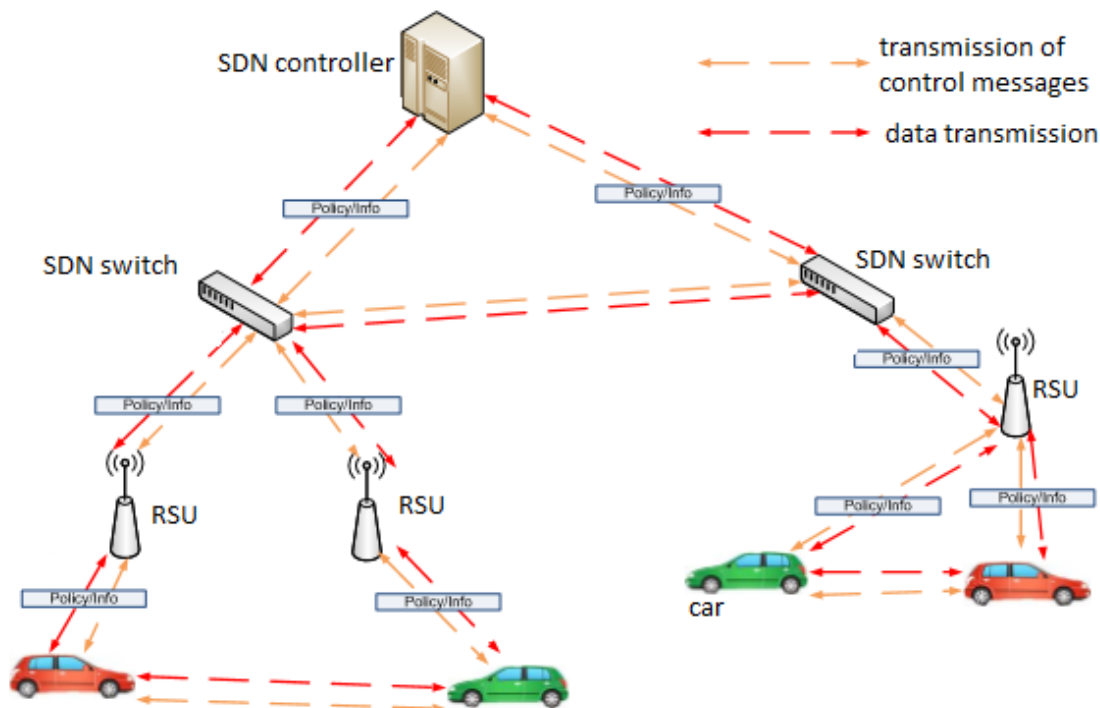


Figure 16 - a Hybrid network work

The Central control mode behaves similarly to the wired SDN architecture, where the SDN controller defines all rules. However, one of the most pressing problems of wireless communication is its reliability / availability, there is always a possibility of possible loss of communication between mobile nodes and the controller. This is the reason why SDN VANET should have crash recovery mechanisms that would ensure that the system can function, communication with the SDN controller is lost or broken. For this purpose, each WIRELESS SDN node has a local agent equipped with artificial intelligence. For example, if communication with the SDN controller is lost, the system may revert to managing a traditional routing Protocol such as GPSR. The study of the topology of the network is of great importance to the SDN controller in making intelligent decisions, so in software-defined networks VANET use of message-tags, and widespread technology in VANET systems. Each WIRELESS SDN node will exchange beacon

messages to find out information about nearby neighbors. This information must be continuously updated on the SDN controller, which in turn uses THIS data to build tables of connected nodes and make decisions such as choosing a path for routing packets through the network. By exploiting this function, can provide many benefits for mobility management in SDN VANET.

2.3 Advantages and New Services of SDN VANET Networks

In a separated control plane, SDN provides flexibility and programmability to the network, allowing the system to adapt to changing conditions and requirements. This feature allows the software-defined VANET network to make more informed decisions based on combined information from different sources. In addition, dynamism and flexibility allow for response to sudden events, such as emergencies and changing requirements. In this section, we describe the benefits of Software-Defined VANETs, and describe a few services that can be improved by taking advantage of these benefits.

Classifying the benefits of using SDN VANET networks, we can distinguish 3 areas:

- select the path: understanding the SDN controller of the entire network allows the system to make better-informed decisions about routing. For example, in standard VANET networks, data traffic can become unbalanced, either because the shortest route of traffic cannot be determined because the system is focused on some selected nodes, or because an application that works with video information requires a large amount of bandwidth is on the way. When a similar situation is detected by the SDN controller, IT can start the process of redirecting traffic to improve network utility and reduce congestion.

- Frequency/channel selection: when SDN nodes have several available wireless interfaces or configurable radio stations, such as cognitive radio, a software-defined VANET network can allow to optimize the selection of the channel/frequency used. For example, the SDN controller can dynamically decide at what time, what type of traffic will use a particular radio interface/frequency. This advantage can be used to reserve channels for VANET emergency services.

- Power selection: the VANET SDN controller will have enough information to determine whether the power of wireless interfaces should be changed to increase/decrease the data transmission distance. For example, the SDN controller collects information from nodes and determines that the node density is too low, and issues the appropriate commands to increase power in order to achieve a more reasonable and stable package delivery and reduce interference.

Based on the advantages described above, a number of services can be identified that can be improved with the help of software-configured VANET networks.

- SDN Assisted VANET Safety Service: Improving road safety through the use of V2V communication is one of the main use cases of VANETs. We will show how Software-Defined VANET can improve services compared to traditional methods. SDN can be used to reserve or limit certain frequencies, so only

emergency traffic uses this reserved path. The difference with traditional emergency channels is that redundancy in SDN architecture is dynamically configured. The SDN controller can assign streams to specific channels or remove them depending on current traffic conditions and application requirements. This feature can also be used to offer a different level of services based on policies. As it can be done by changing the rules during a state of emergency. Emergency traffic takes precedence over the rest of the traffic.

- SDN-based VANET On Demand Surveillance Service: surveillance service for vehicles is another area in which software-defined VANET networks allow you to achieve a number of advantages. In traditional architecture, the requesting party (e.g. a police car) must send a request for surveillance data. In the SDN VANET system, this request is performed by the SDN controller. The SDN controller installs the rules flow for observation data, that these data have reached all of the necessary components. Thus, the transmission of data resembles a broadcast carried out by the controller in respect of a group of police vehicles.

- Wireless Network Virtualization Service: network virtualization services are designed to provide abstract logical networks on shared physical network resources. SDNS are already used in data centers to provide network virtualization services, and the same idea can be applied to software-configured VANET networks. The idea is to have different data streams choose different interfaces using different frequencies. If the radio frequencies used by each individual network are different, the traffic of the individual subnets is isolated from each other, and so you can effectively divide the network and create virtual wireless networks.

2.4 Addressing the Issues Identified

The proposed architecture and the proposed centralized approach allows to solve several problems described in the previous Chapter, and also gives advantages in comparison with traditional transport peer-to-peer networks:

- increased reliability due to the aggregation of information on the controller. Using the classic architecture, each node stored a database of the state of channels, routes, and nodes, but using a centralized approach allows you to collect information in one place – on the controller. Thus, such a centralized database will contain much less inconsistent information, and this approach will reduce the likelihood of cycles in the network;

- simplification of the structure and logic of network devices, since the centralized approach does not require processing a large number of standards and protocols, and it is enough to perform only the instructions received from the controller;

- increasing the security of transmitted data due to the possibility of creating a security policy on the controller, ensure reliable identification, placement of firewalls and network anti-virus;

- programmability and flexibility of network management, as well as a significant simplification of the modification capabilities of network management by creating new applications or modifying existing ones. In addition, a centralized

approach allows you to increase the level of automation of management and ease of network administration;

- adaptability of network management, that is, the ability to change the behavior and condition of the network in real time, taking into account the changing conditions of operation. It is also possible to adapt to the changing needs of network users by creating new network applications and services. In addition, the development of network applications requires much less time compared to the reconfiguration of the entire network in manual mode;

- independence from the equipment and proprietary software of network equipment manufacturers;

- the possibility of independent deployment and scaling management level and the level of data transfer that increases the ease of maintenance of the transport network;

- reducing the cost of switches and network infrastructure in General due to the removal of intelligence to the controller.

Thus, the SDN approach allows to significantly automate and simplify the management of networks due to the possibility of their "programming", allowing to build flexible scalable networks that can easily adapt to changing operating conditions and user needs. The implementation of this approach should have a significant impact on the management of the network infrastructure in VANET transport networks.

3 Simulation of VANET networks

In order to compare the developed variants of SDN VANET network architecture with the traditional architecture of transport networks, it is necessary to conduct a study of the effectiveness of VANET protocols in this or that scenario. This Chapter provides modeling options, configurations, and results. For carrying out experiments, NS-3 and SUMO simulators, as well as the SDN – Mininet-WiFi emulator were used. The purpose of the simulation is to evaluate the effectiveness of the SDN approach in VANET transport networks and to increase the level of security in conditions close to reality.

3.1 Comparison of VANET Routing Protocols

The NS-3 program was chosen as the medium in which the simulation was carried out, which allows to form a road network (figure 17) and to carry out the necessary measurements. The road network is a section of space of 1000 x 400 meters. The location of nodes in a given area is random, the average distance between the nearest nodes is 50 meters. A total of 50 nodes were generated in this model. These nodes move within the selected area at a speed not exceeding 10 meters per second. Each wireless node has several wireless interfaces: small radius, where 802.11 and Friis model is used to limit the transmission distance to 250 meters, as well as large radius using LTE technology. Packet generation is performed at a rate of 10 packets per second, the packet size is 1024 bytes, the

selected beacon message interval is 500ms. The duration of each simulation was 30 seconds.

