

Návrh zabezpečeného systému prenosu dát v NB-IoT prostredí

Diplomová práca

Autor práce: Bc. DANIEL KLUKA

Vedúci práce: Ing. et Ing. PETR MUSIL

Oponent: Ing. RADEK MOŽNÝ, Ph.D.

Brno, 9. 6. 2025

- Člen tímu Meteo Telcorain
- Zaoberáme sa oportunistickým snímaním mikrovlnnými spojmi - **nikto to nerobí**
- Tradičné profesionálne meteostanice môžu stáť **2 000 000 Kč**, servisovanie ďalších **100 000 Kč**
- Presné meteorologické dátá sú dôležité - monitorovanie a predpovedanie počasia
- Rozmiestnenie meteostaníc po Brne
- Daniel Kluka Weather Station - DKWS
- <https://meteo.telcorain.cz/>



Ciele diplomovej práce

- Znížiť cenu profesionálnych meteostaníc a zachovať ich vysoké štandardy
- Kyberneticky bezpečné zariadenie pre NB-IoT s využitím šifrovania TLS
- Komplexný HW a SW meteostanice pre meranie živ. prostredia a odosielanie dát
- Systém pre zber, správu a vizualizáciu dát bez kompromitácie bezpečnosti
- Optimalizovať spotrebu energie a dát meteostanice
- Overiť odolnosť systému voči útokom prostredníctvom bezpečnostnej analýzy

