DNSSEC aggressive cache (RFC 8198)

Protection from random subdomain attacks

Petr Špaček • petr.spacek@nic.cz • 2018-05-16

CZ DOMAIN REGISTRY

Talk outline

- Aggressive cache
  - theory
  - expectations
  - efficiency
- Normal traffic
  - measurements
- Random subdomain attack
  - theory
  - measurements

Aggressive cache: Theory

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

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

Aggressive cache: Expectations

- Use of NSEC/NSEC3 RRs to
  - decrease **latency**
  - decrease **resource utilization**
  - increase **privacy**
  - increase **resilience**

Aggressive cache: Efficiency

- Query pattern
  - normal traffic
  - random subdomain attack
- Distribution of names in DNS zones
- Wildcards
- TTL

Aggressive cache

vs.

Normal traffic

Normal traffic: Experimental setup

- Replay query PCAP to BIND 9.12.0
  - synth-from-dnssec yes / no;
- Record to PCAP
  - traffic to auth
  - answers
- Analyze
  - # packets to auth
  - bandwidth to auth
  - latency for answers

Expectations vs. normal traffic

- Root zone
  - eliminates query leaks
    - stops 50-65 % queries to root
  - ☑ **privacy protection**

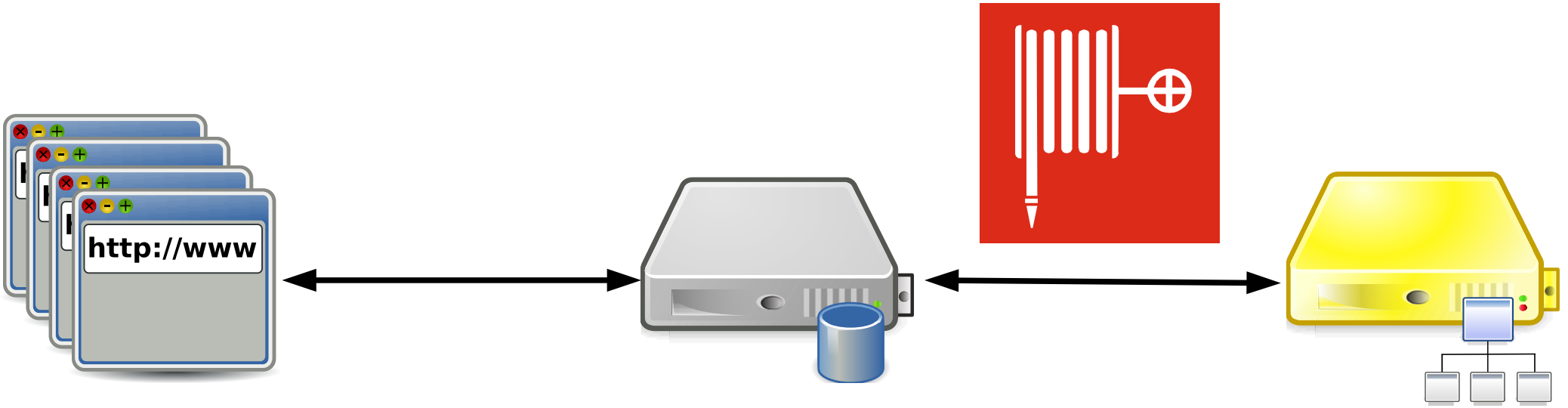
- Others zones
  - nothing to see here
  - negligible impact on normal traffic
  - not enough signed domains?

Aggressive cache

vs.

Random subdomain attack

R.S.A. traffic: Theory



attacker's JavaScript

recursive resolver

auth server

unknowing collaborators

not a target

target

collateral damage

R.S.A. traffic: Query pattern

- 1000 simulated clients
- Next query right after answer
- Pseudorandom unique query names (256 bits)
  - GCZDKQIS7F7TTHXBIBC4HHZDYTFCPH5XLR6P GEI3WIESK7BS45WQ.test.knot-resolver.cz. A
  - GCZDKQIS7F7TTHXBIBC4HHZDYTFCPH5XLR6P GEI3WIESK7BS45WQ.test.knot-resolver.cz. AAAA
  - OF6OVT2SNIV54B7HI77V5TJ3TFVULN5AMQ2Z6I WQX6GBHQ254LNQ.test.knot-resolver.cz. A

R.S.A. traffic: Experimental setup

- Auth server with a test zone
  - signed using NSEC
  - extrapolation for NSEC 3: `(size * 1.5)`
- Replay random query names to Knot Resolver
- Record **traffic from resolver to auth**
- Analyze
  - # packets to auth
  - bandwidth to auth

