Identifying Anomalous Geographical Routing Based on the Network Delay

Evgeny Sagatov[1], Konstantin Lovtsov[1], and Andrei Sukhov[1,2]
(Corresponding author: Andrei Sukhov)

The Department of Computer Science, Samara National Research University[1]
34, Moskovskoye shosse, Samara, 443086, Russia
The Department of Computer Science, Togliatti State University[2]
14, Belorusskaya ul., Togliatti, 445020, Russia
(Email: amskh@yandex.ru)

(Received May 11, 2018; Revised and Accepted Oct. 18, 2018; First Online June 5, 2019)

Abstract

In this paper we analyse the problem of anomalous geographical routing that leads to significant increases in network delays. The detection of anomalous routing uses the method of threshold values for the efficiency factor of geographical routing. An attempt has been made to estimate the share of national traffic that is serviced on foreign routers and can easily be intercepted. In order to analyse the quality of network connections, the NetTestBox monitoring system has been tested.

Keywords: Anomalous Geographical Routing; Efficiency Factor of Geographical Routing; Internet Exchange Points

1 Introduction

New Internet protocols and services often require enhancements to the quality of network connections. This paper discusses ways to reduce network delay. Until recently, multimedia voice and video services were the most sensitive to delay [6]; However, while distributed cloud services now crucially require the optimization of connection latency and available bandwidth [8], the leader in the field of systems which require reductions in network delays are the low-latency networks which serve to transmit tactile sensations [13].

There are several methods for reducing network delays, and a whole series of research has been devoted to this problem. The nature of the network delay indicates that the primary method should be associated with the reduction in the length of the communication line over which packets are transmitted. In order to reduce the length of communication channels, traffic exchange points are created where local Internet service providers can exchange traffic directly within the general geographical area [9]. Also, local caches and content delivery networks can bring information sources closer to users.

This paper presents a new method for detecting anomalous geographical routing based on network delays. Previously, several authors' collectives investigated this problem, which they called "boomerang routing" or "circuitous routing" [3,5]. However, our approach has a number of significant differences in the research methodology. We make an initial selection of candidates for abnormal routes using network delay and geographical distances, the latter of which is determined using Google or Yandex maps. Previous researchers used the traceroute utility, which we used in the second stage for the final test of the route.

Our approach will be illustrated by an assessment of the effectiveness of geographical routing in the example of the European part of Russia. Attention will be paid to assessing the effectiveness of Russian traffic exchange points. Some of the domestic channels are served by foreign routers which are in Europe or even the US. Such routing results in significant increases in network delays. In addition, the maintenance of domestic Russian traffic abroad entails threats to security.

According to Snowden's revelations and the subsequent scandal regarding the National Security Agency (NSA)'s spyware, most traffic, even when it is encrypted, can be intercepted and read. In this paper, an attempt is made to estimate the portion of domestic traffic that is serviced overseas. Thus, the detection of anomalous geographical routing can be seen as an identifiable problem which is closely related to the quality of network connections.

2 Measuring Tools

There now exist several tools that can measure IP performance metrics [12], the most common of which are RIPE Atlas [7] and PingER [16]. The monitoring nodes of these projects are installed by Internet providers around the world and constantly measure the status of network channels. RIPE Atlas is financed by RIPE NCC independently at the expense of funds collected from providers to support LIR (Local IP registry) and AS (autonomous system).

The RIPE Atlas project was founded in 2010 and is being developed by the RIPE NCC. Its simplified hardware does not allow for the measurement of an extremely important performance metric, namely one-way packet delay [1]. To access the measurements, a person must set the RIPE Atlas node on his/her local network. For the maintenance of each node, points are awarded daily which can be spent on making measurements [2]. One can also access the measurements by becoming a sponsor of the project. It is possible to take ping, traceroute, and check the status of DNS systems, SSL certificates, HTTP, and NTP. As of November 2017, there were 10,327 nodes (the number varies within a few hundred points) in 183 countries.