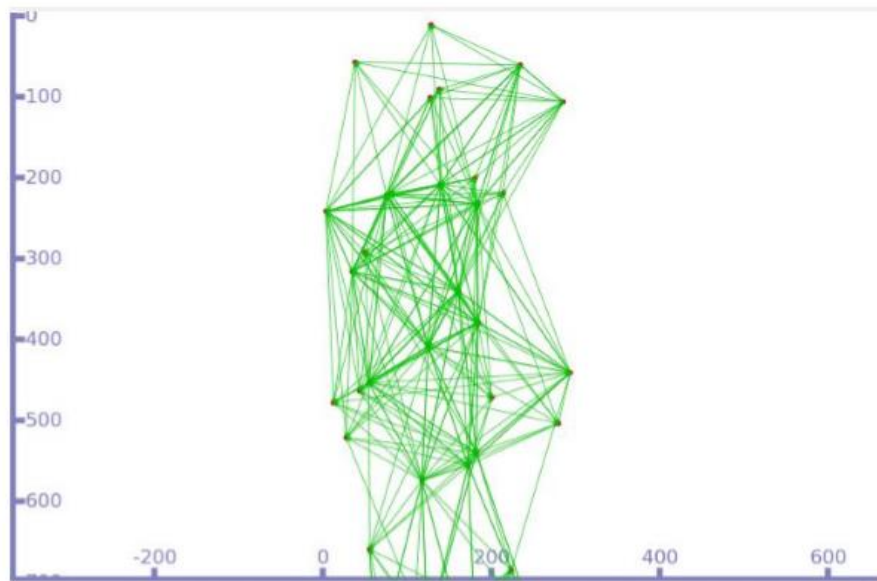


Figure 17 – Model of the road network

Similarly, the simulation was carried out for a larger number of nodes, respectively, the size of the road network was also increased. Thus, the results were obtained for a different number of network nodes at different speeds of vehicles. Based on the theoretical study of the VANET protocols in the first Chapter, reactive protocols AODV and DSR, as well as proactive – OLSR and DSDV were chosen for modeling. As modeling criteria, the rate of data transfer and the percentage of delivered packets were selected. Figure 18 shows a graph showing the results of a comparison of VANET routing protocols: AODV, DSR, OLSR and DSDV by average data rate with different number of nodes:

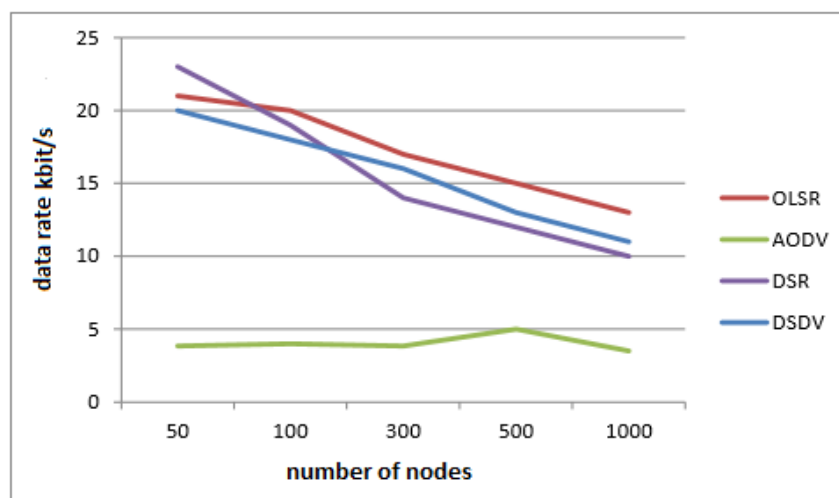


Figure 18-comparison of protocols by data rate

As can be seen from this graph, with a large number of nodes, proactive protocols show the highest data rate, despite the large amounts of information transmitted about changes in the topology. It is also worth noting that for small networks it is advisable to choose a reactive DSR Protocol, when using which the data transfer rate was the highest. For rice. 19 shows a graph showing the percentage of packets delivered at different node speeds:

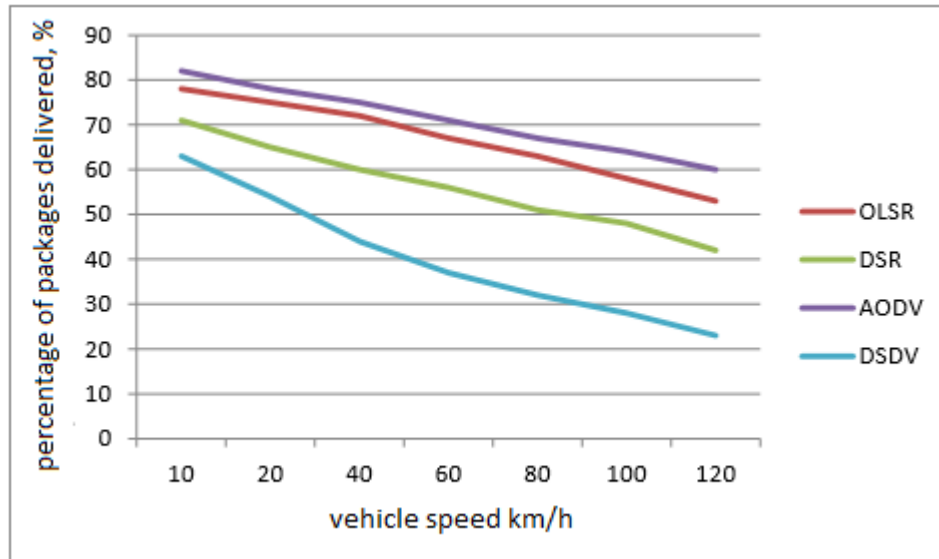


Figure 19 - Protocol Comparison by percentage of packets delivered

As can be seen from this graph, the percentage of delivered packets significantly decreases with the increase in the speed of the nodes. The best performance was achieved using the aodv and OLSR protocols. Thus, based on the results obtained during the simulation, it is advisable to use the OLSR Protocol in transport networks. The proposed architecture options SDN VANET, as well as modes of operation described in the second Chapter, allow the use of the OLSR Protocol.

3.2 Comparison of VANET architectures, SDN

This simulation was carried out using the computing resources of the supercomputer center of St. Petersburg Polytechnic University Peter the Great-SCC "Polytechnic". 1000 virtual machines were created using OpenStack Dashboard. On virtual machines CentOS OS was installed, created virtual machines play the role of dynamic network nodes: cars, traffic police, buses, smart homes. Since the main characteristic of VANET networks is its dynamism, rapid change of network structure, creation of new subnets, in the created simulation model dynamism is achieved by moving virtual machines from one subnet to another. Figures 20 and 21 show the results of a study of VANET network architectures discussed in the second Chapter:

- Architecture 1 - classical VANET architecture;

- Architecture 2-architecture with Central control-servers solving security problems;
- Architecture 3-architecture with partial decentralization;
- Architecture 4-hierarchical architecture.

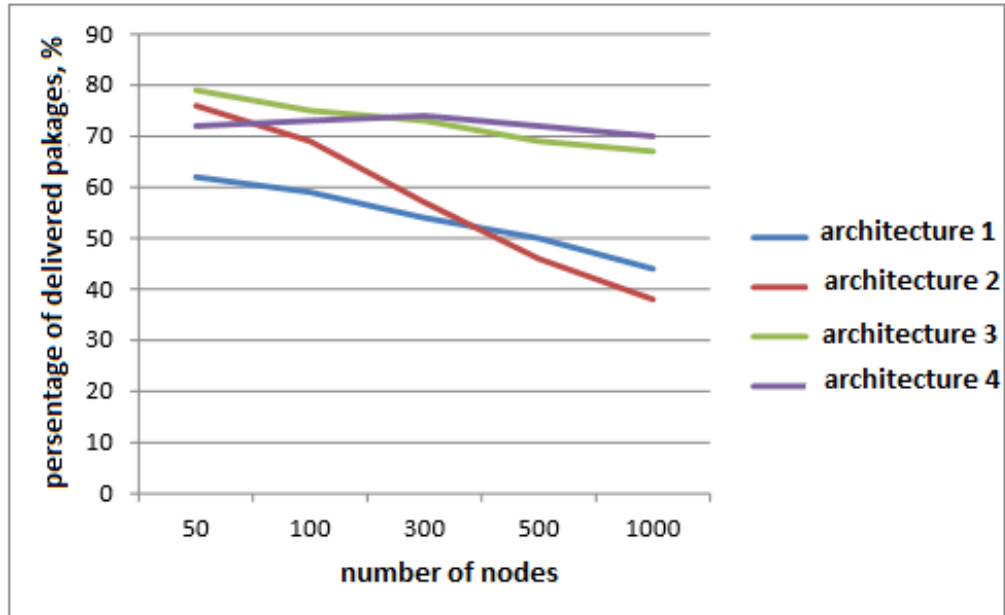


Figure 20 – Comparison of architectures on the delivered packets percentage

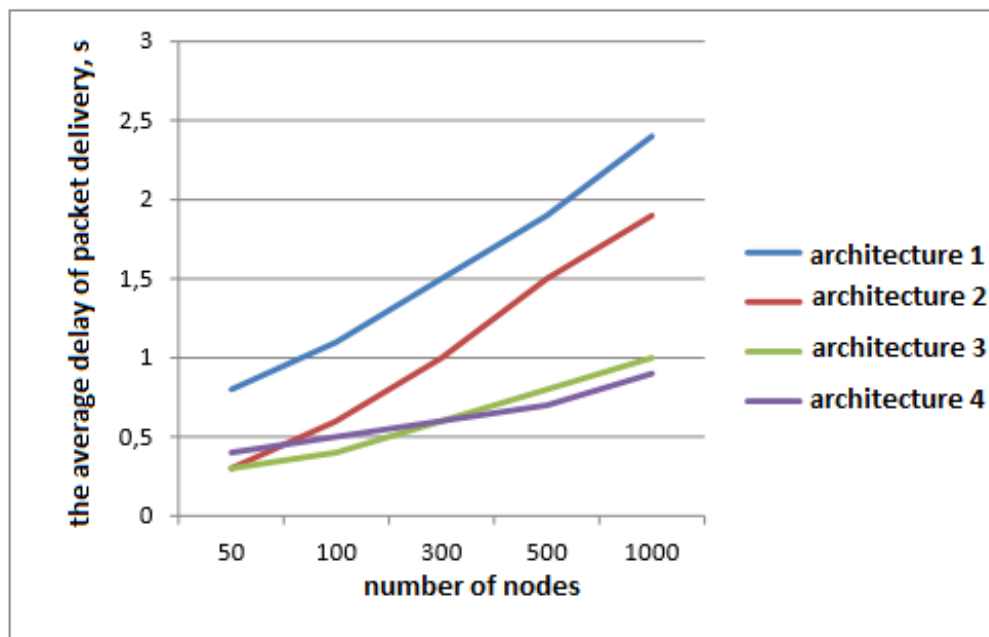


Figure 21 - comparison of architectures by average packet delivery delay

Based on the results obtained, we can conclude that the VANET architectures developed using the SDN approach are superior to the classical VANET networks. For large-scale transport networks, architectures with multiple controllers are most effective: partial decentralization and hierarchical architecture. In small networks up

to 100 nodes architecture with a Central link of management - servers that solve security problems, also significantly exceeds the classical architecture.

3.3 SDN VANET security

In this section, using the car traffic simulator – SUMO and SDN emulator

- Mininet-WiFi implemented services aimed at solving security problems, which were described in the first Chapter:
- organization of security policy;
- implementation of the backup mechanism;
- implementation of adaptive transmission distance.

