2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), 7 October 2019, Shah Alam, Malaysia

Mesh Network Dynamic Routing Protocols

Zhanserik Nurlan
faculty of information technology
(of Affiliation)
L.N. Gumilyov Eurasian National University
(of Affiliation)
Nur-Sultan, Kazakhstan
zhanserik.nur@gmail.com

Tamara Zhukabayeva
faculty of information technology
(of Affiliation)
L.N. Gumilyov Eurasian National University
(of Affiliation)
Nur-Sultan, Kazakhstan
tamara.kokenovna@gmail.com

Mohamed Othman
dept. of communication technology and network
(of Affiliation)
Univsiti Putra Malaysia
(of Affiliation)
Serdang, Selangor, Malaysia
mothman@upm.edu.my

***Abstract*—The main course of this paper will be to assess the applicability of dynamic routing protocols in Mesh networks. In the process, evaluation criteria were identified, an evaluation method was developed and implemented using simulation in the NS-3 environment, a method for describing a topology has been proposed, and an experiment was conducted using the method on a simulated network topology. The experiment showed the possibility of applying the method to evaluate such indicators as throughput and error rate, loss coefficient, delay variation and network delay. The results obtained allowed to conclude about the applicability of particular routing protocol to specified topology with specific network quality requirements.**

Keywords—routing protocols, mesh, manet, wmn.

I. INTRODUCTION (*HEADING 1*)

Total informatization has a significant impact on the modern world, changing the mechanisms of interaction in society, provides new opportunities in almost all areas of activity. Due to the development of electronics, its miniaturization and cheapening, information-sharing devices show significant quantitative growth, and such concepts as "Internet of Things" (IoT), Internet of Everything (IoE) and Machine-to-Machine Communication (M2M) are in our everyday life.

According to a forecast published in the 10th annual report Cisco, the Visual Networking Development Index (Cisco® Visual Networking Index, Cisco, VNI) Wi-Fi and mobile devices in 2019 will generate 67% of IP traffic. The share of Wi-Fi will be 53% [13]. In many industries will be observed the proliferation of the Comprehensive Internet, as well as the introduction of smart home technologies (security video systems, smart meters, lighting and temperature control, etc.). The greatest growth will be observed in the consumer segment of health.

48% of machine-to-machine connections will be held by "smart home" in 2019. During this period, global machine-to-machine IP traffic will grow 15 times: from 308 petabyte in 2014 (0.5% of global IP traffic) to 4.6 exabyte by 2019 (2.7% of global IP traffic) [21]. For example, the article [5] describes the construction of an automated process control system (APCS) based on the implementation of an industrial wireless sensor system for collecting telemetric information for a territorially distributed technological object for storing natural gas.

The development of wireless data transfer technologies, including a set of 802.11 standards (Wi-Fi), has resulted in the emergence of a promising class of broadband networks with the MESH topology. In 2011, the IEEE 802.11s-2011 standard was adopted [14].

MESH networks most fully realize the flexibility of being able to scale, speed and ease of deployment.

II. TYPES OF DYNAMIC ROUTING PROTOCOLS

Routing protocols can be divided into two large classes: proactive and reactive [3].

A. Proactive Routing Protocols

In this protocol, when a network topology is changed, a broadcast of messages about these changes is initiated. All routes are stored in the memory of each node, and it can use them at any time. Due to the fact that, in fact, each node has a network connectivity graph, it is possible to construct the shortest route, for example, using the Dijkstra algorithm [23] [4]. An example of a proactive protocol is OLSR (Optimized Link-State Routing), the full description of which is presented in RFC 3626, and schematically the mechanism of operation is shown in Fig. 1.

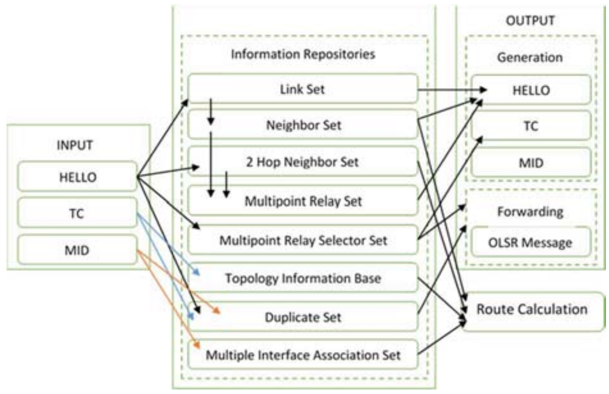

Fig. 1. The scheme of the OLSR routing protocol.