The PingER (Ping End-to-End Reporting) project was founded in 1995 by a community of high-energy physicists [16]. It is now part of the project Internet End-to-End Performance Measurement (IEPM) headed by the Stanford Linear Accelerator Center (SLAC), and it includes the development of the Centre for Applied Network Research, Fermilab, the International Centre for Theoretical Physics, University Technology Malaysia, University Utara Malaysia, etc. The function of this measuring complex is based on the network delay measurement programme, Ping. As of November 2017, there were 1,277 nodes at 1,097 sites in more than 160 countries.

The project NetTestBox [19] was launched on July 28th, 2015; it was developed, and is managed by, a team of employees from the Samara University. The project is based on the Raspberry Pi microcomputer, to which a multi-band GLONASS + GPS receiver is connected. In order to install a miniature node, it is sufficient to connect it to the power and the twisted pair to the Internet. In order to operate the receiver, it is necessary to place the device on a window or in any other place where it is likely that a satellite signal will be received. The software uses the GNU Debian/Linux operating system. The GLONASS+GPS receiver makes it possible to synchronise time with high accuracy on all NetTestBox devices, thus allowing for the measurement of one-way delay (OWD).

It should be emphasised that competing systems measure an RTT. Since round-trip routes often differ, information about one-way delay is indispensable when it comes to the network state and routing analytics. The project site [metrics] builds charts for all IP performance metrics. Tabular data can be easily obtained for additional analysis in the future, as well as route tracing. As of November 2017 there were four NetTestBox points in Togliatti, Samara, Rostov-on-Don and Moscow. Data on the discontinued points in the USA has been saved.

For ease of comparison, Table 1 summarises the characteristics of the above-mentioned measuring instruments.

3 Criteria for the Effectiveness of Geographical Routing

Here, we provide basic information regarding the nature of network delays and explain the criteria used to gauge the effectiveness of geographical routing. From a mathematical point of view, a one-way delay consists of a constant component D_{const} and some variable components D_{var}:

$$D = D_{const} + D_{var}.$$

From the physical point of view, this delay can be described as the sum of physical D_{phys} and telecommunication D_{tel} components:

$$D = D_{phys} + D_{tel},$$

where D_{phys} is the signal transmission time through the communication path. This is the propagation delay, which is determined by the speed of light and the special theory of relativity. D_{tel} is the telecommunications component of the delay. It represents the sum of the delay components that occur with all kinds of signal actions (for example, processing on routers, waiting for a packet in queues, etc.).

Back in 2003, Carbone *et al.* [4] suggested using the relationship

$$\tau = \frac{RTT c_{opt}}{2L}$$

to assess the quality of an Internet path. Here, $c_{opt} \approx$ 200km/ms, c_{opt} is the speed of light in the optical fibre, because overwhelmingly fibre is used as the data transfer medium along the route. L is the geographic (great circle) distance between two sites and RTT is the most widely used metric of Internet performance (known as Round Trip Time).

The telecommunication length l_{tel}, the geographical length l_g, and the efficiency factor of the geographical routing are introduced in paper [18] to describe the effectiveness of

$$k = \frac{l_{tel}}{l_g},$$

where l_{tel} is the telecommunication length of the route and D_{min} is the minimum value of the one-way delay. l_g is the geographical distance between the two route endpoints, which is easily determined from a Google or Yandex map.

The question arises of how many measurements N of one-way delay should be made to find the value D_{min}? It is known [17] that the network delay values are distributed according to an exponential law for small time intervals (10–30 mins). Cumulative distribution function is

$$F(D) = 1 - \exp\left(-\frac{D - D_{min}}{j}\right), D \geqslant D_{min}, \quad (1)$$

where j is a network jitter.

