Radio call signs of consumer electronics as a data source in human geography

Sinitsyn Nikita, Research assistant, Department of Economic and Social Geography of Russia, Faculty of Geography, Lomonosov Moscow State University.
nicksinus@yandex.ru

Konnov Andrey, Fourth-year bachelor student, Department of Ecology and Environmental Management, Faculty of Geography, Kazakh Branch of Moscow State University.
konnovandrey55@gmail.com

Speaker: Konnov Andrey

Background

Today, most people use wearable electronics. These devices interact with each other via radio communication using Bluetooth or Wi-Fi protocols. The call signs of Bluetooth and Wi-Fi protocols are unencrypted and open and **can be recorded** using specialized software.

The number of wearable electronic devices can be an **indirect indicator** of the number of people.

The main questions of our research:

1. How to **organize field observations?**

2. Could this data provide **valuable analytical insights?**

3. Can we **trust** the results?

Basic technical principles

Radio signal types of electronic devices

Wi-Fi

max dist. = 500 m.

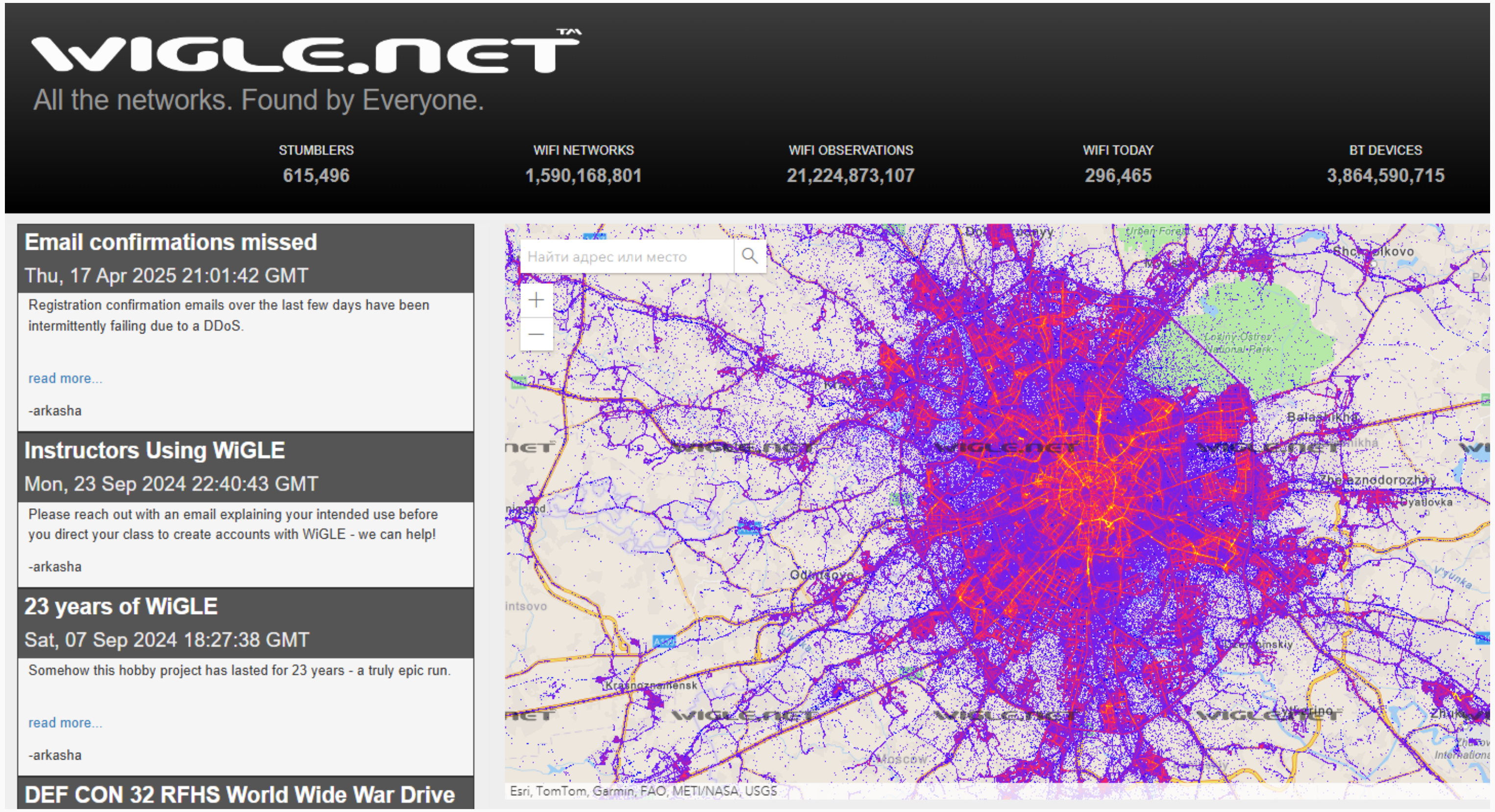
Bluetooth (BT)

max dist. = 150 m.

Bluetooth Low Energy (BLE)

max dist. = 100 m.

Wardriving



All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES
615,496	1,590,168,801	21,224,873,107	296,465	3,864,590,715

Email confirmations missed

Thu, 17 Apr 2025 21:01:42 GMT

Registration confirmation emails over the last few days have been intermittently failing due to a DDoS.

read more...

-arkasha

Instructors Using WiGLE

Mon, 23 Sep 2024 22:40:43 GMT

Please reach out with an email explaining your intended use before you direct your class to create accounts with WiGLE - we can help!

-arkasha

23 years of WiGLE

Sat, 07 Sep 2024 18:27:38 GMT

Somehow this hobby project has lasted for 23 years - a truly epic run.

read more...

-arkasha

DEF CON 32 RFHS World Wide War Drive

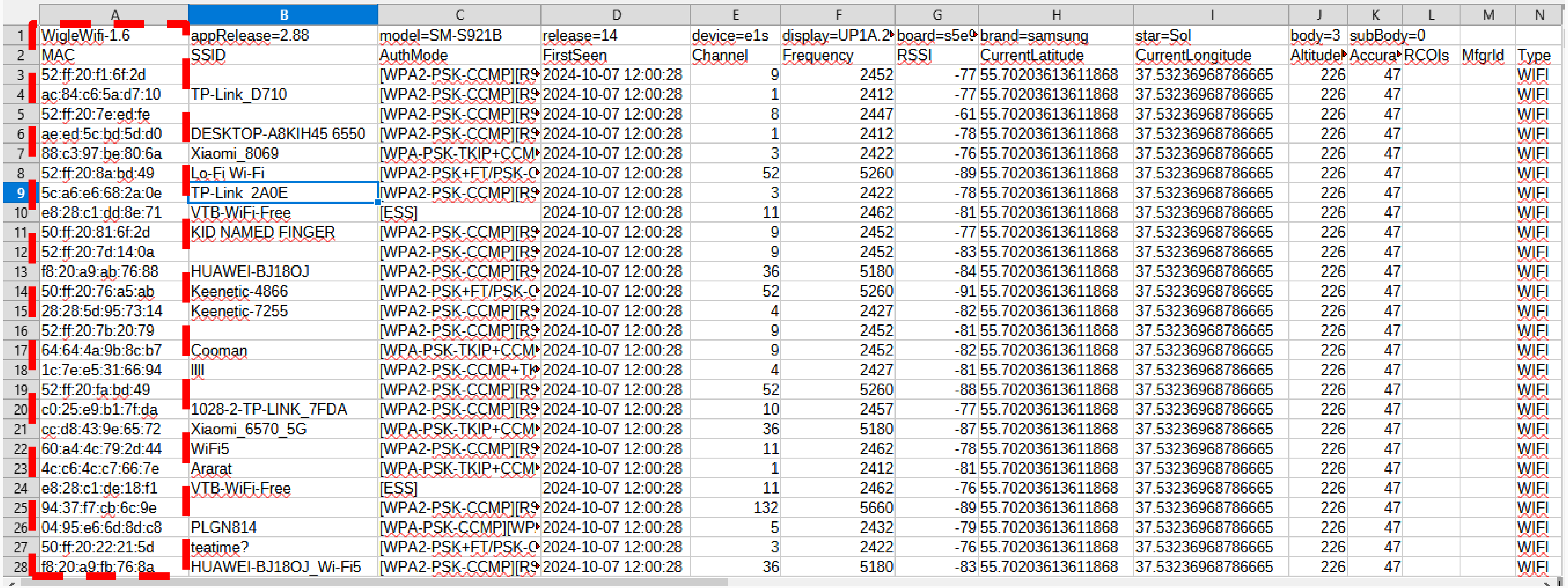
Esri, TomTom, Garmin, FAO, METI/NASA, USGS

Wardriving is the act of recording Wi-Fi and Bluetooth signals, usually moving by car or on foot and using a laptop or smartphone. Wardriving software is freely available on the internet.

The world's largest wardriving project is **Wigle.net**. It is an open crowdsource database of wireless electronics devices call signs.

