Mobilized Construction

Project Presentation
Niels & Troels

Problem

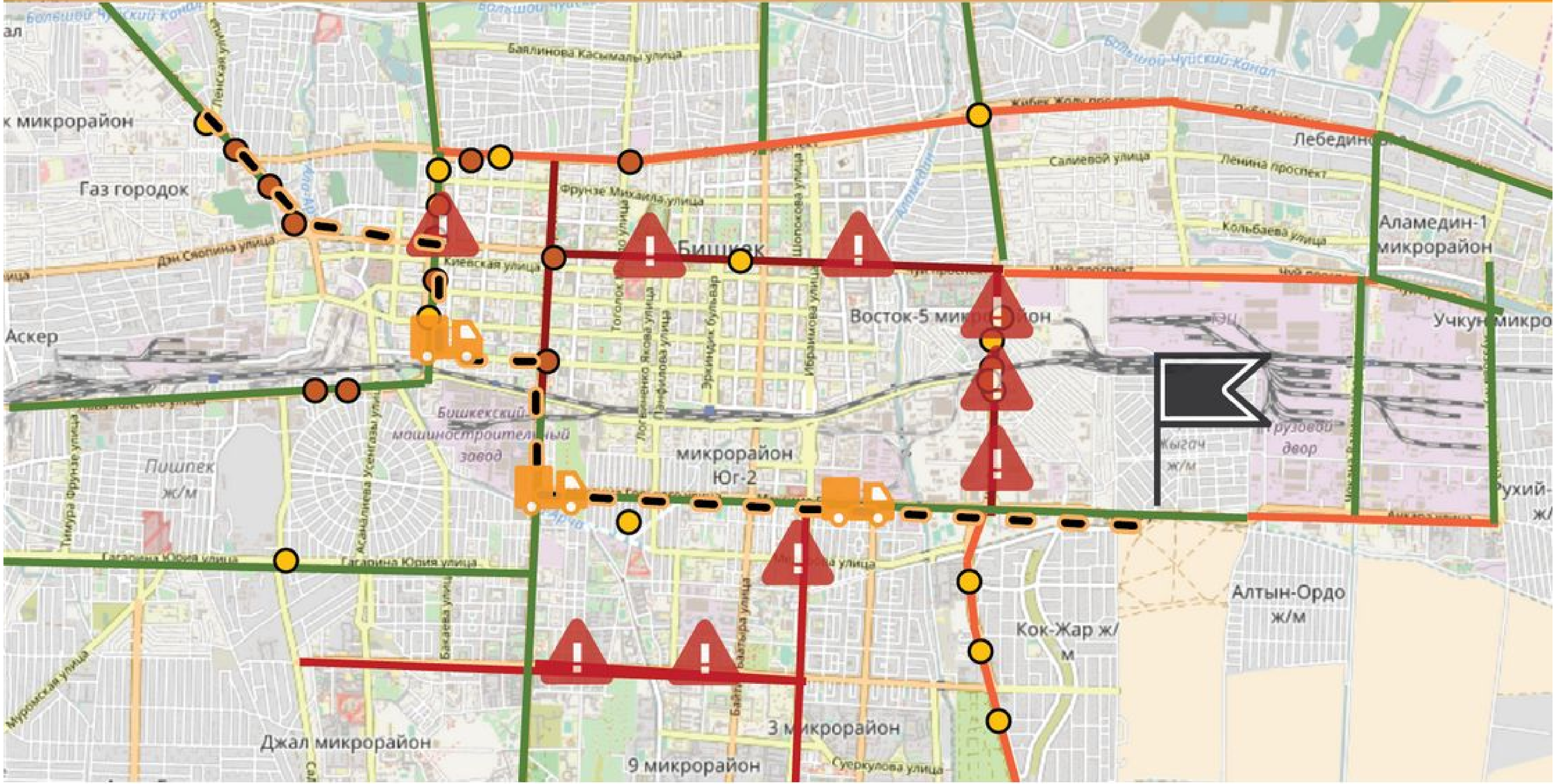
Recent research shows that it is possible to make sufficiently accurate **road roughness** measurements using **accelerometers mounted in cars**, as opposed to using **large, expensive laser equipment**.