Table 1: Characteristics of measuring instruments

	OWD	RTT	Jitter	Packet loss	Available bandwidth	Traceroute
RIPE Atlas	−	+	−	−	−	+
PingER	−	+	+	+	+	−
NetTestBox	+	+	+	+	+	+

In order to estimate the number of measurements required, N, of the one way delay, we will use the generating function

$$D = D_{min} - j\ln(1 - F(D)).$$

The generating function is an inverse of the distribution function $F(D)$ of the one-way delay from Equation (1).

For a series of N tests, where a standard random number generator gives the values of the distribution function $F(D)$, we obtain:

$$D_{min} - \min_{i=\overline{i,N}} D_i = \frac{j}{N+1}$$

where $\min_{i=\overline{i,N}} D_i$ is the minimum value of the one-way delay, obtained as a result of the measurements. Taking into account the fact that the measurements are carried out once a second, a 30 s interval for measurements will be sufficient.

The question of the anomalous values of the coefficient of geographical routing will be discussed in Section 5. However, there is one simple application of a theory that does not require measurements. It is possible to calculate the limiting value of the minimum one-way delay for connections between subscribers within the European part of Russia. If the packets are forwarded only across Russian territory, the distance between subscribers cannot exceed 2,000 km, while the minimum delay will be limited to 30ms. If the route extends into Europe itself, then the geographical distance rises to a maximum of 5,000 km, and when traffic is routed beyond the Atlantic Ocean this maximum increases to 10,000 km. That is, for any geographical route, it is possible to calculate the threshold value of the minimum delay, and when this threshold is exceeded one can speak of anomalous routing.

Table 2 summarises the data pertaining to the limiting values of one-way delays. According to this data, it is possible to determine the yield of traffic outside the Russian Federation.

This section presents a method for detecting anomalous routes using the value of the geographical routing factor. When the value of this factor is above a certain threshold, such a route must be subjected to additional checks. It should be emphasised that the rule found for the detection of anomalous routes is a necessary condition, but not a sufficient one. The final determination must be made according to the traceroute command. Nevertheless, the condition that has been discovered greatly simplifies the detection process, as it involves the monitoring of only one numerical parameter.

Table 2: Criteria for the exit of traffic from the russian federation

Route of domestic traffic	**The value of one-way delay D_{min}**
Through Europe	$\geqslant 35 - 70$ms
Through America	$\geqslant 75 - 120$ms
Inside Russia	$\leqslant 30$ms

4 Internet Exchange Points and Their Role

An Internet Exchange Point (IX) represents a network infrastructure that is used for exchanging traffic between autonomous systems (the so-called peer-to-peer systems). Operators of communication and other organisations that have their own autonomous systems can exchange traffic through the IX without organising direct channels to each other, but rather through using the channel to the Internet Exchange Point.

According to the paper [10], in Russia in November 2017, 39 traffic exchange points were organised. Administrators of autonomous systems connect to Internet Exchange Points and conclude agreements with each other on the traffic exchange. It should be noted that there is currently no obligatory "all with all" principle within the Internet Exchange Points. The exchange is organised in the framework of bilateral agreements. Therefore two autonomous systems, included in one Internet Exchange Point, may not be directly connected.

Border Gateway Protocol (BGP) is a dynamic routing protocol between autonomous systems. In this boundary routing protocol, the route selection criterion is the routing policy that the system administrator sets up. He decides with whom the managed system will have a direct traffic exchange (peering) and with which AS there will be no direct communication. In addition, the BGP settings assume the indication of the main and backup external channels. External channel data and access paths to each autonomous system are recorded in the global routing table. That is, the exchange between autonomous systems within the access point can be carried out at the local level and is prioritised. If the autonomous system is not in the list of nearest neighbours, then routing takes place in accordance with the global table.

Despite these shortcomings, the role of Internet Exchange Points cannot be overestimated. If the routing is set correctly, the proportion of traffic that is serviced outside these points will tend to be zero. The present work is devoted to the analysis of the work of Russian Internet Exchange Points, as well as the development of recommendations on how to avoid situations where domestic traffic is serviced on foreign routers.