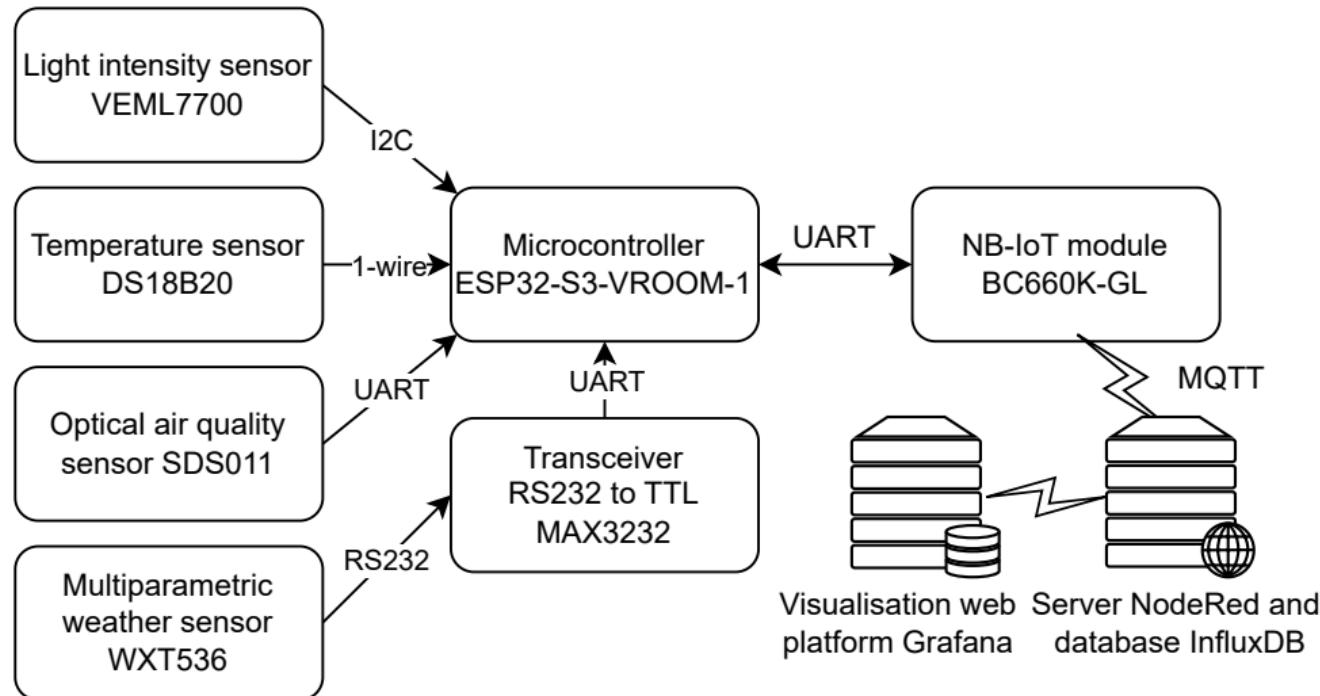


Meranie životného prostredia

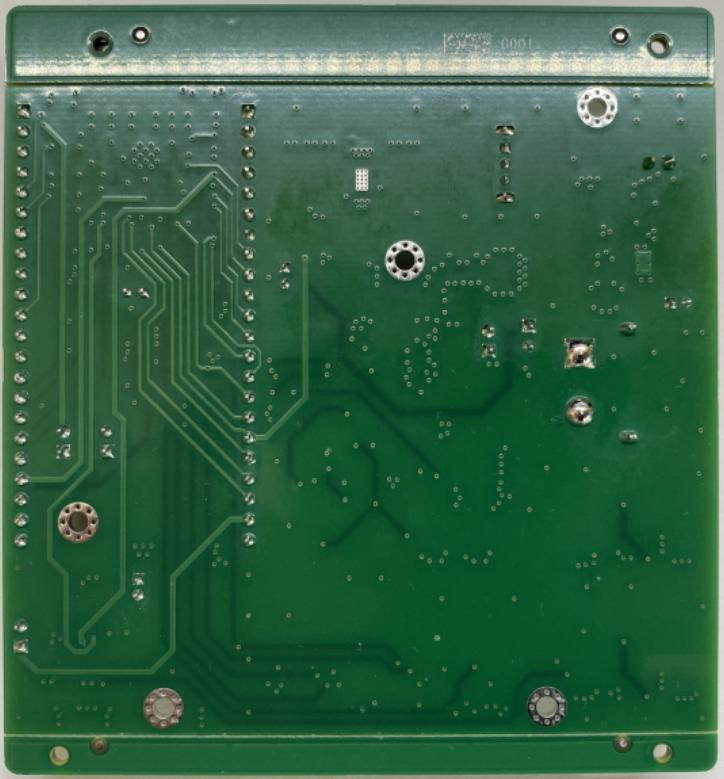
- Teplota - DS18B20
- Slnečný svit - VEML7700
- **Kvalita ovzdušia** - SDS011
- Teplota
Vlhkosť
Tlak
Veternosť (ultrazvukový senzor)
Dažďové zrážky (akustický senzor)
- Vaisala WXT536 - **cena 67 000 Kč**



Vytvorený zabezpečený systém

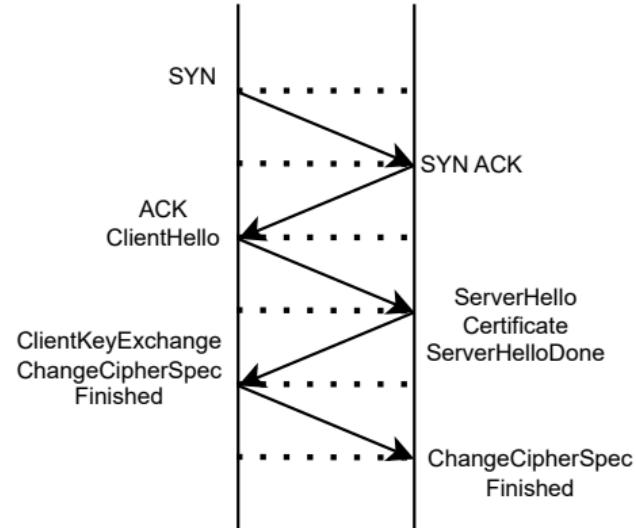


NB-IoT zariadenie - DKWS DPS (89x81 mm)



Zabezpečenie komunikačného systému

- Lokálne spracovanie dát pred odoslaním
- Prenos dát zašifrovaný prostredníctvom TLS - integrita a dôvernosť dát
- BC660K-GL podporuje TLS 1.2 bez session resumption
- MQTT broker Mosquitto autentifikuje používateľov a zariadenia
- Vytvorený systém časového razítkovania správ a logovanie brokera
- Správa so 6 meraniami - meteorologické veličiny a diagnostické dáta
- SW odpojenie senzorov v prípade manipulácie útočníkom