The startup **Mobilized Construction** have been using **smartphones** with built-in accelerometers as data collecting devices for this, but it is **not scalable or stable enough** for their ambitions and they are looking at the possibility of using a **dedicated device** instead.

This device must be **small, cheap, robust and fairly autonomous**.

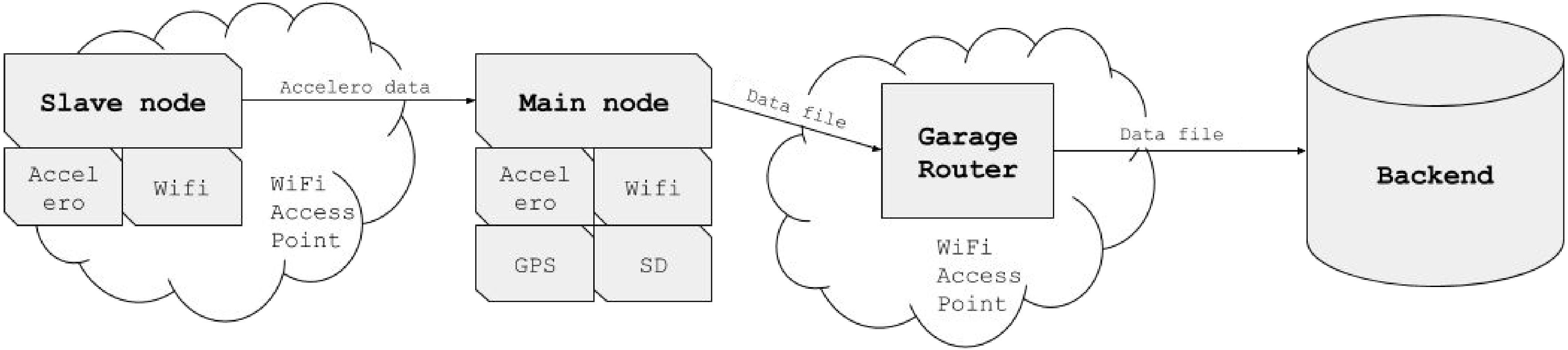
Mobilized Construction

Home



System Design

System architecture



Preliminary Results

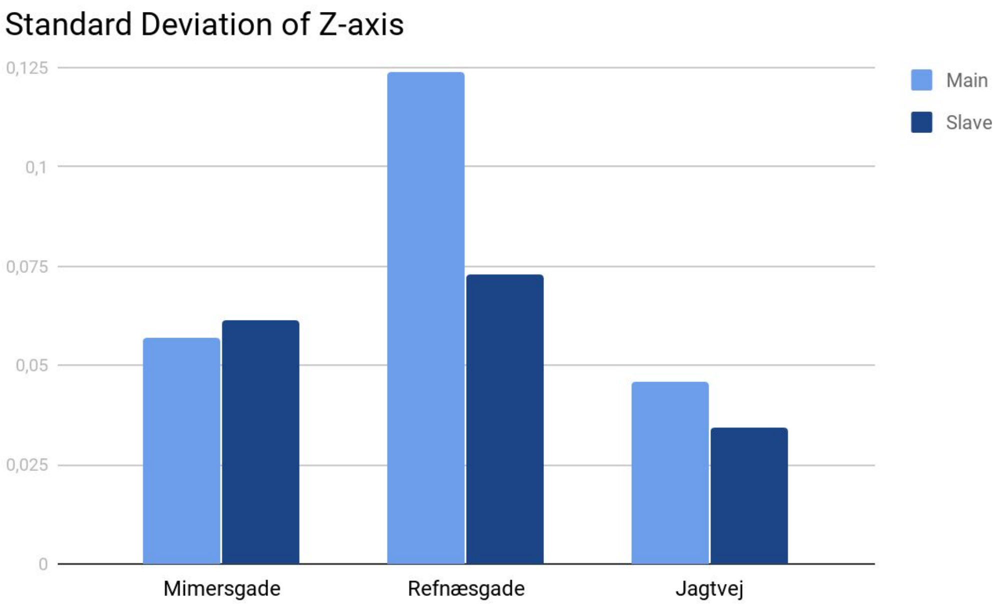
Preliminary Results (I)