A special wardriving app was developed within this project. The **Wigle app is Android only.**

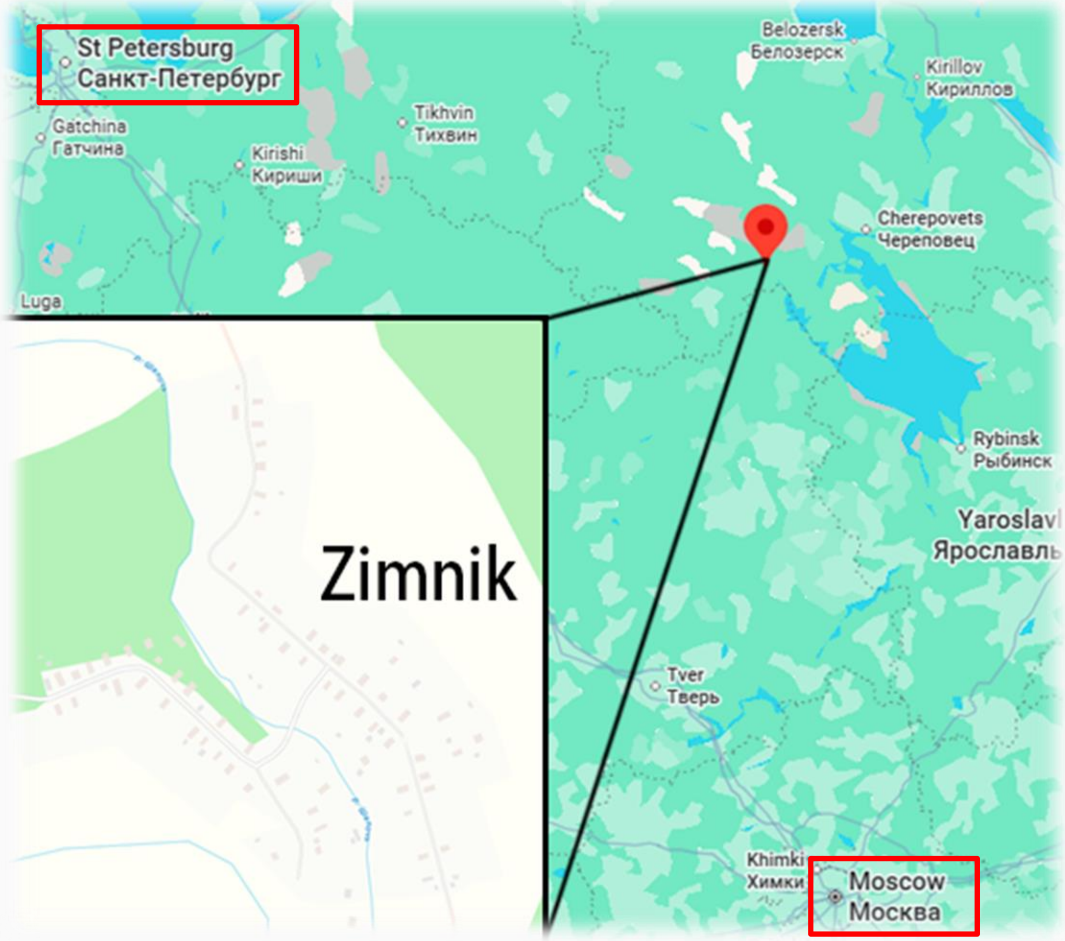
Recording results of Wigle app: table of call signs



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	WigleWifi-1.6	appRelease=2.88	model=SM-S921B	release=14	device=e1s	display=UP1A.2	board=s5e9	brand=samsung	star=Sol	body=3	subBody=0			
2	MAC	SSID	AuthMode	FirstSeen	Channel	Frequency	RSSI	CurrentLatitude	CurrentLongitude	Altitude	Accura	RCOIs	MfgrId	Type
3	52:ff:20:f1:6f:2d		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	9	2452	-77	55.70203613611868	37.53236968786665	226	47			WIFI
4	ac:84:c6:5a:d7:10	TP-Link_D710	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	1	2412	-77	55.70203613611868	37.53236968786665	226	47			WIFI
5	52:ff:20:7e:ed:fe		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	8	2447	-61	55.70203613611868	37.53236968786665	226	47			WIFI
6	ae:ed:5c:bd:5d:d0	DESKTOP-A8KIH45 6550	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	1	2412	-78	55.70203613611868	37.53236968786665	226	47			WIFI
7	88:c3:97:be:80:6a	Xiaomi_8069	[WPA-PSK-TKIP+CCM	2024-10-07 12:00:28	3	2422	-76	55.70203613611868	37.53236968786665	226	47			WIFI
8	52:ff:20:8a:bd:49	Lo-Fi Wi-Fi	[WPA2-PSK+FT/PSK-C	2024-10-07 12:00:28	52	5260	-89	55.70203613611868	37.53236968786665	226	47			WIFI
9	5c:a6:e6:68:2a:0e	TP-Link_2A0E	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	3	2422	-78	55.70203613611868	37.53236968786665	226	47			WIFI
10	e8:28:c1:dd:8e:71	VTB-WiFi-Free	[ESS]	2024-10-07 12:00:28	11	2462	-81	55.70203613611868	37.53236968786665	226	47			WIFI
11	50:ff:20:81:6f:2d	KID NAMED FINGER	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	9	2452	-77	55.70203613611868	37.53236968786665	226	47			WIFI
12	52:ff:20:7d:14:0a		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	9	2452	-83	55.70203613611868	37.53236968786665	226	47			WIFI
13	f8:20:a9:ab:76:88	HUAWEI-BJ18OJ	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	36	5180	-84	55.70203613611868	37.53236968786665	226	47			WIFI
14	50:ff:20:76:a5:ab	Keenetic-4866	[WPA2-PSK+FT/PSK-C	2024-10-07 12:00:28	52	5260	-91	55.70203613611868	37.53236968786665	226	47			WIFI
15	28:28:5d:95:73:14	Keenetic-7255	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	4	2427	-82	55.70203613611868	37.53236968786665	226	47			WIFI
16	52:ff:20:7b:20:79		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	9	2452	-81	55.70203613611868	37.53236968786665	226	47			WIFI
17	64:64:4a:9b:8c:b7	Cooman	[WPA-PSK-TKIP+CCM	2024-10-07 12:00:28	9	2452	-82	55.70203613611868	37.53236968786665	226	47			WIFI
18	1c:7e:e5:31:66:94	IIII	[WPA2-PSK-CCMP+TK	2024-10-07 12:00:28	4	2427	-81	55.70203613611868	37.53236968786665	226	47			WIFI
19	52:ff:20:fa:bd:49		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	52	5260	-88	55.70203613611868	37.53236968786665	226	47			WIFI
20	c0:25:e9:b1:7f:da	1028-2-TP-LINK_7FDA	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	10	2457	-77	55.70203613611868	37.53236968786665	226	47			WIFI
21	cc:d8:43:9e:65:72	Xiaomi_6570_5G	[WPA-PSK-TKIP+CCM	2024-10-07 12:00:28	36	5180	-87	55.70203613611868	37.53236968786665	226	47			WIFI
22	60:a4:4c:79:2d:44	WiFi5	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	11	2462	-78	55.70203613611868	37.53236968786665	226	47			WIFI
23	4c:c6:4c:c7:66:7e	Ararat	[WPA-PSK-TKIP+CCM	2024-10-07 12:00:28	1	2412	-81	55.70203613611868	37.53236968786665	226	47			WIFI
24	e8:28:c1:de:18:f1	VTB-WiFi-Free	[ESS]	2024-10-07 12:00:28	11	2462	-76	55.70203613611868	37.53236968786665	226	47			WIFI
25	94:37:f7:cb:6c:9e		[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	132	5660	-89	55.70203613611868	37.53236968786665	226	47			WIFI
26	04:95:e6:6d:8d:c8	PLGN814	[WPA-PSK-CCMP][WP	2024-10-07 12:00:28	5	2432	-79	55.70203613611868	37.53236968786665	226	47			WIFI
27	50:ff:20:22:21:5d	teatime?	[WPA2-PSK+FT/PSK-C	2024-10-07 12:00:28	3	2422	-76	55.70203613611868	37.53236968786665	226	47			WIFI
28	f8:20:a9:fb:76:8a	HUAWEI-BJ18OJ_Wi-Fi5	[WPA2-PSK-CCMP][R	2024-10-07 12:00:28	36	5180	-83	55.70203613611868	37.53236968786665	226	47			WIFI

MAC address is a unique device number, usually assigned during manufacturing (Wi-Fi), or it can be random (Bluetooth).

First case: Zimnik village (Vologda region)



Zimnik village

- There are **81 houses** (average size for this region).
- There is **almost no local population** (only a few people).
- The majority of the houses is used as a **second-housing** by residents from Cherepovets. It is 95 km to this city (an hour by car).
- The nearest cell tower is far away (4 km), so a **Wi-Fi router** with an external antenna **is required** for mobile internet.

Yandex
Yandex

Methodology of rural settlement observation

- Measurements were taken over 12 months (July 2024 – June 2025).
- Typical weekends (not holiday Saturday-Sunday) were selected in the middle of the month.
- **Saturday** evening was considered a **weekend**, and **Sunday** evening was considered a **weekday** (in the second half of Sunday, most people commute from Zimnik to Cherepovets).
- Measurements were taken in the **evening**, after sunset (while everyone is already home but not yet asleep).
- In summer, the observer traveled by bicycle, and in winter, on skis (the phone was kept **in a glove**🧤 in winter to prevent it from turning off).
- Radio call signs were recorded on a phone using the Wiggle app.

