Journal of the Nigerian Association of Mathematical Physics
***Volume 63, (January – March, 2022 Issue)*, pp99 – 108**
© J. of NAMP

INVESTIGATING TRUSTED ROUTING MECHANISM ON A FULL-MESHED TELECOMMUNICATION NETWORK MODEL

OSUOLALE A. TIAMIYU

Department of Telecommunication Science, University of Ilorin

Abstract

The article is on the study of the properties of the trusted routing mechanism via simulation experiments of a fully-meshed telecommunication network model. The description of the model, the experimental results and their interpretations are given.

***Keywords**:* Trusted routing, routing mechanism, telecommunication network, node monitoring, trusted node, network agent.

1. INTRODUCTION

One of the main requirements for a modern telecommunication network (TN) is the scalability, which implies the ability of the network to be quite large and complex without reduction in the expected QoS level, while it is still secured and controllable [1-3]. The dominant role of routers for scaling TN involves the maximum use of a special protection mechanism - routing control [1, 3]. This mechanism clearly requires trust in the intermediate nodes, which in this context implies controlling routing equipment by excluding the possibility of modification or substitution of information in the transit traffic [1, 4, 5]. This, therefore, should be about a certain mechanism of trusted routing. Trusted routing (TR) is perceived as process of planning and organizing traffic on a calculated route through network nodes, avoiding possibility of tampering with information in any form while the information stream is passing through those network nodes [6, 7]. From the standpoint of the pervasive security mechanisms, the TR implements the so-called trusted functionality, according to the subsection 5.4.1.1 of ISO 7498-2 – "any functionality directly providing security mechanisms or access to them should be trustworthy" [8]. In addition, it could be said that the TR implements the formula «routing control + trusted functionality» [1, 8, 9].

2. LITERATURE REVIEW

The issue of scaling of telecommunication structures of complex systems for special purposes nowadays is paramount [10-14]. [12] [13] [14]. Firstly, the system can scale in relation to its size, which means other users and resources can easily connect to it. Secondly, the system may scale geographically, i.e., users and resources can be in different areas or locations worldwide. This entails connection security problems for new objects connecting to open networks like the Internet [15]. Thus, as dependent on telecommunication networks grows, so also the users' perception of threats [16, 17]. Transmission of confidential information between computers of different networks is not safe, as there is a risk of unauthorized access (UnA) to such information in the course of its route from a sender to a receiver [1, 10, 18, 19]. All these necessitate researching into data routing process and routing control methods, as well as existing security mechanisms, to proffer possible solutions.

3. RELATED WORKS

Authors in [20] proposed a novel trust routing decision algorithm based on fuzzy dynamic programming theory. The model tried to analyze the physical requirements and psychology of the malicious attackers. Further, authors in [15] proposed a new trusted routing protocol in VANET based on GeoDTN+Nav by using trust management model of Bayesian and the three opportunistic routing forwarding models, which includes four steps of the routing initialization, the routing discovery, the trusted routing establishment and the routing deletion. In the model proposed by the authors in [15], when a node was abnormal or attacked, the trust value was gradually reduced until it was less than the threshold. This implies that attackers could have gotten access to part or whole of some information being sent, very unlike the proposed TR mechanism being studied.

A trusted routing to locate and preserve trusted routes in MANET was proposed by authors in [20,21]. The work extended dynamic source routing (DSR) protocol to identify trustworthy of nodes by using the dynamic trust mechanism under the presence of selfish or malicious nodes. However, no mechanism for detection and/or protection from attacks.

Even though MPLS provides data flow control benefits (improves efficiency, integrates IP and ATM-based network, allows the creation of virtual channels), there is an issue with integrity and confidentiality of the traffic passing through the MPLS network [4, 6, 9].

While theoretically, the TR mechanism ensures the integrity and confidentiality of the network traffic, in the work of the author in [6] were analyzed and compared these two mechanisms with respect to data security, QoS and network scalability.

Corresponding Author**:** Osuolale A.T., Email: ozutiams@yahoo.com, Tel: +2349057151350

Based on the analysis of the VPN and MPLS for trusted functionality, the TR mechanism will work well only on a fully meshed network because there is a possibility of traffic passage on many and, simultaneously, different routes from one point to another on the same network [21]. Moreover, an advantage of such a network is that no node relies on a single connection, and this broadens a choice based on the trust level of nodes to be used in the data transmission in a network, and thus, assists in the process of calculating route.
The absence of TR specifically hinders the widespread use of the routing control mechanism for scaling TN. Such state of affairs is caused, among other things, by the lack of a clear understanding, among specialists, of the limits of applicability of the mechanism and the possibility of implementing TR using standard TN tools [2,9 ,16, 22]. [2] [9] [16] [23]. The lack of wide access to publications on this topic only underlines the prevailing lack of the knowledge. The developed simulation model of TN with failures and node monitoring is designed to provide new knowledge about the properties of the TR mechanism by conducting a number of experiments.