From a **single car ride** around Copenhagen.

Used **GPS-coordinates** to determine road.

Standard deviation for **each road** calculated from the **accelerometers z-axis**.

Street	length [m]	avg. speed [km/h]
Mimersgade	383.9	27.5
Refnæsgade	100.3	10.7
Jagtvej	927.1	27.4



Mimersgade

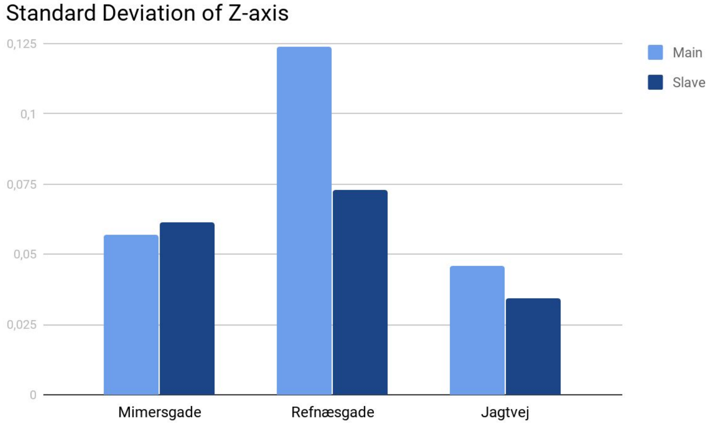
Refnæsgade

Jagtvej

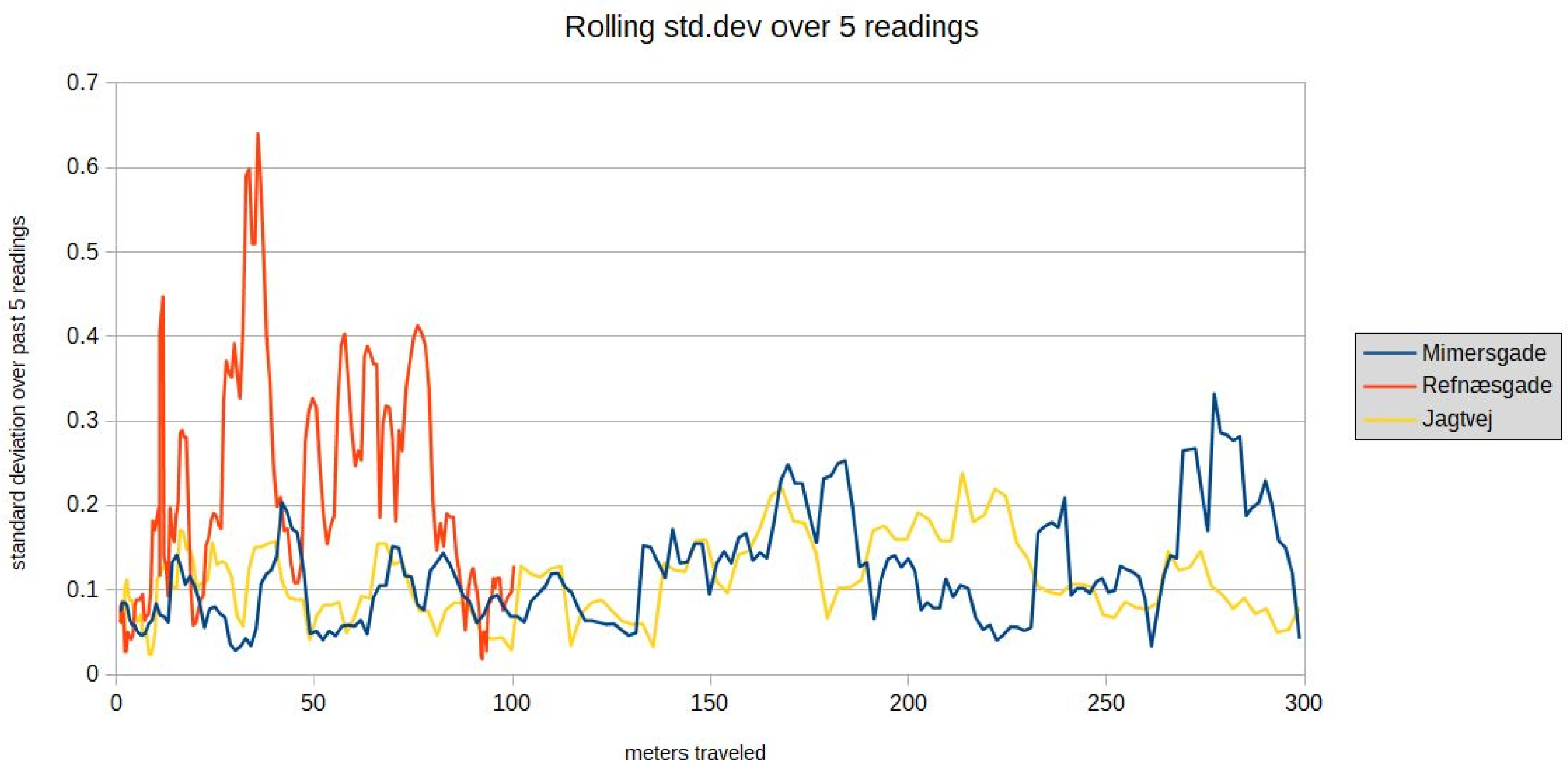