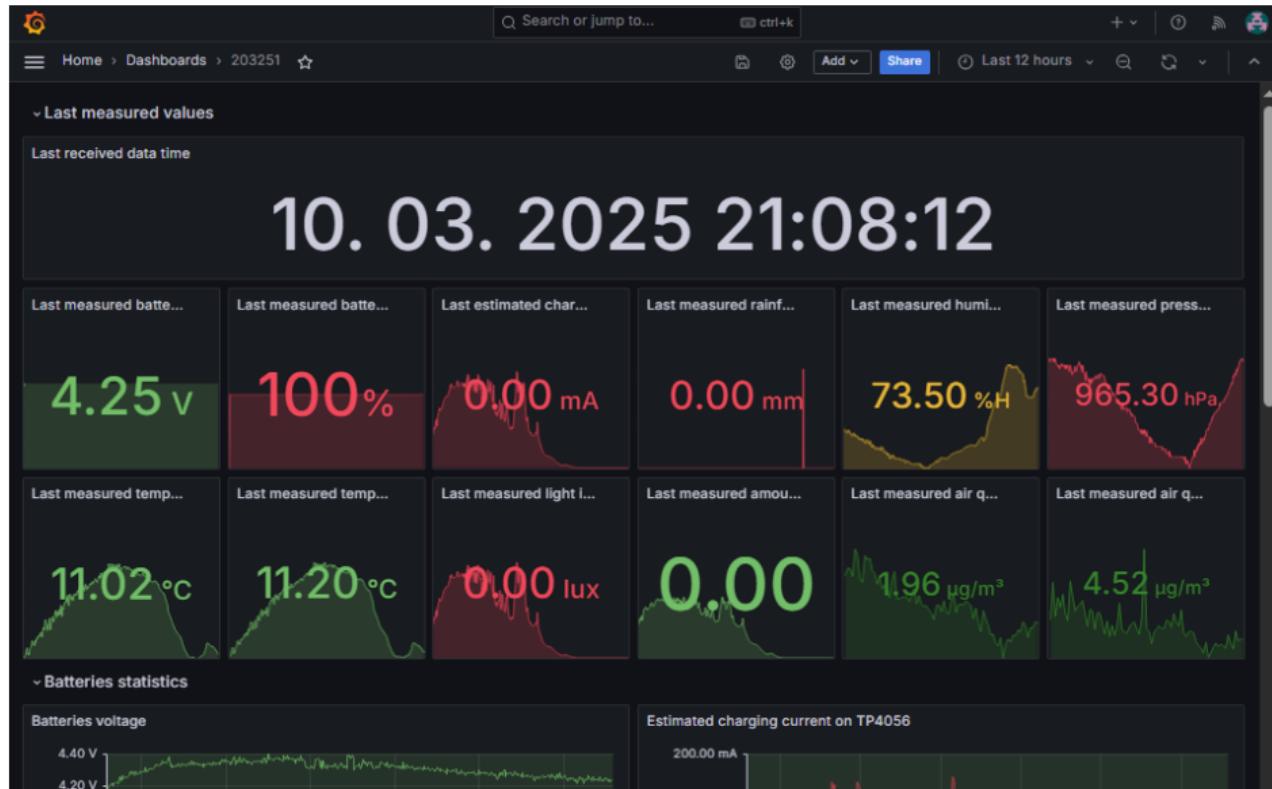


MQTT broker Mosquitto

- Broker vyžaduje prihlásenie pomocou mena a hesla; anonymný prístup je zakázaný (allow_anonymous false).
- MQTT komunikácia prebieha cez port 8883 s použitím protokolu TLS 1.2 a vlastnoručne generovaných certifikátov (CA, server, klient).
- Broker overuje klientské certifikáty a loguje všetku prevádzku, čím je možné späťte overiť, kto a kedy bol pripojený.

```
May 23 20:28:47 vmdev mosquitto[19547]: 1748024927: New connection from [REDACTED] on port 8883.  
May 23 20:28:54 vmdev mosquitto[19547]: 1748024934: New client connected from [REDACTED] as DKWS ([REDACTED] u'danielkluka').  
May 23 20:28:57 vmdev mosquitto[19547]: 1748024937: Client DKWS closed its connection.  
May 23 20:29:13 vmdev mosquitto[19547]: 1748024953: New connection from [REDACTED] on port 8883.  
May 23 20:29:20 vmdev mosquitto[19547]: 1748024960: New client connected from [REDACTED] as DKWS ([REDACTED] u'danielkluka').  
May 23 20:29:23 vmdev mosquitto[19547]: 1748024963: Client DKWS closed its connection.  
May 23 20:29:39 vmdev mosquitto[19547]: 1748024979: New connection from [REDACTED] on port 8883.  
May 23 20:29:46 vmdev mosquitto[19547]: 1748024986: New client connected from [REDACTED] as DKWS ([REDACTED] u'danielkluka').  
May 23 20:29:50 vmdev mosquitto[19547]: 1748024990: Client DKWS closed its connection.  
May 23 20:30:11 vmdev mosquitto[19547]: 1748025011: New connection from [REDACTED] on port 8883.  
May 23 20:30:18 vmdev mosquitto[19547]: 1748025018: New client connected from [REDACTED] as DKWS ([REDACTED] u'danielkluka').  
May 23 20:30:21 vmdev mosquitto[19547]: 1748025021: Client DKWS closed its connection.  
May 23 20:30:42 vmdev mosquitto[19547]: 1748025042: New connection from [REDACTED] on port 8883.  
May 23 20:30:49 vmdev mosquitto[19547]: 1748025049: New client connected from [REDACTED] as DKWS ([REDACTED] u'danielkluka').  
May 23 20:30:52 vmdev mosquitto[19547]: 1748025052: Client DKWS closed its connection.
```

