

# Ochrana proti random subdomain útokům

**pomocí technologie DNSSEC**

Petr Špaček • petr.spacek@nic.cz • 2018-06-12

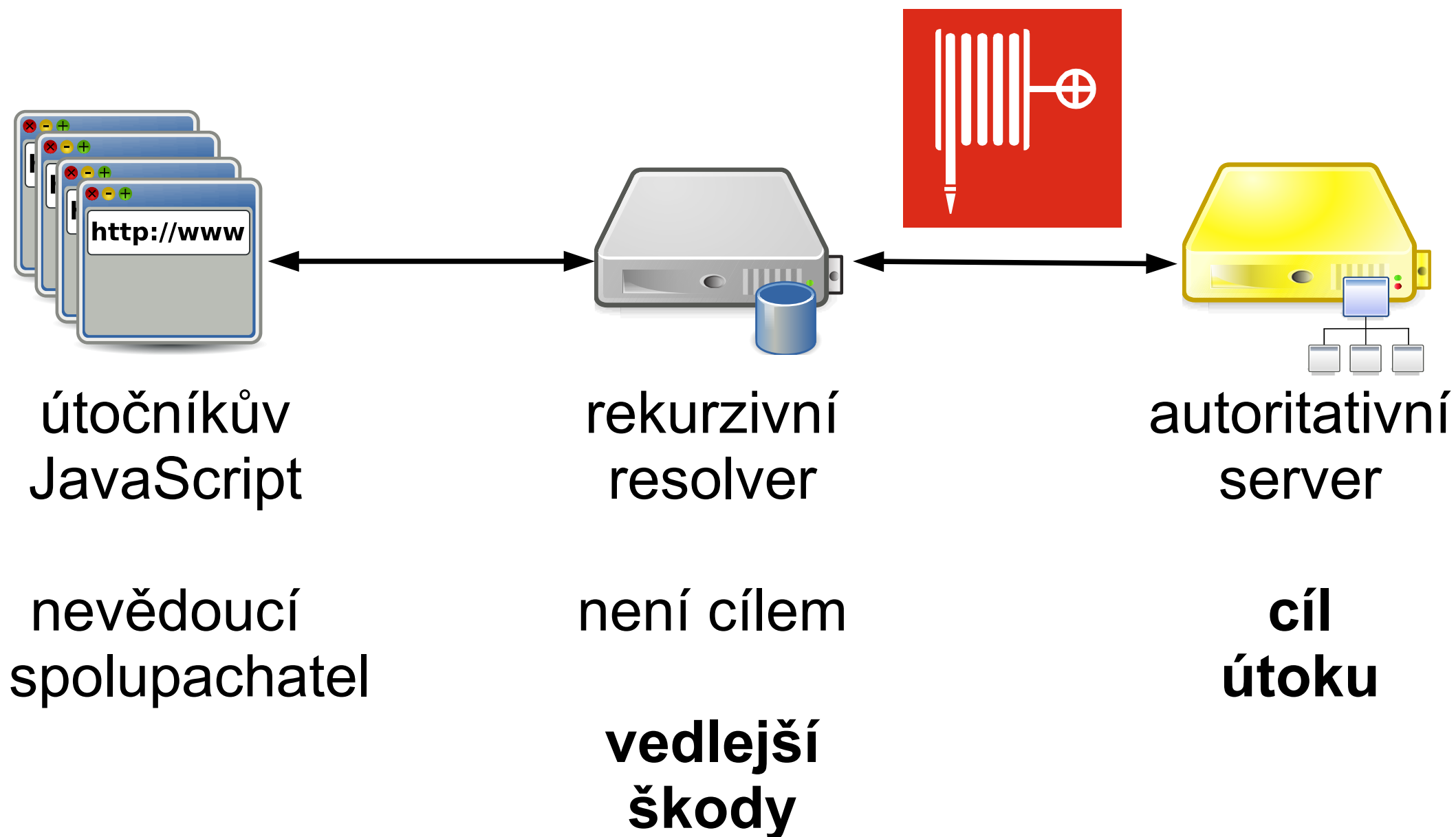


# Obsah

- Random subdomain útok teoreticky
- Agresivní DNSSEC cache
  - princip
  - očekávání
- Normální provoz
- Random subdomain útok prakticky



# Random subdomain útok: princip



# Random subdomain útok: obrana

- Bez DNSSEC
  - komplikovaná heuristika
  - nutno přizpůsobovat útokům
  - i nepodepsané domény
- S DNSSEC
  - deterministické řešení – agresivní cache
  - jen podepsané zóny



# Agresivní cache: princip

```
$ dig +dnssec nonexistent.example.com
```

```
;; AUTHORITY SECTION:  
example.com. NSEC www.example.com.  
NS SOA
```



# Agresivní cache: očekávání

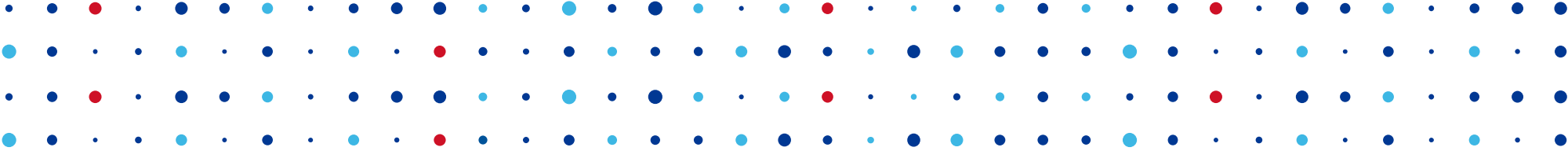
- Použijeme NSEC/NSEC3 záznamy
  - snížení **latence**
  - snížení **spotřeby zdrojů**
  - zlepšení **ochrany soukromí**
  - zlepšení **odolnosti proti útokům**



# Agresivní cache: efektivita

- Způsob dotazování
  - normální provoz
  - random subdomain útok
- Rozložení jmen v DNS zóně
- Wildcardy
- TTL





# Agresivní cache vs. Normální provoz





# Normální provoz: experiment

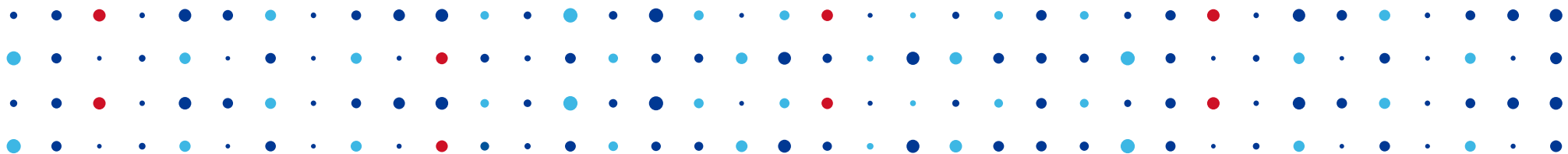
- Přehráváme PCAP na resolver
  - agresivní cache vypnuta / zapnuta
- Zaznamenáváme
  - provoz k autoritám
  - odpovědi resolveru
- Měříme
  - počet paketů k autoritám
  - datový tok k autoritám
  - latenci odpovědí



# Očekávání vs. Normální provoz

- Root zóna
  - omezení nesmyslných dotazů
    - zastaví 50-65 % dotazů na root
  - ☒ **ochrana soukromí**
- Ostatní zóny
  - minimální dopad
  - nedostatek podepsaných zón?