Mimersgade has a four gentle speed-bumps

Refnæsgade is a brick road

Jagtvej is a fairly flat road



Rolling standard deviation



Preliminary Results (II)

Street	length [m]	avg. speed [km/h]
Mimersgade	383.9	27.5
Refnæsgade	100.3	10.7
Jagtvej	927.1	27.4

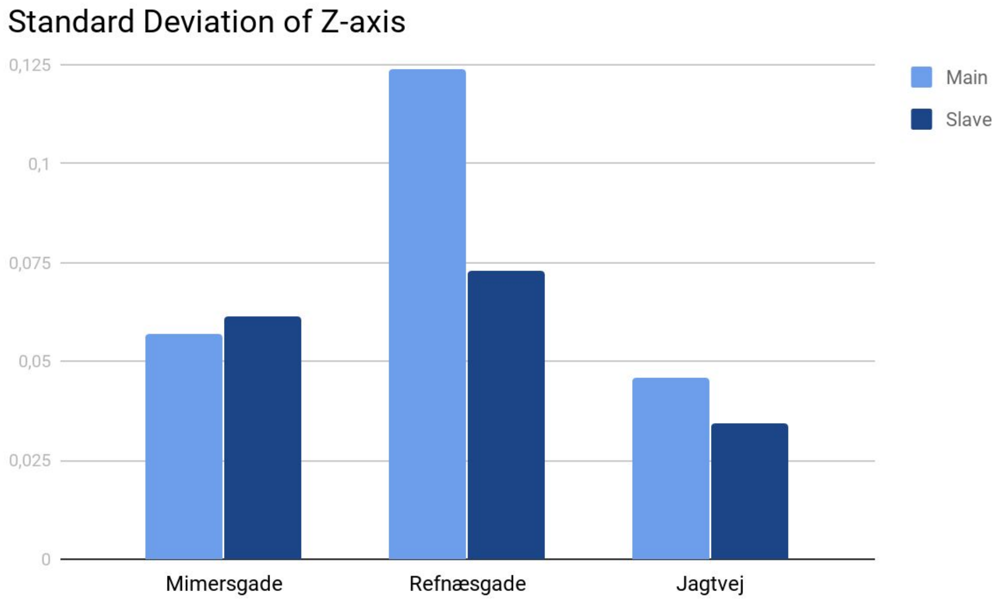
Refnæsgade stands out from all the roads we sampled.