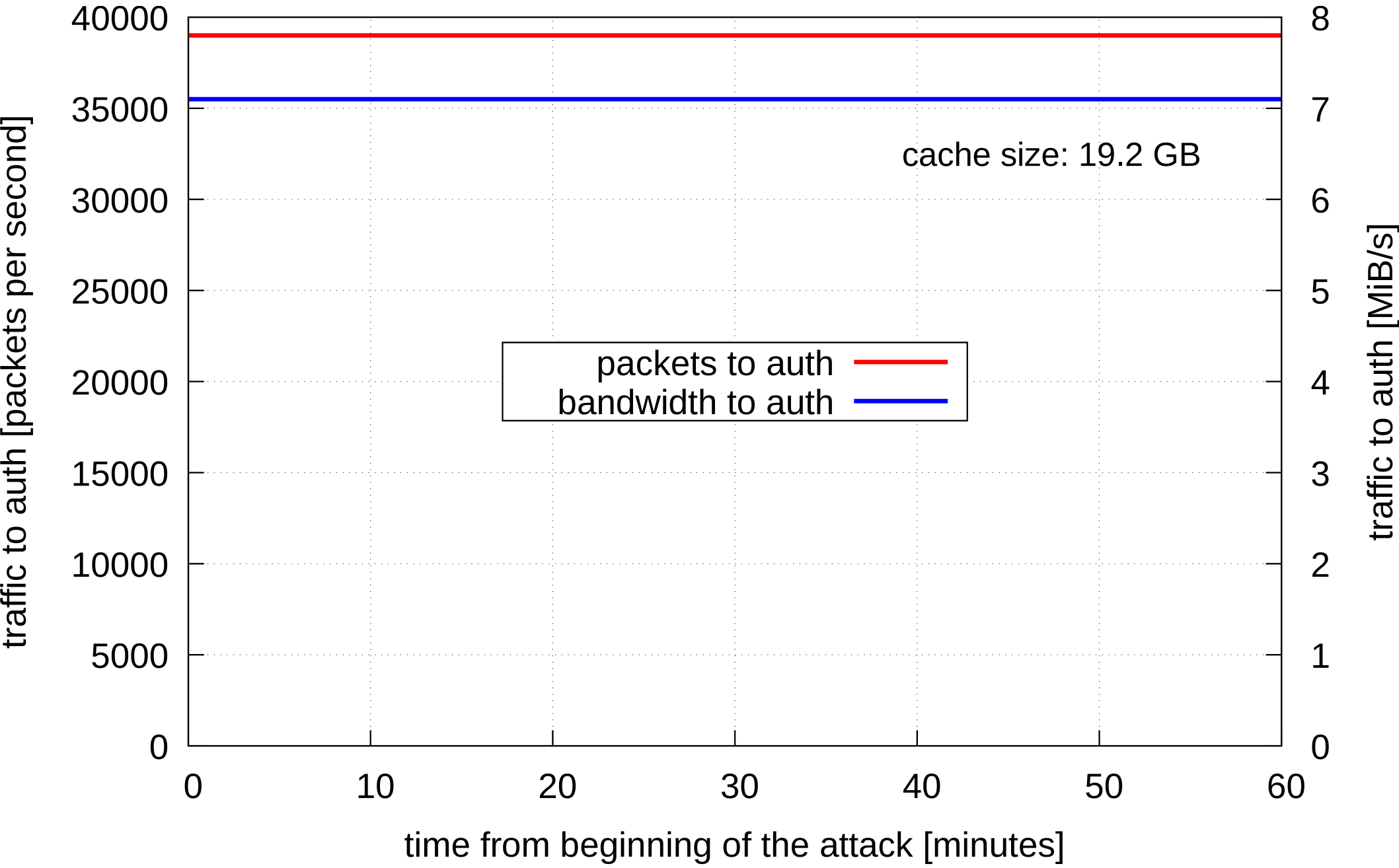
R.S.A. traffic: Tools

- Knot DNS 2.6.4
  - RSASHA256 2048 b, automatic signing
    - **big answers**
- Knot Resolver 2.1.1
  - "unlimited" cache size (20 GiB)
- dnsperf 2.1.0 to replay queries
- libtrace 3.0.21 to analyze packet #, bandwidth

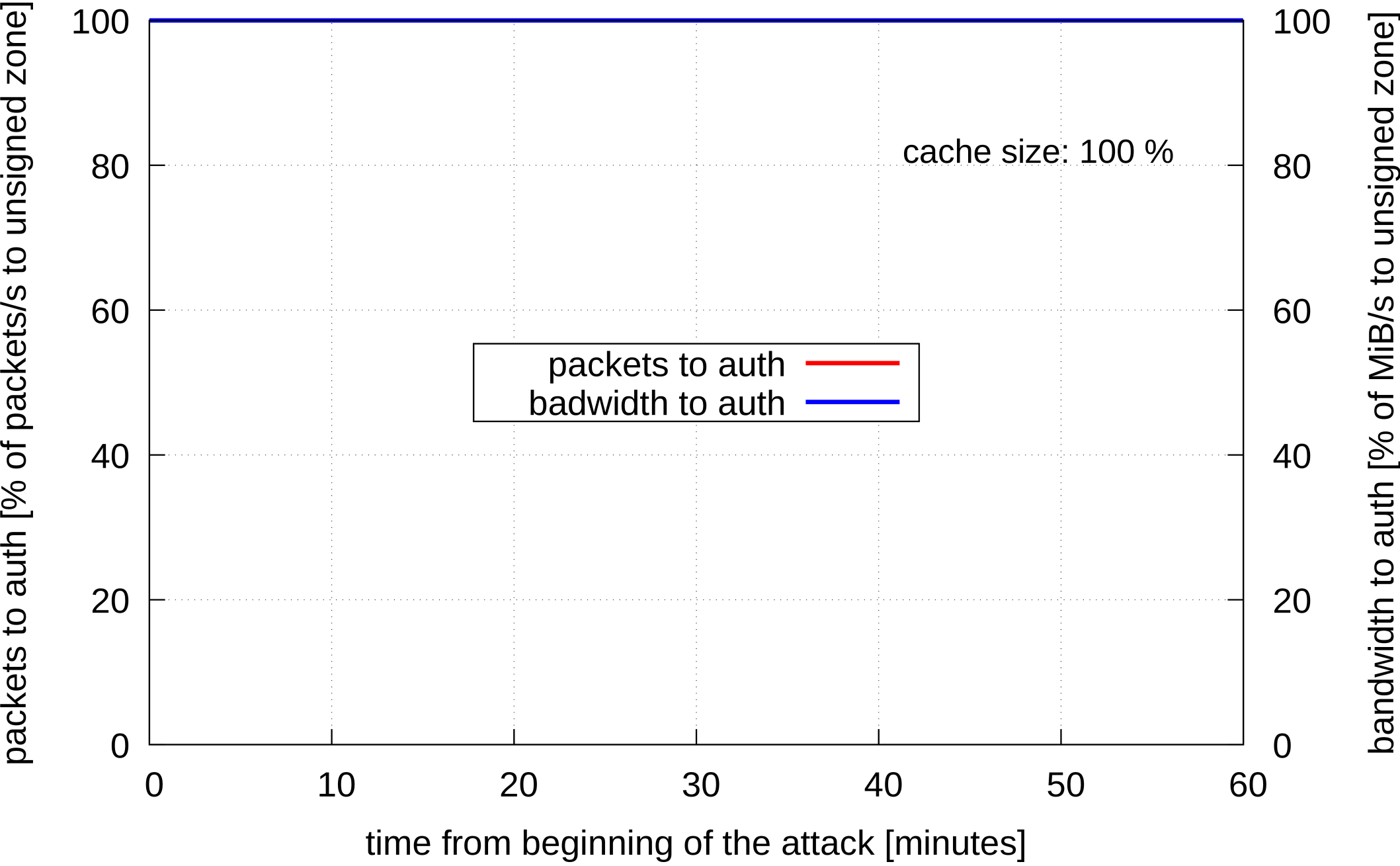
R.S.A. scenarios

- Unsigned zone (baseline)
- Signed zone
  - SOA minimum, NSEC TTL
    - 3600 s / 60 s
  - name distribution (real zones)
    - small zone with wildcard (50 names + 1 wildcard)
    - medium size zone (14k names)
    - big zone (110k names)
    - huge zone (1M names)