# Agresivní cache VS. Random subdomain útok



# R.S.Ú. provoz: dotazy

- 1000 simulovaných klientů
- Další dotaz po odpovědi na předchozí
- Pseudonáhodná jména (256 bitů)
  - GCZDKQIS7F7TTHXBIBC4HHZDYTFCPH5XLR6P  
GEI3WIESK7BS45WQ.test.knot-resolver.cz. A
  - GCZDKQIS7F7TTHXBIBC4HHZDYTFCPH5XLR6P  
GEI3WIESK7BS45WQ.test.knot-resolver.cz. AAAA
  - OF6OVT2SNIV54B7HI77V5TJ3TFVULN5AMQ2Z6I  
WQX6GBHQ254LNQ.test.knot-resolver.cz. A

# R.S.Ú. provoz: experiment

- Testovací autorita
  - podepsaná pomocí NSEC
  - extrapolace pro NSEC 3: ( $\text{tok} * 1.5$ )
- Přehráváme náhodná jména na Knot Resolver
- Zaznamenáváme **provoz k autoritám**
- Měříme
  - počet paketů k autoritám
  - datový tok k autoritám



# R.S.Ú. provoz: nastavení

- autorita – Knot DNS 2.6.4
  - RSASHA256 2048 b, automatické podepisování
    - **velké odpovědi**
- resolver – Knot Resolver 2.1.1
  - cache 20 GiB

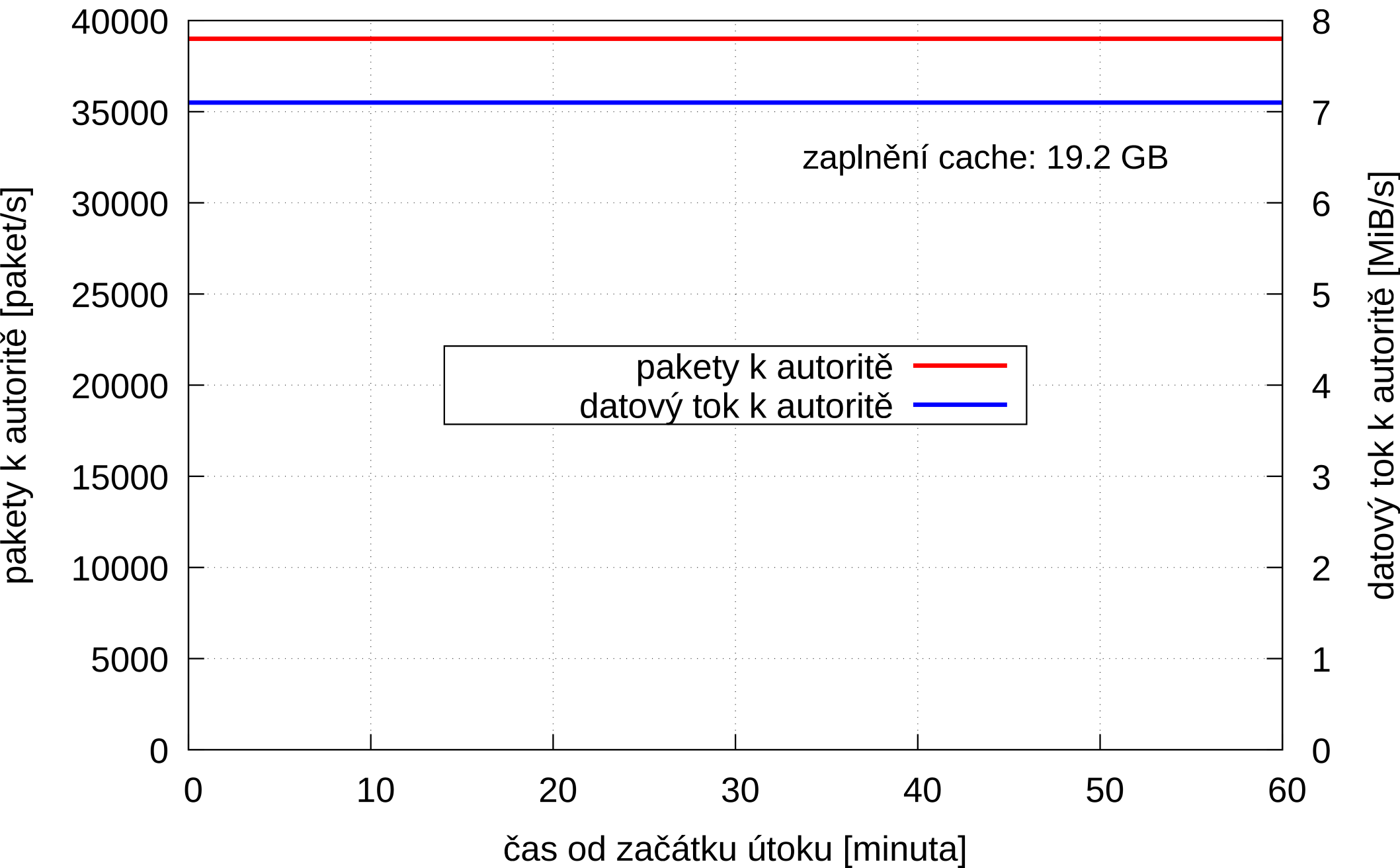


# R.S.Ú. scénáře

- Nepodepsaná zóna – referenční hodnota
- Podepsané zóny
  - SOA minimum, NSEC TTL
    - 3600 s / 60 s
  - rozložení jmen – **skutečné zóny z .cz**
    - malá s wildcardem (50 jmen + 1 wildcard)
    - středně velká (14k jmen)
    - velká (110k jmen)
    - obrovská (1M jmen)