It's the only **brick road.**

It's also the **slowest average speed.**

"*The relationship between* ***the IRI and the speed*** *is not a monotonic increase or decrease, but it is* ***very complex***"
(Du et al., 2014)

Further experiments are needed!



Planned experiments

- Pick out a set of **representative roads**
- Sample each road **several times**
  - Calculate **collective standard deviation** of the set of standard deviations for each road
- Sample the same road at **different speeds**
  - Compare the standard deviations of each speed

Why WiFi?

Why WiFi?

Pros:

1. **Widely used** technology, possible to piggyback on existing networks
2. Existence of **cheap chips** with good support (e.g. ESP8266).
3. **Ease of deployment**. Less setup necessary.

Cons:

1. Relatively **high power consumption** (compared to ex. Bluetooth LE).
2. **“Golden Hammer”**. We know WiFi-networks and TCP/UDP, but there might be better alternatives.
3. **Time consuming**. It takes time to connect to both at network itself and to make a TCP-connection.

Why WiFi?

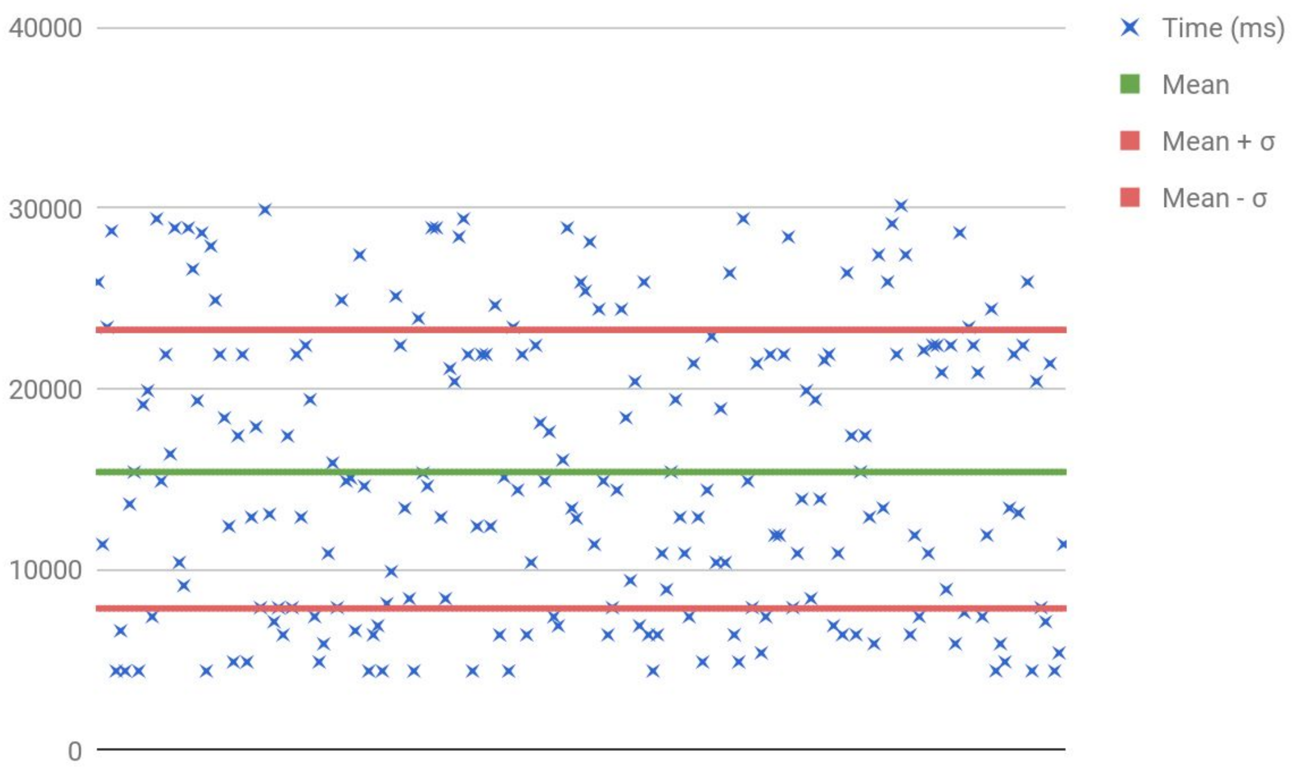
- Why WiFi for the connection to the backend?
  - Is only used once or twice per day, after normal use, so the **high power or time consumption is not so big an issue**.
  - WiFi has a **fairly large range**, allowing **ease of AP setup in garage** or similar.
  - WiFi is so popular, that **the garage might already have a network** we can use.