5 Analysis of Measurement Results and Ways to Improve Geographical Routing

In order to illustrate the search for anomalous routes, we first use the data from the NetTestBox monitoring system. Data on one-way delay make it possible to identify not only anomalous routes, but also directions within the routes, if these routes are asymmetric ones.

The experimental results are summarised in Table 3. The values of the minimum delay in milliseconds are shown below the diagonal. A brief analysis yields the fact that, in a number of directions (Togliatti-Samara, Samara-Moscow, Togliatti-Moscow), these values are asymmetric. That is, the routing is conducted asymmetrically. In addition, suspicious values for the one-way delay D and the efficiency factor of geographical routing k are shown in bold. These values indicate that the abovementioned routing is most likely carried out through Europe (see Table 2).

Our additional refinement of the route by the traceroute command shown in Table 4 confirms our hypothesis.

As can be seen in Table 3, above the diagonal, the values of the efficiency factor of geographical routing k were calculated. The data in the table confirms the previously-stated hypothesis about the limiting values of the coefficient k.

The next step will be to try to estimate the percentage of Russian autonomous systems (AS) that are connected to Internet Exchange Points (IX). It is quite difficult to achieve this, and it is also rather difficult to find data on the number of Russian AS or registrars (LIRs). It is not very clear whether such statistics are even available to Russian authorities. Nevertheless, it was possible to find [15] that in Russia 1,930 LIR from 17,394 LIR, registered in RIPE. This is approximately 11 % of the all-European number, which was a surprise. As stated earlier, a third of European LIRs were registered in Russia.

Using a specially-written script, it was possible to identify 5,119 Russian AS (IPv4) in the RIPE NCC database. Taking into account that the total number of ASs registered by RIPE is little more than 36,000, the part of Russian AS is 14 %.

The total number of all connections to the Russian IX was 1,683 at the end of November 2017, when the remaining data was collected. It should be noted that some ASs are connected to different traffic exchange points, and thus the real number of unique autonomous systems is lower [11]. At the same time, the maximum coverage of Russian AS connections to traffic exchange points does not exceed 32.9%.

The following estimates are made using the RIPE Atlas measuring system. The random sampling method selects 25 RIPE Atlas probes in the Moscow and St. Petersburg regions. We estimate how many of them are connected to the corresponding Internet Exchange Points. For Samara and Novosibirsk, the number of Atlas probes is small, while the percentage of coverage can be estimated at all points. The obtained data is summarised in Table 5.

That is, among autonomous systems with RIPE Atlas probes, the part of connections to Internet Exchange Points is much higher. On average, it is twice as high as for an ordinary Russian AS. The RIPE Atlas measuring system also makes it possible to estimate the efficiency factor of geographical routing between points connected to and outside the Internet Exchange Points. Knowledge of intra-urban distances is necessary in order to assess the effectiveness of Internet Exchange Points. Calculating this distance is difficult because the nodes are not exactly tied, and the exact lengths of the cable ducts are not known. Therefore, it can be assumed that the route length inside the millionth city is equal to approximately 150km, and for the capitals of Moscow and St. Petersburg it is 250km. The threshold value of the coefficient for determining anomalous routing exceeds 9. This data was collected only for Moscow and St. Petersburg and is summarised in Table 6.

In Moscow (see Table 7), there are several anomalous routes between autonomous systems connected to the Internet Exchange Point. This is due to the fact that not all autonomous systems within one point have set up peering among themselves. Selectivity is one of the big drawbacks of the existing systems. Suspicious values for the one-way delay D and the efficiency factor of geographical routing k are shown in bold. In general, the efficiency factor of geographical routing and the part of anomalous routes look good. In St. Petersburg (see Tables 8 and 9), the situation with routing is worse, which is confirmed by both indicators.