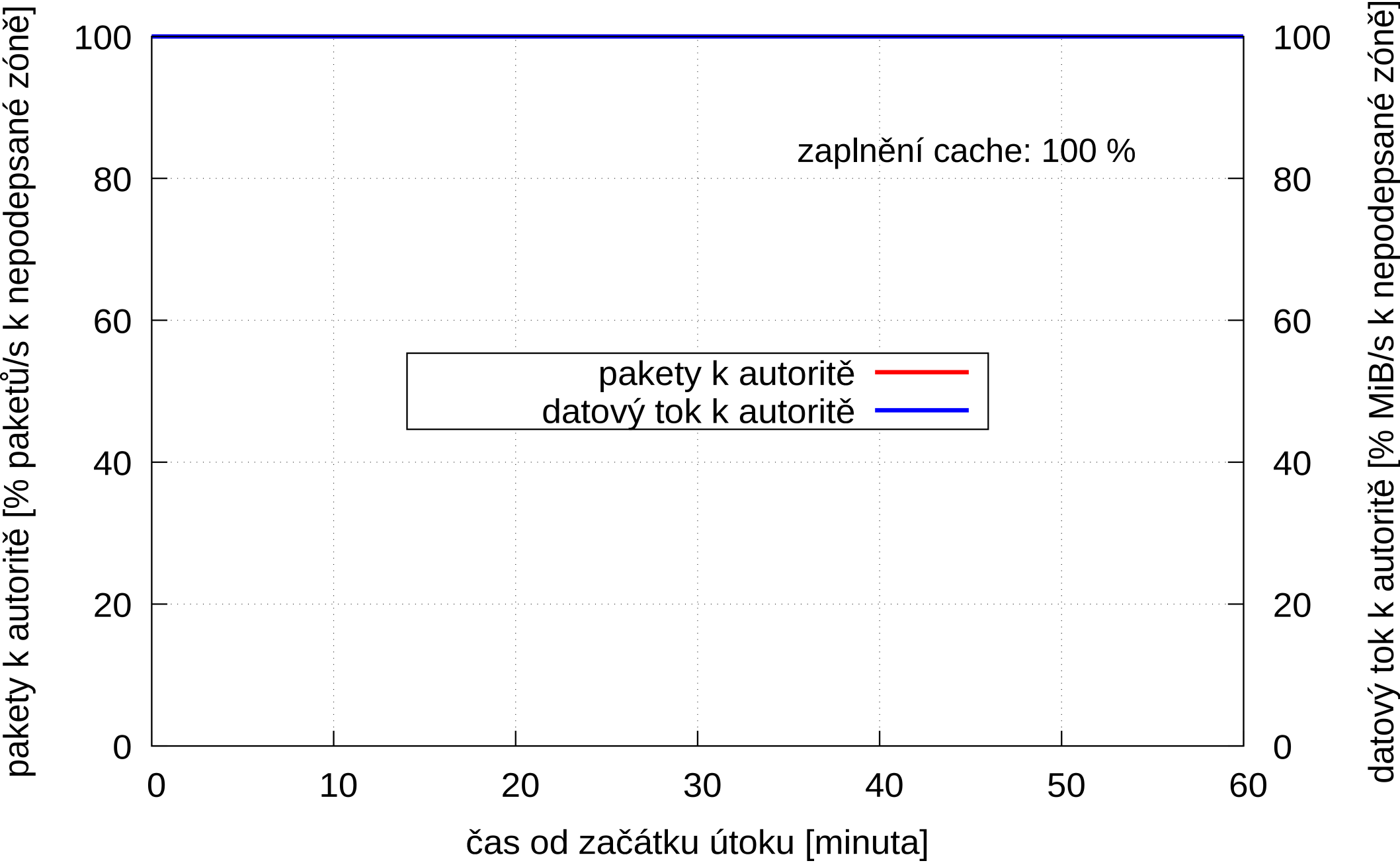


# R.S.Ú.: nepodepsaná zóna (abs.)

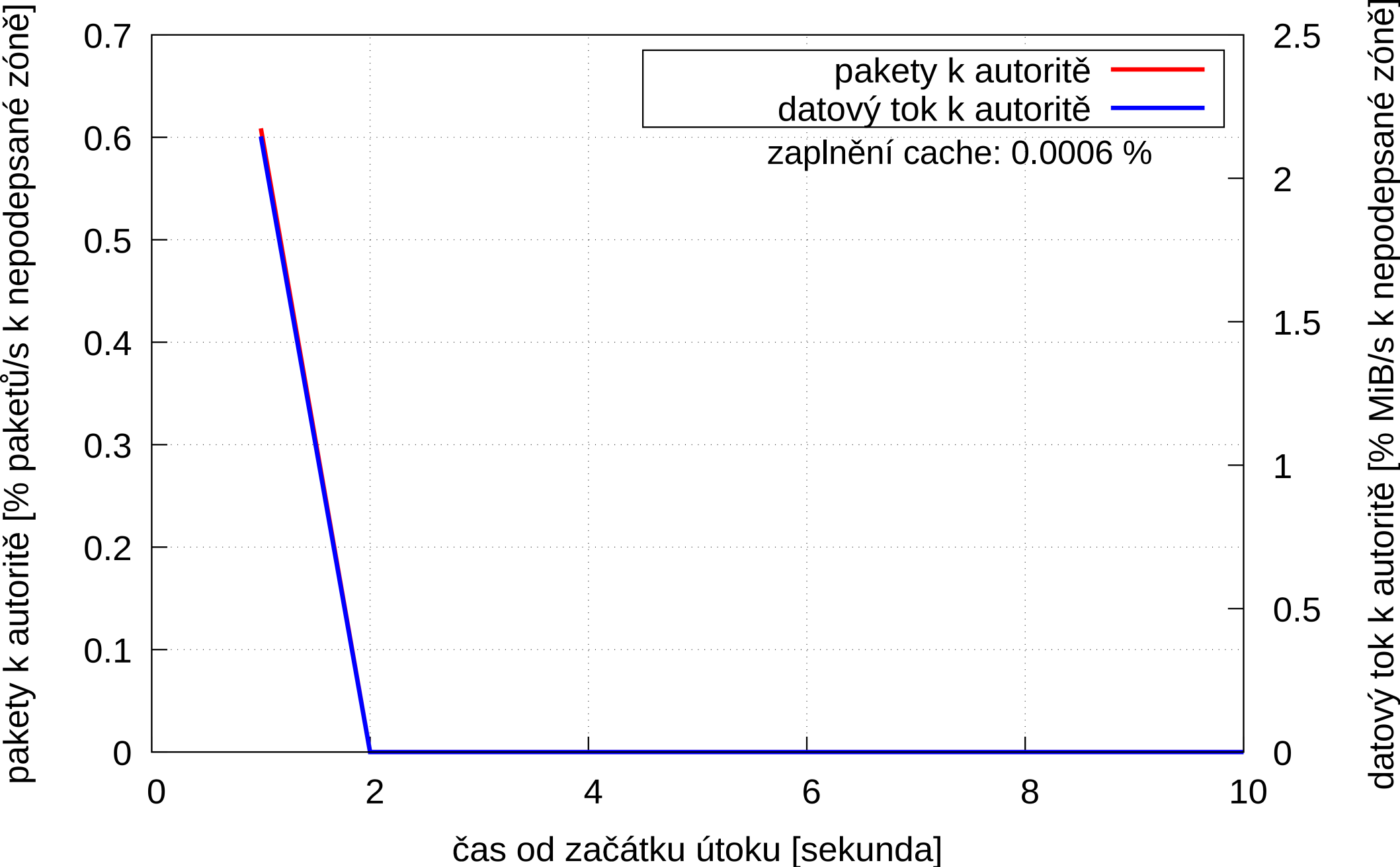




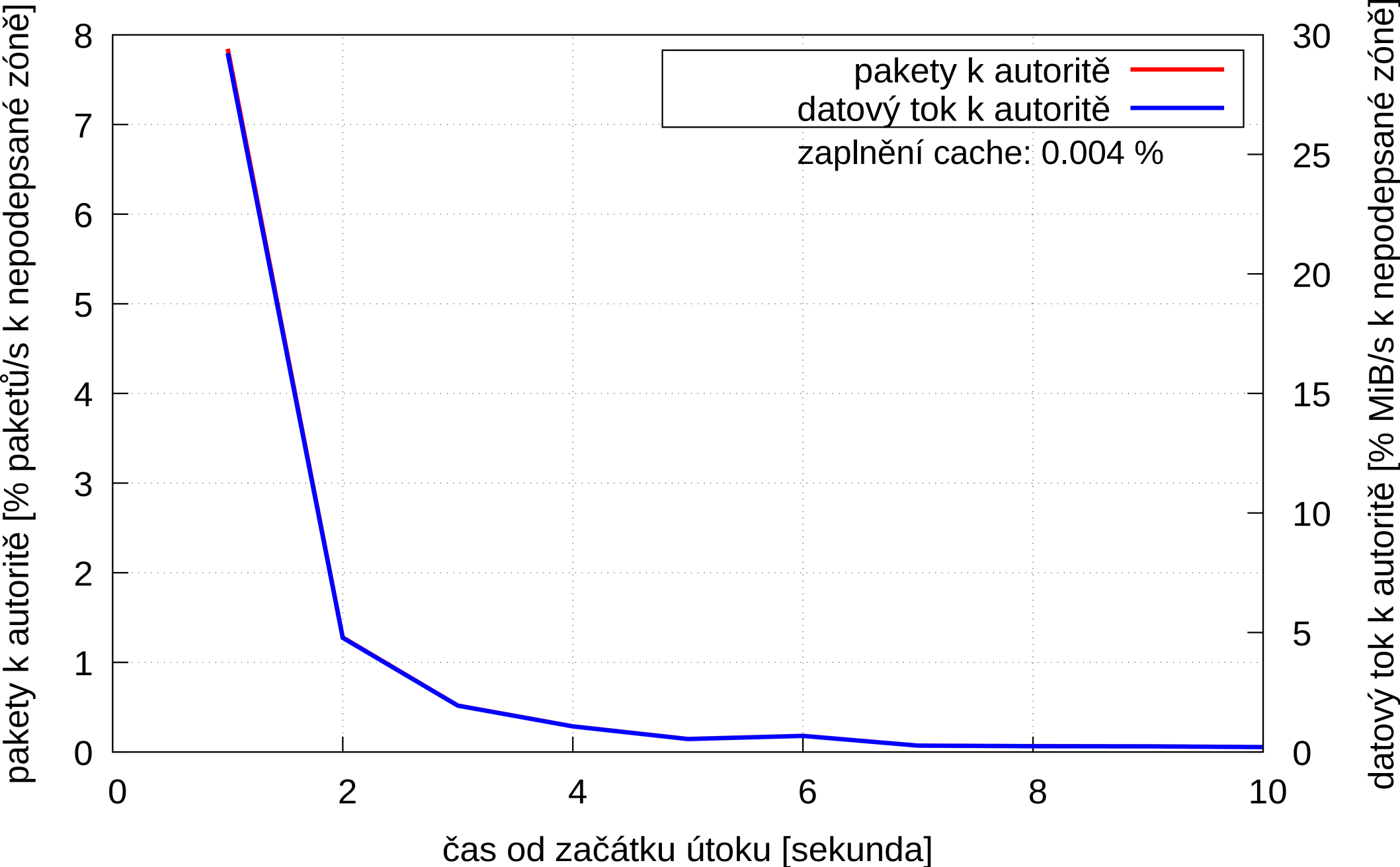
# R.S.Ú.: nepodepsaná zóna (v %)