3.3.1 Organization of SDN VANET security policy. In this simulation, we consider the case when a node is found in the VANET SDN network that needs to be isolated from other network participants. To simulate this situation, the following network topology was implemented in The mininet-WiFi emulator (figure 22):

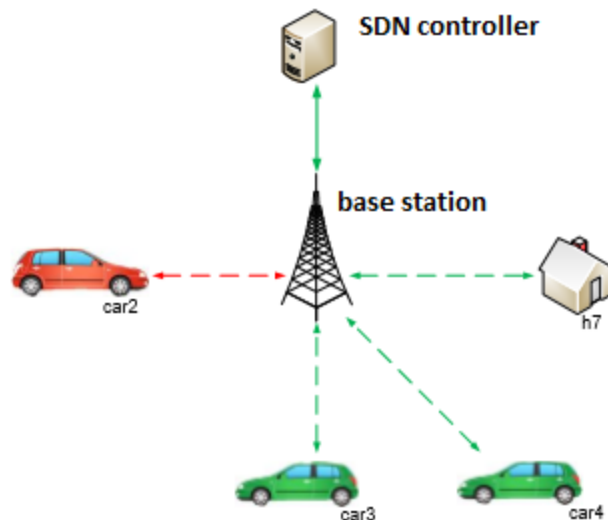


Figure 22-network Topology

It is assumed that car2 with ip address 10.0.0.2 performs actions that pose a danger to other network participants, then the controller immediately sends the following command to the base station:

```
ap1.cmd("ovs-ofctl add-flow ap1priority=65535,ip,nw_src=10.0.0.2,actions=drop")
```

The results are shown in figure 23 below, and indicate that car2 can now communicate only with the base station, and the rest of the network continues to interact with each other. Thus, an example of the simplest security policy in the SDN VANET network was implemented, which is impossible in traditional VANET networks.

```

mininet-wifi> car2 ping car3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
^C
--- 10.0.0.3 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms

mininet-wifi> car2 ping h7
PING 10.0.0.7 (10.0.0.7) 56(84) bytes of data.
^C
--- 10.0.0.7 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1007ms

mininet-wifi> car2 ping ap1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms
^C
--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.035/0.037/0.039/0.002 ms

mininet-wifi> car3 ping car4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=0.269 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.104 ms
^C
--- 10.0.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.104/0.186/0.269/0.083 ms

```

Figure 23 – interaction of the members of the network after packet filtering

3.3.2 Network When Loss of Connectivity with the SDN Controller. A scenario has been implemented in which communication with the SDN controller is interrupted and routing is managed by local agents. The simulation is performed using the NS3 program, the road network is generated using the same parameters as in the first experiment. Figure 24 shows a scenario in which the controller failed within 100 seconds, as shown by solid lines:

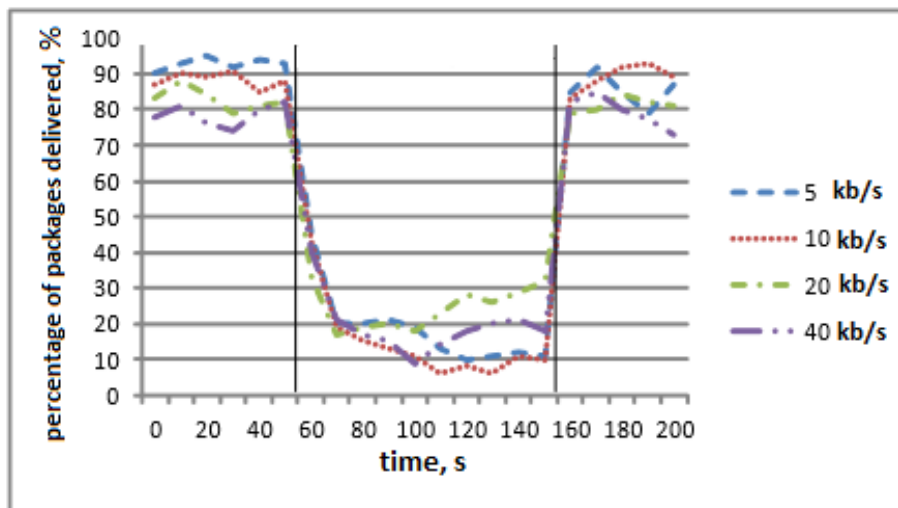


Figure 24 – Work SDN VANET when no alternate mechanism

You may notice that the percentage of packets delivered starts to drop dramatically, as the SDN controller no longer establishes new rules for wireless SDN nodes. This indicates that SDN VANET in Central control mode is dangerous if the SDN controller communication is not reliable enough. The feature of VANET

is that the nodes move very quickly and the rules become obsolete much faster compared to the scenario where the mobility of the nodes is low. The following scenario has been considered, except that this time there is a backup mechanism in the network that uses OLSR routing, which is triggered when communication with the SDN controller is lost. Figure 25 shows the percentage of data packets delivered during the entire modeling phase:

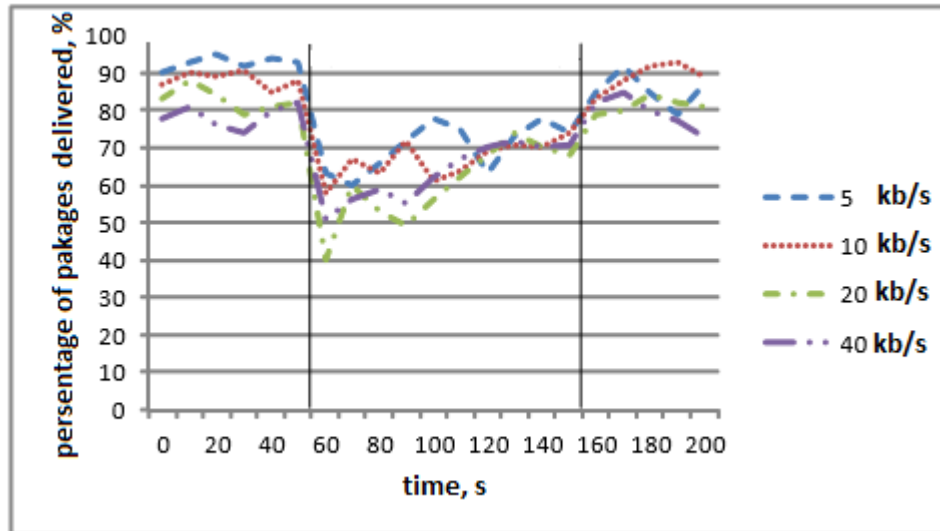


Figure 25-operation of SDN VANET in the presence of a spare mechanism

This graph shows that after the loss of communication with the SDN controller and activated OLSR, maintaining a high ratio of delivered packets. After communication with the SDN controller is restored, the system reverts back to SDN routing. At the organization of the network with the backup mechanism, the security and stability of VANET significantly increase.

3.3.3 Adaptive Transmission Distance. This simulation considers the case where the SDN controller is given the right to dynamically control the transmission capacity of SDN wireless nodes, in order to improve the delivery of packets. The simulation is also performed in the program Mininet and SUMO, where the road network was generated, and added 3 cars connected to the SDN-controller (figure 26):

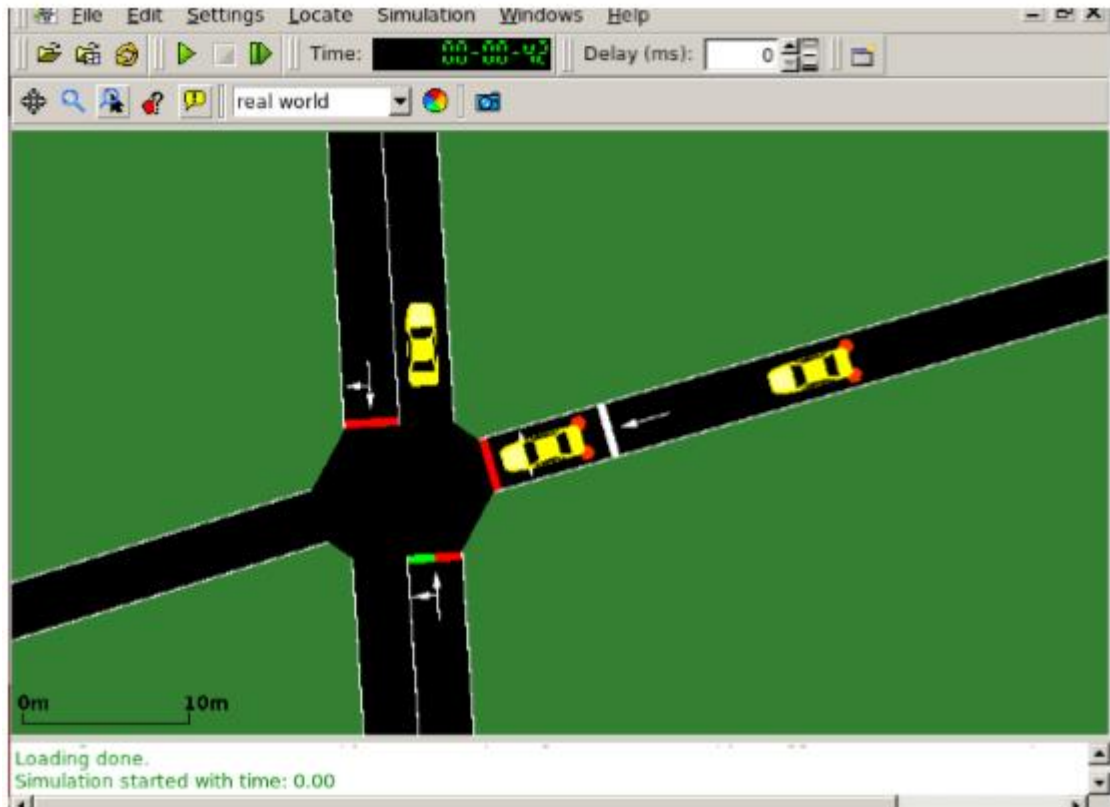


Figure 26-simulation of SDN VANET in the SUMO

Program in figure 27 shows the result of the experiment, after sending the 3rd echo request on the occurrence of the 5th cycle of the program the transmission range increases from 100 to 300 meters:

```
mininet-wifi> car1 ping car2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.244 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.124 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.112 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.065 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.067 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.072 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=0.072 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=0.103 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=0.073 ms
64 bytes from 10.0.0.2: icmp_seq=11 ttl=64 time=0.085 ms
64 bytes from 10.0.0.2: icmp_seq=12 ttl=64 time=0.074 ms
64 bytes from 10.0.0.2: icmp_seq=13 ttl=64 time=0.072 ms
```

Figure 27-SDN VANET Operation when power changes

In this screenshot, you can see how the time to send echo requests decreases with increasing power, as the new transmission range provides better communication between nodes. In this experiment, the change in power was implemented at a certain time. Theoretically, the SDN controller can make a judgment to adjust the transmit power as it full information the information

throughout the VANET scenario. Thus, the SDN controller can increase the transmit power based on the information collected from the wireless SDN nodes, determining that the connectivity between the wireless SDN nodes is too low. On the basis of the conducted experiments it can be concluded that the use of the SDN mechanism allows to solve the existing problems of VANET network security, namely: the problem of noise immunity, the problem of ensuring the security of transmitted data, the problem of the total network bandwidth and the problem of the efficiency of the routing methods used.

4 Broadband access Calculations

4.1 Calculation of Losses in Microwave Communication Systems

The range extends from 2 to 40 GHz. At the same time, the wider the bandwidth and data rate, the higher the frequency (table 4.1).

Table 4.1-characteristics of microwave speed and frequency

Range, GHz	Bandwidth, MHz	Data transfer rate, Mbit / s
2	7	12
4	30	90
11	40	135
18	220	274

The losses are mainly caused by signal attenuation, which depends on the path from the source to the destination and frequency. For ultra-high radio frequencies, signal attenuation looks like this

$$L_p = X \log\left(\frac{4\pi df}{c}\right) dB, \quad (4.1)$$

where X - is the attenuation coefficient, which is 20 for the wire;

d - is the path from the transmission point;

C - is the speed of light;

f - is the frequency of the signal.

Microwave systems use repeaters with an average distance of 10100 km.

In Kazakhstan for these purposes, a frequency of 800 MHz, 1800 MHz and 2100 MHz.