In order to estimate the all-Russian situation, we randomly selected 20 RIPE Atlas probes scattered throughout Russia and measured the delays between them. As a result, it was found that the part of anomalous channels in Russia is approximately 11.7 %, while the threshold value of the efficiency factor of geographical routing depends on the geographical distance, l_g. Its threshold value is 5 for geographical distances less than 2000km, and if the distance is more than 3000km the threshold value is reduced to 3.5. The data on the dependence of the threshold value of the coefficient from the geographical distance is summarised in Table 10.

The data obtained in this section can be independently verified with the help of RIPE Atlas analytical tools [14]. Such tools offer analysis of connections to IX (IXP Country) and analysis of RTT data (RTT Mash). The data

Table 3: NetTestBox routing information

	Togliatti	**Samara**	**Rostov-on-Don**	**Moscow**
Togliatti	$D_{min}\backslash k$	3.1(20.5)	4.6(4.5)	2.7(**11.7**)
Samara	3.13(20.45)	$D_{min}\backslash k$	3.5(4.3)	2.2(**10.9**)
Rostov-on-Don	23.12(22.52)	17.42(21.45)	$D_{min}\backslash k$	2.5(2.6)
Moscow	11.34(**49.74**)	10.34(**51.74**)	12.42(12.77)	$D_{min}\backslash k$

Table 4: The Samara-Moscow Route

City	**Traceroute Samara→Moscow**
Samara	1 big.ssau.ru (91.222.128.24) 0.273ms 0.366ms 0.282ms
Samara	2 sw15-vlan55.ssau.ru (91.222.130.254) 0.538ms 0.545ms 0.654ms
Samara	3 r1-vlan254.ssau.ru (91.222.130.237) 0.666ms 1.033ms 1.330ms
Nizhniy Novgorod	4 79.126.112.69 (79.126.112.69) 18.810ms 18.872ms 18.907ms
Moscow	5 ae40.frkt-cr4.intl.ip.rostelecom.ru (217.107.67.15) 66.486ms 62.179ms 61.126ms
London	6 100ge4-1.core1.fra1.he.net (216.66.89.225) 68.474ms 65.965ms 66.053ms
Frankfurt	7 fiord-as-as28917...switch1.fra2.he.net (216.66.87.178) 64.099ms 67.200ms 64.054ms
Moscow	8msk-m9-b1-xe4-2-1-vlan2049.fiord.net (93.191.9.156) 70.195ms 66.350ms 63.919ms
Moscow	9 as39134-gw.fiord.net (62.140.239.223) 63.587ms 66.765ms 66.702ms
Moscow	10 mapripn-gw.exepto.ru (88.212.194.70) 61.069ms 64.356ms 65.612ms
Moscow	11 MSK-M9-MR1.Ripn.net (193.232.226.17) 66.832ms 63.763ms 66.936ms
Moscow	12 MSK-M9-Relarn-1.relarn.ru (193.232.226.10) 70.577ms 64.682ms 68.490ms
Moscow	13 MSK-KHOUSE-Relarn-2.Relarn.ru (194.226.29.181) 68.060ms 65.211ms 65.807ms
Moscow	14 nettestbox.relarn.ru (194.190.138.140) 68.027ms 65.470ms 68.081ms

Table 5: The part of autonomous systems with RIPE atlas probes connected to internet exchange points

№	**Region**	**Coverage**
1	Moscow	70%
2	St. Petersburg	77.8%
3	Samara	50%
4	Novosibirsk	75%

was collected and analysed for 119 Russian AS. During the analysis, all routes between the AS were divided into 4 groups:

- With the passage of the route through one of the Russian IX, but without service on foreign routers;
- With the passage of the route through one of the Russian IX and service on foreign routers;
- Without routing on one of the Russian IX and without service on foreign routers;
- Without routing on one of the Russian IX, but with service on foreign routers.

Each of these groups is allocated a cell with its own colour.