OLSR uses "HELLO" and "TC" (Topology Control) messages to detect neighbors to exchange network topology status information with other nodes: with the members of wireless Mesh network routing in OLSR domain. Each node in this domain uses the collected topology information to calculate the next hop when forwarding traffic to each destination node. It calculates the route with the least number of transitions. OLSR does not use a reliable delivery mechanism; instead, the protocol simply performs more frequent distribution of informational messages. Despite the fact that OLSR shows good results in large networks, has a small delay in connections, it inefficiently consumes the energy of inactive devices [24]. In addition, being a Link-State protocol, OLSR maintains large routing tables in large networks, which imposes increased requirements on computing resources.

978-1-7281-0758-5/19/$31.00 ©2019 IEEE

B. Reactive Routing Protocols

In reactive routing protocol, as in DSR (Dynamic Source Routing), routes exist only when they are needed, that is, when data is being transmitted over them [27]. If it is necessary to transmit data, the source node starts broadcasting a message: a probe. When processing it, the intermediate nodes add a route to the source node (reverse route) and continue its broadcast. If a packet is received again, a loop is detected and the message is deleted. When the message probe reaches the destination node, it generates a confirmation message and sends it along the already formed return route [25]. When working according to this scheme, an increase in the packet size occurs with an increase in the number of intermediate nodes passed, which is an obvious disadvantage. Therefore, the cached route label is used [9], to compensate for this particular feature during retransmissions, which reduces overhead costs for traffic transmission.

Another example of a reactive protocol is AODV [12]. This protocol uses a different mechanism of routes formation. The protocol creates routing tables at each node of the network member. The shortest routes to each node of the wireless network are entered into these tables through each neighboring node. Each node exchanges route information with neighboring nodes. As in DSR, the AODV protocol establishes routes when they are necessary, and with the expiration of the timer, unused routes are removed from the tables. Consequently, the protocol has the disadvantage of delaying the initial search for a route.

C. Hybrid routing protocols

These routing protocols combine reactive and proactive protocol mechanisms. Hybrid protocol operation scheme implies separation of Mesh networks into zones: clusters. Within these clusters, a proactive protocol is functioning, but the routes between clusters are built through reactive protocol.

The advantage of such a shared work scheme is to reduce the protocol traffic service, the distribution of which is limited by the boundaries of the cluster to which the node belongs. For the same reason, the size of the routing tables on each node is reduced. It is expected that these benefits should become more pronounced as the size of the Mesh network increases. An example of a hybrid protocol is the Hybrid Wireless Mesh Protocol (HWMP). This protocol combines reactive and proactive mechanisms based on the AODV protocol, which has been refined for Mesh networks. The description of this protocol is already in the IEEE 802.11s standard, and it is already mandatory for this standard as the default protocol [26]. The Mesh IEEE 802.11s network frame format is almost identical to the IEEE 802.11 standard frame format. The structure of the frame headers of both types completely coincides. The frame difference is in the payload field, which, in the case of the 802.11s frame, accommodates the Mesh header at the beginning of this field. This header is present in frames only when shipped between the Mesh nodes of the network. The content of the Mesh header consists of four fields. The flag field controls the processing of the header itself. Currently 2 out of 8 bits are used, which are responsible for determining the size of the Mesh address. The TTL field is responsible for the remaining number of shipments before the frame is destroyed. The Mesh sequence number prevents duplicate frames from being sent during multicast or broadcast. The MESH address extension field is intended for additional addresses of the traffic source and its destination, if one or both of them are not members of the Mesh network. The 802.11s frame format and the fields described above are illustrated in Fig. 2.