Formula (4.1) shows that if the frequency of the propagating signal increases, the signal attenuation increases accordingly. For example, if the signal propagates in air with a frequency of 2.4 GHz, it will diminish by 60 dB when passing from the source to 10 m And if the frequency is 5 GHz to 66 dB when you run the same 10 meters.

Figure 4.1 shows a graph of the attenuation of the propagating signal from the path of its removal from the source when using the frequency of 800 MHz.

Figure 4.2 shows a graph of the attenuation of the propagating signal from the path of its removal from the source using the frequency of 1800 MHz.

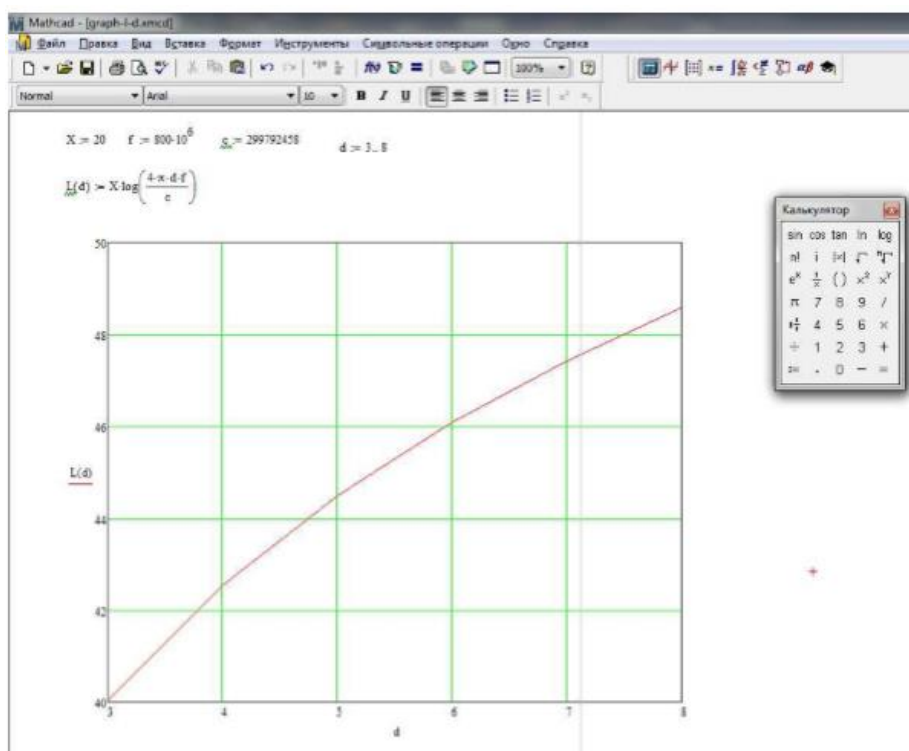


Figure 4.1-signal attenuation Dependence on the path of its removal from the source when using 800 MHz frequency

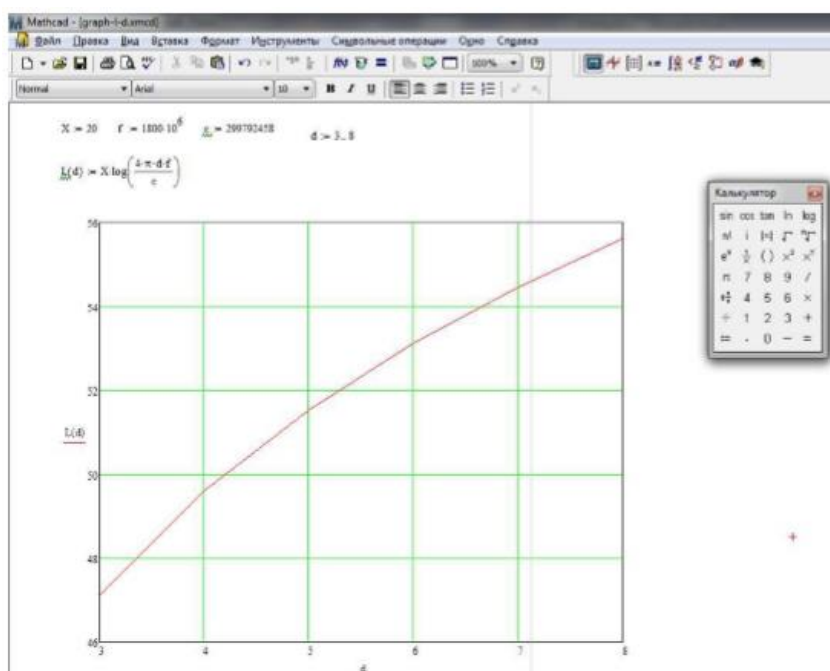


Figure 4.2-signal attenuation Dependence on the path of its removal from the source when using 1800 MHz frequency

Figure 4.3 shows a graph of the attenuation of the propagating signal from the path of its removal from the source using the frequency of 2100 MHz.

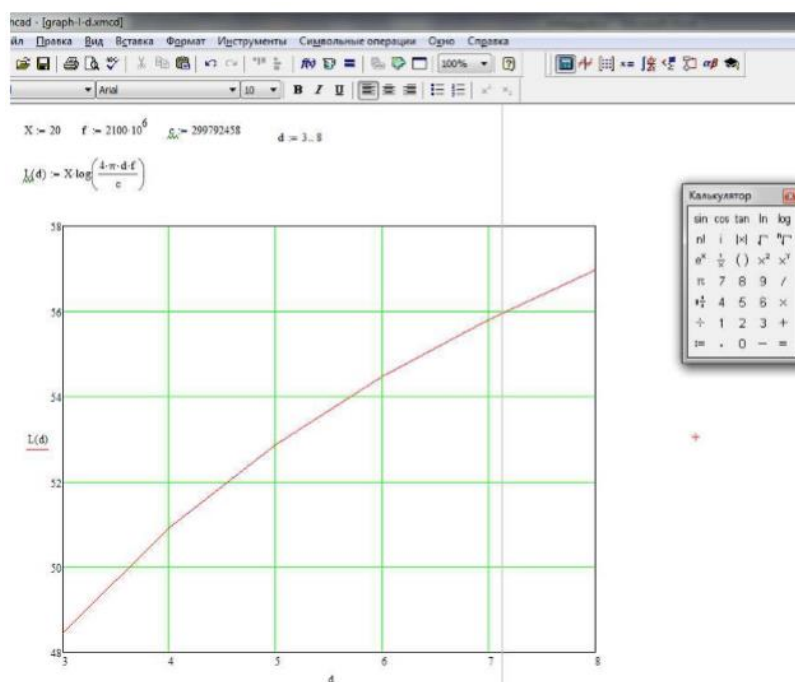


Figure 4.3 – Dependence of the attenuation of the signal from the path it was deleted from the source when the use frequency 2100 MHz

4.2 Calculation of capacity balance

Uninterrupted functioning wireless systems require that the total amount of system gain is greater than the total amount of all losses. At the same time, there is a recommendation on the power reserve (fade margin), which is regulated by 10-15 dB. This will allow the system to work steadily regardless of weather conditions. Table 4.2 shows the parameters for the calculation in the 2.1 GHz range.

Table 4.2-calculation Parameters in the 2.1 GHz range

Parameter	Value
The gain of the transmitter, dBm	15
Cable loss, dB / m	0,23
Loss per connector, dB	0,5
The gain of the transmitting antenna (parabolic grid), dB	24
Losses in the propagation medium, dB	100
Receiving antenna gain, dB	24
Receiver sensitivity, dBm	-85

At the same time adding up the values of the gain, including the plus value of the receiver sensitivity (15+24+24+85=148) and subtract the values of the attenuation (-0,23-0,5-100=100,73). On the basis of the above it is seen that the balance of power has a margin above the regulated and is (148-100,73=47,27).

4.3 Calculation of the Fresnel zone

In the operation of wireless technology, electromagnetic energy is concentrated in a certain ellipsoid of rotation, which is called the Fresnel zone, which is based on the principle of Huygens, according to which each point of the medium to which the disturbance reaches, itself becomes a source of secondary waves, and the radiation field can be considered as a superposition of all secondary waves. Based on this principle, it can be shown that objects lying inside concentric circles around the line of sight of two transceivers can affect the quality both positively and negatively. All obstacles that fall inside the first circle, the first zone of the Fresnel, have the most negative impact. Consider the point located on the direct path between the transmitter and receiver, the distance from the point to the transmitter is S , and the distance from the point to the receiver is D , i.e. the distance between the transmitter and the receiver is $S + D$ (see figure 4.4). We calculate the radius of the first Fresnel zone at this point by the formula:

$$R = \sqrt{\frac{\lambda SD}{S + D}}$$

where R , S and D are measured in the same units, λ denotes the wavelength of the signal along the path.

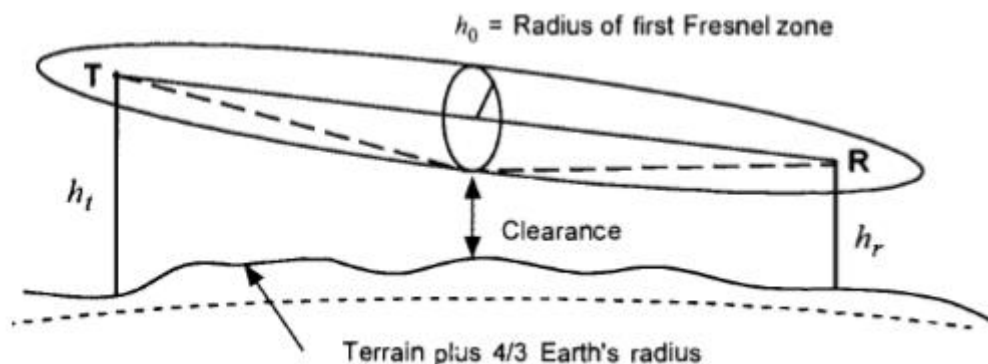


Figure 4.4-transmitter receiver line-of-sight Path

For convenience, the formula can be rewritten as follows:

$$R_m = 17,3 \sqrt{\frac{1}{f_{GHz}} \frac{S_{km} D_{km}}{S_{km} + D_{km}}}$$

where R-is expressed in meters, the other two distances-in kilometers, and the frequency of the signal - in gigahertz.

Let the distance between the two transceivers be 10 km and the carrier frequency 2.1 GHz. Then the radius of the first Fresnel zone at a point located in the middle between the transceivers is 17.66 m. If there are no obstacles inside the circle, the radius of which is about 0.6 of the radius of the first Fresnel zone, drawn around any point between the two transceivers, then the signal attenuation due to the presence of obstacles can be neglected. One of these obstacles is the earth. The height of the two antennas should be such that there is no point along the path, the distance from which to the ground would be less than 0.6 of the first Fresnel zone. Part of the communication pathway can pass through vegetation, mostly through the foliage of tall trees. In some suburban areas and in small towns such obstacles are likely to be eliminated, even by installing antennas on the roofs. The study led to the conclusions: the presence of trees near the subscriber's location can lead to fading due to multipath propagation; the main multipath effects, which leads to the presence of hardwood cover, are diffraction and scattering; measurements carried out in gardens with a periodic structure, gave the following results: the absorption of 12-20 dB per tree for hardwood and up to 40 dB for a group of 1-3 coniferous trees, when the foliage is within 60 percent of the first Fresnel zone; the effects of multipath propagation are strongly dependent on wind.