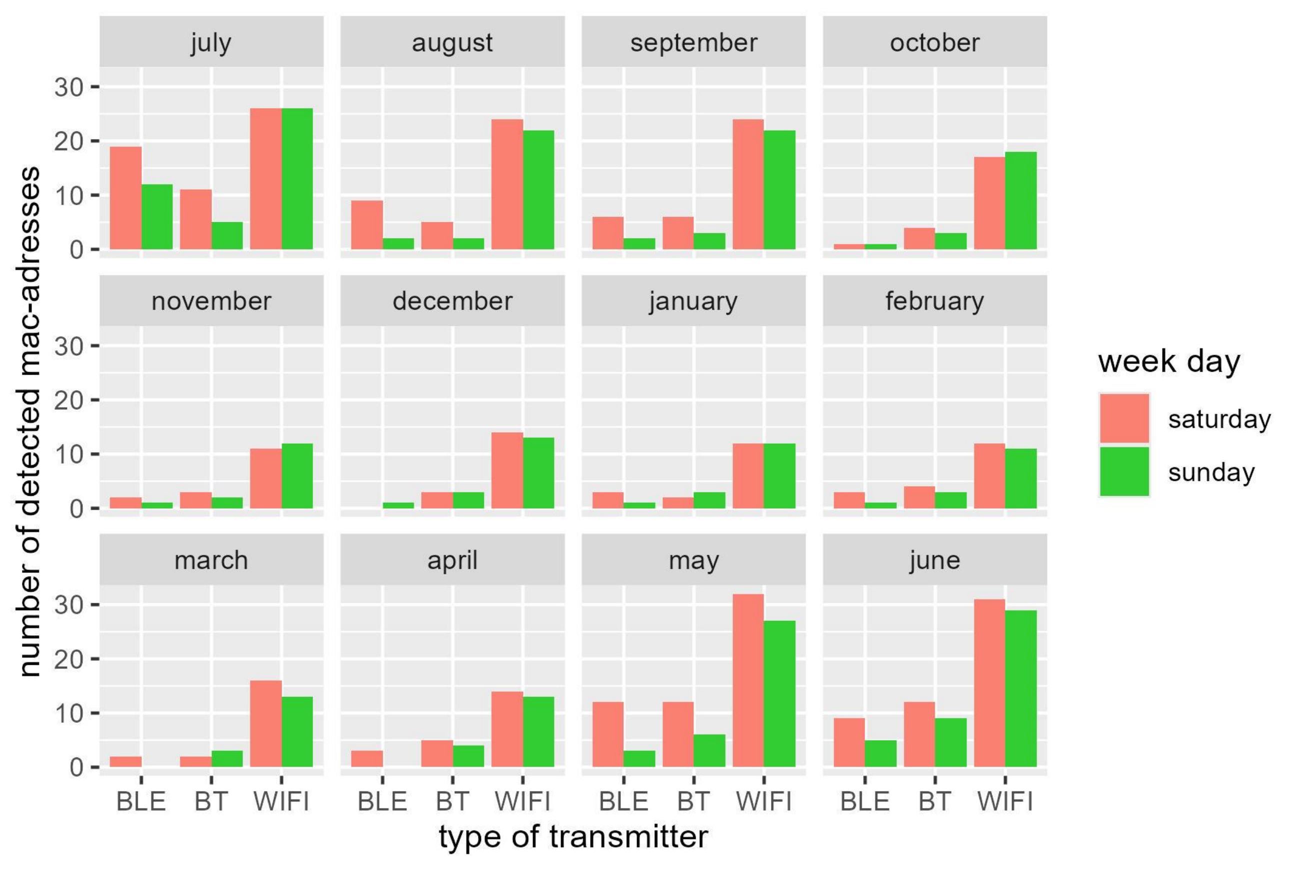
The yearly dynamics of the radio transmitters structure in Zimnik

Trend #1:
The number of Wi-Fi transmitters drops by half (from 20-25 in summer to 10-15 in winter).
The number of Bluetooth transmitters drops tenfold (from 10-20 in summer to 1-2 in winter).

Reason:
Bluetooth – young people.
Wi-Fi – young people and retirees.
Young people come for the weekend **only** in summer (it is dark and cold in winter).

Trend #2:
During summer holidays, the number of Bluetooth transmitters is 2-4 times higher than on weekdays.

Reason:
Some young people commute to the city, while others stay in the countryside on vacation.

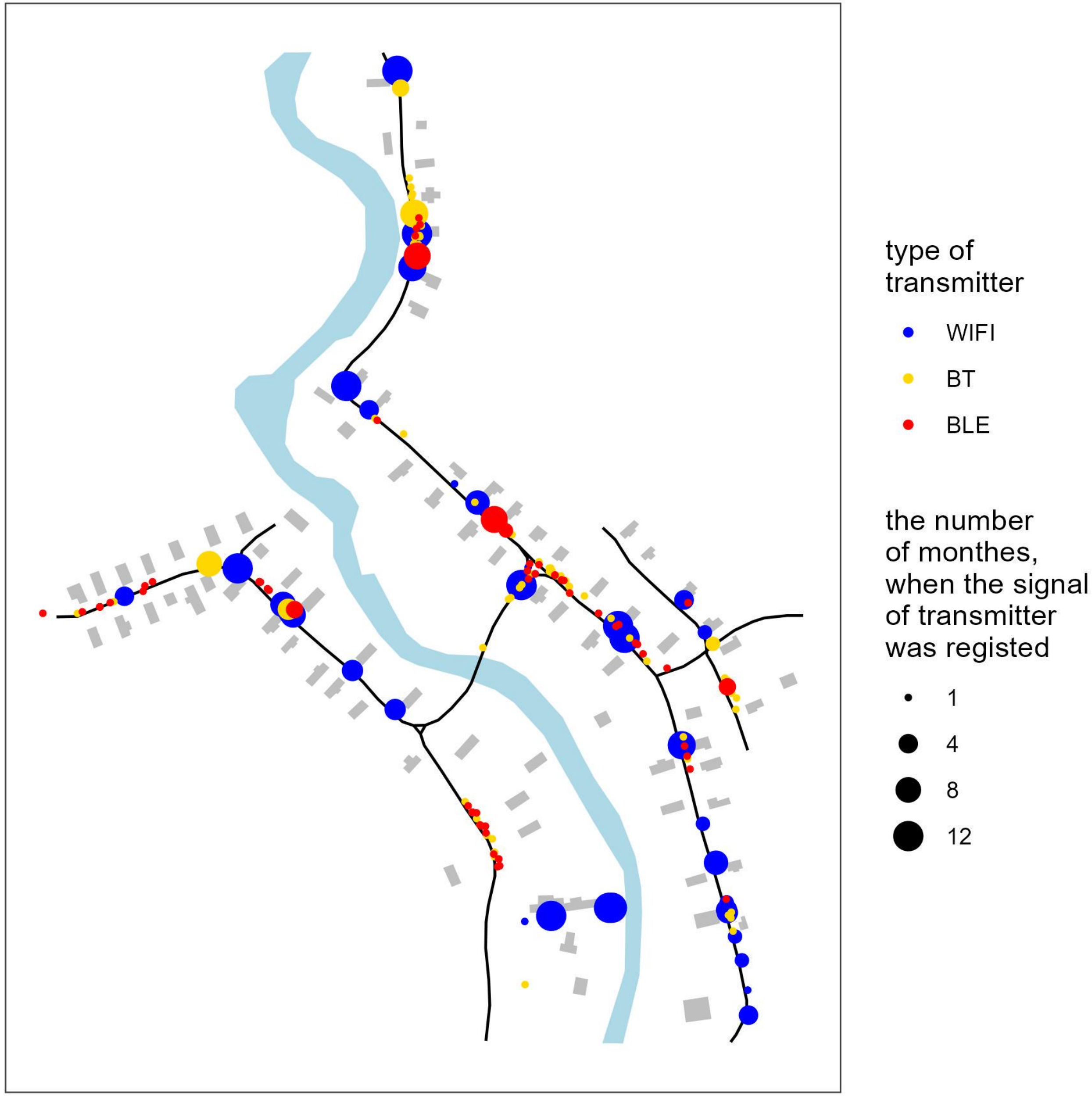


Types of houses in Zimnik

- Large blue circles represent the houses of urban retirees who live there year-round. They also represent local residents.

- Medium and small blue circles represent the homes of urban retirees who live there during the warm season.