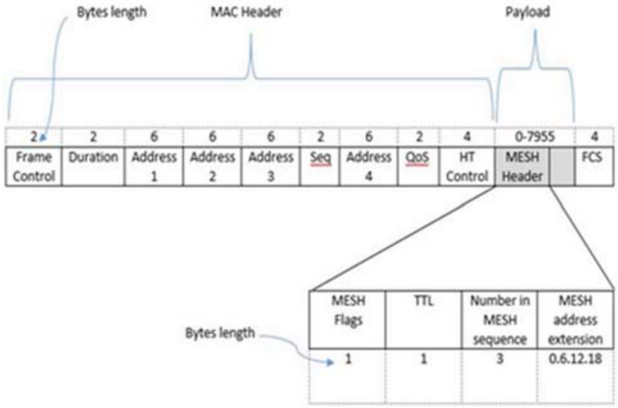

Fig. 2. 802.11s frame format.

The disadvantages of HWMP as a hybrid protocol is the need to partition the network into clusters, which complicates the initial deployment of the network and its support.

Several popular protocols as: CJDNS, B.A.T.M.A.N, DTN, Npv7_HT (Netsukuku), and OSPF are presented in Table I to compare their functionality [20].

TABLE I. ROUTING PROTOCOL FUNCTIONALITY COMPARISON TABLE

Functionality	***Protocol***				
	CJDNS	***B.A.T. M.A.N***	***DTN***	***Npv7_HT***	***OSPF***
Auto-destination address	Yes	No	No	Yes	No
Auto configuration routing	Yes	Yes	Yes	Yes	partially
Distributed marshalling	Yes	Yes	Yes	Yes	partially
IPv4 / IPv6	IPv6	Yes	Yes	IPv4	IPv4
Traffic encryption	Yes	No	No	No	No
Auto-tuning	Yes	Yes	Yes	No	Yes
LINUX support	Yes	Yes	Yes	Yes	Yes
Windows support	Yes	No	No	No	No
Mac OS X support	Yes	Yes	Yes	Yes	Yes
Requirement to computing resources	Low	Low	Low	High	Low
Linux kernel integration	No	Yes	No	No	Yes
Networking over the Internet	Yes	No	No	No	No

Based on the above comparison, the functionality of the protocol can be one of the determining criteria.

III. Routing Protocol Metrics

Today, many metrics have been developed specifically for Mesh networks [10]:

1) Hop Count: Is the metric of the shortest way. This metric is used in the above-mentioned AODV, DSR protocols.

2) ETX (Expected Transmission Count): The ETX metric determines the number of required data packet transmissions to ensure guaranteed delivery via communication channels and is calculated using the formula $ETX = 1 / (Df * Dr)$, where Df is the success rate of the packet forwarding, and Dr is the return rate of the successful forwarding. These coefficients, in turn, are calculated using regular probing by service packets by each node towards its neighbors.

3) ETT (Expected Transmission Time): The metric takes into account the size of user data packets and bandwidth. The metric is calculated using the formula $ETT = ETX * Size / Bandwidth$. The ETT of the entire route is calculated as the sum of all ETT intermediate nodes. A lower metric value means a better metric.

4) Airtime Link Metric: The IEEE 802.11s standard for the compatibility of data transfer devices prescribes the use of the Airtime Link Metric (transmission time per channel) as a default metric. The metric is calculated by the formula (1) [11].

$$C = (O + Bt / r) * 1 / (1 - ef) \quad (1)$$

Where:

C metric is the packet transmission time in seconds

O – overhead for the implementation of the transfer frame in the channel

Bt – Frame size in bits

r – Bitrate (Mb / s)

ef is the frame error probability. The method for determining this parameter is not given in the standard.

IV. PERFORMANCE CLASSIFICATION

Standards for network service quality indicators were pre-established based on the guidelines of ITU-T Y.1541 Recommendation (requirements for target values of IP network performance indicators) developed by the International Telecommunication Union (ITU) [18].

Y.1540 describes the standard characteristics for data transmission in IP-based networks [16].

Y.1221 provides a general description as well as tasks and procedures for traffic control and congestion control in IP-based networks [17].