Thus, when installing high-frequency systems for each subscriber, it is necessary to try to avoid foliage in 60 percent of the first Fresnel zone. Table 4.3 shows the working channels.

Table 4.3 - Working channels

Channel number	The Central frequency of the spectrum	frequency spectrum, MHz	Channel number	The Central frequency of the spectrum	frequency spectrum, MHz
1	2101-2123	2112	8	2136-2158	2147
2	2106-2128	2117	9	2141-2163	2152
3	2111-2133	2122	10	2146-2168	2157
4	2116-2138	2127	11	2151-2173	2162
5	2121-2143	2132	12	2156-2178	2167
6	2126-2148	2137	13	2161-2183	2172
7	2131-2153	2142	14	2173-2195	-

In figure 4.5 the calculations in the shell Mathcad Professional for different distances between the two transceivers is equal to 10, 15 and 20 km.

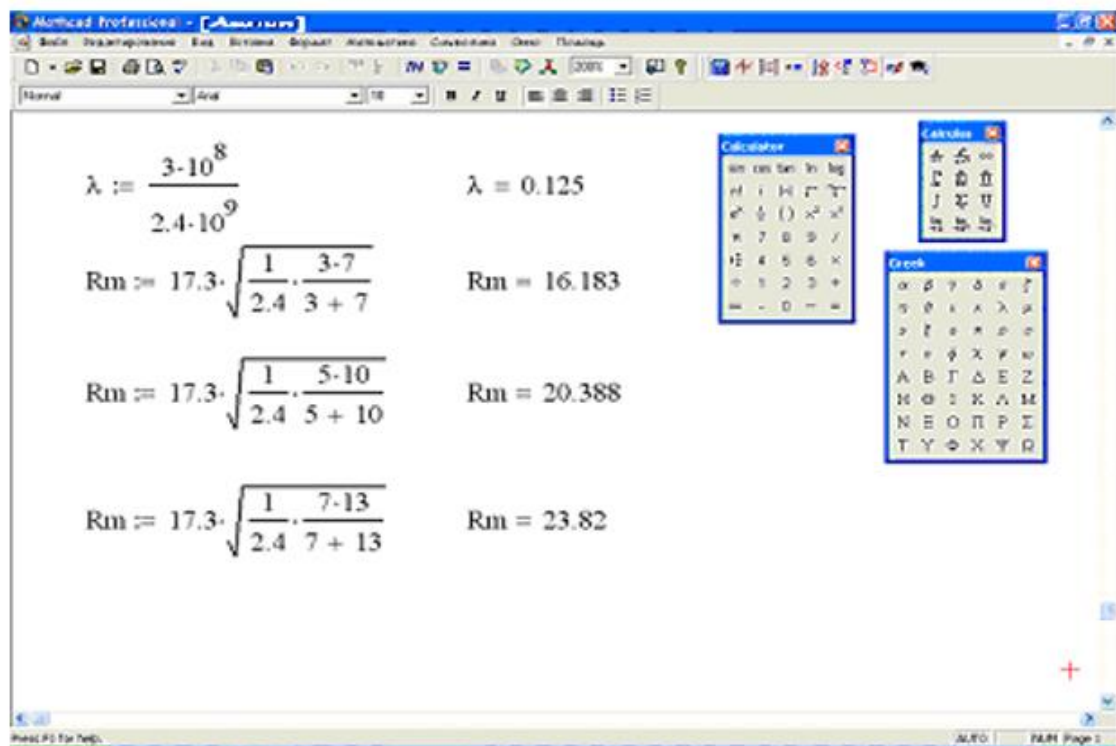


Figure 4.5 - Calculation on Mathcad Professional

4.4 Coverage Area Calculation for the LTE Network

The difference between LTE radio network planning is the use of a new type of multi-station access based on OFDM technology, and therefore new concepts and design algorithms are changing. LTE radio network planning will be carried out in urban areas, which means that the density of subscribers will be low and base stations should be installed at the maximum distance from each other in order to close each eNB as much territory as possible. In this regard, it is necessary to choose the appropriate frequency range (791 – 862 MHz is quite suitable for this task). Type duplex choose the frequency – FDD. The analysis of radio coverage will start with the calculation of the maximum allowable losses on the line (MAL). The MAL is calculated as the difference between the equivalent isotropic radiated power of the transmitter (EIRP) and the minimum required input power of the mated side receiver, which, taking into account all losses in the communication channel, provides a normal demodulation of the signal in the receiver. The MAL calculation principle is shown in figure 4.8.

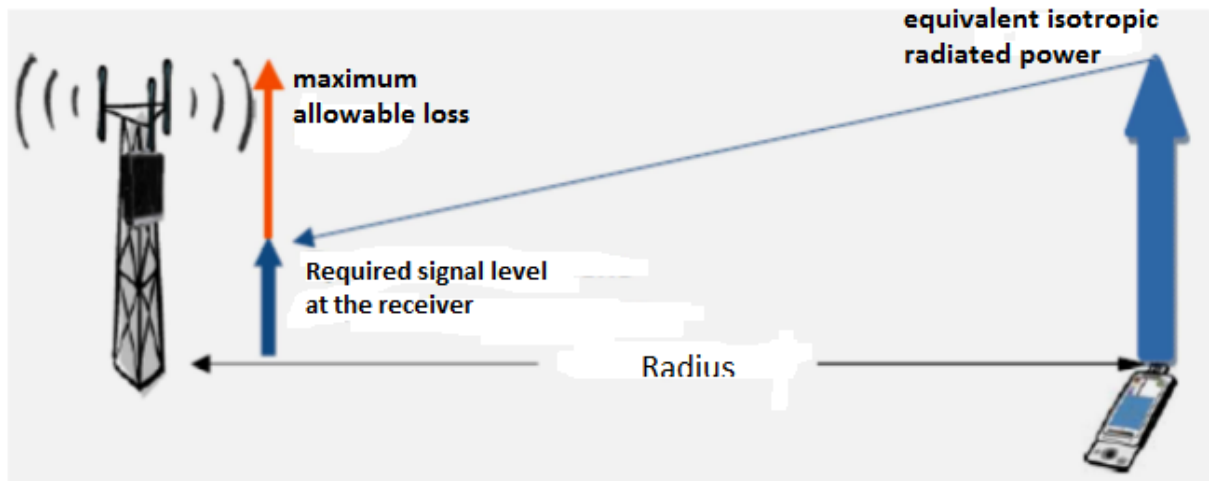


Figure 4.8 - calculation Principle of the MAL

In the calculations we will use the following parameters:

- system band: 20 MHz; for FDD = 10/10 (DL/UL);
- eNB - on each sector one TRX, TRX output power = 40 W (46 dBm); works on the DL line in MIMO 2×2 mode;
- UE – subscriber terminal-USB modem, class 4 – EIRP 33 dBm;
- frame length ratio DL/UL: 100%/100%.

The calculation of the maximum allowable losses is made according to the formula:

$$L_{MAL} = P_{EIRP} - S_{rs} + G_{gta} - L_{lfp} - M_{pen} - M_n - M + G_{xo}$$

where P - is the equivalent radiated power of the transmitter;

S - is the receiver sensitivity;

G - is the gain of the transmitter antenna,

G: DL = 18 dBi, UL = 0 dBi;

L - losses in the feed path of the transmitter,

L: DL = 0.3 dB;

M - margin for signal penetration in the operator for Urban areas,

M = 12 dB;

M - margin for interference.

M - is determined by the results of system level modeling depending on the load in neighboring cells;

M corresponds to the load in neighboring cells 70%.

M: DL = 6.4 dB; UL = 2.8 dB;

G - handover win. The value of the gain from the handover is the result of the fact that in case of deep fading in the serviced cell, the

subscriber terminal can carry out a handover in the cell with the best reception characteristics.

$G = 1.7$ dB.

P is calculated by the formula:

$$P_{EIRP} = P_{out} + G_{gta} - L_{lfp},$$

where P - is the output power of the transmitter;

P_{out} is in the "down" line (DL) in LTE depends on the site bandwidth, which can range from 1.4 to 20 MHz, within up to 5 MHz rationally select TRX transmitters with power of 20 W (43 dBm), and over 5 MHz – 40 W (46 dBm).

R: DL = 46 dBm,

UL = 33 dBm.

For downlink

$$P = 46 + 18 - 0,3 = 63,7 \text{ dBm},$$

For uplink

$$P = 33 \text{ dBm}.$$

S calculated by the formula:

$$S = P_{tn} + M_{s/n} - L_n,$$

where P - is the thermal noise power of the receiver,

P: DL = -174,4 dBm,

UL = -104,4 dBm;

M - the required signal/noise ratio of the receiver.

M is taken for the model of the channel is "Enhanced Pedestrian A5".

M: DL = -0.24 dB; UL = 0.61 dB;

L - noise ratio of the receiver, L: DL = 7 dB, UL = 2.5 dB.

For downlink

$$S = -174,4 + (-0,24) + 7 = -167,64 \text{ dBm},$$

For uplink

$$S = -104,4 + 0,61 + 2,5 = -101,29 \text{ dBm},$$

Taking into account the results obtained, we calculate the value of MAL. For downlink:

$$L=33-(-101,29)+18-0,4-12-6,4-8,7+1,7=126,5 \text{ Db.}$$

Figure 4.9 shows the calculations in Matcad:

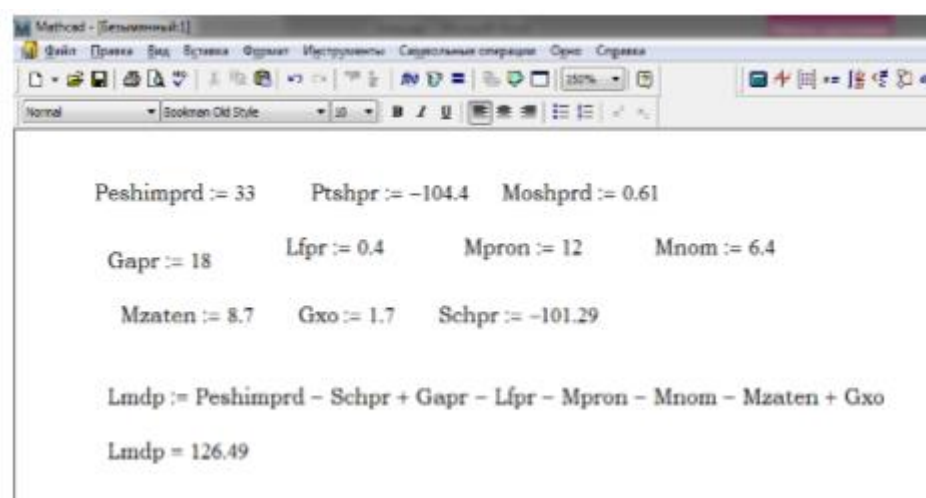


Figure 4.9 – Calculations in Mathcad

From the two MAL values obtained for downlink and uplink, select the minimum to make subsequent calculations of the communication distance and the radius of the cell. The limiting line on the communication distance is usually the line up.