Vizualizácia dát meteostanice



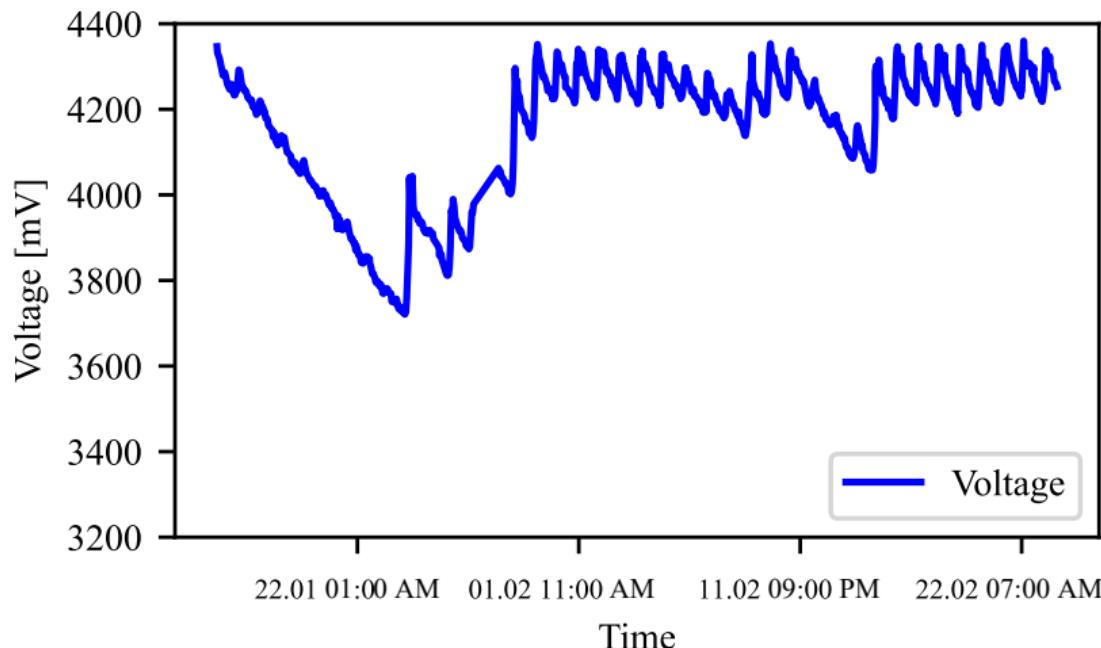
Vyhodnotenie mesačnej spotreby siete

Fáza	Velkosť	Zdroj
Random Access + RRC Setup	200–300 B	3GPP TS 36.331, TS 36.321
NAS Attach (Request/Accept)	300–400 B	3GPP TS 24.301, TS 23.401
PDCP + RLC + MAC hlavičky	50–150 B	3GPP TS 36.323, TS 36.322, TS 36.321
IP + TCP hlavičky	40–60 B	RFC 791, RFC 793
TCP handshake + teardown	200–300 B	GSM IoT Guide
TLS handshake (plný)	3000–6000 B	RFC 5246 (TLS 1.2)
MQTT CONNECT + CONNACK	30–100 B	MQTT 3.1.1 (OASIS)
MQTT PUBLISH + PUBACK	202–232 B	MQTT 3.1.1, RFC 793
MQTT DISCONNECT (vol.)	10–20 B	MQTT 3.1.1
RRC Release (vol.)	~500 B	3GPP TS 36.331
MQTT správa (payload)	182 B + TLS rézia	–
Celkovo (typicky, nezašifrované)	1000–1500 B	–
Celkovo (so šifrovaním)	1300–1800 B + TLS handshake	–

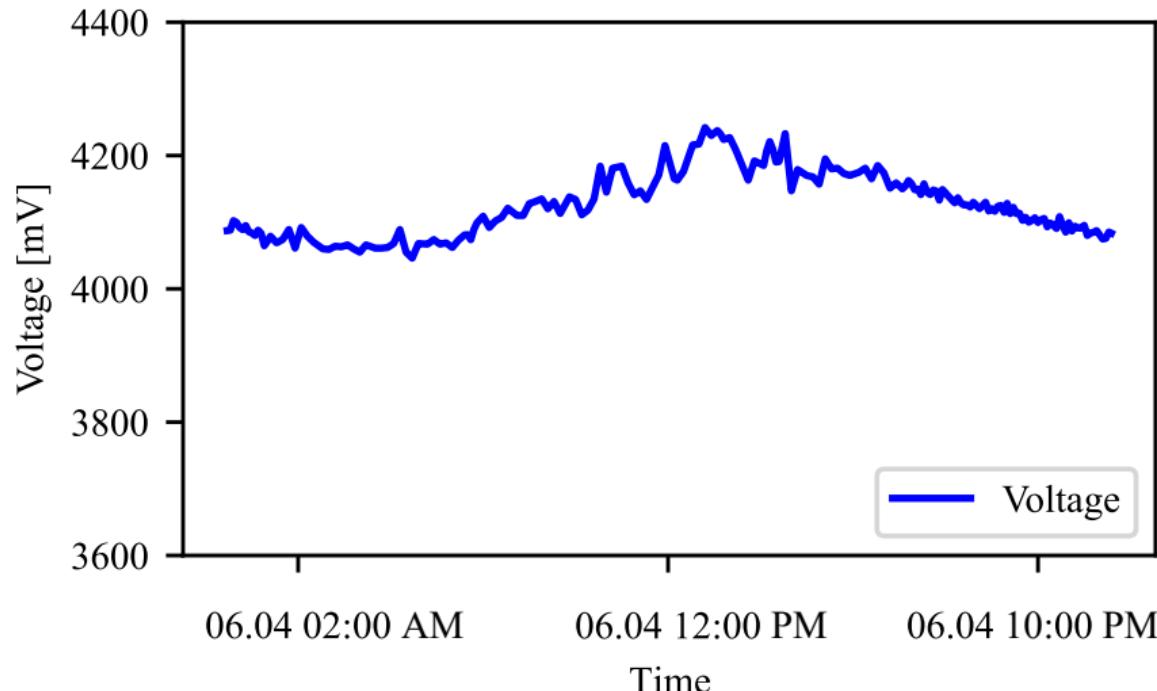
- Prototyp odosielal každú hodinu – mesačne 720 prenosov:
 - **0.47 MB** (optimálne podmienky) bez TLS, **3.63 MB** s TLS
 - **0.81 MB** (realistické podmienky) bez TLS, **3.97 MB** s TLS
 - **1.15 MB** (zlé podmienky) bez TLS, **4.31 MB** s TLS
- DKWS každých 6 minút: **8.12 MB** → **3.31 MB** bez TLS, **34.95 MB** s TLS