- Why WiFi for the connection to the slave node.
  - Is used almost constantly, probably **quite power consuming**, but if we assume that **we can source power from the car** this is no longer a problem.
  - Using **UDP-packets** eliminates the time consumption of TCP-connections, and **it is now sufficiently fast**.
  - Since WiFi is already a good choice for the connection to the backend, **we keep the complexity down** by not introducing new technologies/components/chips
  - The WiFi-modules internal buffer gives us a **bit of asynchronicity**.

WiFi Connection to Slave - Test (I)

Success	215	72%
Fail	85	28%
Total	300	

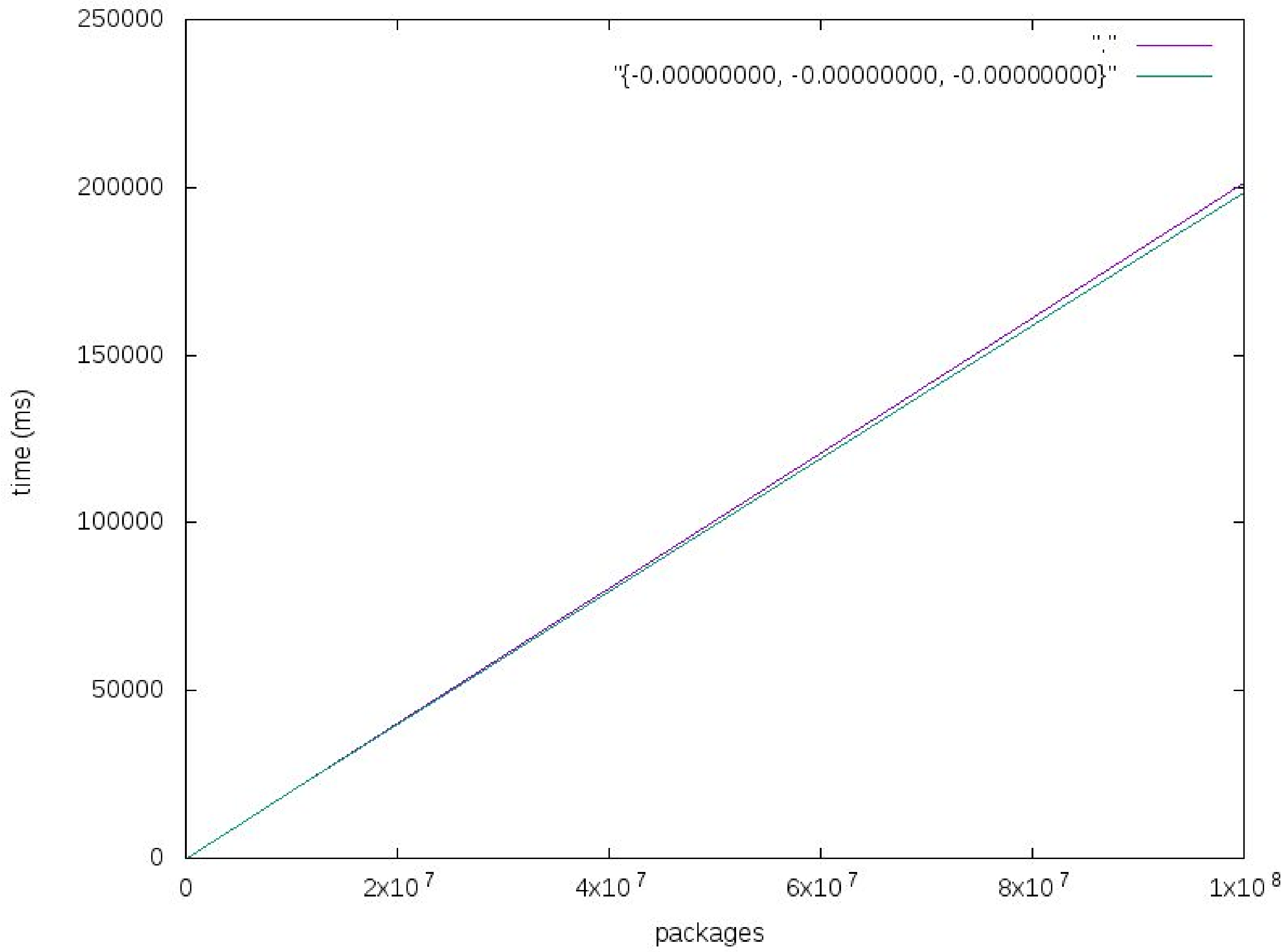
WiFi Connection to Slave - Test (II)



Benchmark UDP-test (I)

Packages	**“.”**	**“{-0.00000000, -0.00000000, -0.00000000}”**
100	0 ms	0 ms
1,000	1 ms	1 ms
10,000	20 ms	19 ms
100,000	183 ms	179 ms
1,000,000	1,895 ms	1,842 ms
10,000,000	20,335 ms	20,261 ms
100,000,000	201,517 ms	198,531 ms
~ 2 µs/pkg	**0.00201517 ms/pkg**	**0.00198531 ms/pkg**

Benchmark UDP-test (II)



Ending Remarks

Security and Privacy Concerns

- Sensitive data:
    - GPS data tracking the movements of the device and the driver.

- Risks:
    - **Sending over HTTP**
        - Adversary could sniff the data packets and retrieve information about the travels of the device(s)
    - **Injection in UDP-stream**
        - The SSID and password to the slave nodes AP is static and could be leaked. Adversary could then send packets to the slave node to change the registered IP and send packets to the main node containing false or corrupted data.
    - **WiFi jamming**
        - The system could be made unavailable by a simple WiFi-jammer in the garage.

Further work

- Test and insure **stability and robustness** during long term operation.
  (*How does the system handle sudden power failure or hardware crash?*)

- Add possibility for **three slave** nodes.
  (*How do we determine which slave is in which corner of the car? Should the main node control the AP?*)

- Explore the possibility of a **battery driven** version.
  (*How much power do we use, and how can we reduce it?*)

Conclusions

In Road Roughness measurements:

- A cheap IoT-device can replace a mobile phone
- Sensor data reflects the surrounding environment.
    - Further experiments are planned to confirm the validity of the results.
- WiFi is a suitable networking technology for this use case.