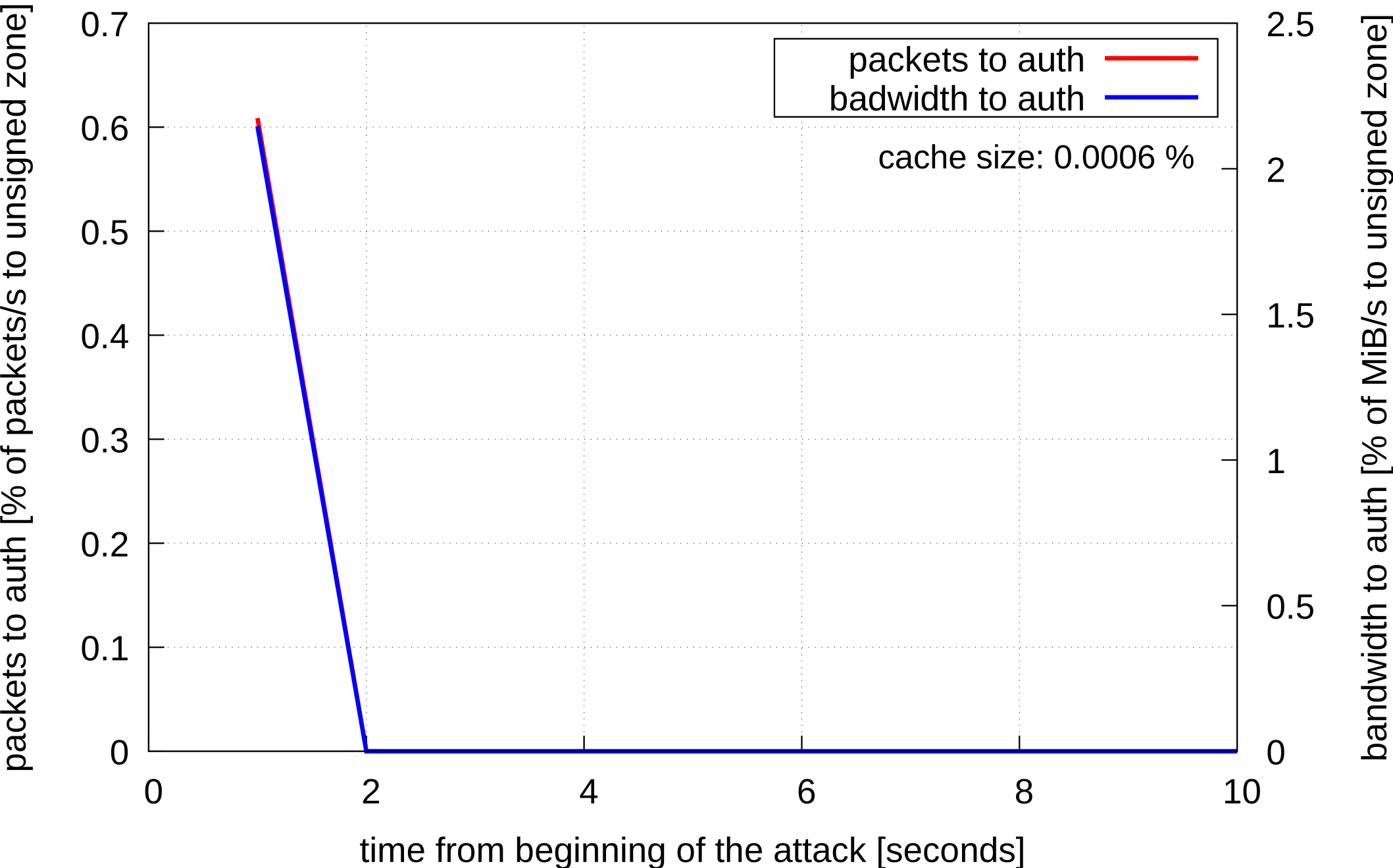
R.S.A.: unsigned zone (abs baseline)



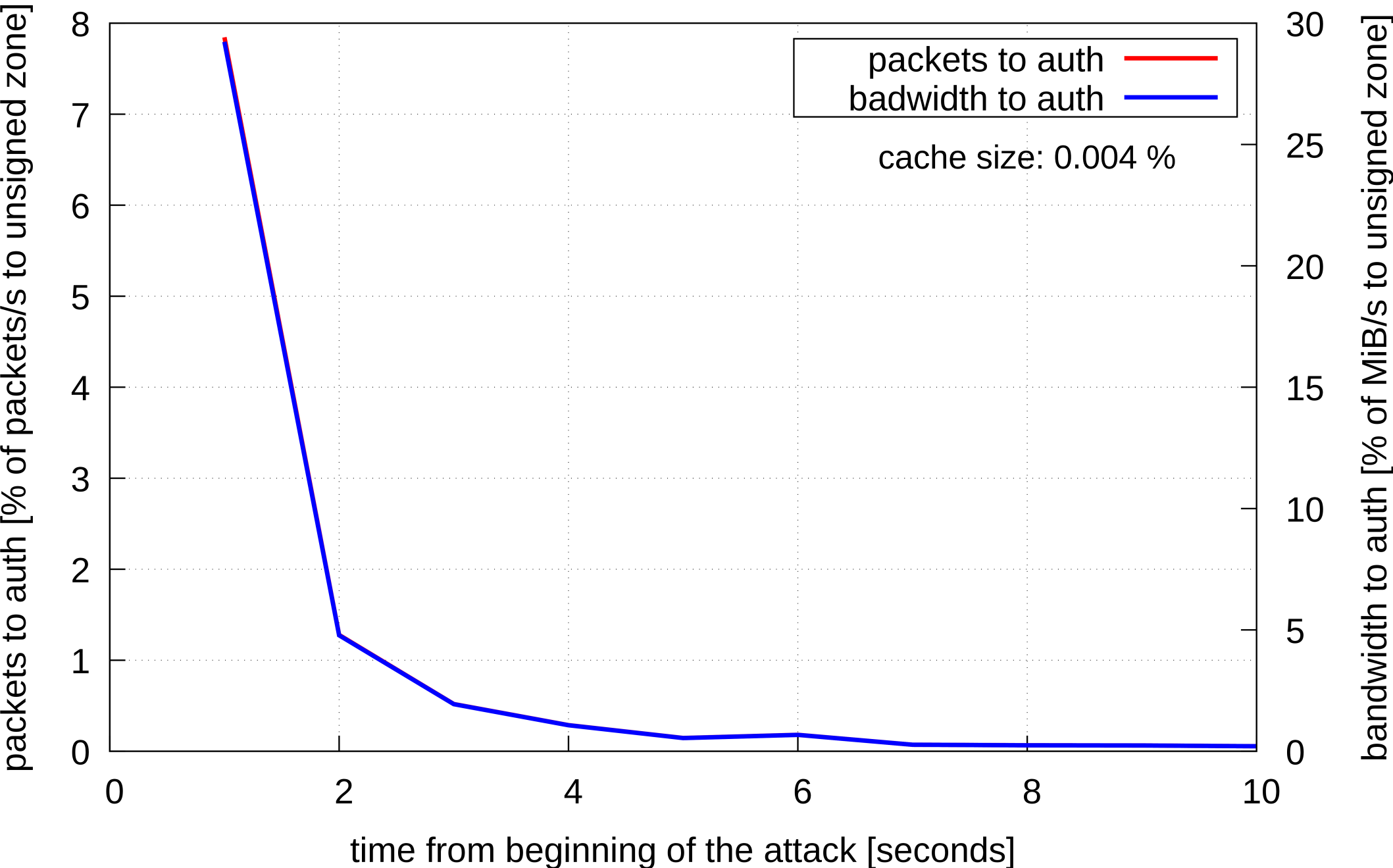
R.S.A.: unsigned zone (baseline %)