In general, the data on the percentage of Russian routes served on Russian IX and on foreign routers coincides with our measurements. However, RIPE analytical tools draw conclusions based on the analysis of routes, which increases labor intensity. It should be noted that the route data contains the minimum delay values. The analysis of this data confirms our hypothesis about the threshold value of the coefficient k.

The RTT data is simply divided into three groups (less than 10ms, 10-50ms, more than 50ms) and is not tied to the geographical distance l_g between the end nodes. Such a breakdown does not allow us to draw conclusions about the effectiveness of geographical routing. That is, it seems appropriate to supplement the RIPE analyst with data on the efficiency of geographical routing.

Conclusions and Recommendations

For the monitoring of network topology, it was proposed to use a new approach based on the threshold values of the efficiency factor of geographical routing. This approach made it possible to move from route analysis to analysing just the one-way delay value, and this greatly simplifies

Table 6: Efficiency factor of geographical routing

№	Region	Coverage		Part of anomalous channels	
		Inside IX	Outside IX	Inside IX	Outside IX
1	MSK	2.2	2.5	7,70%	10,0%
2	SPB	3.1	4.0	17.2%	33.30%

Table 7: The k value for AS entering the MSK-IX

AS	**12714**	**8402**	**42610**	**8241**	**13238**	**5467**	**200161**	**28738**	K_{av}
12714	$D_{min}\backslash k$	–	1.8	2.0	1.2	**17.8**	1.0	1.3	4.2
8402	–	$D_{min}\backslash k$	2.6	3.2	2.2	**9.4**	1.9	2.3	3.6
42610	4.5	6.4	$D_{min}\backslash k$	2.4	1.5	1.9	1.5	1.5	1.8
8241	4.9	8.0	6.1	$D_{min}\backslash k$	1.7	1.3	1.1	1.6	1.4
13238	3.1	5.4	3.7	4.2	$D_{min}\backslash k$	1.0	1.0	1.0	1.0
5467	**44.6**	**23.6**	4.8	3.2	2.6	$D_{min}\backslash k$	1.0	1.2	1.1
200161	2.6	4.6	3.7	2.8	2.2	2.2	$D_{min}\backslash k$	–	–
28738	3.2	5.7	3.8	4.0	2.6	3.1	–	$D_{min}\backslash k$	–
								FINAL:	**2.2**

Table 8: The k value for AS entering the SPB-IX

AS	**31323**	**196750**	**8897**	**44050**	**3500**	**42688**	**56334**	**28968**	K_{av}
31323	$D_{min}\backslash k$	1.0	4.3	1.0	1.3	1.0	1.0	7.1	2.2
196750	1.2	$D_{min}\backslash k$	4.4	1.0	1.0	–	1.0	6.2	2.7
8897	10.8	11.1	$D_{min}\backslash k$	**23.4**	1.8	1.5	1.5	1.1	5.9
44050	1.4	1.2	**58.6**	$D_{min}\backslash k$	1.3	1.0	**12.5**	7.0	5.5
3500	3.3	2.5	4.6	3.4	$D_{min}\backslash k$	1.3	1.3	3.8	2.1
42688	2.2	–	3.9	2.0	3.2	$D_{min}\backslash k$	1.0	3.1	2.1
56334	2.0	1.4	3.8	**31.4**	3.2	1.3	$D_{min}\backslash k$	3	1.3
28968	17.8	15.6	2.7	17.7	9.5	7.9	3.2	$D_{min}\backslash k$	3.0
								FINAL:	**3.1**