4. RESEARCH METHODOLOGY

The conceptual model of TN with TR was developed under the assumption that: the network is fully meshed, with the first and last nodes being terminals; nodes are unreliable (the probability of failures and the rate of restoration of nodes depend on their number); the probability of choosing the next node (route) depends on the type of the message and the number of the current node; all communication lines are absolutely reliable; the processing time of a message in a node depends on its number; if the next node is busy or out of order, the mechanism of controlling additional nodes is activated; there is a restriction on the time the message spends on the network and the control intensity; time of controlling additional nodes, of course.

As a means of developing a software model of a TN with TR, GPSS was chosen - a fairly powerful and at the same time quite simple language for writing simulation models. The program model has a modular structure, namely: segments for setting source data, generating-servicing transaction-message flows and node failures; blocks for routing messages, processing transactional messages in a node, trusted routing, accounting for failures, successful completion of a transaction, and restart.

The first experiment will determine the dependence of the influence of simultaneously acting factors on the responses of the developed simulation model of TN with TR.

5. RESULTS AND CONCLUSION

The name (content) of the factors being evaluated, the model name of the corresponding input variable, and also the lower and upper levels (assuming that a possible range of changes are covered, based on experience and common sense) are given in Table 1.

In order to obtain the most complete and reliable information about the behavior of TN with TR, we plan and conduct a fractional factorial experiment with a total number of 2^5 observations. According to [23-25]. a plan constructed by this method has the properties of symmetry, normalization, orthogonality, and rotatability, which provides improved quality of the conducted experiment. The matrix for planning a fractional factorial experiment for the 7-factor case and 32 observations is given in Table. 2.

The name (content) of the evaluated responses, the model name of the corresponding output variable are given in table. 3.

The 32x4 matrix of the results is shown in table. 4.

For regression equations of the type:

$y = m_1x_1 + m_2x_2 + ... + b$, (1)

where y is a function of independent *value x*,

m is coefficients corresponding to each independent variable x,

b is constant,

built-in Excel-function «LINEST» is used to calculate linear series statistics, using the least-squares method to calculate a line of best fit through a supplied set of points.

For probability of non-delivery of message LINEST function returns an array which describes received y_1 straight line (see table 5) where: se_1, se_2,..., se_n are standard error values for coefficients m_1, m_2,..., m_n; r_2 is *coefficient* of determination; se_y is standard error for y assessment; F is F-observed value; d_f *is* degrees of freedom; ss_{reg} *is* regression sum of squares; ss_{res} *is* residual sum of squares.

Table 1: Evaluated factors

Factor			**Levels**	
Denomination (content)	**Variable name**	Input variable	**–1**	**1**
Acceptable transmission time	time_limit	x_1	500	1000
specified transmission time over the network	Tz	x_2	150	500
Waiting time for controlling	time_control	x_3	1	50
Handling waiting time at node	time_node	x_4	1	50
Limit of the intensity of controlling	control_limit	x_5	0.0	1.0
Waiting time between failures of nodes	time_crash	x_6	200	2000
Waiting time for node recovery	time_restore	x_7	50	200

Table 2: Experiment planning matrix

	1	2	3	4	5	6	7		1	2	3	4	5	6	7
	1	1	1	1	1		1	**7**	1	1	1	1			
		1	1	1	1	1	1	**8**		1	1	1		1	
	1		1	1	1	1	1	**9**	1		1	1		1	
			1	1	1		1	**0**			1	1			
	1	1		1	1			**1**	1	1		1			1
		1		1	1	1		**2**		1		1		1	1
	1			1	1	1		**3**	1			1		1	1
				1	1			**4**				1			1
	1	1	1		1			**5**	1	1	1				1
0		1	1		1	1		**6**		1	1			1	1
1	1		1		1	1		**7**	1		1			1	1
2			1		1			**8**			1				1
3	1	1			1		1	**9**	1	1					
4		1			1	1	1	**0**		1				1	
5	1				1	1	1	**1**	1					1	
6					1		1	**2**							

Table 3: Evaluated responses

Denomination (content)	**Model variable name**	**Input variable**
probability of nondelivery of message	prop_fail	y_1
Probability of delivering data for a time, not more than specified	prop_tz	y_2
Intensity of controlling	control_intensive	y_3
Average message transmission time on network	time_transfer	y_4