1) Network latency ITU-T Y.1540 (03/2011): Is the time interval obtained as the difference between the time of receiving a data packet and the time it was sent. Calculated by the formula (2)

$$IPTD = T2 - T1 \quad (2)$$

Where:

IPTD – IP transfer delay

T2 – time to receive the package

T1 – package departure time

2) Jitter ITU-T Y.1540 (03/2011): IPDV (IP Delay Variation) is the difference between the current IPTD value and the minimum IPTD value. Formula (3)

$$IPDV = IPTDac - IPTDmin \quad (3)$$

Where:

IPDV – Jitter

IPTDac – Current Delay Value

IPTDmin – Minimum delay value

3) Reliability ITU-T Y.1540: Reliability can be calculated as the ratio of network availability to data transmission in the time interval during which the measurement is made to the same interval. Formula (4)

$$K = Tav / Tmax \quad (4)$$

Where:

Tav – the availability of network infrastructure to transmit traffic of a particular class.

Tmax – The time interval during which the measurement is made.

4) Packet loss ITU-T Y.1540 (03/2011): IPLR (IP loss ratio) - packet loss ratio. This ratio is calculated as the ratio of lost packets to the total number of transmitted packets in the observed time interval. Formula (5)

$$IPLR = lostPacketsSum / PacketsSum \quad (5)$$

Where:

IPLR – packet loss ratio.

lostPacketsSum – the amount of lost packets. The value can be calculated as the difference between the sum of received packets and the amount sent.

PacketsSum – the amount of transmitted packets.

5) IPER (IP error ratio): The ratio of damaged packets, which can be calculated by the formula (6) in the selected time interval.

$$IPER = errPacketsSum / errPacketsSum + rxPacketsSum \quad (6)$$

Where:

IPER – the ratio of damaged packets.

errPacketsSum – the amount of damaged packets received on the addressee's interface during the observation period.

rxPacketsSum is the sum of received packets without errors.

6) Bandwidth. ITU-T Y.1221 (06/2010): This is the amount of data delivered in a certain period of time.

7) Quality of service in the network: Any traffic flow, the characteristics of which satisfy the performance values of the corresponding class of service given in Table II, can be considered as fully compliant with the ITU-T Y.1541 regulatory recommendations for this class.

TABLE II. REGULATORY PARAMETER VALUES FOR TRAFFIC CLASSES

Parameter	*Service Classes*					
	Class0	***Class1***	***Class2***	***Class3***	***Class4***	***Class5***
IPTD	100ms	400ms	100ms	400ms	1s	-
IPDV	50ms	50ms	-	-	-	-
IPLR	$1x10^{-3}$					-
IPER	$1x10^{-4}$					-

The values shown in the table are the maximum allowed for the average IPTD delay, IPDV and IPLR. ITU-T Y.1541 recommends a minimum observation interval. For example, for telephony, it is 10 seconds at a data transfer rate of 50 to 100 packets per second.

We can use the resulting set of values as control points when conducting an experiment with our Mesh network model. For definiteness, we will use the parameters specified in recommendation Y.1541 for G.711 voice traffic, namely:

IPTD – 100ms, IPLR – 0.1%, Bitrate – 87kbit for network class = 0

V. IMPLEMENTATION OF THE ASSESSMENT METHOD

To assess the applicability of the routing protocols of MESH networks, a NS-3 (Network Simulator 3 – a free license software distributed under the "GNU GPLv2 license") simulation method was chosen. which implements reactive and proactive mechanisms for routing protocols of Mesh networks, such as AODV and OLSR.

Services such as "Maps.yandex.ru" YMapsML (Yandex Maps Markup Language) and "maps.google.com" KML (Keyhole Markup Language) provide a convenient way to place your own labels on maps for the designed MESH network. Both services allow you to export a dataset to XML. In 2008, KML was published as an OGC standard. (Open Geospatial Consortium) [22].

For the purpose of the experiment, a topology with a coverage area of about 45 hectares and comprising 50 nodes was compiled. The topology diagram is shown in Fig. 3.

Fig. 3. Network topology diagram.