Table 9: The k value for AS outside the SPB-IX

AS	**11458**	**196750**	**8997**	**35000**	**42668**	**56334**	**35807**	**60252**	**59627**	**51093**	K_{av}
11458		–	–	–	–	–	1.0	1.1	**10.1**	4.7	4.2
196750	–		–	–	–	–	3.5	1.0	**10.8**	1.0	4.1
8897	–	–		–	–	–	1.1	1.5	**10.8**	1.5	3.7
35000	–	–	–		–	–	1.2	1.7	**10.8**	1.5	3.8
42668	–	–	–	–		–	1.0	1.0	**9.9**	1.0	3.2
56334	–	–	–	–	–		1.0	1.2	7.1	4.8	3.5
35807	1.8	8.7	2.8	2.9	0.7	1.6	$D_{min}\backslash k$	1.0	**10.0**	1.0	4.0
60252	2.7	2.5	3.8	4.3	2.0	2.9	2.1	$D_{min}\backslash k$	**10.4**	1.1	5.8
59627	**25.3**	**27.2**	**27.0**	**27.0**	**24.9**	17.9	**25.1**	**26.2**	$D_{min}\backslash k$	3.8	3.8
51093	11.7	2.2	3.8	3.7	1.8	12.0	2.0	2.8	4.5	$D_{min}\backslash k$	3.0
										FINAL:	**4.0**

the monitoring process. It should be noted that this statement is a necessary condition, but it is not a sufficient one. The statement is used for initial data selection, and the final decision is taken based on the traceroute result.

As a result of the measurements, it was possible to show that, for a significant proportion of intra-Russian traffic, routing is not geographically optimized. This fact leads to the uncontrolled growth of network delays, which negatively affects the quality of communications. Another consequence of this situation is that a proportion of domestic traffic is served on foreign routers. National monitoring tools cannot detect such anomalies, since the relevant nodes are not deployed in sufficient quantities.

However, Russian systems that address this problem

Table 10: Dependence of the threshold value of the efficiency factor of geographical routing

No.	The geographical distance	Threshold value of the efficiency factor
1	less than 250km (IX)	9
2	less than 2000km	5
3	more than 3000km	3.5

are available; they are patented, and experimental networks have been deployed. These developments show more potential than the European RIPE Atlas system. The Russian NetTestBox system measures a one-way delay, and this makes it possible to detect anomalous channels and to find anomalous directions during routing.

To solve the problem of the optimization of intra-Russian traffic, it has been suggested that Internet Exchange Points should be used. The existing Internet Exchange Points have significant disadvantages. First, they have low coverage of the regional autonomous systems. Second, within each traffic exchange point not all autonomous systems allow free traffic exchange among themselves. Ideally, it is necessary to build a single all-Russian Internet Exchange System where peering will be registered among all Russian ASs.

Acknowledgments

The reported study was funded by RFBR according to the research project №16-07-00218a and the public tasks of the Ministry of Education and Science of the Russian Federation (2.974.2017/4.6).

References

[1] G. Almes, S. Kalidindi, M. Zekauskas, and A. Morton, *A One-Way Delay Metric for IP Performance Metrics (IPPM)*, RFC 2330, 2016.

[2] V. Bajpai, S. J. Eravuchira, and J. Schönwälder, "Lessons learned from using the ripe atlas platform for measurement research," *ACM Sigcomm Computer Communication Review*, vol. 45, no. 3, pp. 35–42, 2015.

[3] I. N. Bozkurt, A. Aguirre, B. Chandrasekaran, P. B. Godfrey, G. Laughlin, B. Maggs, and A. Singla, "Why is the internet so slow?!," in *International Conference on Passive and Active Network Measurement*, pp. 173–187, 2017.

[4] L. Carbone, F. Coccetti, P. Dini, R. Percacci, and A. Vespignani, "The spectrum of internet performance," *Pasive and Active Measurements (PAM'03)*, pp. 75–88, 2003.