- The scattering of small red and yellow circles represents relatively young generations of urban residents. More circles mean more young people (according to our field observations).


type of transmitter
● WIFI
● BT
● BLE
the number of monthes, when the signal of transmitter was registed
● 1
● 4
● 8
● 12

First case conclusions

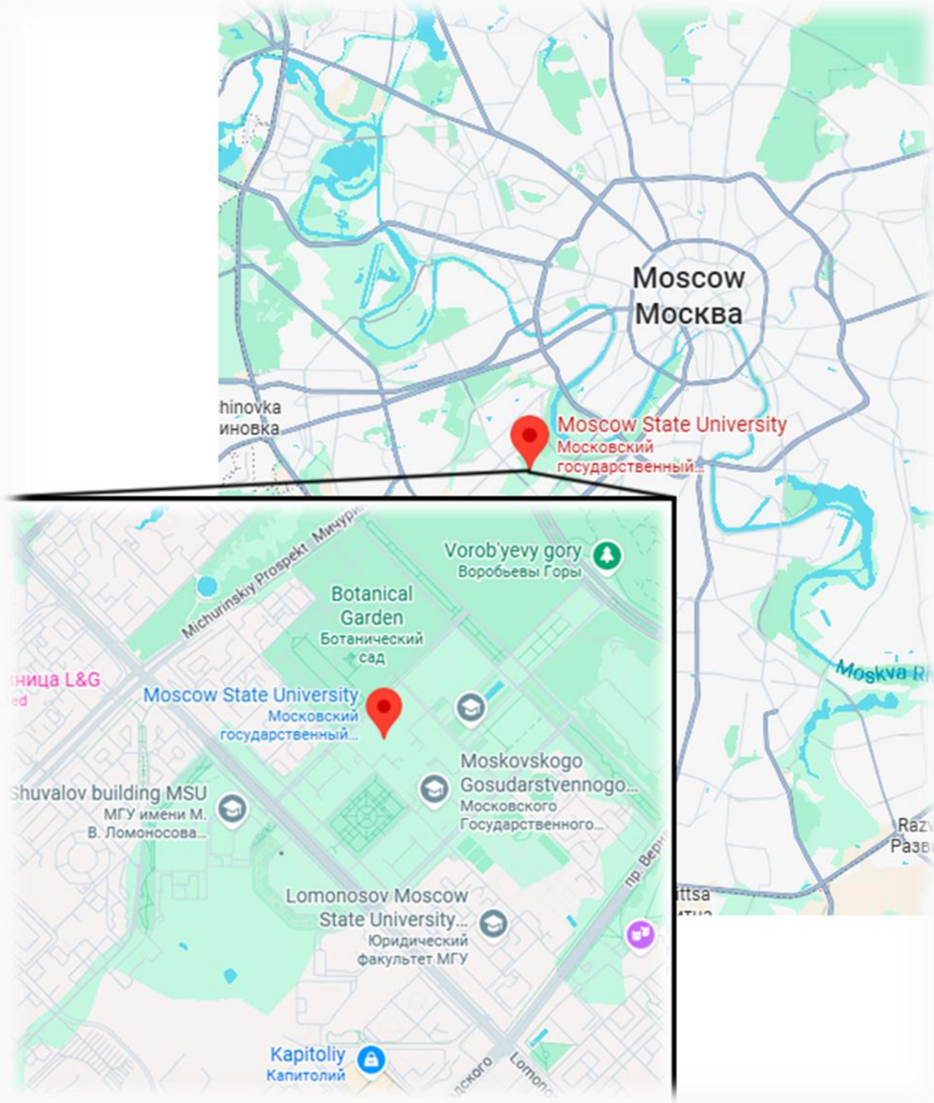
- The annual dynamics of the number of radio transmitters shows that Zimnik is a second-housing settlement (**many devices in summer, few in winter**).

- The increased proportion of **Wi-Fi** transmitters indicates that retirees and local residents dominate in the village's population structure **in winter**.

- The increased proportion of **Bluetooth** transmitters indicates that young generations dominate in the village's population structure **in summer**.

- The **number** of different types of transmitters in a house can indicate the **age structure** of the residents.

Second case: MSU campus area



Methodology of measuring pedestrian flows in the public space

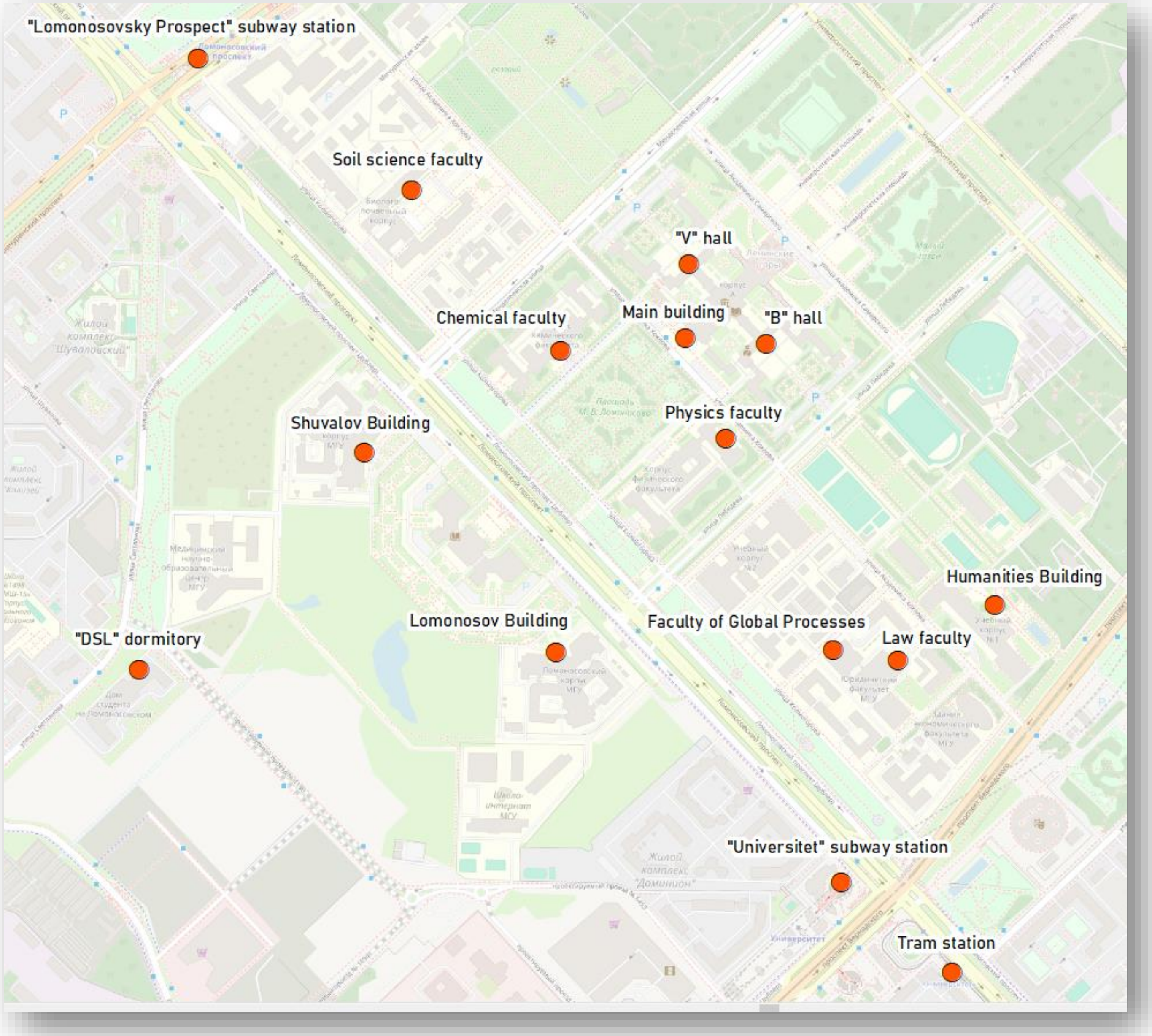
- We consider that **the flow of people is proportional to the flow of wearable devices**.
- **Only Bluetooth** devices were used (Wi-Fi is usually a static router).
- Devices were identified by their **MAC addresses**.
- Bluetooth signals were recorded at **15 points** by students of the Faculty of Geography, Moscow State University. Measurements were taken on **Monday, October 21, 2024, from 2:30 p.m. to 5:30 p.m.**
- Pedestrian flow between two points is equal to the number of devices detected at both points.

Map of recording points

Choosing the right location for the measurement point is very important. **The main problem is parasitic traffic**.

Example:
Let’s consider two faculties located in two different buildings.

- If observers are placed **inside the building**, near the exits, they will register only signals from students and teachers.
- If observers are placed **outside the building** near the exits, they will register signals not only from students and teachers, but also from people passing by. These random passersby are “parasites”.