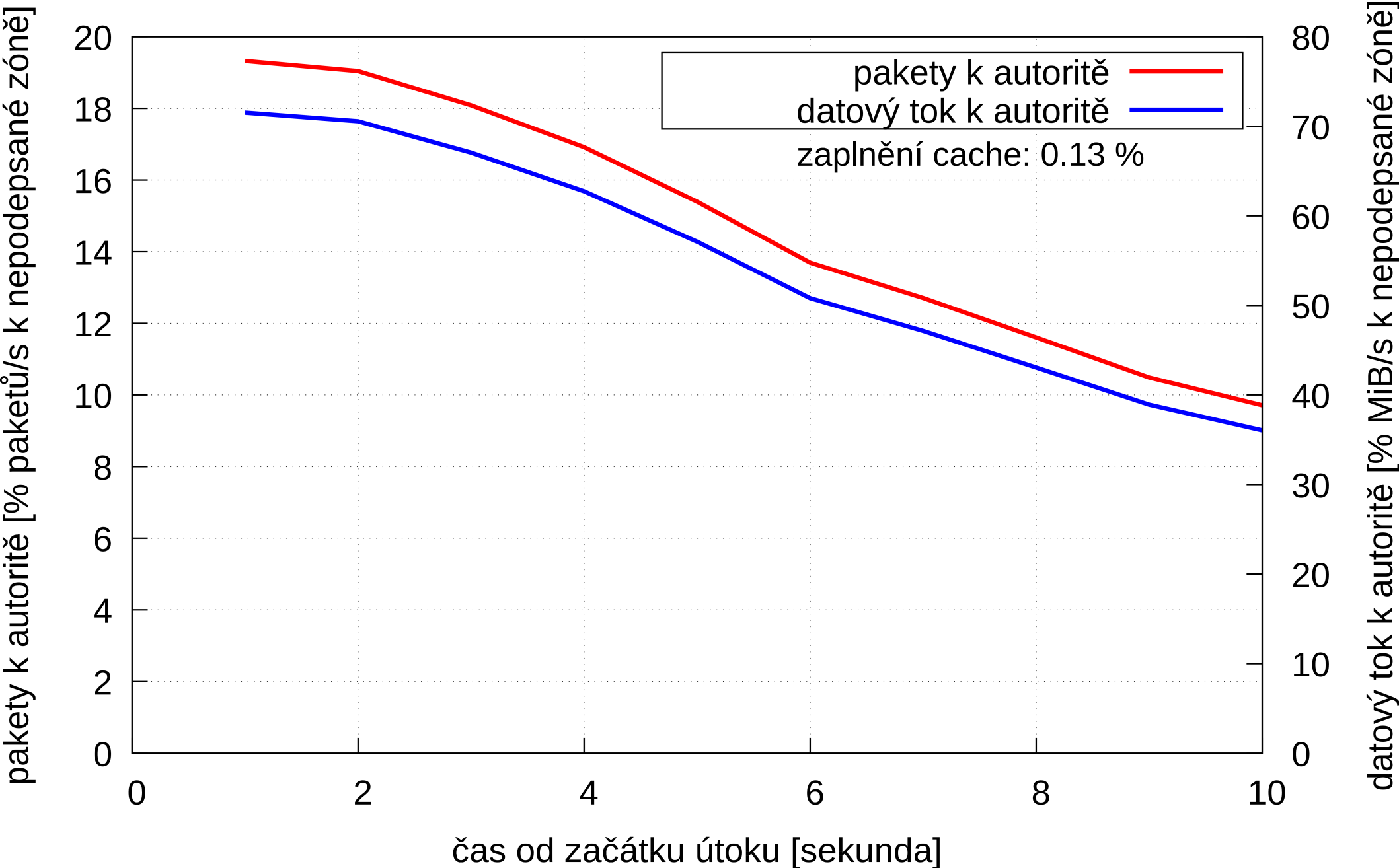
# R.S.Ú.: 50 jmen + wildcard, TTL 60



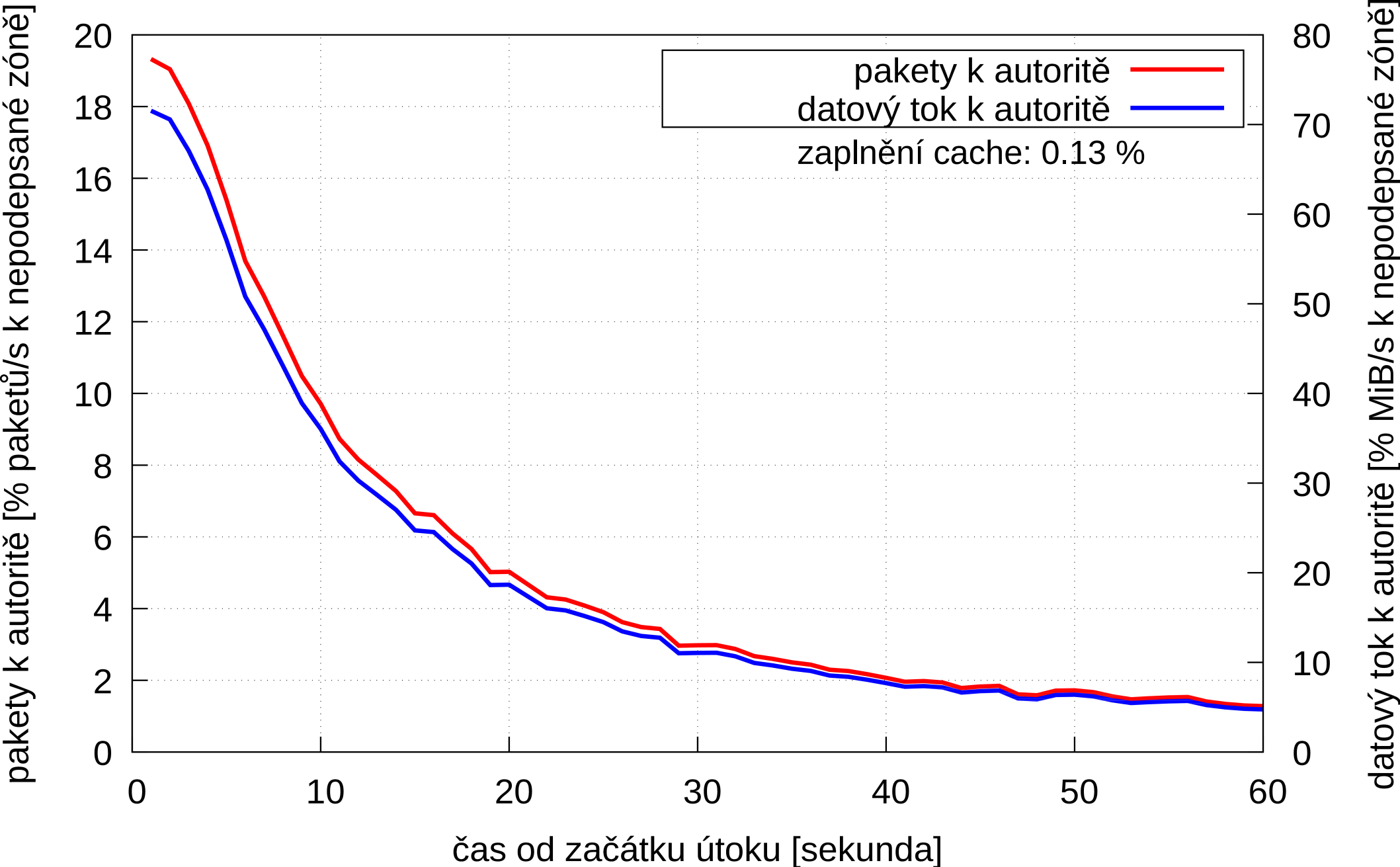
# R.S.Ú.: 14k jmen, TTL 3600



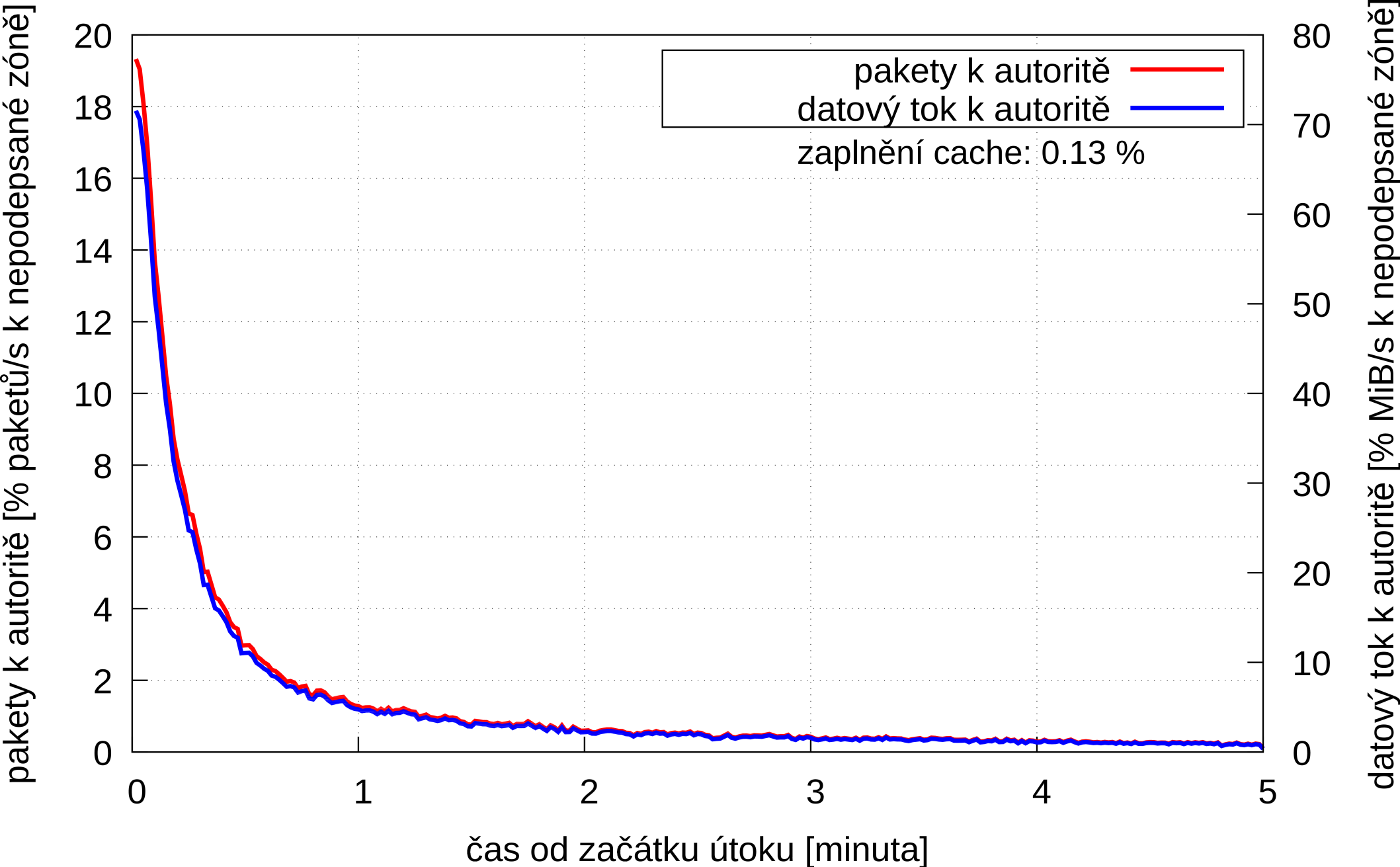
# R.S.Ú.: 110k jmen, TTL 3600



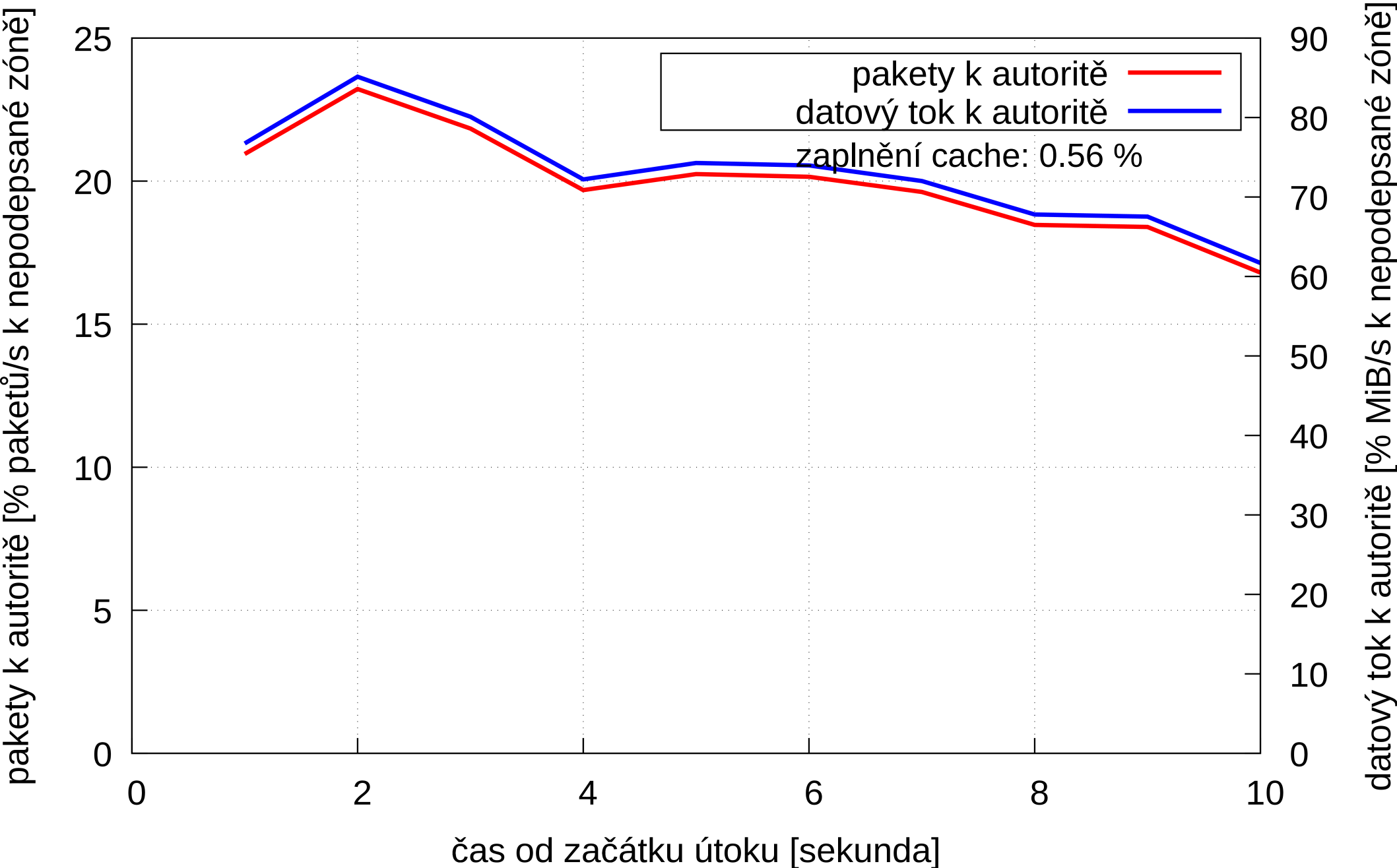