5 Life Safety

5.1 Analysis of the company's environmental impact

The purpose of this work is to organize the VANET SDN network, in which the interaction of applications of one car with another, as well as from the interaction with stations located on the roadside. One of the types of energy pollution of the environment is the electromagnetic field. The use of electromagnetic energy in various fields of human activity has led to the addition of the electromagnetic field of artificial origin to the existing natural electric and magnetic fields of the Earth, atmospheric electricity, radio emission of the Sun and galaxies. As a biologically active factor, the electromagnetic field of artificial origin can have adverse effects on the environment and on humans. In this regard, the problem of environmental pollution by electromagnetic radiation of telecommunications facilities and facilities needs to be solved. It, traditionally being sanitary, has now become part of the overall environmental problem. Monitoring of the natural environment by electromagnetic factor is a serious theoretical and technical-economic task, which is closely connected with the problem of environmental and human protection from the adverse effects of EMF. However, the main sources of electromagnetic pollution of the environment are communications designed to increase public awareness. At the same time, the use of

various means of telecommunications is a powerful means of ideological influence on the population of the country as a whole and the region.

High-frequency (RF) equipment is used for both radio broadcasting and long-distance radio communication. The transmitter power is 250 kW or more. Over 100 standard sizes of antennas are widely used in this wave range, among which there are antennas and antenna systems with very high efficiency (narrow radiation patterns, high gain values). The main type of propagation of RF waves is propagation by reflection from the ionosphere (ionospheric or spatial waves). The earth wave is also present, but only near the radiating system, as it is strongly absorbed in the semiconductor soil. These systems are designed to transmit various messages and operate normally in continuous mode and in the range of 0.7–40 GHz. In the world practice of research there are two types of effects of EMF on biological objects: - thermal action, which include losses on currents of conductivity and displacement in the tissues of the body, having a finite resistivity, reflection at the interface and, in particular, at the border of "air-tissue", the depth of penetration into the tissue, standing waves in closed volumes, the redistribution of energy through the blood; - specific action, which manifests itself in a variety of phenomena and effects, such as resonance absorption of electromagnetic energy by protein molecules (this explains the mutagenic phenomena), direct and indirect effects on the Central nervous system, neuromuscular effects, the phenomenon of "pearl thread" (building suspended molecules parallel to the field lines, which leads to breaks in molecular bonds), polarization of molecules, etc.

5.2 Maximum permissible levels of human exposure to EMR

Maximum permissible levels of exposure to EMR RF per person:

- in the cases specified in paragraph 2.1.1. of these Sanitary norms and rules, the energy exposure per working day (shift) shall not exceed the values specified in table 5.1.

Table 5.1 - maximum permissible energy exposure values

Frequency bands, MHz	Maximum permissible energy exposure		
	On the electrical component, (V/m) 2, h	By the magnetic component, (a / m) 2, h	Energy flow density (mW / cm 2), h
0,03 -3	20000,0	200,0	-
3 – 30	7000,0	Not developed	-
30 -50	800,0	0,72	
50 -300	800,0	Not developed	
300 - 300000	-	-	200

Note: in these Sanitary norms and rules, in all cases, when specifying the frequency ranges, each range excludes the lower and includes the upper limit of the frequency; - PDU EMI intensity RF (EPDU, Napu, Ppepdu) depending on the time

of exposure during the working day (working shift) and the permissible exposure time depending on the intensity of EMR determined by the formulas

$$E = \sqrt{\frac{EE}{T}}$$

$$T = \sqrt{\frac{EE}{E^2}}$$

$$H = \sqrt{\frac{\partial\partial}{T}}$$

$$T = \sqrt{\frac{EE}{H^2}}$$

$$PPE = \sqrt{\frac{EE}{T}}$$

$$T = \sqrt{\frac{EE_{PPE}}{PPE}}$$

- the maximum allowable levels of the density of energy flow (Papu) in the frequency range 0,3 – 300 GHz depending on the duration of RF EMR exposure are shown in table 5.2.

Table 4.2 – RC-density of energy flow

Duration of exposure T, h	PPE, mcW/sm ²
8,0	25
7,0	27
7,5	29
6,5	31
6,0	33
5,5	36
5,0	40
4,5	44

Table 4.2 Continue

Duration of exposure T, h	PPE, $\mu\text{W}/\text{cm}^2$
4,0	50
3,5	57
3,0	67
2,5	80
2,0	100
1,5	133
1,0	200
0,5	400
0,25	800
20	1000

Note: if the duration of exposure is less than 0.2 hours, no further increase in the intensity of exposure is allowed for cases of exposure to persons from antennas operating in a circular view or scan mode, with a frequency of not more than 1 Hz and a duty cycle of not less than 20, the maximum allowable exposure intensity is determined

$$PPE = K \frac{EE_{PPE}}{T}$$

where K is the coefficient of attenuation of biological activity of intermittent effects, equal to 10. Regardless of the duration of exposure, the intensity of exposure should not exceed the maximum values given in tables 4.2 and 4.3 (e.g. $1000 \mu\text{W}/\text{cm}^2$ for the frequency range 300 MHz to 300 GHz). For cases of local irradiation of hands when working with microstrip microwave devices, the impact of the remote control is determined by the formula

$$PPE = K_1 \frac{EE_{PPE}}{T}$$

where K1-the coefficient of attenuation of biological efficiency, equal to 12.5.

At the same time: the density of energy flow on the hands should not exceed $5000 \text{ mW}/\text{cm}^2$. On the basis of the formula 5.8, we determine the maximum permissible values of the energy exposure, the results of the calculations are summarized in table 4.3.

$$EE_{PPE} = \frac{PPE_{GLE} T}{K_1} = \frac{55 \times 6,5}{12,5} = 28,6$$

Table 5.3-calculation Results

Duration of exposure T, h	PPE69DU, mW / cm ²	Remote control of energy exposition
6,5	55	28,6
6,0	58	27,84
5,5	60	26,4
5,0	63	25,2
4,5	67	24,12
4,0	71	22,72
3,5	76	21,28
3,0	82	19,68
2,5	89	17,8
2,0	100	16
1,5	115	13,8
1,0	141	11,28
0,5	200	8
0,25	283	5,66
0,125	400	4
0,08	500	3,2

5.3 Analysis of the Working Conditions of Technical Staff

Statistical analysis of the data network is necessary operator data taken from a personal computer. For normal operation, the computer needs a constant current, and the input of the power supply (PSU) is supplied with an alternating current voltage of 220 V. in the power supply, the alternating current is converted into a constant. The average power of modern PSU is from 300 to 500 watts.

The room for which the calculations will be made, is a camera room. 6 people: 3 replacement of the operator. In the day shift employs 3 people: a senior engineer and 2 engineers. Room: Length L=8 (m), width B=5m, height H=4 m. the Building is located in Almaty, which has 44 latitude. On the South side of the operator's room there are 2 Windows 2.2 m wide and 2.5 m high each.

The company has an eight-hour duration of the day. In according to the labor code of the law of the Republic of Kazakhstan in article 1 “on labor in the Republic of Kazakhstan”, working time is the time during which the employee in accordance with the acts of the employer and the terms of the individual employment contract performs labor duties. Acts of the employer or the collective agreement may be set 5-day or 6 day working week. For a six-day working week, the daily work may not exceed 7 hours, and for a five - day working week-8 hours.

To provide artificial lighting, fluorescent gas-discharge lamps with a capacity of 40 W and a nominal luminous flux of 3120 LM are used. as lamps, we will use lamps of the LOW-2x40-1001 type. To maintain the necessary microclimate. In the

operator room there are 6 desktops, which are personal computers necessary for the operators. Figure 5.1 shows the layout of the room.

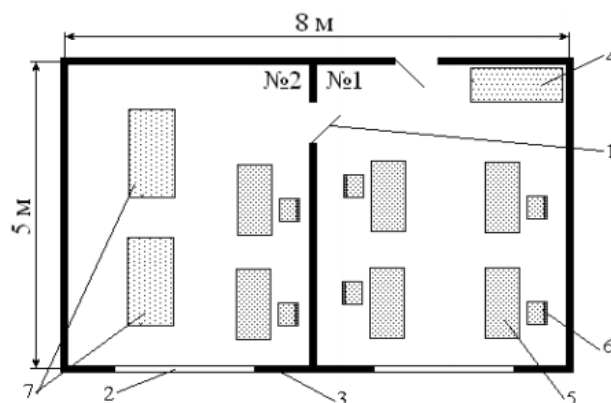


Figure 5.3 – Plan of the premises

where: 1-door; 2-window; 3-wall; 4-wardrobe; 5-table; 6-chair; 7-stand

When working with a computer for a long time, the employee often begins to feel a certain discomfort: he has headaches and pain in the eyes, fatigue and irritability. In the operator work is carried out on 1B category of work. Microclimatic conditions according to GOST 12.1.005. The microclimate parameters can be described as optimal, as indicated in table 5.1.

Table 5.1-Optimal norms of microclimate parameters

Period of work	Job category	T, °C	Air speed, m/s, not more than
Cold	I 6	31-23	0,1
Warm	I 6	22-24	0,2

Work tables should be placed in such a way that the monitors are oriented sideways to the light openings, so that the natural light falls mostly to the left. Artificial lighting is especially necessary in the evening. In addition, the long-term performance is affected by the state of the air in the working room. In accordance with GOST 12.1.005-88 in the work of medium gravity, 1B, the air temperature in the workplace should be 17-23 °C, the relative humidity - no more than 75 %, the air velocity - no more than 0.3 m/s. To maintain the microclimate in the production of air conditioning is used. The air conditioning system, in addition to performing the tasks of ventilation and heating, allows you to create a favorable microclimate in the summer, hot period of the year, thanks to the use in its composition of freon refrigeration machine. Operator's workplace this is a place in the "man - machine" system, equipped with information display facilities, controls and auxiliary equipment on which his work is carried out (see figure 5.2).

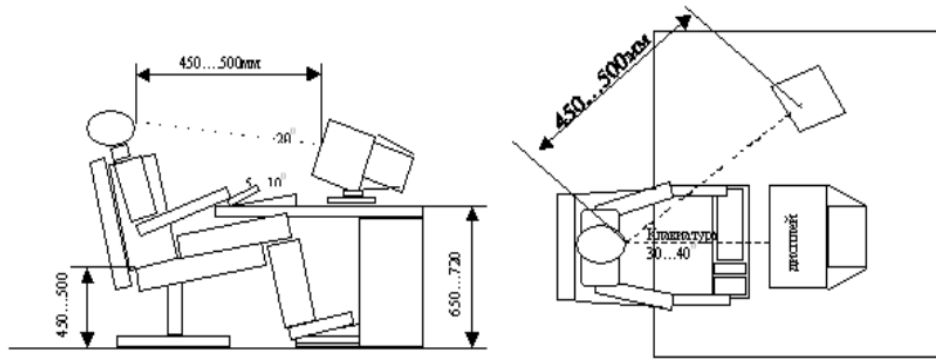


Figure 5.2-operator's Workplace (side and top view)

The room where the operator room will be located, which will be two operators, has a size: an area of 40 m², which corresponds to sanitary standards. After analyzing the working conditions of the technical staff of the operator Department, in this section we will solve the following tasks:

- calculate natural and artificial lighting;
- the device and the calculation of the air conditioning system.