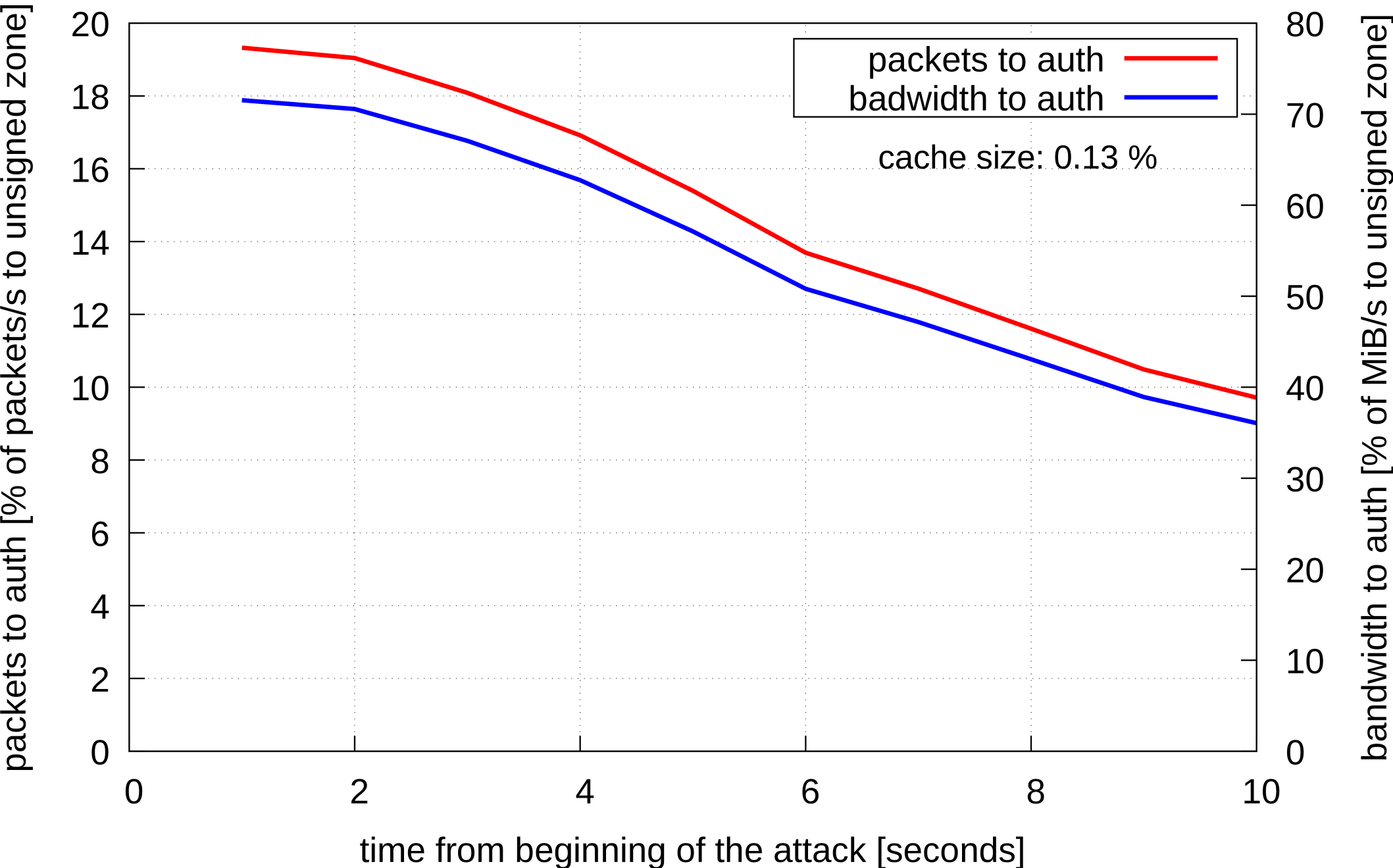
R.S.A.: 50 names + wildcard, TTL 60



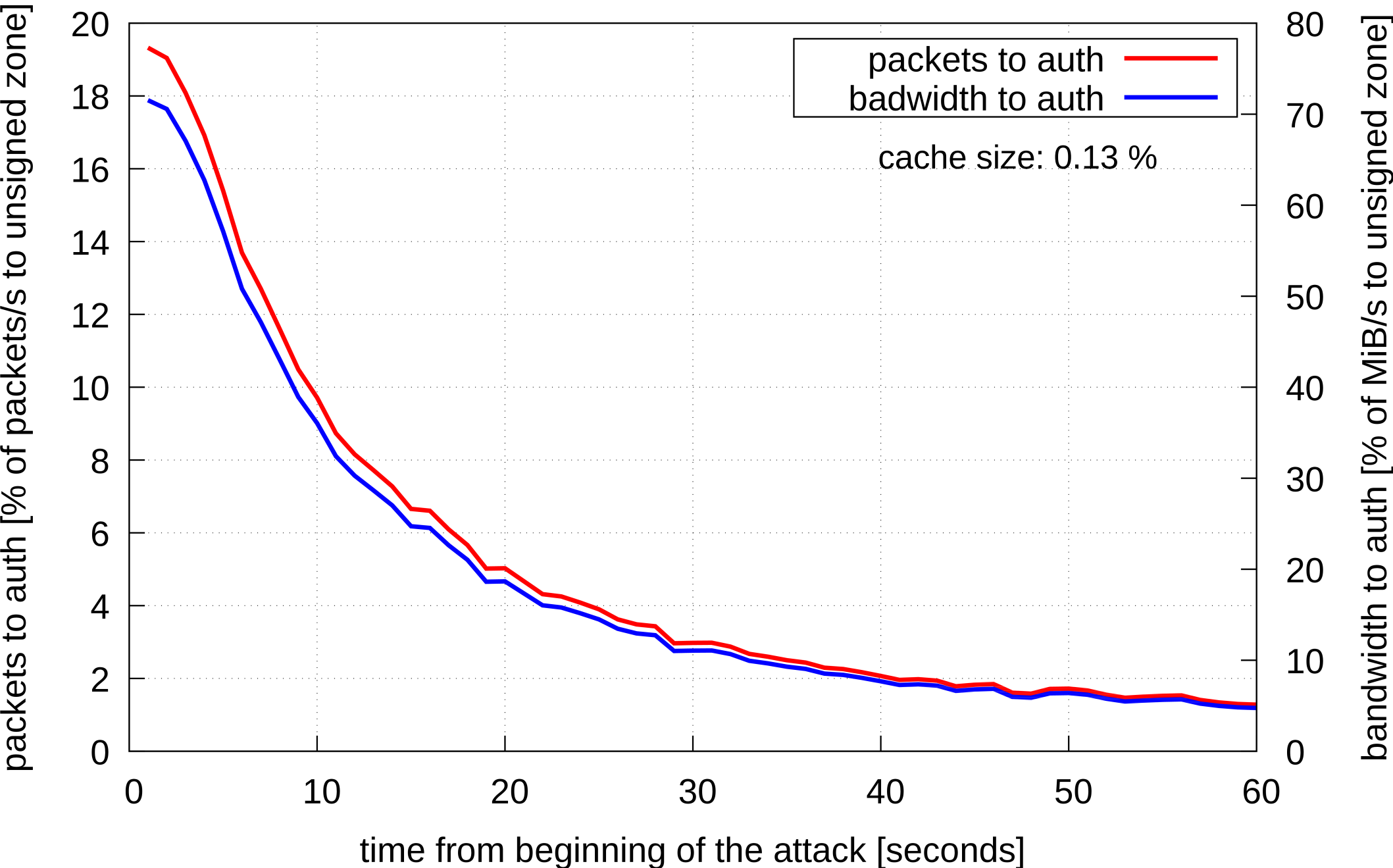
R.S.A.: 14k names, TTL 3600



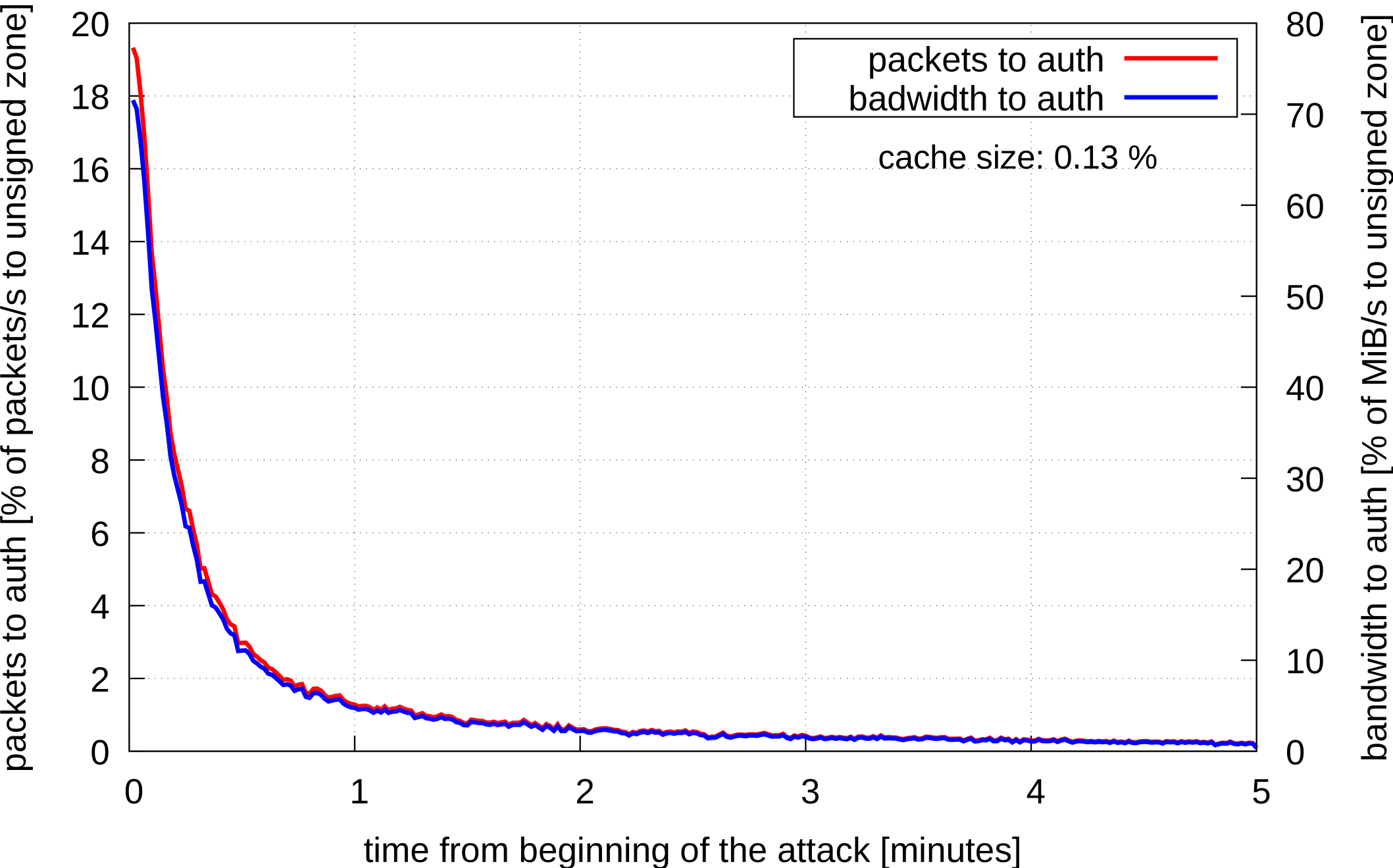
R.S.A.: 110k names, TTL 3600



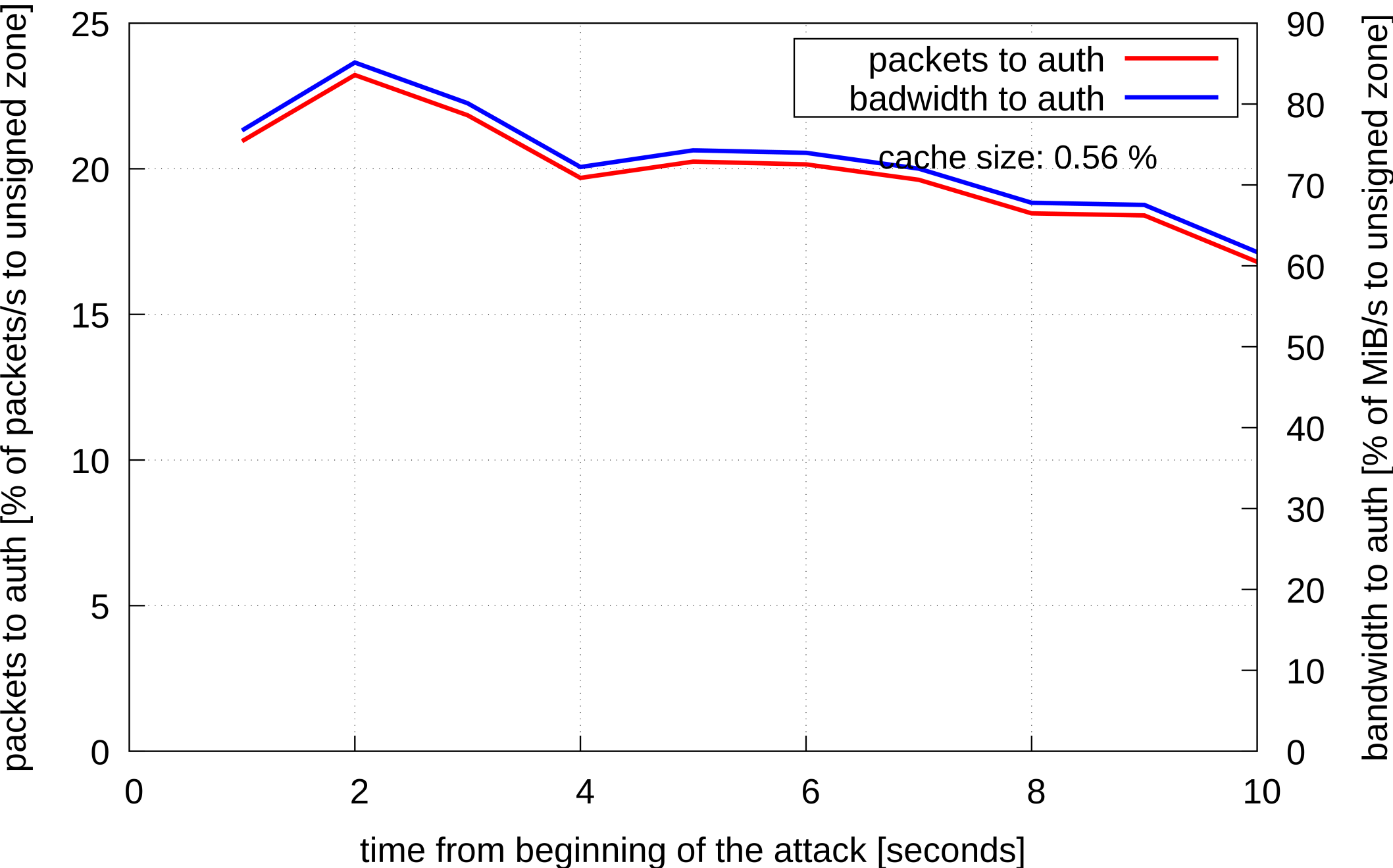