Table 4: Numerical array of experimental results

№	y_1	y_2	y_3	y_4	№	y_1	y_2	y_3	y_4
1	0.24	0.447	0.002	148.404	**17**	0.116	0.507	0.691	154.201
2	0.202	0.441	0.003	191.559	**18**	0.02	0.458	0.593	228.037
3	0.263	0.737	0.001	150.233	**19**	0.149	0.85	0.539	172.703
4	0.191	0.745	0.005	187.552	**20**	0.022	0.89	0.65	205.93
5	0.261	0.452	0.002	145.569	**21**	0.156	0.472	0.402	157.636
6	0.219	0.405	0.001	206.708	**22**	0.056	0.464	0.543	215.279
7	0.263	0.737	0	168.428	**23**	0.154	0.846	0.375	163.74
8	0.179	0.772	0.001	173.97	**24**	0.034	0.85	0.418	223.275
9	0.703	0.104	0	229.621	**25**	0.667	0.115	0.41	233.275
10	0.592	0.086	0	396.255	**26**	0.494	0.129	0.625	404.285
11	0.767	0.232	0	236.774	**27**	0.683	0.317	0.333	229.099
12	0.582	0.273	0.001	407.86	**28**	0.438	0.332	0.782	435.365
13	0.715	0.114	0.001	213.918	**29**	0.658	0.104	0.329	238.036
14	0.575	0.097	0.002	399.034	**30**	0.52	0.097	0.473	432.138
15	0.727	0.273	0	209.638	**31**	0.744	0.256	0.266	235.464
16	0.57	0.291	0	375.972	**32**	0.486	0.3	0.606	452.383

Table 5: Array describing linear function y_1

m_7	m_6	m_5	m_4	m_3	m_2	m_1	b
0.0036...	–0.0128...	–0.0516...	0.2311...	0.0058...	0.0018...	–0.0651...	0.3889...
se_7	se_6	se_5	se_4	se_3	se_2	se_1	se_b
0.0071...	0.0071...	0.0071...	0.0071...	0.0071...	0.0071...	0.0071...	0.0071...
r_2	se_y						
0.9801...	0.0404...						
F	d_f						
169.1004	24						
$ss_{рег}$	$ss_{ост}$						
1.9375...	0.0392...						

Based on table 5, equation of multiple linear regression for probability of non-delivery of message is written:

y_1= 0.39–0.07x_1+0.002x_2+0.006x_3+0.23x_4–0.05x_5–0.01x_6+0.004x_7. (2)

Similarly, equations of multiple linear regression for probability of timely delivery; y_2, intensity of controlling, y_3 and average message transmission time, y_4:

y_2 = 0.41+0.002x_1+0.135x_2–0.004x_3–0.22x_4+0.02x_5+0.01x_6–0.004x_7, (3)

y_3 = 0.25+0.04x_1–0.003x_2–0.038x_3–0.014x_4+0.25x_5+0.017x_6+0.008x_7, (4)

y_4 = 251+58x_1+x_2+0x_3+70x_4+11x_5–2x_6+5x_7, (5)

and corresponding coefficients of determination to them: 0.9655...; 0.9101...; 0.8640...

From the analysis of table 5, it is visible that the coefficient of determination of r_2 equals 0.9801... that points to a strong correlation between independent variables and probability of non-delivery of the message. Let us use F-statistics to prove a non-randomness of receipt of results with such high r_2. Assuming the probability of erroneous output that there is a strong dependence, α = 0.05. To receive critical F-distribution value, built-in Excel-function «FINV» will be used: F_{crit} = 2.422628534... F-observed value from table 4.5 is much more than F_{crit} (169.1004 >> 2.423), as such, hypothesis that there is no relation between independent variables and probability of non-delivery of the message is rejected. Similarly for the equations (3 − 5): 96.126 >> 2.423; 34.717 >> 2.423; 21.785 >> 2.423.

Calculated, using built-in Excel-function "FDIST", probabilities of obtaining highest value of F is also extremely small: 7.6179E-19; 5.40104E-16; 4.70913E-11; 6.01274E-09.

Conducted F-test suggest that received multiple linear regression equation (2 – 5) can be used to predict the probability of non-delivery of the message, probability of timely delivery, the intensity of controlling and average message transmission time.

Estimating impact of factors on the probability of non-delivery of message for which coefficients of the equation (2) in the form of a histogram is displayed (see Fig. 1).

From the graphic analysis of Fig. 1, it is established that on prop_fail (probability of non-delivery of the message), factors impact as follows (see table 6).