T1 acting as a gateway (MPP);

T2 is the most remote node in the network from the T1 gateway

The distance between nodes T1 and T2 is 623 meters.

Table III shows the parameters of the experiment scenario for our model, which are determined from the downloadable network topology. The values given are identical for each involved routing protocol.

TABLE III. EXPERIMENT SCRIPT PARAMETERS

IPTD(T2-T1) delay	100ms
IPDV jitter	50ms
IPLR packet loss rate	0.001
IPER packet loss rate with errors	0.0001
Bitrate speed of each packet	87Kbit
Number of threads	3 to 10
Flow measurement time	10s
Nodes: destination and source of streams	T1, T2

The IPTD, IPDV, IPLR, and IPER values are the maximum allowable values for each stream, and the Bitrate is the minimum flow rate.

The NS-3 offers 802.11a / b / n / ac standards, n in the 2.4 and 5 GHZ range. During the experiment, for definiteness, we will use 802.11n_5GHZ.

For our topology, we will use the address range 10.0.0.0/8.

It should be noted that the Cartesian coordinate system is used in NS-3.

The coordinates of our topology are presented in the WGS84 system used by google for its maps.

VI. ANALYSIS OF THE RESULTS OBTAINED

A total of 7 measurements were made for each type of protocol. At each iteration, the number of threads was increased by 1.

Each protocol was evaluated under equal conditions: with the same models of signal attenuation and error handling, with the same start-up intervals and the time of their existence. The results are presented in the form of a pivot Table IV.

TABLE IV. TRAFFIC FLOW CHARACTERISTICS

Number of threads	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
IPTD Delay								
AODV IPTD	24	40	37	93	47	52	77	74
OLSR IPTD	21	30	46	98	205	225	200	186
IPDV Jitter								
AODV IPDV	11	30	12	44	10	8	23	5
OLSR IPDV	4	8	13	28	20	20	21	21
IPLR Loss Ratio								
AODV IPLR	0,1135	0,4794	0,3969	0,3673	0,0935	0,4583	0,6426	0,3265
OLSR IPLR	0	0	0	0	0	0	0	0
IPER Error Ratio								
AODV IPER	0	0	0	0	0	0	0	0
OLSR IPER	0	0	0	0	0	0	0	0
RxBitrate Kbps								
AODV rx_bitrate	73	41	51	52	79	49	31	56
OLSR rx_bitrate	90	89	90	90	85	78	67	62

A. Packet loss rate (IPLR parameter)

The results show that network performance is significantly different when applying the routing protocols AODV and OLSR on this network topology. When using the AODV protocol, the network does not meet the requirements of the traffic flows used in our test scenario for the IPLR (Lost Packet Ratio) characteristic, significantly exceeding the allowed value of 0.1%. As it can be seen from the data of the table and graph in Fig. 4. At the same time, OLSR, on the contrary, demonstrates satisfactory performance on this parameter.

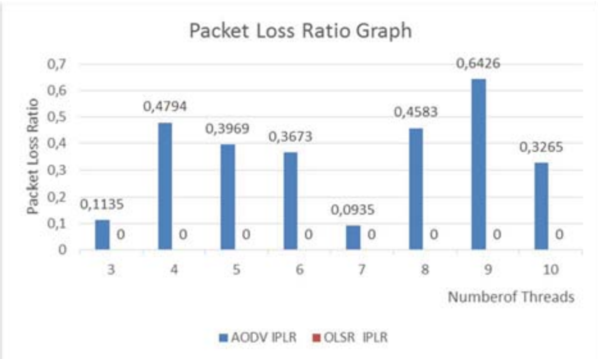

Fig. 4. Packet Loss Ratio Graph.

B. Network latency and traffic flow rates (Delay)

For this parameter, the AODV indicators are within the allowable values, but the flow rate is below the allowable value of 87 Kbps. When using OLSR, the network latency value is within acceptable limits with 6 concurrently executed threads. Fig. 5.