# R.S.Ú.: 110k jmen, TTL 3600



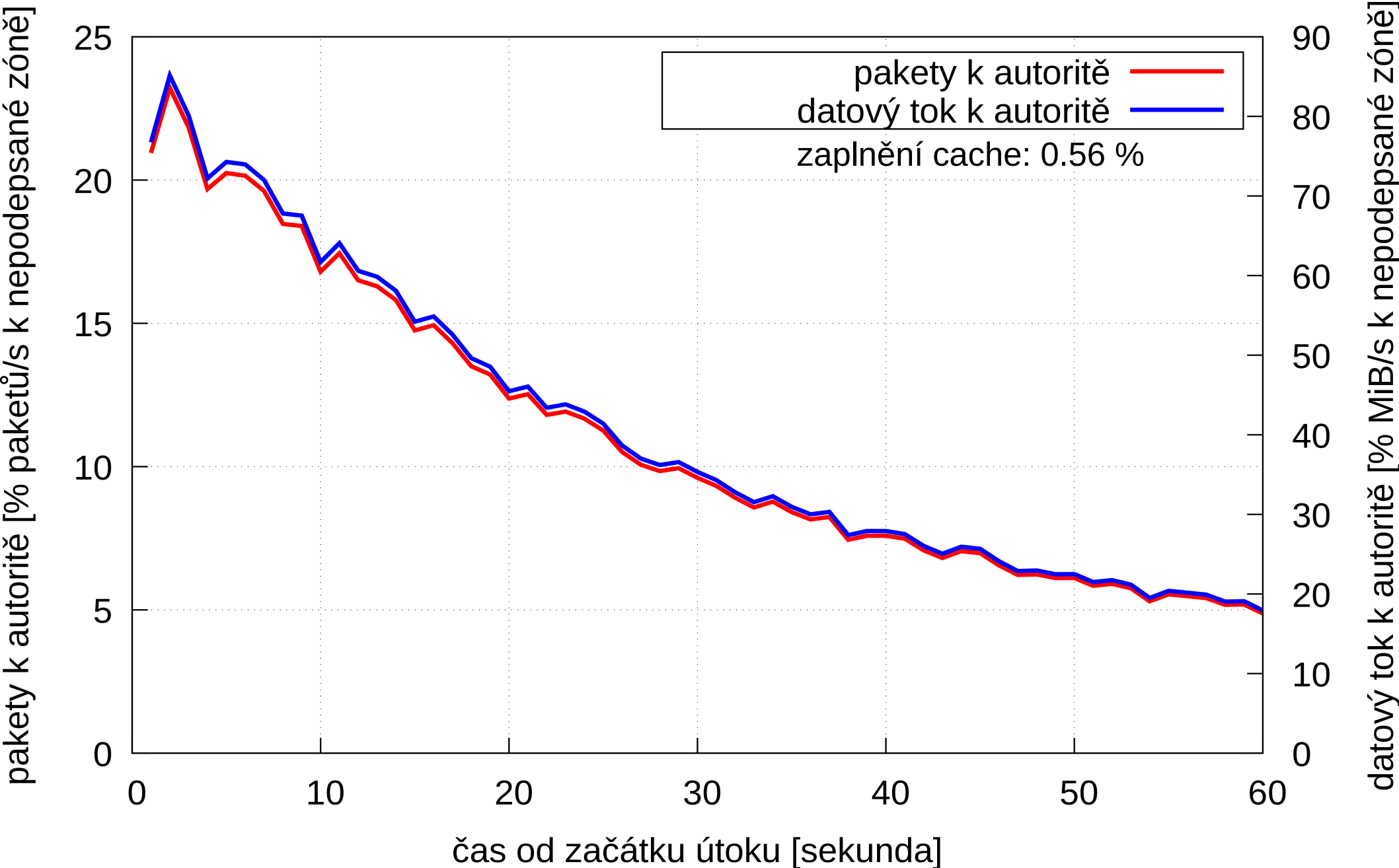
# R.S.Ú.: 110k jmen, TTL 3600



# R.S.Ú.: 1M jmen, TTL 3600

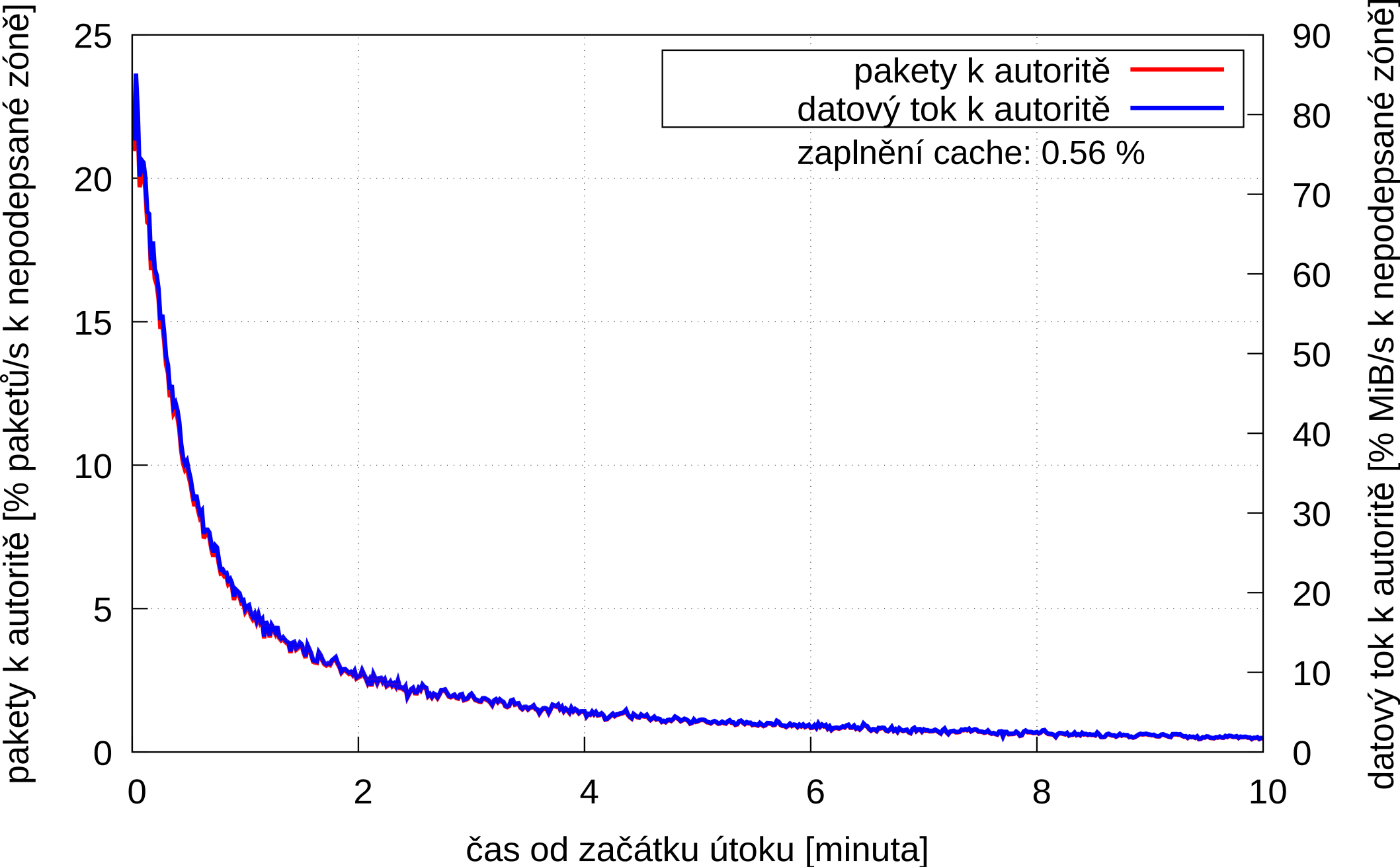


# R.S.Ú.: 1M jmen, TTL 3600

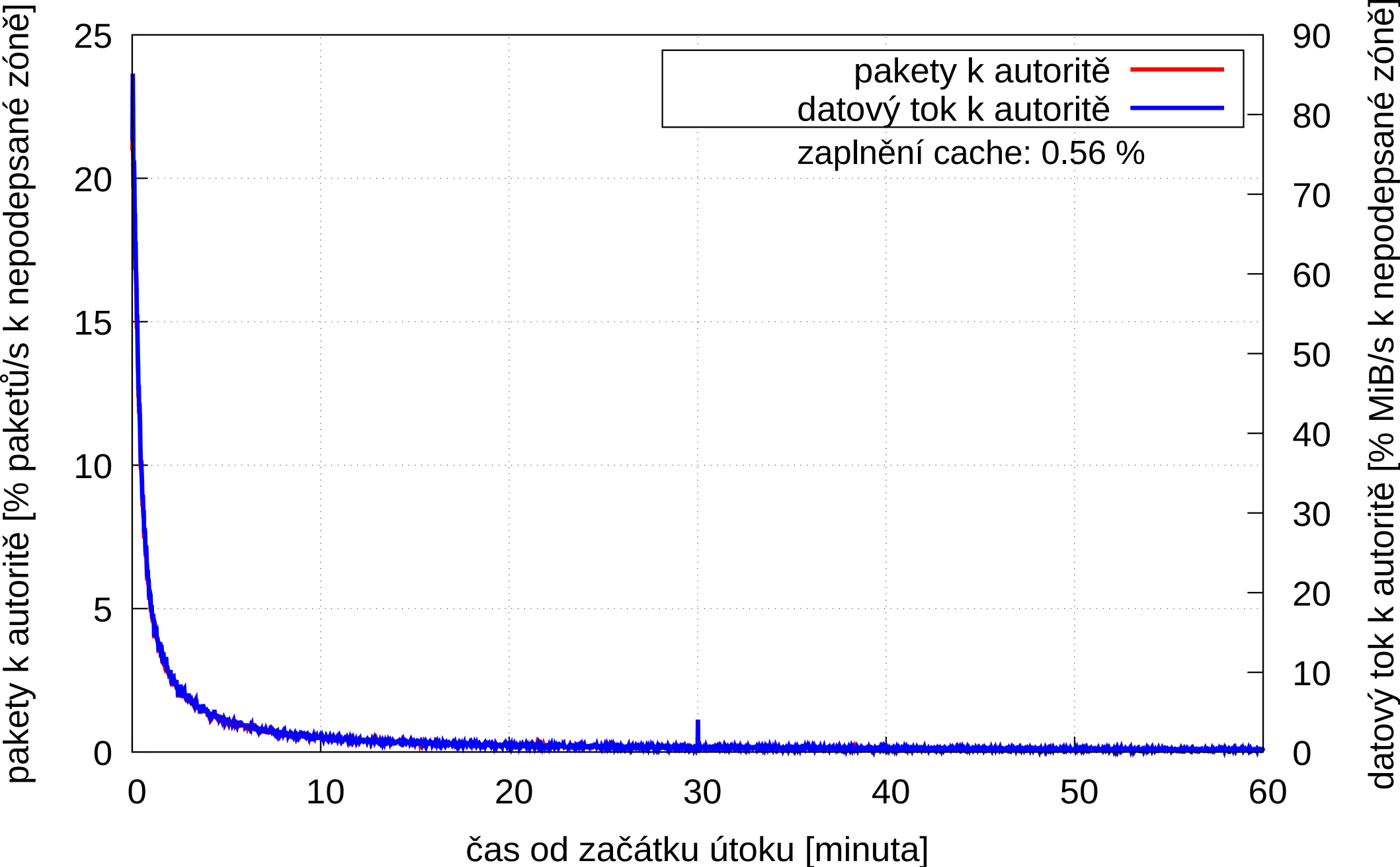




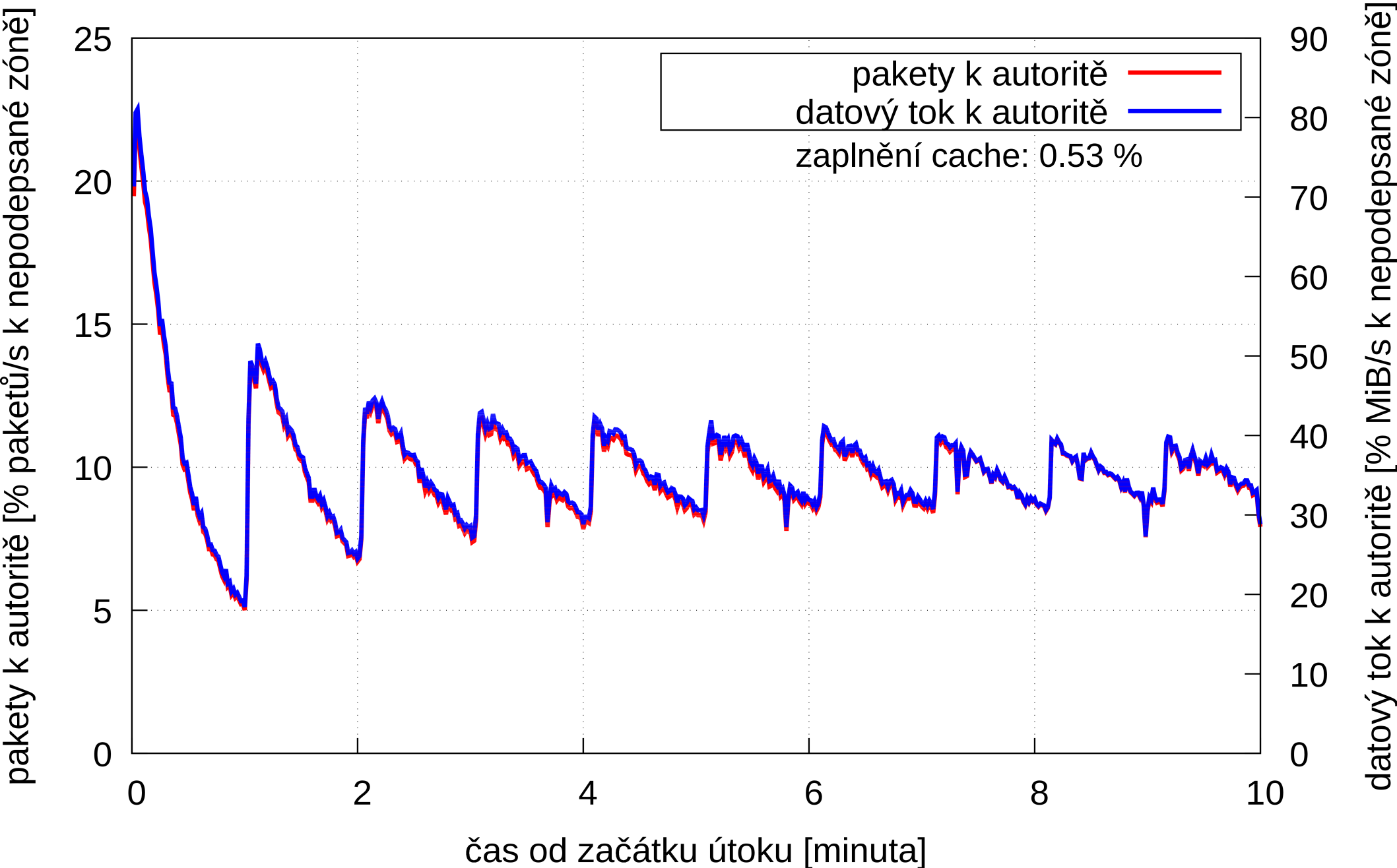