R.S.A.: 110k names, TTL 3600



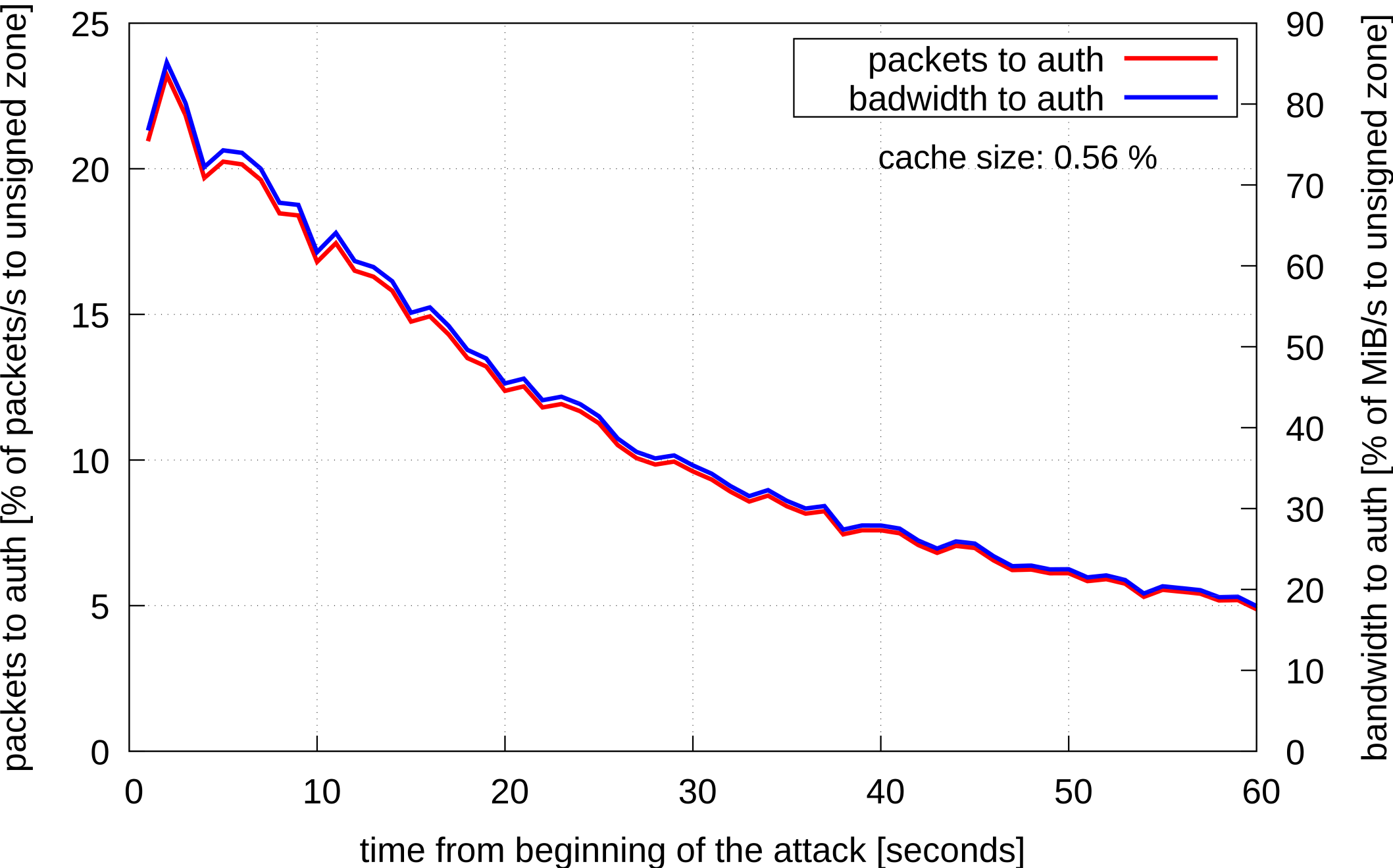
R.S.A.: 110k names, TTL 3600



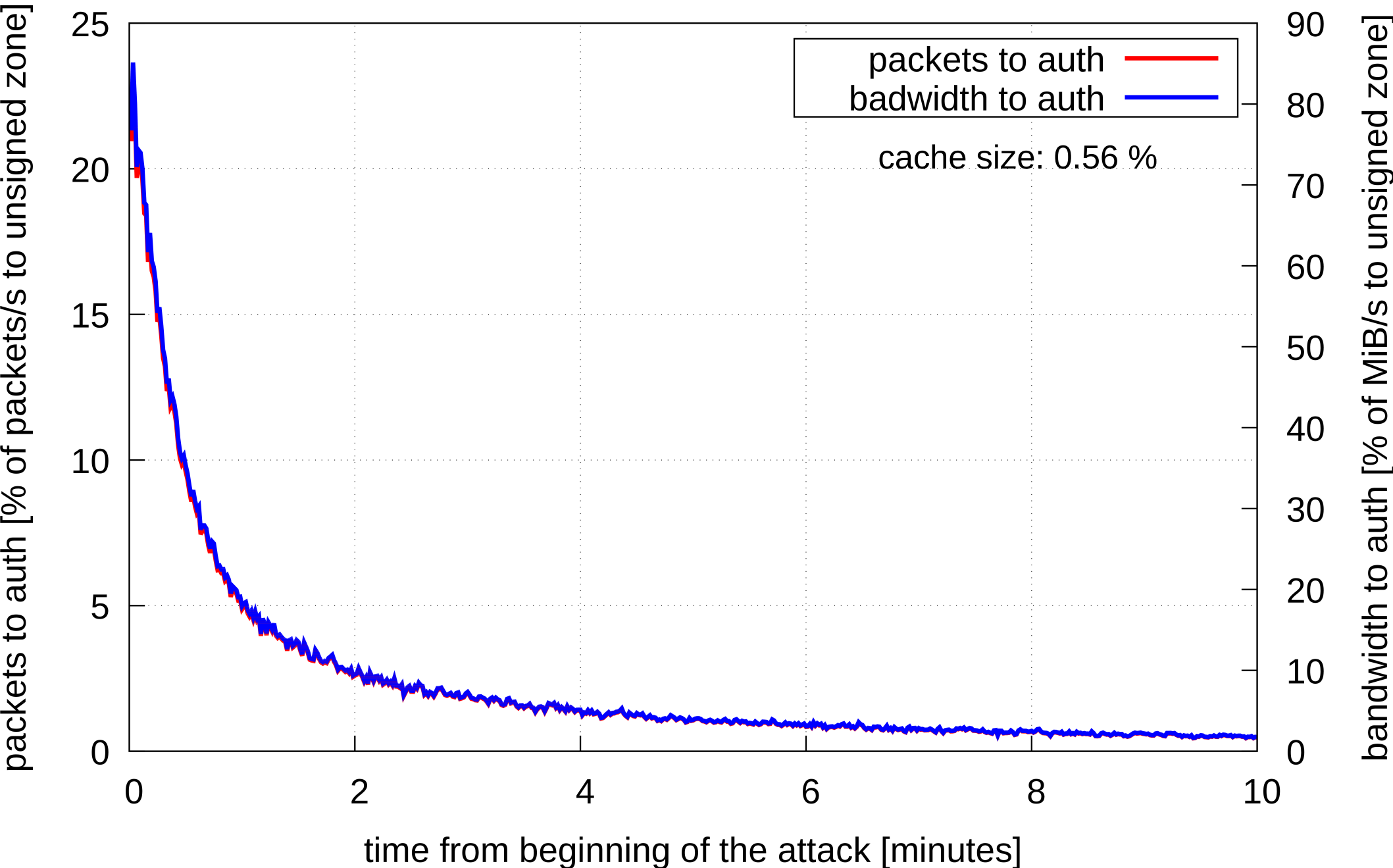
R.S.A.: 1M names, TTL 3600



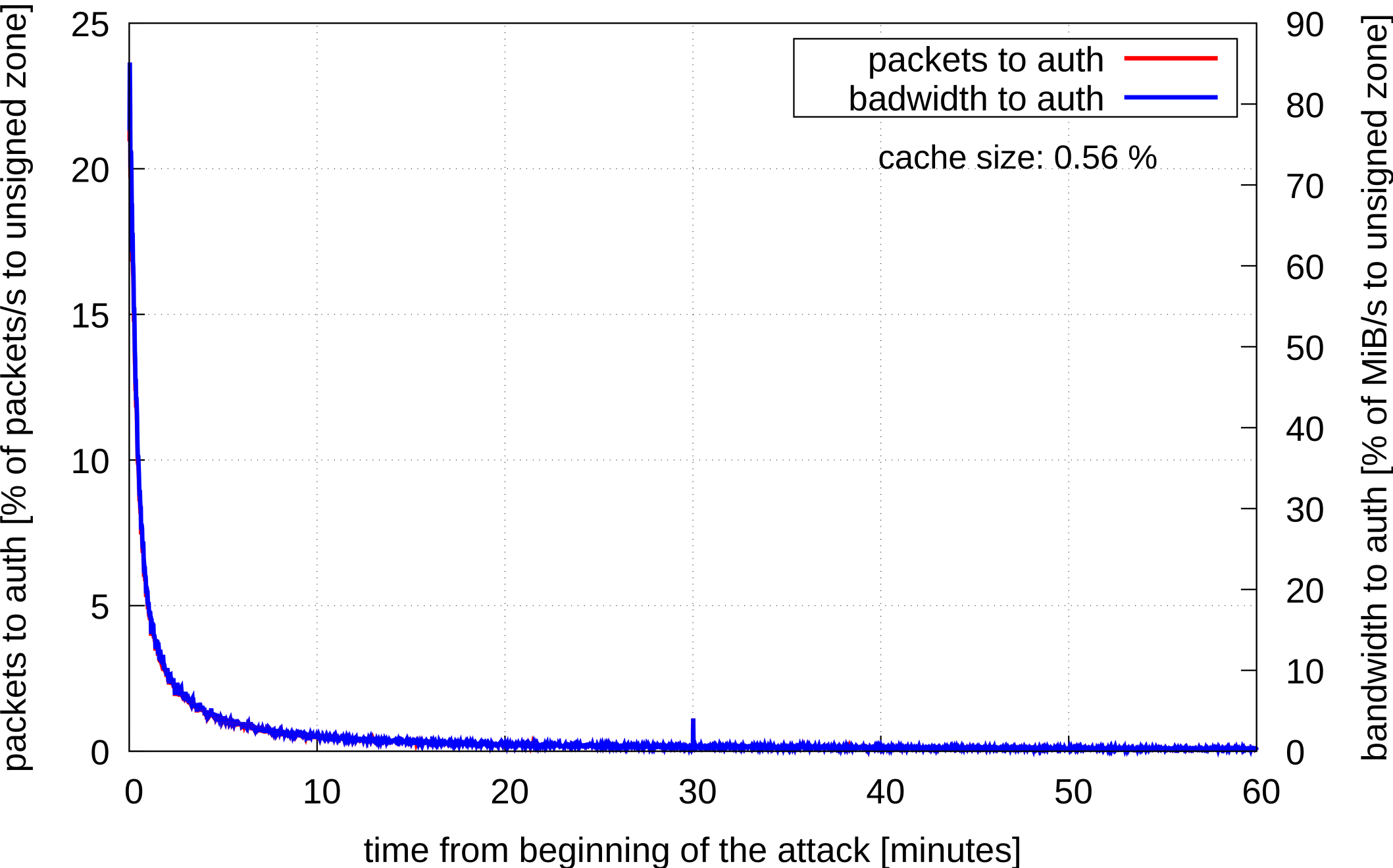
R.S.A.: 1M names, TTL 3600



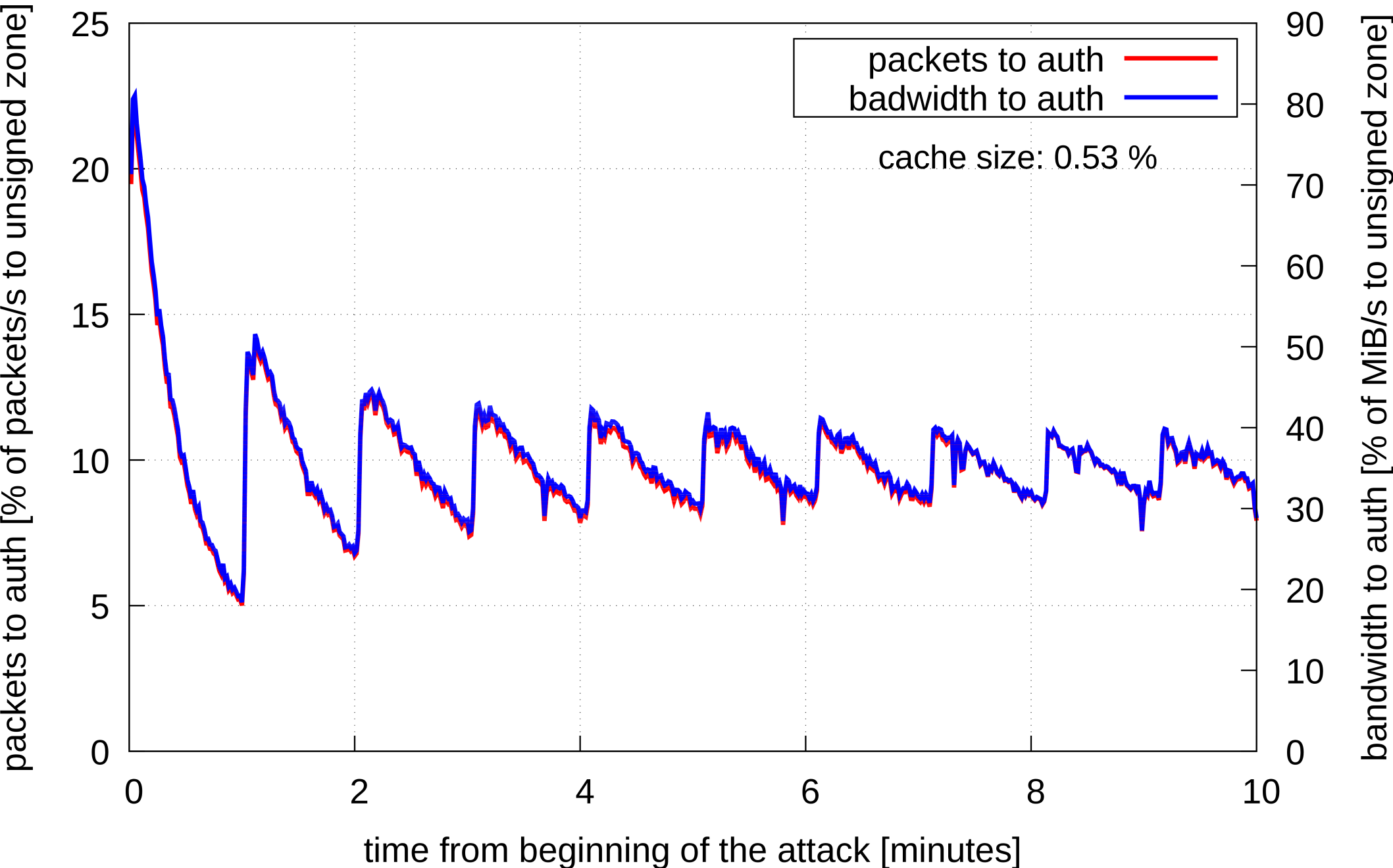