[5] A. Clement and J. A. Obar, "Internet boomerang routing: Surveillance, privacy and network sovereignty in a north american context," *Research Gate*, 2013. (https://www.researchgate.net/publication/256055599_Internet_Boomerang_Routing_Surveillance_Privacy_and_Network_Sovereignty_in_a_North_American_Context)

[6] ITU-T Rec. G.1010, "End-user multimedia qos categories," *ITU-T*, 2001. (https://www.itu.int/rec/T-REC-G.1010-200111-I)

[7] P. Gigis, V. Kotronis, E. Aben, S. D. Strowes, and X. Dimitropoulos, "Characterizing user-to-user connectivity with ripe atlas," in *Proceedings of the Applied Networking Research Workshop*, pp. 4–6, 2017.

[8] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 68–73, 2008.

[9] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett, "Peering at the internet's frontier: A first look at isp interconnectivity in africa," in *International Conference on Passive and Active Network Measurement*, pp. 204–213, 2014.

[10] PriMetrica, Inc., *Internet Exchange Map*, (https://www.internetexchangemap.com/)

[11] J. Kukkola, J. Nikkarila, and M. Ristolainen, "Asymmetric frontlines of cyber battlefields," *GAME CHANGER Structural Transformation of Cyberspace*, pp. 69, 2017.

[12] J. Mahdavi and V. Paxson, *IPPM Metrics for Measuring Connectivity*, RFC 2678, 1998.

[13] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The tactile internet: vision, recent progress, and open challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 138–145, 2016.

[14] RIPE NCC, "Ixp country jedi - ixp country," *Internet Measurements*, 2017. (http://sg-pub.ripe.net/emile/ixp-country-jedi/latest/RU/ixpcountry/index.html)

[15] RIPE NCC, "Members ordered by country code," June 3, 2019. (https://www.ripe.net/membership/indices/RU.html)

[16] R. Sampson, S. Rajappa, A. S. Sabitha, A. Bansal, B. White, and L. Cottrell, "Implementation of pinger on android," in *7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 306–312, 2017.

[17] A. M. Sukhov, M. A. Astrakhantseva, A. K. Pervitsky, S. S. Boldyrev, and A. A. Bukatov, "Generating a function for network delay," *Journal of High Speed Networks*, vol. 22, no. 4, pp. 321–333, 2016.

[18] A. M. Sukhov and A. V. Onoprienko, "Evaluating the effectiveness of geographic routing based on ripe atlas data," in *Telecommunications Forum Telfor (TELFOR'14)*, pp. 107–110, 2014.

[19] N. Vinogradov, E. Sagatov, A. Sukhov, "Measurement of one-way delays in IP networks," *Measurement Techniques*, vol. 60, no. 4, pp. 359–365, July 2017.

Biography

Evgeny Sagatov is an Associate Professor of Samara National Research University, Russia and was awarded a PhD in Samara State Aerospace University in 2014. His current research interests include computer networks: security, DDoS attacks, botnets, sensor and wireless networks, routing protocols, quality characteristics; broadcast video along wireless networks: transmission methods, codecs, protocols, Wi-Fi, WiMAX, 3G, 4G, LTE networks. He participated in many international and national conferences on computer networks and network security. These are IFIP WD 2011 (Student Travel Grant), LCN 2017, ITNT 2017 (Best paper award in Cyber Security Section), PHDays 2018, etc. E-mail: sagatov@ya.ru.

Konstantin Lovtsov, 1995 is a master of the second year of study. His field of research is quality connection in computer networks. He made a presentation at the IEEE Telfor 2015 conference, Belgrade, Serbia.

Andrei Sukhov, 1962 is a Professor of Samara National Research University, Russia and was awarded a PhD in Moscow in Physics and Mathematics in 1993. In 2007 he received Dr.Sc. degree in Computer Networking at Moscow State University of Electronics and Mathematics (MIEM HSE). Over the last 25 years he has been involved in acting as an investigator for more than 15 telecommunication projects supported by the Russian government, RFBR, INTAS, NATO, ESA, etc. His research area is computer networks and network security. His hope page is https://ssau.ru/english/staff/64258001-sukhov-andrey-mikhaylovich.