Dormitories map

○ Educational buildings

□ Dormitories

LHS - Lomonosovskiy house of students
MB - Main Building
HSI - House of students and interns

The size of the circle and the height of the bar are proportional to the amount of students in the educational buildings and dormitories

Faculties

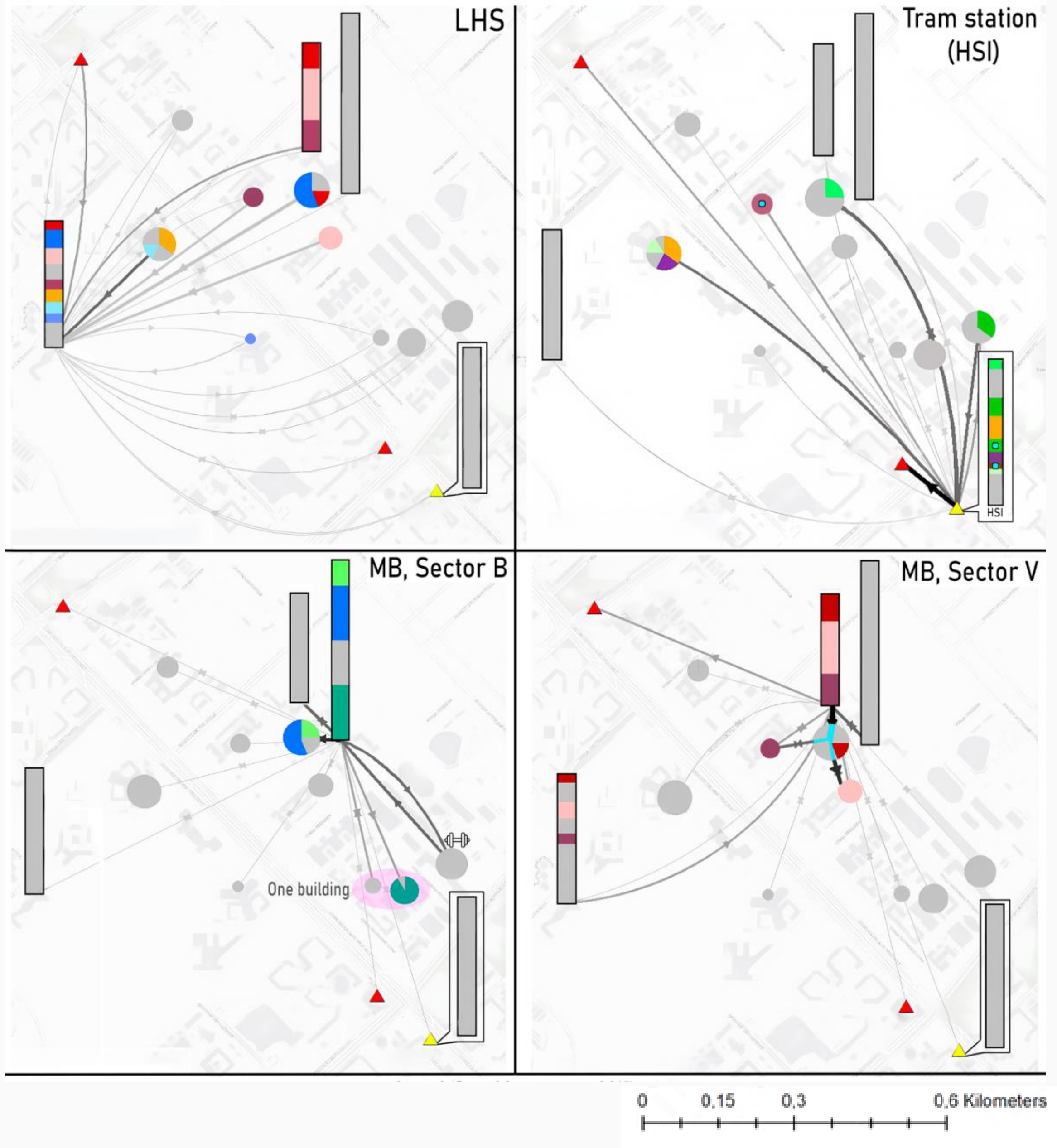
- 🟩 Philological
- 🟥 Physical
- 🟥 Chemical
- 🟧 Historical
- 🟫 Soil Science
- 🟩 Biological
- 🟩 Law faculty
- 🟪 Philosophy
- 🟨 World politics
- 🟦 Public administration
- 🟩 Higher School of Translation
- 🟩 Political Science
- 🟦 Mechanics and Mathematics
- 🟩 Geographical
- 🟥 Geological

Flow intensity (ppl.)

- ➤ 0-6
- ➤ 7-24
- ➤ 25-85
- ➤ 86-186
- ➤ 177-275

Other

- ▲ Subway station
- ▲ Tram station
- □ Dormitories connected to public transportation stations
- ● Classes at other faculties
- — Transit flows
- Sports grouds and gyms

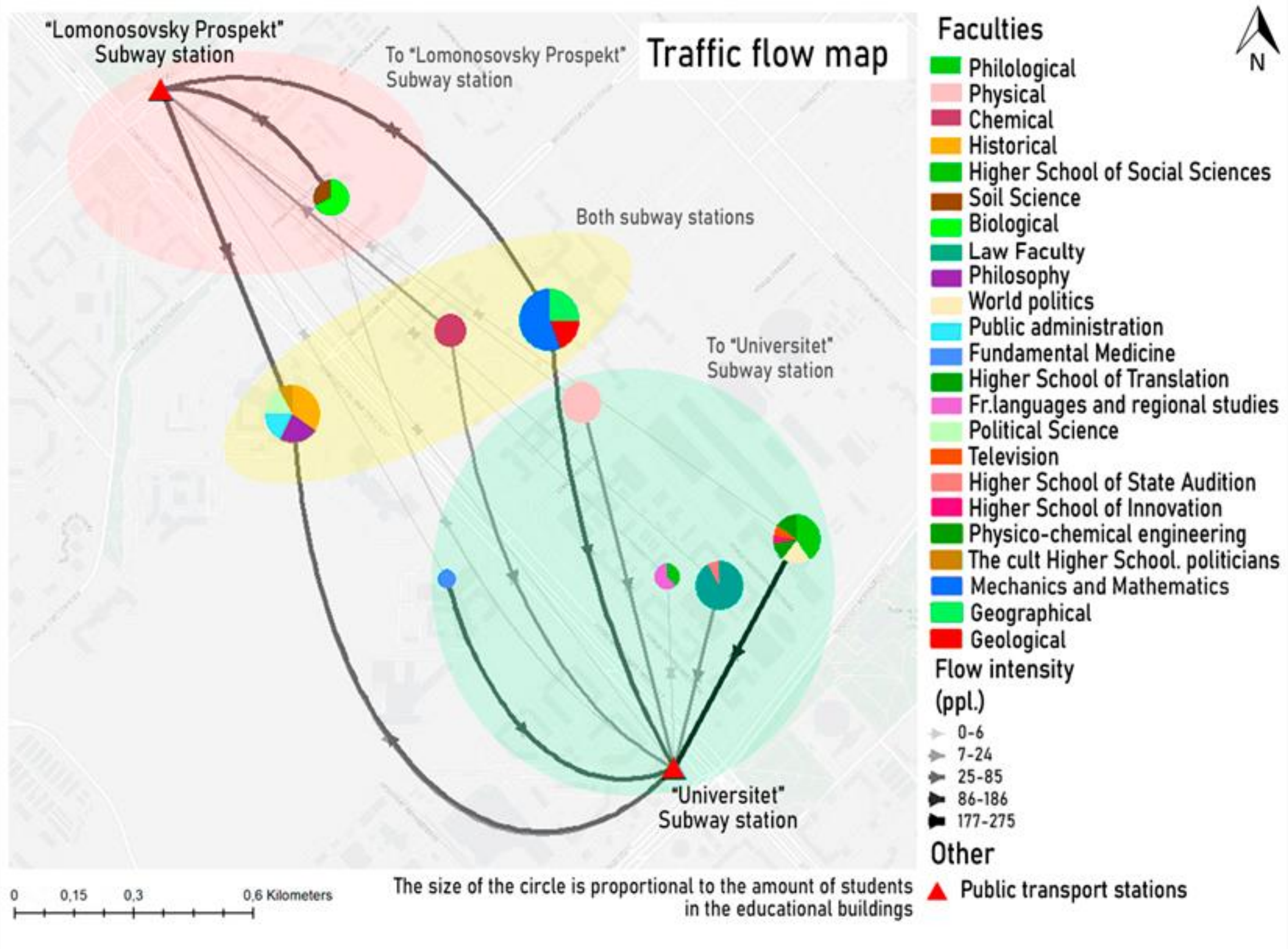


- There are two metro stations near the university campus. The service area to the «Universitet» station is larger because:

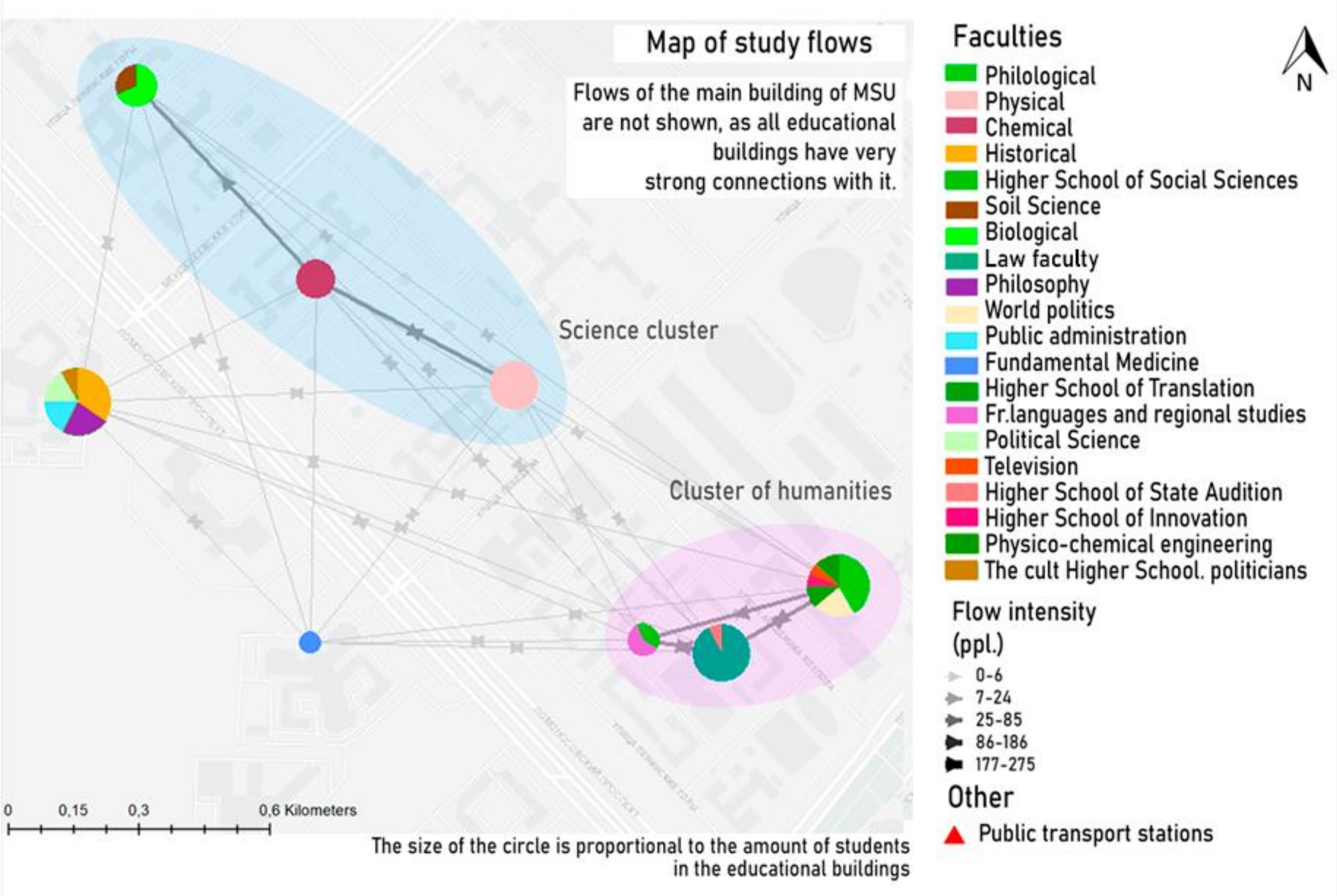
- There are more faculties near this station (it was opened in 1959, while «Lomonosovsky Prospekt» was opened in 2017)

- «Universitet» is located at the same level as many university buildings, but «Lomonosovsky Prospekt» is elevated lower, so people have to climb uphill, it is inconvenient.

- The common service area of both stations is located between their individual service areas.


Traffic flow map
"Lomonosovsky Prospekt" Subway station
To "Lomonosovsky Prospekt" Subway station
Both subway stations
To "Universitet" Subway station
"Universitet" Subway station
0
0,15
0,3
0,6 Kilometers
N
Faculties
🟩 Philological
Physical
Chemical
Historical
Higher School of Social Sciences
Soil Science
Biological
Law Faculty
Philosophy
World politics
Public administration
Fundamental Medicine
Higher School of Translation
Fr.languages and regional studies
Political Science
Television
Higher School of State Audition
Higher School of Innovation
Physico-chemical engineering
The cult Higher School. politicians
Mechanics and Mathematics
Geographical
Geological
Flow intensity (ppl.)
0-6
7-24
25-85
86-186
177-275
Other
▲ Public transport stations

The size of the circle is proportional to the amount of students in the educational buildings



Map of study flows

Flows of the main building of MSU are not shown, as all educational buildings have very strong connections with it.

The size of the circle is proportional to the amount of students in the educational buildings

There are two educational clusters in the pedestrian flow network: the natural sciences cluster and the cluster of humanities.

- Science cluster: Chemistry, Physics, Soil Science, and Biology.
- Cluster of humanities: Philology, Law, Regional Studies, and Translation.

Second case conclusions

Before call signs recording, it is necessary to:

- set up observation points so as to exclude “parasitic traffic” from people passing by;

- conduct preliminary test measurements to check the power of Bluetooth receivers on smartphones and laptops (in the subway during rush hour).

Large and medium flows connect:

- academic buildings and dormitories where the same departments are located;
- academic buildings and subway stations.

There are two educational clusters in the pedestrian flow network:

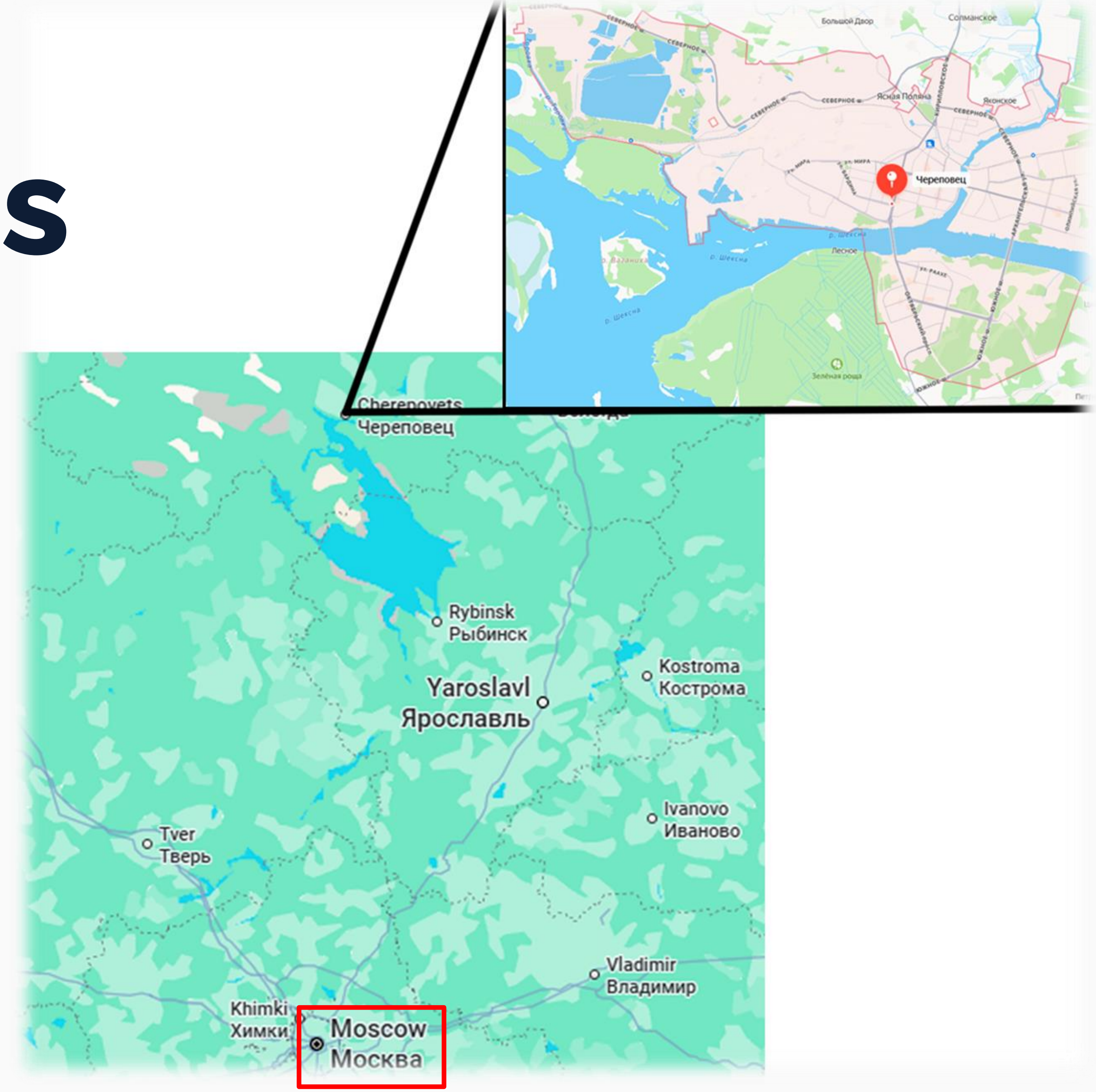
- natural sciences;
- humanities.

There are three transport clusters in the pedestrian flow network:

- the service area of the Universitet metro station;
- the service area of the Lomonosovsky Prospekt metro station;
- the common service area of both stations.

Third case: Cherepovets

How to work with random MAC address?