R.S.A.: 1M names, TTL 3600



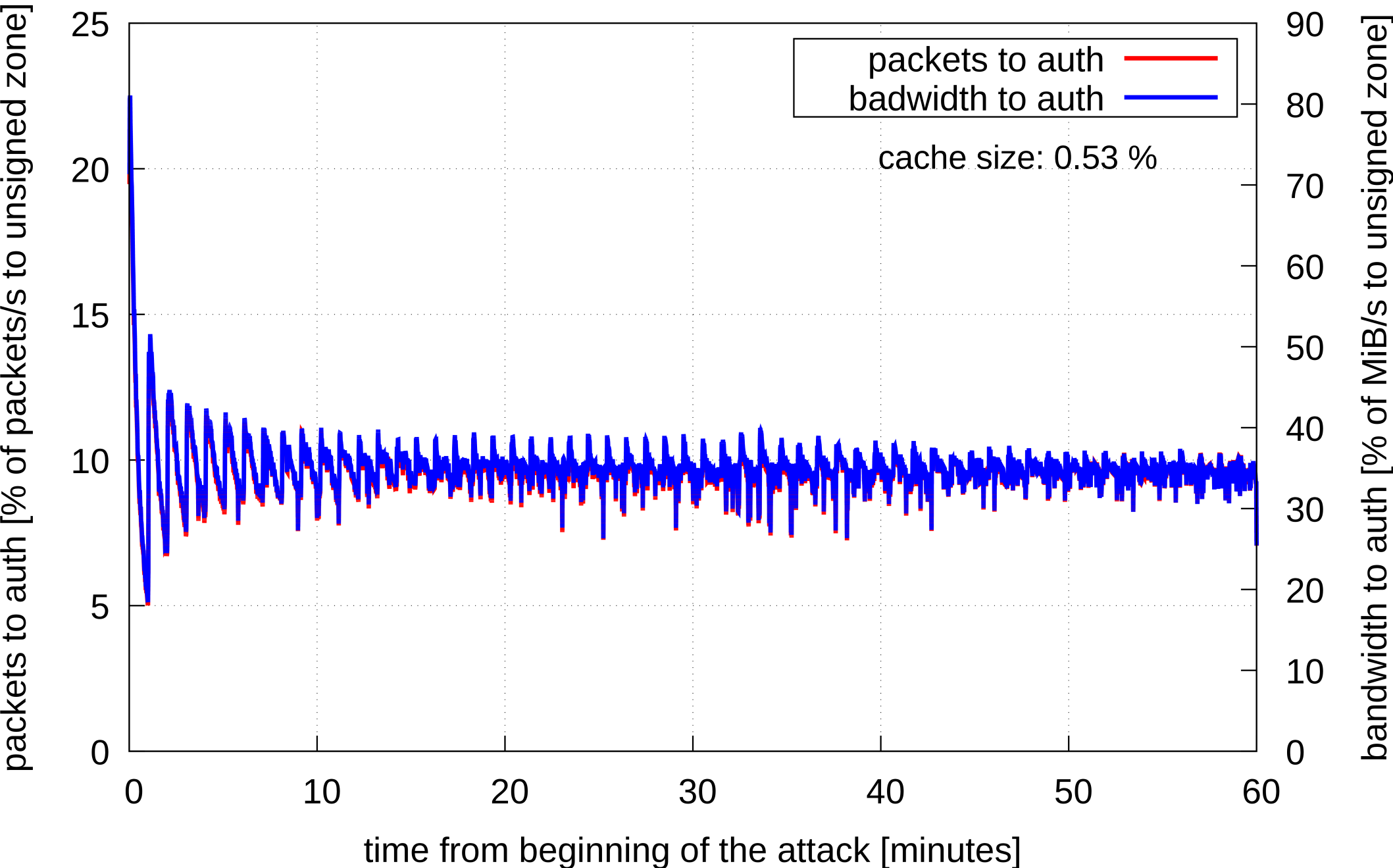
R.S.A.: 1M names, TTL 3600



R.S.A.: 1M names, TTL 60



R.S.A.: 1M names, TTL 60



Promises & R.S.A. traffic

- ☑ **Much** better cache usage
- ☑ **Significantly** lower network utilization
  - Eliminates R.S.A. traffic (over time)

- NSEC is more efficient than NSEC 3
  - RSA 2048 b NSEC 3 => 150 % size of NSEC
- NSEC & NSEC 3 provide effective protection
  - NSEC 3 not supported by resolvers yet

Upgrade, sign, VALIDATE

- ☑ Privacy protection (leaked queries)
- ☑ Protection from random subdomain attacks
- ☑ Avoids problems with EDNS
  - EDNS workaround sunset in 2019

Knot news for summer 2018

- **Knot DNS 2.7**
- Performance optimizations
- Security audit
- DNS cookies

- **Knot Resolver 2.4**
- NSEC 3 support for aggressive cache

follow **@KnotDNS**