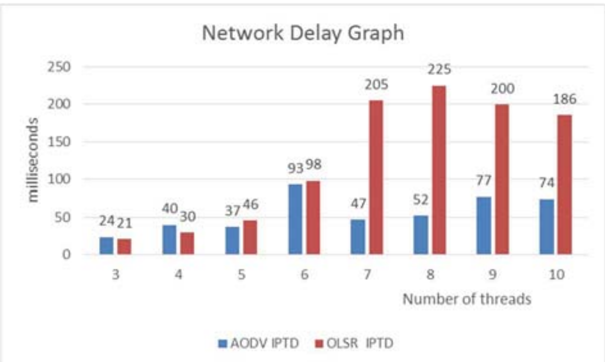

Fig. 5. Network Delay Graph.

Network latency when using the OLSR protocol increases when testing up to 8 flows inclusive, but then decreases, following a decrease in the flow rate, as illustrated in the summary chart in Fig. 6.

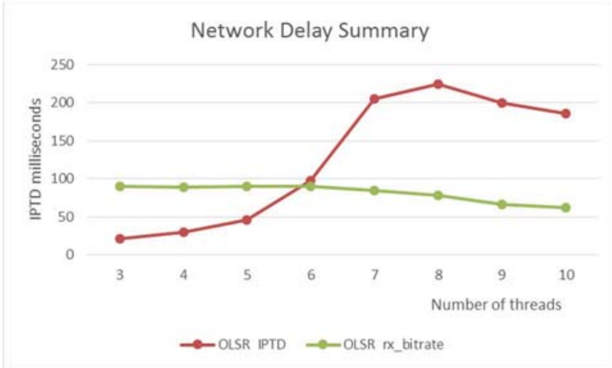

Fig. 6. Network Delay Summary.

Thus, when using OLSR, network latency and flow rates are maintained within the allowable interval when testing up to 6 flows inclusive.

C. Delay variation (Jitter)

Indicators obtained during the experiment on the IPDV parameter are within the allowable range of values when testing up to 10 simultaneously launched threads inclusive. Fig. 7.

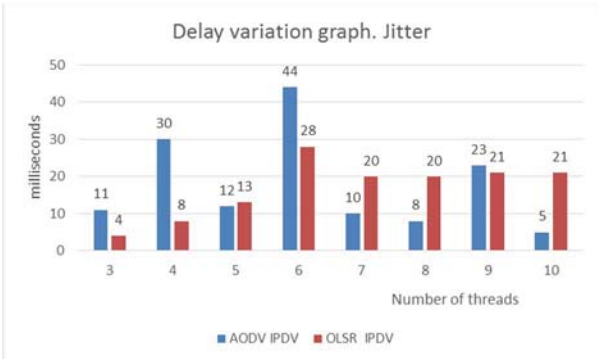

Fig. 7. Delay variation graph. Jitter (IPDV).

D. Traffic flow rate

When evaluating the flow rates, it should be noted that during the experiment using the AODV protocol, the flow rates did not satisfy the script requirements in all testing attempts. There are also strong fluctuations in the obtained values for the protocol relative to the OLSR, which is obviously due to the high packet loss rate (IPLR). The cumulative graph presented in Fig. 8 illustrates the relationship between the packet loss rate and bit rate (Bitrate) when using the AODV protocol in the network.

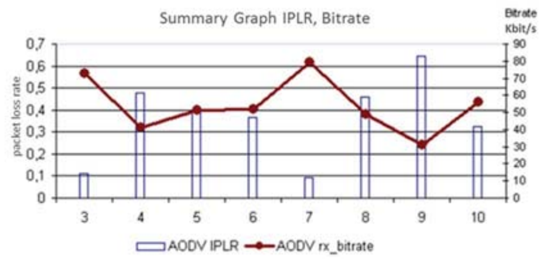

Fig. 8. Summary Graph IPLR, Bitrate.

Thus, despite the fact that the obtained network delay and jitter values when using the AODV protocol are within acceptable limits, this protocol can be considered not applicable for the network topology specified in the scenario with the type of traffic being tested.

VII. CONCLUSION

During the study, a method to evaluate the applicability of dynamic routing protocols on a given topology of the Mesh network was developed and implemented, based on the recommendations of the International Telecommunication Union (ITU-T Y.1541). An experiment with a network model was conducted. Based on the results of the experiment, the performance of the proposed method was determined.