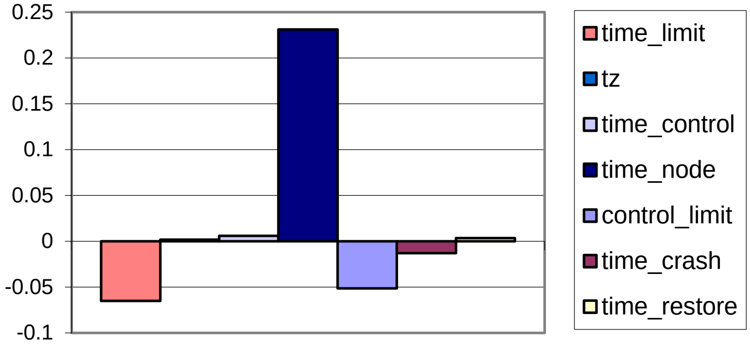

Fig.1: Impact of factors on prop_fail (probability of non-delivery of a message)

Table 6: Impact of factors on prop_fail

	«+»	«–»
Greatly	Handling time at node	
Averagely		Acceptable transmission time Limit of the intensity of controlling
Poorly		The time between node failures
Practically not affected	Time for node recovery Time for controlling Specified transmission time	

This implies that of greatest "positive" impact (with sign "+") on probability of non-delivery of message on network is handling time at node: the lower the router performance, the more the time to handle the message and the more the "chances" that transmission time would not be confined to acceptable, this does not contradict common sense. Respectively, essentially acceptable transmission time impacts on the probability of non-delivery of message on the network "negatively" (with a sign "-"), but not so strong. Limit of the intensity of controlling also increases the survivability of TN by increasing the number of trusted routers and, in this sense, impacts on the probability of non-delivery of message on the network "negatively".

The time between failures impacts "negatively" on the probability of non-delivery of message on the network: the more reliable is routers, the less the "chances" that there would be DoS on message and, therefore, be removed from the network, the truth is that this impact is rather weak.

On the probability of non-delivery of message on the network is practically no impact by:

time of node recovery as it is always possible to redirect traffic to operational (controllable) node;

time of controlling as "regular routers" dominate in the transfer of traffic.

By definition, specified message transmission time does not have an impact on the probability of non-delivery of the message on the network in any way.

Estimating impact of factors on the probability of timely delivery for which coefficients of the equation (4.3) in the form of the histogram is displayed (see Fig. 2).

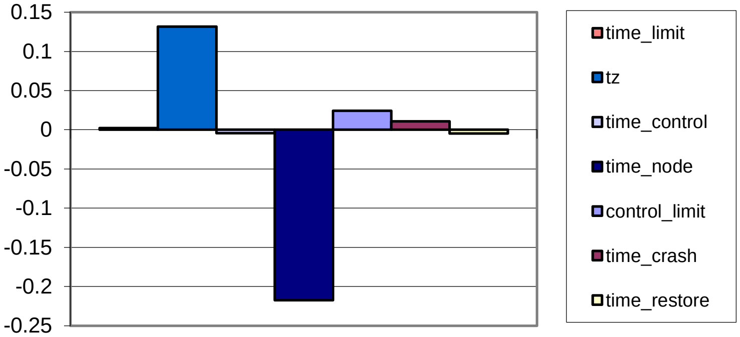

Fig. 2: Impact of factors on prop_tz (probability of timely delivery)

From the graphic analysis of Fig. 2, it is established that on the probability of timely delivery, factors have impacts as follows (see Table 7).

Table 7: Impact of factors on prop_tz

	«+»	«–»
Greatly	Specified transmission time	Handling time at node
Averagely	Limit of the intensity of controlling	
Poorly	The time between node failures	
Practically not affected	Acceptable transmission time Time for node recovery Time for controlling	

Specified transmission time has the most "positive" impact on the probability of delivery of message over the network in a time not less than specified. The reliability of routers through time between failures also "positively" affects "chances" of the message reaching destination point and, thereby, on the probability of timely delivery, however, much weaker.

It is also obvious that the lower the router performance, the more the time to handle the message and the more the "chances" that transmission time would not be confined to acceptable, thus the handling time at a node has a strong "negative" impact on the probability of timely delivery.

The practical absence of impacts of time of node recovery and time of controlling on the probability of timely delivery of messages on the network has a similar explanation (see Table 7). As for acceptable transmission time, it has no impact on the probability of timely delivery of messages on the network by "absorption" of specified transmission time.

Estimating impact of factors on the intensity of controlling for which coefficients of the equation (4) in the form of a histogram is displayed (see Fig. 3).

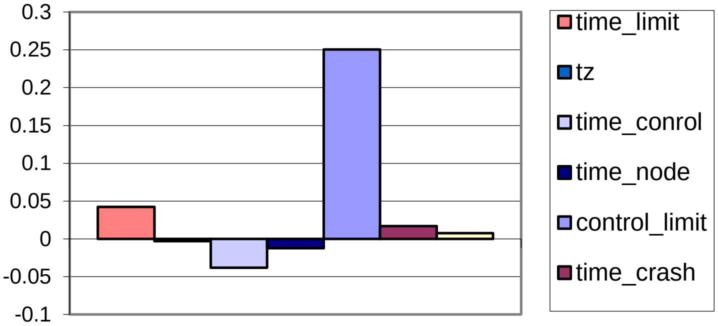

Fig. 3: Impact of factors on control_intensive (intensity of controlling)

From the graphic analysis of Fig. 3, it is established that on the intensity of controlling, factors have impacts as follows (see Table 8).