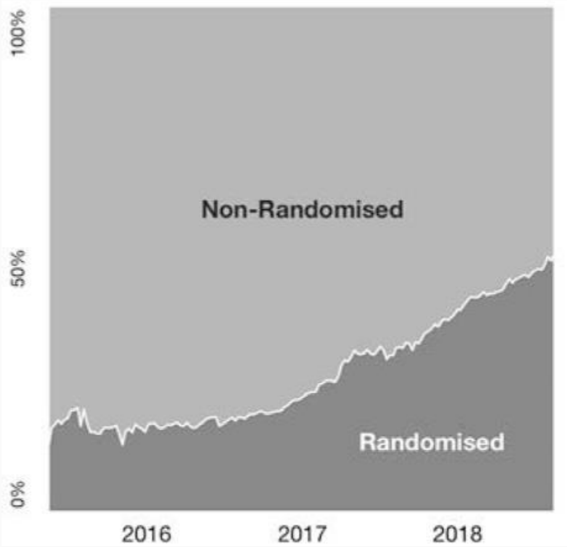
MAC-address randomization

Year of implementation:

- IOS: 2014, V8.0
- Android: 2015, V6.0

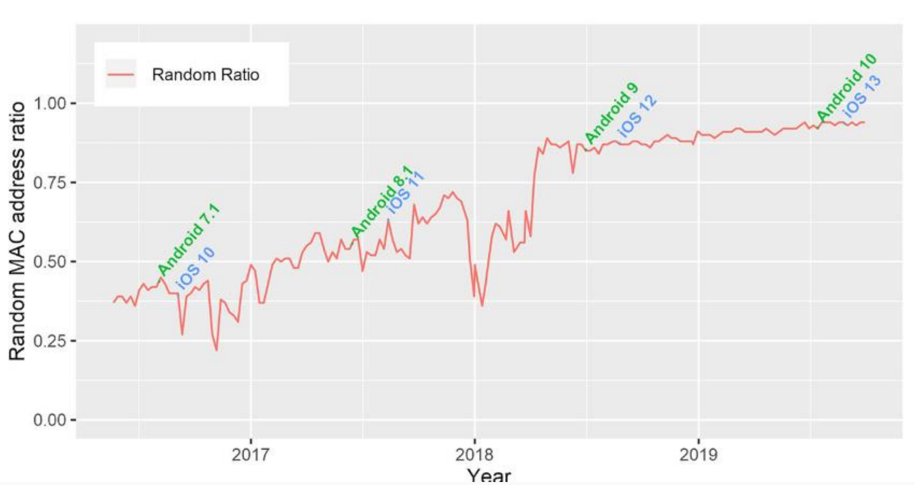
Bluetooth SIG recommended manufacturers to implement a **15-minute** period of Bluetooth MAC address randomization

Problem: How to work with large territories and long periods?



The proportion of randomised vs non randomised from 2016-18 showing increase in randomised MAC addresses in SmartStreetSensor Data.

Source: *Using Wi-Fi probe requests from mobile phones to quantify the impact of pedestrian flows on retail turnover*, Figure 1 **(Trasberg T et al., 2021)**



Ratio of random devices from the total detected for the 4 years of the deployment, plotted against the major Android and iOS release dates.

Source: *Passive Wi-Fi monitoring in the wild: a long-term study across multiple location typologies*, Figure 3 ***(Ribeiro M et al., 2020)***

Methodology of observation in public transport

Most Bluetooth devices send call signs (advertising packets) every 100-300 milliseconds.

In public transport, the observer moves with the passenger devices at the same time.

Let’s consider that we have a record log with a high frequency of call signs recording (every device is observed approx. every second).

The moment of MAC address change can be detected in such a log:
One MAC address disappears, while the second one appears at the same second.

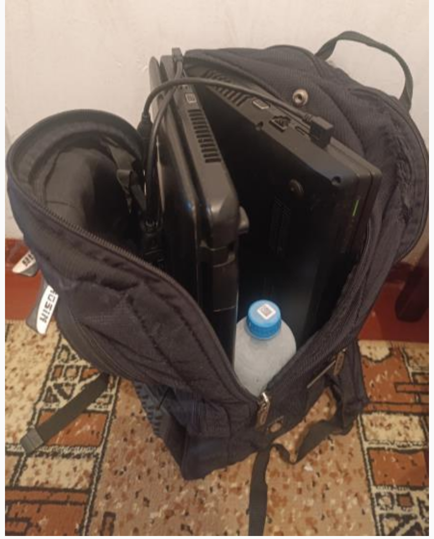
If Bluetooth devices change their MAC addresses every 15 minutes, there is a low probability that two devices **change** their MAC addresses at the same second **simultaneously**.

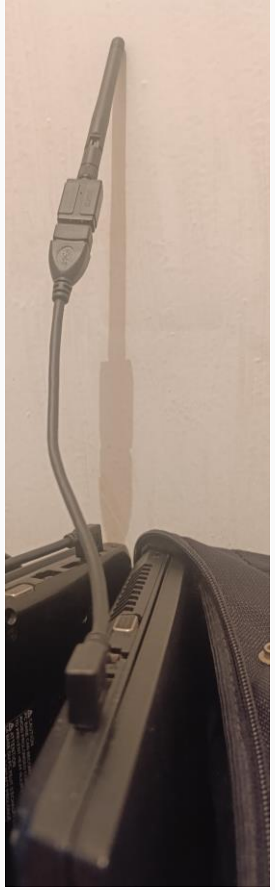
How to record a detailed Bluetooth log?

No Wigle app, the battery controller of every smartphone restricts a high-frequency Bluetooth call sign recording.

Use raw signal data from the laptop Bluetooth transmitter.

- Activate the BL transmitter on a laptop via any BL monitoring app (we used BluetoothLEView[1]).
- Capture raw data from the activated transmitter by using the Wireshark program.





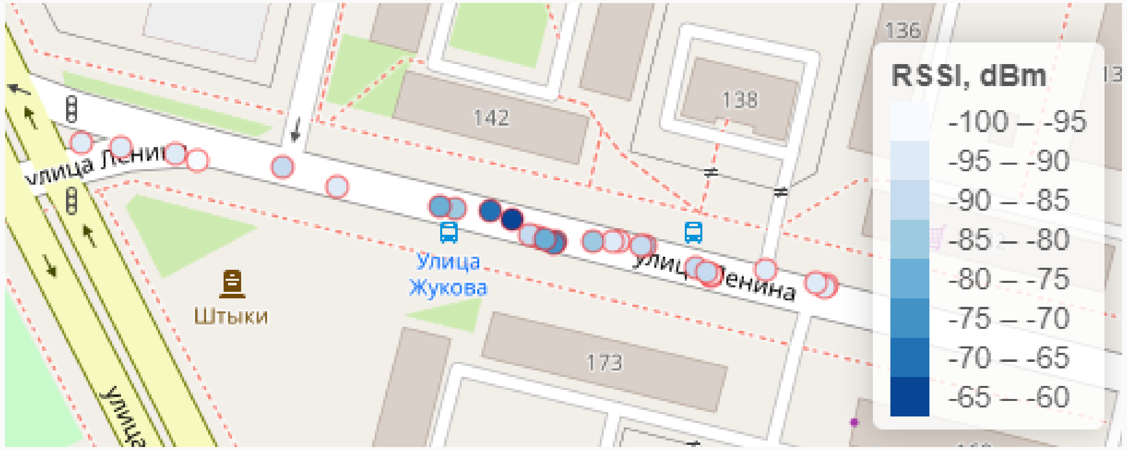
Equipment requirement:

- Don't use the integrated BL adapter of a laptop. **Use an external adapter with a big antenna.**
- One laptop isn't enough. **Use at least three laptops** to avoid data gaps in recordings.
- Working laptops in one backpack produce **a lot of heat**, so we recommend using a cooling device (**a bottle with frozen water**).

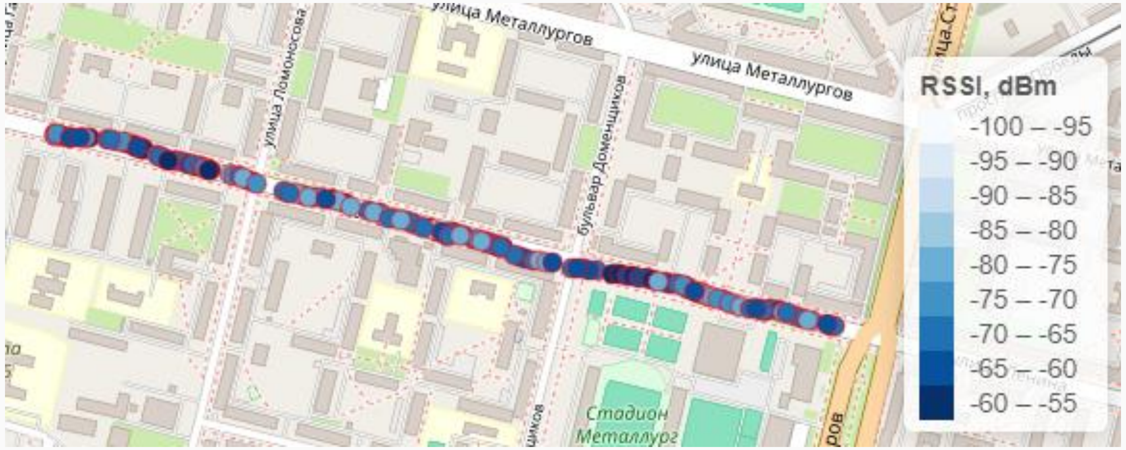
[1] BluetoothLEView: https://www.nirsoft.net/utils/bluetooth_low_energy_scanner.html

Data preprocessing

The log of Bluetooth call signs includes not only devices from the bus, but also from moving cars, walking pedestrians, etc. These **parasitic devices should be excluded** from the log.