5.4 The choice of the lighting system of workplaces. Calculation of industrial lighting

5.4.1 Calculation of natural light. Rooms with permanent stay of people should have natural light. In the design of new premises, the reconstruction of old, in the design of natural lighting of the vessel and other objects, it is necessary to determine the area of light openings, providing a normalized value of KEO in accordance with the requirements of SNiP RK 2.04-05-2002 " Natural and artificial lighting. Design standards". Rooms with permanent stay of people should have natural light. The operator room consists of two identical rooms. The length of the room L=4 m room width B=5 m, room height H=4 m. the Height of the working surface above floor level R=0,75 m. light Sources discharge lamps. Rated power- 40 W, rated luminous flux-3120 LM. The room has one window width of 2.2 m and a height of 2.5 m. the Lower edge of the window begins at 1.5 m from the floor. The window is located on one side of the room, depth l=B-1=4. Category of visual work III. Nearby is a 1-storey office building, located at a distance of P=15 m. the Plan of production facilities is shown in figure 4.1. Since both rooms are the same size and size of the Windows are also the same, the Windows are plastic with retractable, exterior adjustable blinds. The normalized value of K_{eo} is given to an administrative group 4 according to the formula

$$e_N = e_H \times m_N$$

where e_N is the value of KEO, the category of visual work III, then e_H = 1,2; m is the coefficient of light climate, for the administrative group 4 m_N = 1,1.

The value of KEO taking into account the coefficients m is

$$e_N = 1,2 \times 1,1 = 1,44$$

The window area is determined by the formula (4.2)

$$S_0 = \frac{e_N \times S_n \times \eta_0 \times K_{zd} \times K_z}{100 \times \tau_0 \times r_1}$$

where S_0 – total area of side light openings;

S_n - floor area of the room (m^2),

e_N - normalized value KEO;

K_3 - safety factor,

$\tau_0 = \tau_1 * \tau_2 * \tau_3 * \tau_4 * \tau_5$ - the overall coefficient of light transmission;

η_0 - light characteristic of windows;

r_1 - coefficient that takes into account the increase in KEO in side lighting due to the light reflected from the surfaces of the room and the underlying layer adjacent to the building;

K_{zd} - coefficient taking into account the shading of the Windows of opposing buildings.

Floor area of the room

$$S = L \times B = 4 \times 5 = 20m^2,$$

where K_3 – safety factor;

$K_3 = 1,2$ under natural side lighting.

For Windows with double-glazed Windows light transmission coefficient $\tau_1 = 0,8$. Since the Windows with double - glazed Windows, $\tau_2 = 0,75$. At side illumination $\tau_3 = 1$. As sun protection devices are used with retractable external adjustable blinds, so $\tau_4 = 1$. τ_5 -the coefficient that takes into account the loss of light in the protective grid, installed under the lights, take equal to 0.9.

$$\tau_0 = 0,8 \times 0,75 \times 1 \times 1 \times 0,9 = 0,54$$

In order to determine the coefficient η_0 , it is necessary to know the ratio of length to depth (to the most remote point from the window). Since the window is only on one side, this ratio is

$$\frac{L}{l} = \frac{4}{4} = 1$$

You also need to know the ratio B/h_1 , where h_1 is the height from the level of the conditional work surface to the top of the window.

$$h_1 = h_{ok} + h_{n.ok} - h_p$$

$$h_1 = 2,5 + 1,5 + 0,75 = 3,25m$$

$$B/h_1 = 1,54$$

Coefficient k_{zd} determined by the ratio P/H_{zd} , which in this case is

$$P/H = \frac{15}{4,5} = 3,33$$

From this ratio, we determine that $k_{zd}=1$. And so, substituting numerical values in the formula (2) we obtain

$$S_0 = \frac{1,44 \times 20 \times 21 \times 1,2 \times 1}{100 \times 0,54 \times 2,1} = 6,4m^2$$

According to the calculation, the window area of one room should be at least 6.4 m, but in one room with an area of 5.5 m . Therefore, the window available in the room does not meet the standards of natural light, so perform artificial lighting.

6 Business Plan

6.1 Summary

This diploma project considers the possibility of implementing an intelligent transport network VANET based on the promising LTE technology in Almaty. The purpose of the market development of new services in accordance with the concept of IoT (Internet of Things), such as VANET (Vehicular Ad Hoc Networks). The project is relatively new in the field of maintenance of wireless devices and is implemented through the deployment of a local network with VANET network components. The modern car contains about 100 electronic control units and they should benefit the driver and with the help of a new unique web service of the intelligent transport network VANET allows you to notify (receive) information about the load of a particular highway, weather conditions, icing of the road surface and so on. In the feasibility study, the economic performance of the network deployment with the presentation of VANET services was calculated, an analysis was made, and on this basis, this system can be considered effective for implementation and use.

6.2 Description of services

Today VANET technology is a promising technology for building wireless networks with small amounts of transmitted information. Being a distributed self-organizing network of multiple sensors and actuators, combined with each other by means of a radio channel LTE technology solves the problem of monitoring and control, almost without human intervention, with a long battery life (see figure 5.1). Huawei Technologies has created a new generation of LTE-B equipment that increases the bandwidth for users on the cell border (CEU) by at least 500%, thanks to the advanced capabilities of multi-band and multi-level network with support for various radio access technologies, which allows implementing seamless high-speed no-Edge networks. LTE provides theoretical peak data rates of up to 326.4 Mbps from base station to user (de facto 5-10 Mbps) and up to 172.8 Mbps in reverse. Thus, the leading mobile operator Kcell conducted LTE tests in its head office in Almaty. During the tests, they were able to obtain a data transfer rate of about 170 Mbit/s.

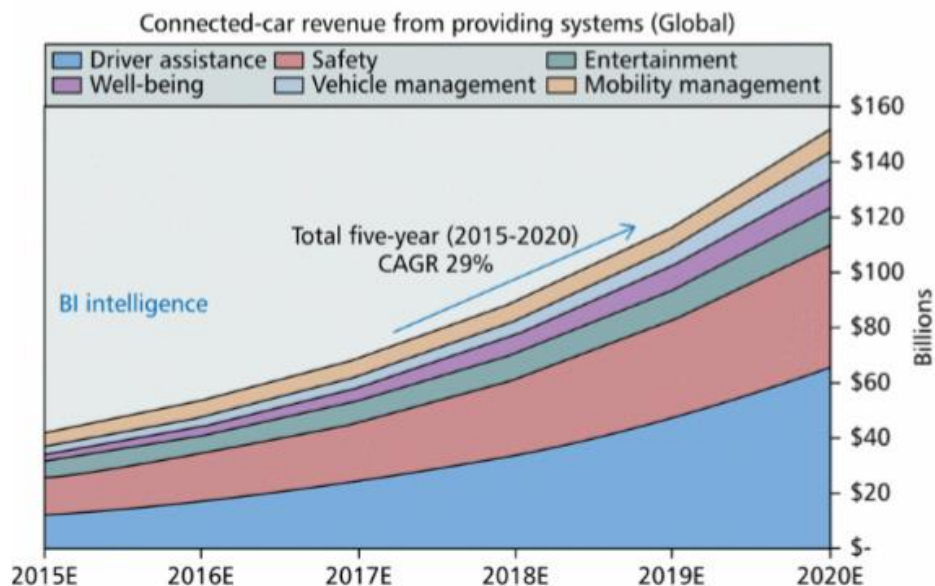


Figure 6.1 – Trends in the growth of applications of VANET technology

An important feature of the LTE network is that it works with a backbone based on the IP Protocol. The main advantage of LTE is that it can be built on the basis of existing equipment with relatively easy integration of GSM and WCDMA, in another way LTE network supports existing 2G and 3G subscriber devices. LTE-network is widespread in Kazakhstan, today they are more than 23% of the population of Kazakhstan. To connect subscribers via wireless communication to the corporate network infrastructure, you need to install the Serving gateway (SGW) – a service LTE network gateway for OS negotiation with the BS (eNodeB). To strengthen the BS on the antenna for the organization of radio. To provide high-speed data transmission services in the district center, we will install a controller (S – GW) - gateway to data networks of other operators for the LTE network). The interface of the connection of the CA and the controller is realized through the

interface V. 5.2 next, the physical circuit will connect the NodeB base station to the controller. The base station then emits power to the connected subscribers.

6.3 Analysis of Sales Market

For global operation of vehicle control devices (mobile devices), it is necessary to organize access to the data highway of Almaty city using wireless broadband LTE technology in the interaction of the vehicle with the infrastructure and the interaction of the car-car with the help of wireless broadband Wi-Fi technology of IEEE 802.11p standard. VANET network services will provide the following intelligent services: - Internet access; - multimedia, telephony; - smart Parking; - tourist information; - road surface services; - weather; - collision warning services; - automatic information service of emergency response services about the accident, etc.

6.4 Management

The implementation of the VANET network, its implementation in the city will ensure safety on the roads, awareness of the repair work and other Staff of technical personnel must meet the appropriate qualifications for work on the project of monitoring objects on the roads of the VANET system. The number of staff on the project is 2 people: 1 – engineer (0.5 rate) and 1 – operator (1 rate). The operator of this project will be engaged on a full-time basis. The engineer will follow the following functional duties: - coordinate and control technical technological processes; - manage the actions of the Department; to solve organizational and administrative issues. Operator - will perform the following duties: - maintenance of LAN and broadband wireless access system; - reporting on the work; - Analytics of the system.

6.5 Marketing Strategy

Providing a large number of services for the implementation of access to the data network for the operation of the VANET network makes it possible to obtain the necessary information from consumers without reducing the production process. Actions aimed at stimulating demand are to provide part of the services at reduced rates, they can be carried out during the advertising campaign. The implementation of actions to stimulate demand will help to reach a wide range of potential customers, show the availability and need to use the services provided.

6.6 Financial plan

6.6.1 Capital expenditures the Financial plan is generally part of a business plan that includes the calculation of total capital costs, revenues, operating costs, profits, profitability and payback period. Capital investments include the cost of equipment, installation and transport services. Total capital investments

$$K = KO + KM + KTP$$

where KO-equipment costs; KM-capital investments in installation work; KTR-capital investments in transportation costs (5% of the cost of equipment).

Equipment costs are given in table 6.1.

Name of equipment types	Quantity, PCs	Price, thousand tenge	The sum, thousand tenge
1. Huawei dbs3900 BS (kit)	2	201.6	403.2
2. Concentrator	1	30.0	30.0
3. Network switch level 3	1	160.0	160.0
4. Subscriber radio units	3800	4.80	18240
5. Gateway (S-GW)	1	120.9	120.9
6. Modular media Converter (MMC RGB)	1	113.8	113.8
7. UTP	1	8.0	8.0
8. Server	1	140.0	140.0
Subtotal			19215.9

Capital investments in transportation costs

$$KTP = KO \times 0,05 = 19215,9 \times 0,05 = 960,8$$

Capital investments are given in table 6.2.