Table 8: Influence of factors on control_intensive

	«+»	«–»
Greatly	Limit of the intensity of controlling	
Averagely	Acceptable transmission time	
Poorly	The time between node failures	Time for controlling Handling time at node
Practically not affected	Time for node recovery Specified transmission time	

The limit of intensity of controlling has the most "positive" impact on the intensity of control.

Acceptable transmission time significantly "positively" influences the intensity of control, which is quite explainable: the longer the message "wanders" on a network, the more the chances that the message gets to a faulty router and prompts controlling mechanism.

Obviously "negative", though weak, impact on the intensity of controlling do have the time for controlling and handling time at a node, the nature of dependence is that the more the delay of the message in the node, the less the need for controlling.

"Positive" impact of time between nodes failures on the intensity of controlling looks paradoxical as the higher the reliability of routers, the less the need for controlling of new nodes, however, this can be explained with a mismatch of temporary scales of ranges of source data and therefore this impact is insignificant.

Specified transmission time does not have an impact on the intensity of controlling by definition, and time of recovery influences too indirectly.

Estimating impact of factors on average transmission time of the message on the network for which coefficients of the equation (5) in the form of a histogram is displayed (see Fig. 4).

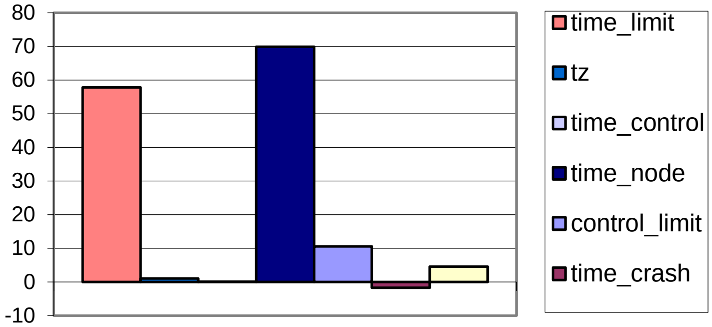

Fig. 4: Influence of factors on time_transfer □ the average time of transfer of the message on a network

From the graphic analysis of Fig. 4, it is established that on average transmission time of the message on the network, factors do have impacts as follows (see table 9).

Table 9: Impact of factors on time_transfer

	«+»	«–»
Greatly	Handling time at nodeAcceptable transmission time	
Averagely	Limit of the intensity of controlling	
Poorly	Time for node recovery	
Practically not affected	Specified transmission time The time between node failures Time for controlling	

This implies that on average message transmission time on the network does have the greatest "positive" impact handling time at node: the less the router performance, the more the time it takes to transfer messages, which does not contradict common sense. Also significantly "positively" on the average delivery time does have an impact on acceptable transmission time. This can be explained by an increase in chances of messages getting to a destination even at the detriment of efficiency. For the same reason, the limit of intensity of controlling has smaller but still a "positive" impact on the average time of delivery.

It is obvious that the more the recovery time for nodes, the more the average time of delivery, however, this influence is rather weak.

Specified message transmission time has no impact on the average time of delivery by definition. The time between nodes failures too indirectly influences the average time of delivery of the message, to be significant. The absence of impact of time of controlling on the average time of delivery, at first glance, is difficult to explain (as time spent on processing message in any node inevitably increases delivery time) and demands further studies.

The result of the calculation of correlation coefficients between the probability of non-delivery of the message, $y_{1;}$ the probability of timely delivery, $y_{2;}$ the intensity of controlling, $y_{3;}$ and average message transmission time, y_4 are shown in table 10.

Table 10: Correlation coefficients among responses

		y_1	y_2	y_3	y_4
Probability of non-delivery of a message	y_1	1			
Probability of timely delivery of the message	y_2	–0.8062...	1		
Limit of the intensity of controlling	y_3	–0.3107...	0.1265...	1	
Average message delivery time on network	y_4	0.4516...	–0.5746...	0.2036...	1

Analysis of contents of table 10 allows to record the following rather obvious interrelations among responses from a simulation model of functioning of TN with TR:

1. Probability of timely delivery of the message is in strong "negative" interrelation with the probability of non-delivery & vice versa, in insignificant "positive" interrelation with a limit of intensity of controlling & vice versa, and insignificant "negative" interrelation with the average time of delivery of message on network & vice versa;
2. Average time of delivery of message on the network is insignificant "positive" interrelation with the probability of non-delivery & vice versa and in insignificant "positive" interrelation with a limit of intensity of controlling & vice versa;
3. The probability of non-delivery of the message is in weak "negative" interrelation with a limit of intensity of controlling & vice versa.

The experiment allowed to establish effect and direction of impacts of each of the considered factors on the evaluated variables, however, practical use of the received results of analysis demand corresponding interpretation.