Efektivita nabíjania

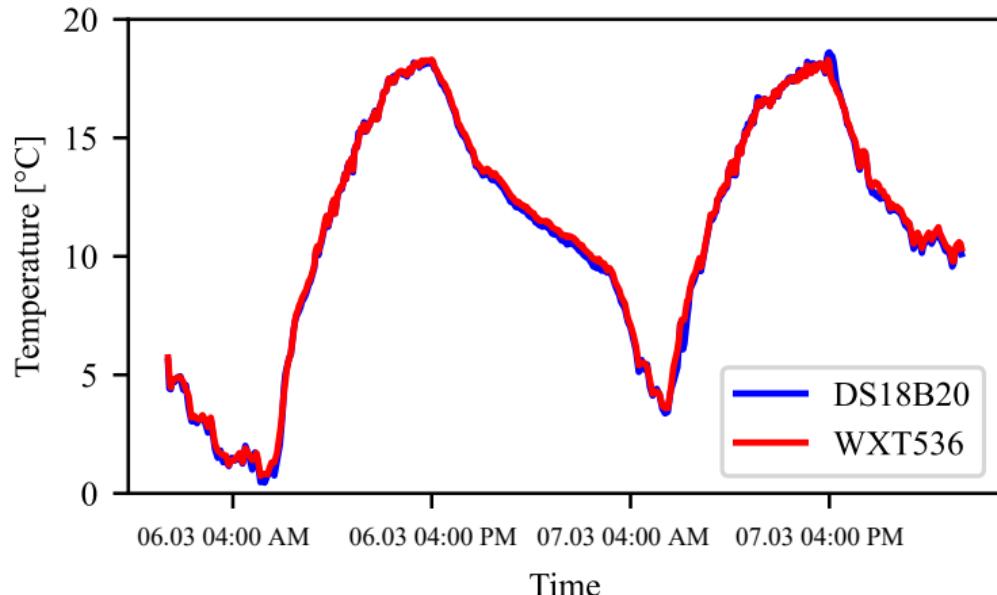
- Efektivita nabíjania počas zamračených (15.1.-23.1. 2025) a slnečných (23.1.-23.2. 2025) dní



- Efektivita nabíjania počas dňa 6.4.2025 v časoch od 0:00 do 23:59



- Multiparametrický senzor počasia Vaisala WXT536 (teplota, tlak, vlhkosť, zrážky, rýchlosť a smer vetra)
- Minimálne odchýlky v porovnaní s DKWS



- Realizovaný kompletný systém pre bezpečný prenos dát cez NB-IoT
- Vytvorený vlastný HW so senzormi a optimalizáciou spotreby energie
- SW riešenie s dôrazom na bezpečnosť - TLS, autentizácia, zabezpečený broker
- Integrácia dátového toku skrz platformy Node-RED, InfluxDB a Grafana
- Analyzovaná komunikačná a energetická efektivita NB-IoT prenosov
- Vykonaná bezpečnostná analýza celého systému vrátane možných zraniteľností
- **Cena meteostanice 7 500 Kč**



1. Akú energetickú záťaž predstavuje šifrovacia vrstva pre prezentované zariadenie?

- Šifrovacia vrstva TLS 1.2 vytvára výrazný dátový a energetický overhead, najmä pri častom nadväzovaní nových spojení.
- Modul BC660K-GL **nepodporuje TLS session resumption**, preto sa pri každom prenose vykonáva plný handshake (4,5 kB).
- To vedie pri odosielaní každých 6 minút k mesačnej záťaži až **34,95 MB**; v optimalizovanom prípade s trvalým spojením by spotreba výrazne klesla.

2. Ako by použitie protokolov ako CoAP alebo LwM2M ovplyvnilo systém v porovnaní s MQTT?

- CoAP a LwM2M sú efektívnejšie z pohľadu dát a latencie, pretože bežia nad UDP.
- Na druhej strane majú zložitejšiu implementáciu a horšiu podporu v použitom NB-IoT module (BC660K-GL).
- MQTT bol zvolený pre podporu TLS a kompatibilitu s Node-RED.

Ďakujem za pozornosť!