# R.S.Ú.: 1M jmen, TTL 3600



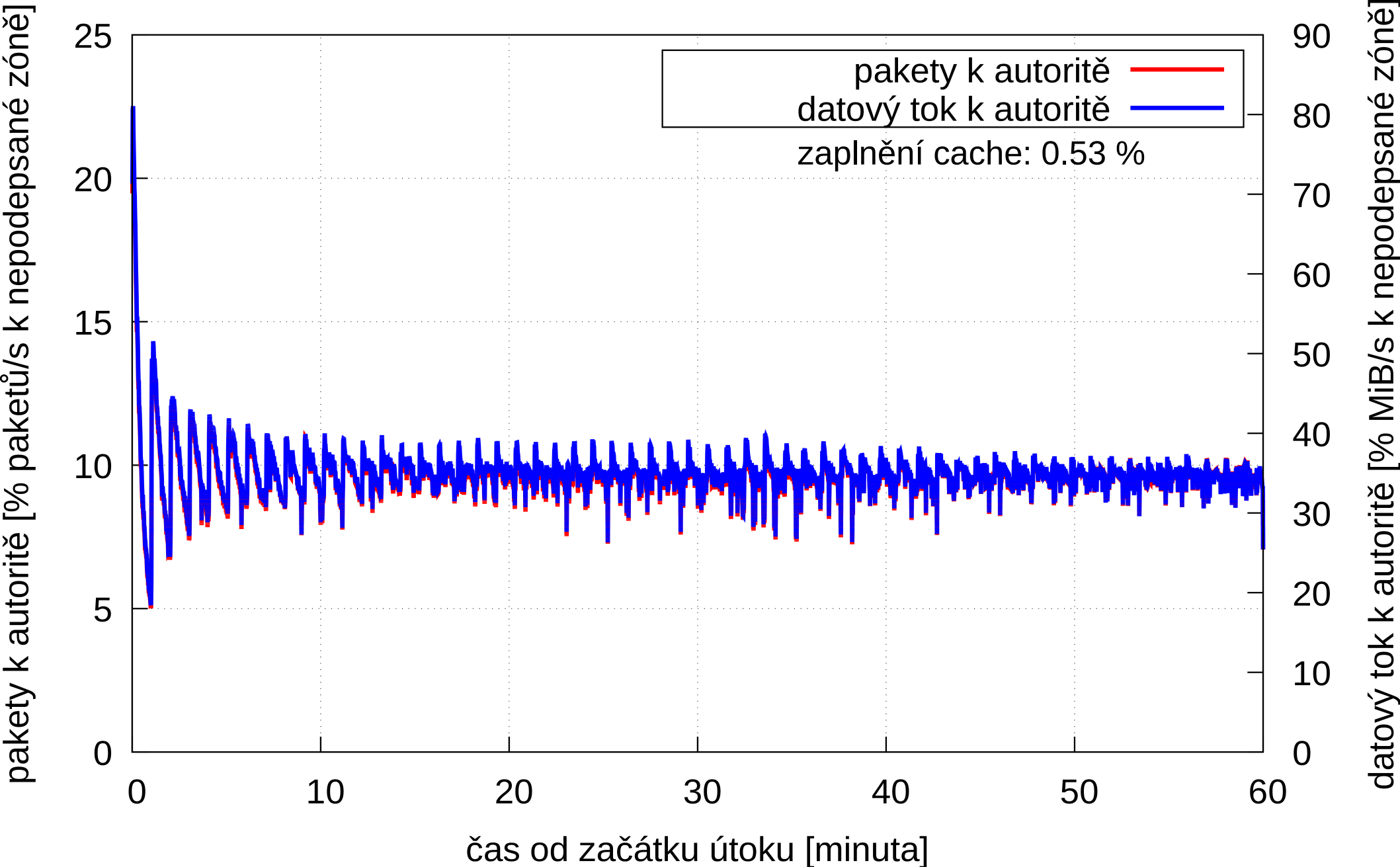
# R.S.Ú.: 1M jmen, TTL 3600



# R.S.Ú.: 1M jmen, TTL 60



# R.S.Ú.: 1M jmen, TTL 60



# Očekávání vs. R.S.Ú. provoz

- ☒ **Výrazně** lepší využití cache
- ☒ **Výrazně** menší zatížení sítě
  - zastaví R.S.Ú. provoz (postupně)
- NSEC je efektivnější než NSEC 3
  - RSA 2048 b NSEC 3 => 150 % velikosti NSEC
- NSEC i NSEC 3 poskytují efektivní ochranu
  - agresivní NSEC 3 zatím resolvery neumí

# Upgradujte, podepiště, VALIDUJTE

- ☒ Ochrana soukromí (únik dotazů jako .home)
- ☒ Ochrana proti random subdomain útokům
- ☒ Odstranění problémů s EDNS
  - konec podpory v únoru 2019
  - lightning talk



# Knot v létě 2018



- **Knot DNS 2.7**
- Zlepšení výkonu
- Security audit
- DNS cookies



- **Knot Resolver 2.4**
- Podpora NSEC 3 v agresivní cache

# Twitter @KnotDNS