According to the methodology of planning experiment, the main effects of factors and effects of interaction will be defined. The availability of established functional dependence does notallow forusing "purely" additive criteria for analysis of the effects of the interaction of factors on a certain integral quality of TN with TR. Therefore, multiplicative pairs that have the greatest correlation coefficient, namely, probabilities of non-delivery and timely delivery of the message, probability of non-delivery of the message and average time of delivery of message on the network, probability of timely delivery of message and average time of delivery of message on network will be introduced into convolution.

Preliminarily the equation (5) will be normalized. For this, all coefficients will be divided by max$\{y_4\}$ = 452.383:

y_4=0.554+0.128x_1+0.002x_2+0x_3+0.154x_4+0.023x_5–0.004x_6+0.01x_7. (6)

The final criterion Y of certain integral quality of TN with TR is as follow:

$Y = y_1 + y_2 + y_3 + y_4 + y_1y_2 + y_1y_4 + y_2y_4$ (7)

and its values are given in table 11.

Table 11: Values of final criterion *Y*

	y_1	y_2	y_3	y_4	y_1	y_2	y_3	***Y***	***R***
x_7	0.0036...	–0.0045...	0.0078...	0.0100...	–1.665E-5	3.651E-5	–4.627E-5	0.0168...	**6**
x_6	–0.0128...	0.0107...	0.0170...	–0.0038...	–0.0001...	4.992E-5	–4.177E-5	0.0109...	**7**
x_5	–0.0516...	0.0244...	0.2505	0.0234...	–0.0012...	–0.0012...	0.0005...	0.2448...	**1**
x_4	0.2311...	–0.2172...	–0.0124...	0.1544...	–0.0502...	0.0356...	–0.0335...	0.1077...	**3**
x_3	0.0058...	–0.0041...	–0.0380	2.417E-6	–2.441E-5	1.42E-8	–1.005E-8	–0.0363...	**5**
x_2	0.0018...	0.1315...	–0.0031...	0.0023...	0.0002...	4.311E-6	0.0003...	0.1331...	**2**
x_1	–0.0651...	0.0020...	0.0422...	0.1277...	–0.0001...	–0.0083...	0.0002...	0.0986...	**4**

Estimating impact of factors on the integral quality of TN with TR, for this coefficient of the equation (7) will be displayed in the form of a histogram (see Fig. 5),

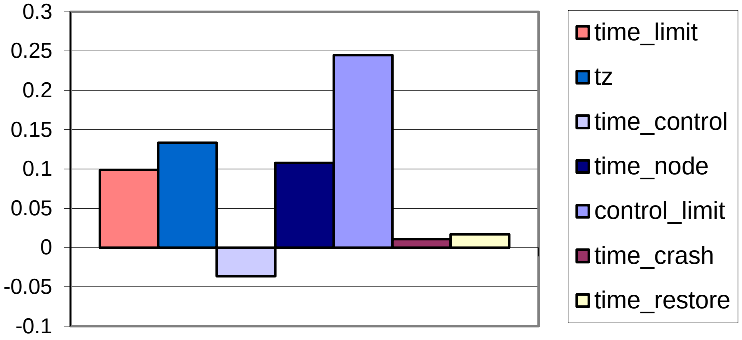

Fig. 5: Impacts of factors on *Y* (integral quality of TN with TR)

Graphic analysis of Fig. 5 allows ascertaining following integral (synergetic) effects:

The limit of the intensity of controlling has the greatest impact (grade R = 1) on the integral quality Y, which is very well in accord with the introduction of TR mechanism into TN, which is designed to significantly improve probabilistic and temporal characteristics.

Specified transmission time that defines the purpose of TN by timely transfer of traffic has a strong impact (grade R = 2) on the integral quality Y.

Significant impact (R = 3) of handling time at a node on the integral quality Y is quite obvious: the router's performance largely determines the characteristic of network nodes, the main source of delays and failures according to the conceptual model of TN.

So also, acceptable transmission time that defines the chances of the message getting to destination point has a significant impact (*R* = 4) on the integral quality Y.

Time of controlling has a weak impact (*R* = 5) on integral quality *Y*, which can be explained by its incommensurability in the original data of model with handling time at the node.

Note: This is particularly important from the standpoint of the fundamental feasibility of applying the method of TR since its introduction contributes a significant positive effect only if the time of controlling RD is small.

Practically, the reliability of characteristics of routers (time between failures and time of node recovery) has no impact (*R* = 6, 7) on integral quality of TN with TR since in presence of TR, it is always possible to redirect traffic to a known-good (controlled) node.

Using the developed simulation model, we will evaluate the dynamics of the impact of key factors of TR (intensity of controlling (control_intensive) and specified time (tz) on the objective function of TN that is a probability of timely delivery of messages (prop_tz). The results of the simulation experiment shown in Figures 6 and 7 confirm high (over 25%) efficiency of TR in TN; that, the more the TN nodes are controlled and the more the specified transmission time, the more the chances of the message getting to the destination.