MAC address of the device from the bus stop



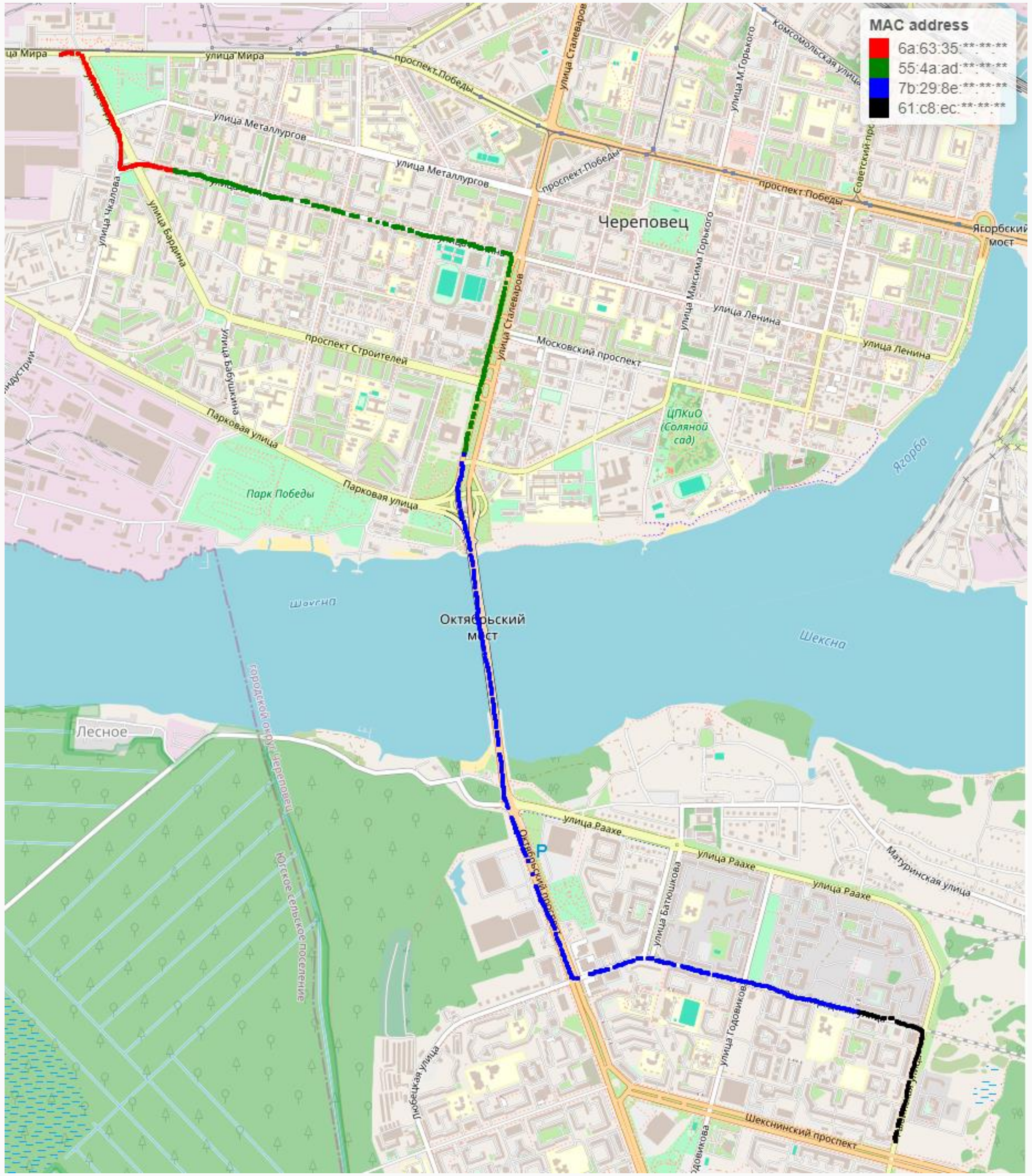
MAC address of the device from the bus

Rules of merging MAC addresses

1. The time interval between the appearance/disappearance of two MAC addresses is **less than 10 seconds**.

2. The difference between the signal power of two MAC addresses is **less than 10 dBm**.

3. The first and the last point of the merged MAC addresses are **further than 30m** from the bus stop.



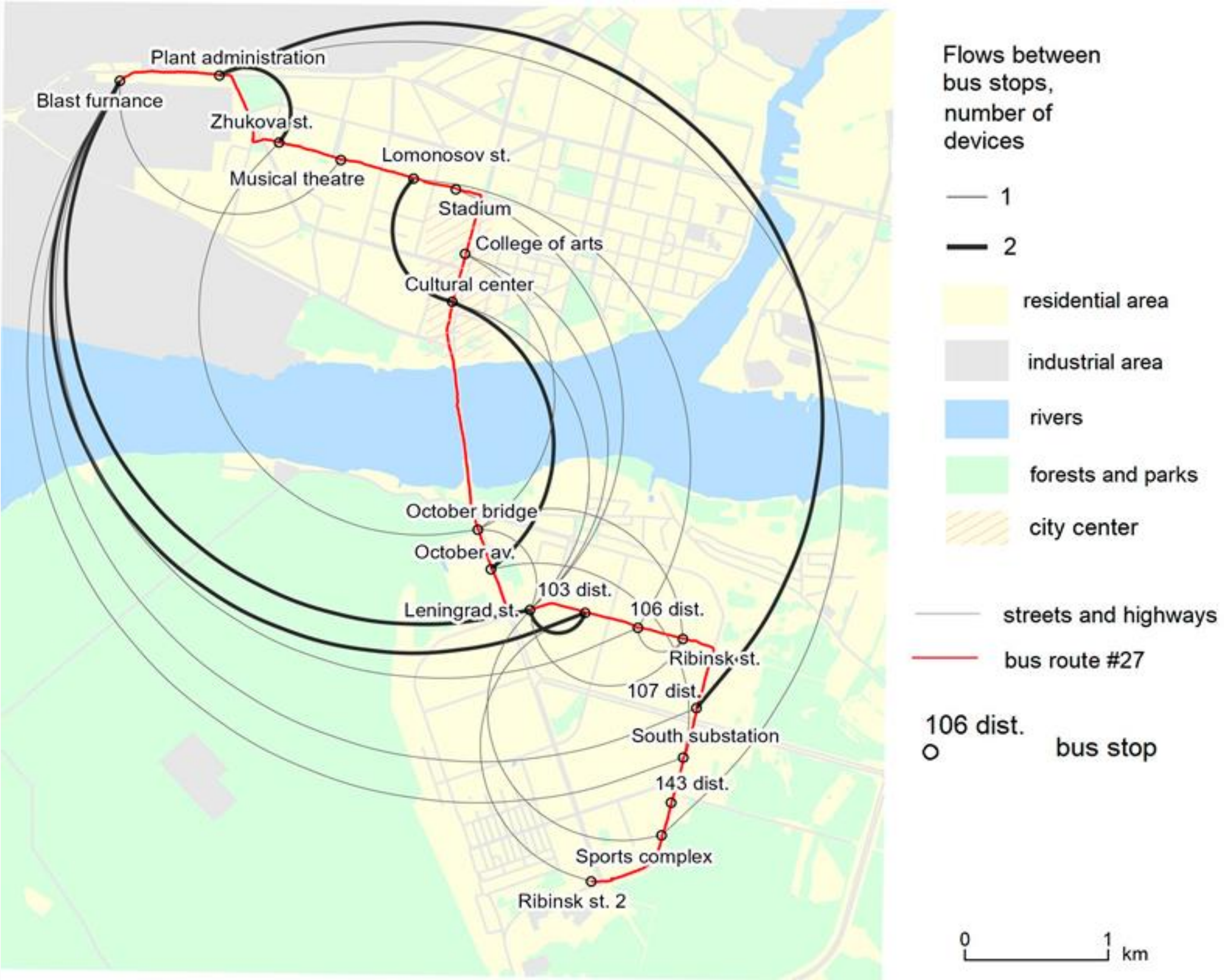
Map of passenger flows

We analyzed **bus 27** in Cherepovets.

The main flows are:

- the entrances of the steel mill – living areas across the river;
- city center – living areas across the river.

> “Blue collars” from the steel mill & “White collars” from the city center => **high income.**
>
> Living areas across the river have better air quality => **expensive housing.**



Third case conclusions

- **It is possible** to solve the problem of MAC address randomization in public transport observation.
- The key feature of our approach is creating a **very detailed** record log with a high frequency of call signs recording.
- Such a log can be created using **multiple laptops with external BL adapters**.

The map based on the collected data **correctly** represents the actual movement of steel mill workers and clerks in Cherepovets city.

Advantages

Much cheaper than mobile operator data.

Suitable for **villages, small towns, urban areas**, and **public spaces**.

High location accuracy (up to 10 m) compared to mobile operator data (from 100 m).

Flaws

Large-area monitoring requires **a lot of people**.

For long-term monitoring, it is necessary to either:

- Regularly change observers
- Somehow hide the devices

Mac-address randomization is the **main problem** for all cases **except** public transport.

Perspectives

The number of “smart” electronic devices **will increase** in the near future, and their analysis will provide more interesting data.

This data can be used in **urban planning** and in the development of **public transport networks**.

Thank you for your attention!

Konnov Andrey
konnovandrey55@gmail.com