The developed method is of practical value for the design of wireless MESH networks, allowing you to check for compliance with the characteristics of network applications when planning a topology. What can allow in advance to make the necessary changes.

REFERENCES

[1] Z. S. Ablyalimova and D. M. Urazaliyeva, “Routing in mesh networks based on chaotic radio pulses,” IV All-Russian Conference Radiolocation and Radio Communication, vol. 4, pp. 457–461, 2010.

[2] V. Vishnevsky, D. Lakontsev, A. Safonov, and S. Shpilev, “Routing in broadband wireless MESH networks,” ELECTRONICS: Science, Technology, Business, vol. 6, pp. 64–69, 2008.

[3] E. S. Zatsepin, “Overview of the characteristics of routing protocols in mesh networks,” International Journal of Experimental Education, vol. 10, pp. 342–345, 2013.

[4] N. A. Kuznetsov and V. N. Fetisov, “Dijkstra's algorithm with improved robustness for controlling routing in IP networks,” Automation and Remote Control, vol. 2, pp. 80–85, 2008.

[5] S. V. Lartsov, V. E. Stolyarov, I. A. Dyachenko, and V. M. Karyuk, “Organization of automated process control systems for distributed objects based on wireless sensor networks,” Exposition Oil Gas, vol. 3, pp. 29–32, May 2013.

[6] A. A. Pavlov and I. O. Datiev, “Wireless Routing Protocols,” Proceedings of the Kola Scientific Center of the Russian Academy of Sciences, vol. 5, pp. 64–75, 2014.

[7] G. V. Popkov, “MESH-networks: development prospects, possible applications,” Computer science problems, vol. 3, pp. 74–79, 2012.

[8] M. L. Sichitiu, “Wireless mesh networks: opportunities and challenge,” Proceedings of the Wireless World Congress, Palo Alto, CA, May 2005.

[9] J. Jun and M. L. Sichitiu, “MRP: Wireless mesh networks routing protocol,” Computer Communications, vol. 31, pp. 1413–1435, May 2008.

[10] V. Kisara, “A new routing metric for wireless networks,” Graduate Theses and Dissertations, 2019.

[11] G. L. Byeong, Ch. Sunghyun, Broadband Wireless Access and Local Networks: Mobile Wimax and Wifi 1st Edition, p. 572.

[12] Ad hoc On-Demand Distance Vector (AODV) Routing, Electronic Document, https://tools.ietf.org/html/rfc3561

[13] Cisco Visual Networking Index: Forecast and Trends, Electronic Document, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

[14] IEEE 802.11s-2011-IEEE Standard for Information Technology, Electronic Document, https://standards.ieee.org/findstds/standard/802.11s-2011.html

[15] Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Electronic Document, https://tools.ietf.org/html/rfc2501

[16] ITU-T Recommendations, ITU-T Y.1540 (03/2011), Electronic Document, http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11079&lang=ru

[17] Y.1221 : Traffic control and congestion control in IP-based networks, Electronic Document, http://www.itu.int/rec/T-REC-Y.1221-201006-I

[18] Y.1541 : Network performance objectives for IP-based services,, Electronic Document, https://www.itu.int/rec/T-REC-Y.1541-201112-I/en)

[19] The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, Electronic Document, https://tools.ietf.org/html/rfc4728).

[20] Wi-Fi Mesh network for the smallest, Electronic Document, http://habrahabr.ru/post/196562

[21] Cisco Visual Networking Index: Op. cit.

[22] GML, YMapsML and KML, Electronic Document, https://tech.yandex.ru/maps/ymapsml/doc/1.x/guide/concepts/langs-docpage/

[23] E. S. Zatsepin, Op. cit.

[24] Ibid

[25] Ibid

[26] J. Jun and M. L. Sichitiu, Op. cit.

[27] Z. Nurlan, T. K. Zhukabayeva, and M. Othman, “Comprehensive review of routing protocols in wireless adhoc networks,” XVI International Conference of Students, Graduate Students and Young Scientists, vol. 7, pp. 107–110, 2019.