Here obvious dependence of the probability of timely delivery of messages over TN on specified time is given also to proof adequacy of the developed simulation model in real networks. This raises a degree of trust in the results of the experiments.

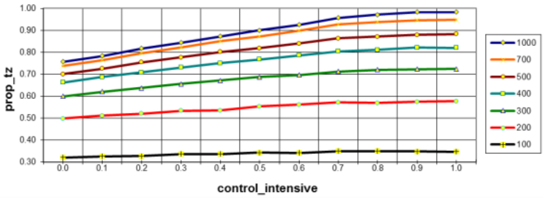

Fig.6: Dependence of probability of timely delivery of messages on the intensity of controlling for different values of tz, specified time

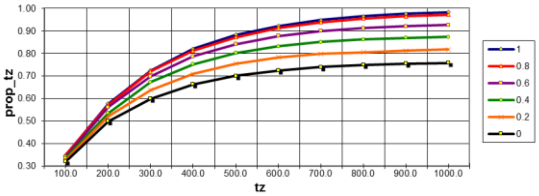

Fig. 7: Dependence of probability of timely delivery of messages on specified transmission time for different values of intensity of controlling, control_intensive

Using the developed simulation model of TN with TR, an optimization experiment is carried out. Its essence lies in the fact that an increase in controlling, on one hand, increases timely delivery of messages, and on the other, level of secrecy of transmission falls since as a result of using TR in the network, irregular activities, "interruptions" in the routing equipment, etc. are being observed. So if the objective function (OF) is timely, but secretively transmission, there is a certain optimum, when timeliness is already quite great, and secrecy is still quite great.

The diagram in Fig. 8 shows the obvious growth of probability of getting the message to destination and falling of secrecy level (an indicator of IS) of transmission while increasing the intensity of controlling (control_intensive).

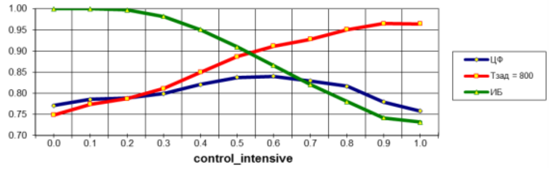

Fig. 8: Results of optimization experiment

For optimization experiment and evaluation of dynamics of impacts of key factors, data from table 4-1??? were used: time_limit = 1000, time_control = 10, time_node = 10, time_repair = 10, time_crash = 5000. As OF, the following structure was chosen:

$$\text{OF} = P_{tz}^{n} \times P_{\text{скр}}^{1-n}, \qquad (8)$$

Where P_{tz} is probability of getting message to destination in no more time than specified (tz);

n is coefficient of importance of quality index, $n = 0 - 1$ (in this case, $n = 0.9$);

$P_{скр}^{1-n} = 1 - e^{-k/\lambda}$ is secrecy of transmission (k is empirical coefficient, λ is intensity of controlling).

The experiment showed the presence of inflection of OF when the intensity of controlling (control_intensive) is around 0.5 to 0.7.

For practical use of the results of such experiments for optimization are needed real source data, the scientifically-based structure of OF, as well as additional studies to determine the effect of increased activity in global TN on the value of secrecy index. At the same time, it should be noted that the use of TR simultaneously improves the security index of the TN, like confidentiality and identifiability of traffic. So also functional stability (in particular, survivability).

References

[1] M. V. Buinevich, O. A. Tiamiyu, "Software Architecture of Trusted Routing Management System in Global Telecommunication Networks (Программная архитектура системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях)," Information and Communication («Информатизация и связь»), vol. 3, pp. 35-38, 2014.

[2] O. A. Tiamiyu, "An Overview of Modern Telecommunication Networks Security Challenges. National Security and Strategic Planning (Национальнная Безопасность и Стратетическое Планирование)," National Security and Strategic Planning (Национальнная Безопасность и Стратетическое Планирование), vol. 2, no. 2, pp. 37-43, 2013.

[3] O. A. Tiamiyu, D. A. Olaode, F. Ahmamush, "Issues on the international standardization in the field of information security," Science Journal VESTNIK ENGEC: Technical Science Series (Научный Журнал «Вестник Инжекона: Серия Технические Науки»), vol. 67, no. 8, p. 100−102, 2012.

[4] V. M. Zima, A. A. Moldovian, N. A. Moldovian, Безопасность глобальных сетевых технологий, СПб: ХВ-Петербург, 2000.

[5] O. A. Tiamiyu, "Trusted Routing Device in Telecommunication Networks (Устройство Доверенной Маршрутизации в Телекоммуникационных Сетях)". Russia Patent RU Patent № 150245, 10 2 2015.