Table 6.2 - Capital investments

Name of the items	The sum, thousand tenge
Equipment costs	19215,9
The capital cost of the installation work	200,0
Capital investments in transportation costs	960,8
Total capital investments	20376,7

Operating costs. In the service process and the provision of telecommunications services is an activity that requires the consumption of resources of the enterprise. The amount of costs for the year and will be the actual production cost or the amount of annual operating costs [19].

$$\sum E = PF + Fa + E + A + M + H$$

Where PF - Payroll Fund for all employees of the enterprise

Fa - social tax;

M- material costs and spare parts (costs for spare parts and maintenance are 0.5% of capital investments);

E- electricity costs;

A - depreciation;

N- overhead costs

Determine the payroll PAYROLL

Overhead costs make up 25% of all costs according to the formula (6.2):

$$PF = W_m + W_{add} \quad (6.2)$$

where: W_m - basic salary;

W_{add} - additional salary.

The bonus, which is an additional salary, is determined on average in the amount of 10% of the basic salary:

$$W_{add} = W_m \times 0.1 \quad (6.3)$$

Pension contributions also make up 10% of the PAYROLL:

$$PC = PF \times 0,1 \quad (6.4)$$

The social tax is 9% of the PAYROLL, together with the deduction of pension contributions:

$$S_t = (PF - PC) \times 0,11 \quad (6.5)$$

To date, the depreciation rate is D_r in the sphere .the connection of about 15% to 40% of the cost of all equipment, then depreciation, A_i :

$$A_i = \frac{D_r \times C \times N}{100 \times 12 \times n} \quad (6.6)$$

where: D_r - depreciation rate;

C - initial cost of equipment;

N - number of days .on performance of work;

n - number of days in the working month.

6.7 Labour Intensity

The working week lasts 22 days, therefore, to determine the salary for one working day, it is necessary to divide the monthly fee into twenty-two working days of a five-day working week. Therefore:

The salary of the head will be:

$$D = \frac{50000}{22} = 2273 \text{ tenge / day}$$

Research engineer will receive:

$$D = \frac{40000}{22} = 1818 \text{ tenge / day}$$

The developer engineer will receive a salary in the form of:

$$D = \frac{40000}{22} = 1818 \text{ tenge / day.}$$

Next, we determine the salary per hour, dividing the salary per day by 8 working hours:

Then the wage per hour at the head will be:

$$H = \frac{2273}{8} = 284 \text{ tenge /hour.}$$

From the research engineer:

$$H = \frac{1818}{8} = 227 \text{ tenge /hour.}$$

From the development engineer:

$$H = \frac{1818}{8} = 227 \text{ tenge /hour.}$$

The experiment consisted of several parts, let's define them in cycles.

The duration of the cycle in the bottom by parts of the experiment is determined by the formula:

$$t_n = \frac{T}{q_n \cdot z \cdot K} \quad (6.10)$$

where: T is the labor input stage, an hourly rate of;
 q_n - quantity. performers on stage;
 z - working hours, $z = 5$ hours;
 K - rate of compliance .time, $K = 1,1$;
The resulting value t_n rounded up to whole days.

$$t_{12} = \frac{15}{2 \cdot 5 \cdot 1.1} = 2 \text{ d};$$

$$t_{21} = \frac{4}{1 \cdot 5 \cdot 1.1} = 1 \text{ d};$$

$$t_{22} = \frac{5}{1 \cdot 5 \cdot 1.1} = 1 \text{ d}$$

Since the salary per hour and per day we have calculated, calculate the W_m :

$$W_m = 130\,130 \text{ tg}$$

The additional salary will be determined by the formula (6.3):

$$W_{\text{add}} = 130130 \cdot 0,1 = 13\,013 \text{ tg}$$

Calculate the wage Fund :

$$PF = 130130 + 13013 = 143\,143 \text{ tg}$$

Determine the amount of pension contributions:

$$P_c = 143143 \cdot 0,1 = 14\,314 \text{ tg}$$

Calculate social security contributions:

$$S_t = (143143 - 14314) \cdot 0,11 = 14\,171 \text{ tg}$$

6.8 Depreciation allocations

Depreciation. deductions for used equipment:

$$A_1 = \frac{40 \cdot 55000 \cdot 22}{100 \cdot 12 \cdot 30} = 1345 \text{ tg};$$

$$A_2 = \frac{15 \cdot 17000 \cdot 22}{100 \cdot 12 \cdot 30} = 155 \text{ tg};$$

$$A_3 = \frac{25 \cdot 9673 \cdot 22}{100 \cdot 12 \cdot 30} = 148 \text{ tg};$$

$$A_4 = \frac{40 \cdot 25000 \cdot 22}{100 \cdot 12 \cdot 30} = 611 \text{ tg};$$

$$A_5 = \frac{40 \cdot 127425 \cdot 22}{100 \cdot 12 \cdot 30} = 1168 \text{ tg}.$$

Table 6.8 - Information on the salary of the working staff

The name of the job	Performer	Laboriousness, an hourly rate of	Wages per hour of operation, Tg	Sum of wages fees per day, Tg	Sum of wages fees per month, Tg
Setting the task, control of the experiment	head	5	455	2 275	50 050
Algorithms, programming, experiment, calculations	developer	2,5	364	1 820	40 040
Registration of the results, providing the necessary information	assistant	5	364	1 820	40 040
Subtotal		2,5	183	5 915	130 130

The economic benefit of the thesis is based on the economic calculations. For this purpose, the work for implementation was determined, which takes into account the number of hours of different kinds of work, the percentage of total work, the hourly cost of work. On the basis of this was received the wage Fund. After calculating the cost of electricity, depreciation, social contributions, other costs, a chart of expenses.

With the help of this work, it is planned to use various methods of controlling the parameters of the navigation module, which in turn will allow to increase the accuracy of determining the location of the user.

Definitions, symbols and abbreviations

GLONASS - global navigation satellite system-Russian satellite navigation system. Ad Hoc - Decentralized wireless network with no permanent structure.

API - Application Programming Interface-a set of ready-made classes, procedures, functions, structures and constants provided by the application (library, service) or operating system for use in external software products.

ARP - Address Resolution Protocol-a Protocol in computer networks designed to determine the MAC address by IP address.

GPS - Global Positioning System is a satellite navigation system that provides distance, time and location measurement in the world coordinate system WGS 84.

MANET - Mobile Ad hoc Network is a decentralized wireless ad-hoc network consisting of mobile devices.

NGN - New Generation Networks are multi-service communication networks, the core of which are IP-based networks that support full or partial integration of voice, data and multimedia services.

P2P Peer — to-Peer is an overlay computer network based on equality of participants.

TCP - Transmission Control Protocol is one of the main Internet data transmission protocols designed to control data transmission.

TLS - Transport Layer Security is a cryptographic Protocol that provides secure data transfer between nodes on the Internet.

SDN - Software-Defined Networking is a data network in which the network management layer is separated from the data transmission devices and implemented programmatically.

VANET - Vehicular Ad hoc Network is a decentralized wireless ad-hoc network consisting of vehicles.

Conclusion

In the course of the thesis all the tasks were solved, and the goal was achieved. The analysis of the existing transport networks was carried out and their shortcomings were identified. Taking into account the weaknesses and strengths of traditional transport networks, it was proposed to use SDN technology. In the work, various options of CENTRALIZED SDN VANET architectures were proposed, network modes were developed. The advantages of using the proposed approach are considered. In the course of simulation in the VANET network simulator, the efficiency of routing protocols was evaluated, the proposed architecture options for a large-scale VANET network were implemented. The recommendations on the use of architecture options for certain scenarios of use are given. On the basis of the study it can be concluded that the use of SDN technology in VANET transport networks can improve the level of security. Unlike traditional VANET networks, the proposed centralized approach allows to establish security policy in the network, increase throughput, increase mobilization capacity, significantly reduce the system response time to external influences. Thus, the integrity, availability and confidentiality of information in transport networks is increased.

List of references

1. Что такое MANET или почему WiFi не решение всех телекоммуникационных проблем. — Режим доступа: <https://habrahabr.ru/post/197860/> (дата доступа: 04.11.2016)
2. Контроллер, NOX, Beacon. Обзорный курс. — Режим доступа: <http://old.arccn.ru/knowledge-base?pdf=5151d43024c96.pdf> (дата доступа: 06.12.2016)
3. Сети MANET и сети транспортных средств-VANET. Проект стандарта IEEE 802.11p. — Режим доступа: <http://www.incore.me/svyaz/seti-manet-i-seti-transportnyxsredstv-vanet-proekt-standarta-ieee-802-11p/> (дата доступа: 12.02.2017)
4. N. B. Truong, G. M. Lee, Y. Ghamri-Doudane. Software Defined Networking-based Vehicular Adhoc Network with Fog Computing. — Режим доступа: http://researchonline.ljmu.ac.uk/706/1/139019_1.pdf (дата доступа: 12.02.2017)
5. M. Gerla. Vehicular Cloud Computing. 2012.
6. C. Harsch, A. Festag, and P. Papadimitratos. Secure position-based routing for VANETs. 2007.
7. N. McKeown. Software-defined networking. 2009.
8. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. 2008.
9. ONF Solution Brief. OpenFlow-Enabled Mobile and Wireless Networks. 2013.
10. Компьютерные сети: учебник для студ. высш. учеб. заведений [Текст]: в 2 т. Т. 2 / Р.Л. Смелянский. — М.: Издательский центр «Академия», 2011. — 240 с.
11. Software-Defined Networking: The New Norm for Networks [Электронный ресурс] // Open Networking Foundation. — [2012]. — Режим доступа: <https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdnnewnorm.pdf> (дата доступа: 15.02.2017)
- 12.— Режим доступа: <http://www.osp.ru/os/2012/09/13032491/> (дата доступа: 09.03.2017)
13. Diego Kreutz, Fernando Ramos, and Paulo Verissimo. Towards secure and dependable soft-ware-defined networks. 2013.
14. Margaret Wasserman and Sam Hartman. Security analysis of the open networking foundation (onf) openflow switch specification. 2013.
15. K.-K. Yap, M. Kobayashi, R. Sherwood, T.-Y. Huang, M. Chan, N. Handigol, and N. McKeown. OpenRoads: empowering research in mobile networks. 2010.
16. J. Vestin, P. Dely, A. Kessler, N. Bayer, H. Einsiedler, and C. Peylo. CloudMAC: towards software defined WLANs. 2013.

17. Wireless & Mobile Working Group (WMWG). — Режим доступа: <https://www.opennetworking.org/images/stories/downloads/workinggroups/charter-wireless-mobile.pdf> (дата доступа: 24.02.2017)
18. P. Dely, A. Kassler, and N. Bayer. Openflow for wireless mesh networks. 2011.
19. I. Ku, Y. Lu, E. Cerqueira, R. Gomes, M. Gerla. Towards Software-Defined VANET: Architectures and Services. 2014.
20. F. Bonomi. The smart and Connected Vehicle and the Internet of Things. 2013.
21. H. Kim, N. Feamster. Improving Network Management with Software Defined Networking. 2013.
22. C.J Bernardos, A. de la Oliva, P. Serrano. An architecture for software defined wireless networking. 2014.
23. А.Е. Кучерявый. Самоорганизующиеся сети и новые услуги. 2009.
24. M. Mendonca, K. Obraczka, T. Turletti. The Case for Software–Defined Networking in Heterogeneous Networked Environments. 2012.
25. Open Network Foundation (ONF). Software-Defined Networking: The New Norm for Networks. 2012.
26. Open Networking Foundation (ONF). Software-Defined Networking: The New Norm for Networks. 2013.