[6] O. A. Tiamiyu, "Trusted routing vs. MPLS: Data security, QoS and network scalability," Electronic Science Journal «Information Technologies and Telecommunications» (Электронный Научный Журнал «Информационные Технологии и Телекоммуникации»), vol. 3, p. 4−13, 2013.

[7] O. A. Tiamiyu, "Comparative Analysis of Imitation Modeling Software Supporting Trusted Routing (Сравнительный Анализ Средств Имитационного Моделирования ТКС, Поддерживающих Доверенную Марщрутизацию)," in Topical issues on problems of information security: collection of scientific articles (Актуальные Проблемы Информационной Безопасности, Сборник Научных Трудов), 2012, p. 49−53.

[8] Open Systems Interconnection. Basic Reference Model Part, 2.

[9] O. A. Tiamiyu, "Analysis of IP Routing Protocols for Trusted Routing in the Global Data Networks.," Science Journal VESTNIK ENGEC: Technical Science Series (Научный Журнал «Вестник Инжекона: Серия Технические Науки»), vol. 59, no. 8, p. 157−160, 2012.

[10] H. Chuanhe, Y. Cheng, Y. Ling, H. Xhou, "Trusted dynamic source routing protocol," in International Conference on Wireless Communications, Networking and Mobile Computing, 2007.

[11] T. Ghosh, N. Pissinou, S. K. Makki, "Towards designing a trusted routing solution in mobile ad hoc networks," Mobile Networks and Applications, vol. 10, no. 6, pp. 985-995, 2005.

[12] A. Datta, C. Mcdonald, A. Pirzada, "Trusted routing in ad-hoc networks using pheromone trails.," in 2004 Congress on Evolutionary Computation, 2004.

[13] K. K. Somasundaram, J. Baras, "Path Optimization and Trusted Routing in MANET: An Interplay Between Ordered Semirings.," in International Conference on Computer Science and Information Technology, Berlin, 2011.

[14] K. YANG, J. I. MA, C. YANG, "Trusted routing based on DS evidence theory in wireless mesh network," Journal on Communications, vol. 32, no. 5, p. 89, 2011.

[15] Q. Wu, Q. Liu, Z. Zhiming, "A trusted routing protocol based on GeoDTN+ Nav in VANET," China Communications, vol. 11, no. 14, pp. 166-174, 2014.

[16] O. A. Tiamiyu, "Recommendations for improving the implementation of trusted routing mechanism (РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ РЕАЛИЗАЦИИ МЕХАНИЗМА ДОВЕРЕННОЙ МАРШРУТИЗАЦИИ)," Electronic Scientific Journal «Information Technologies and Telecommunications» (Электронный Научный Журнал «Информационные Технологии и Телекоммуникации»), vol. 1, p. 413−417, 2015.

[17] T. Chen, O. Mehani, R. Boreli, "Trusted routing for VANET," in 2009 9th International Conference on Intelligent Transport Systems Telecommunications, 2009.

[18] S. S. Hazra , "Trusted routing in AODV protocol against wormhole attack," in Future Information Technology, Application, and Service, Springer, 2012, pp. 259-269.

[19] Z. A. Zardari, J. H. Muhammad, S. Pathan, S. Qureshi, N. Zhu, "Detection and prevention of Jellyfish attacks using kNN algorithm and trusted routing scheme in MANET," International Journal of Network Security, vol. 23, no. 1, pp. 77-87, 2021.

[20] Z. Qin, Z. Jia, X. Chen, "Fuzzy dynamic programming based trusted routing decision in mobile ad hoc networks," in Fifth IEEE International Symposium on Embedded Computing, 2008.

[21] S. Peng, W. Jia, G. Wang, J. Wu, N. Guo, "Trusted routing based on dynamic trust mechanism in mobile ad-hoc networks," IEICE TRANSACTIONS on Information and Systems, vol. 93, no. 3, pp. 510-417, 2010.

[22] O. A. Tiamiyu, "Trusted Routing vs. VPN for Secured Data Transfer over IP-Networks/Internet," in 2nd International Scientific and Practical Conference «Fundamental and applied research in the modern world» (Материалы II Международной Научно-практической Конференции «Фундаментальные и Прикладные Исследования в Современной Мире»), 2013.

[23] O. A. Tiamiyu, "Selection and Rationale of Algorithm for Network Topology Determination in the Interest of Trusted Routing," Electronic Science Journal «Information Technologies and Telecommunications» (Электронный Научный Журнал «Информационные Технологии и Телекоммуникации»), vol. 1, pp. 54-66, 2014.

[24] S. Vasileva, A. Kulchiar, "Options of GPSS World for integrated demonstration models in the educational process," in 2014 Science and Information Conference, 2014.

[25] В. Д. Боев, Моделирование систем. Инструментальные средства GPSS WORLD, Петербург: БХВ-Петербург, 2004.