The IRONSIDES Project: Final Report

Barry Fagin, US Air Force Academy

Martin Carlisle, CMU

Introduction

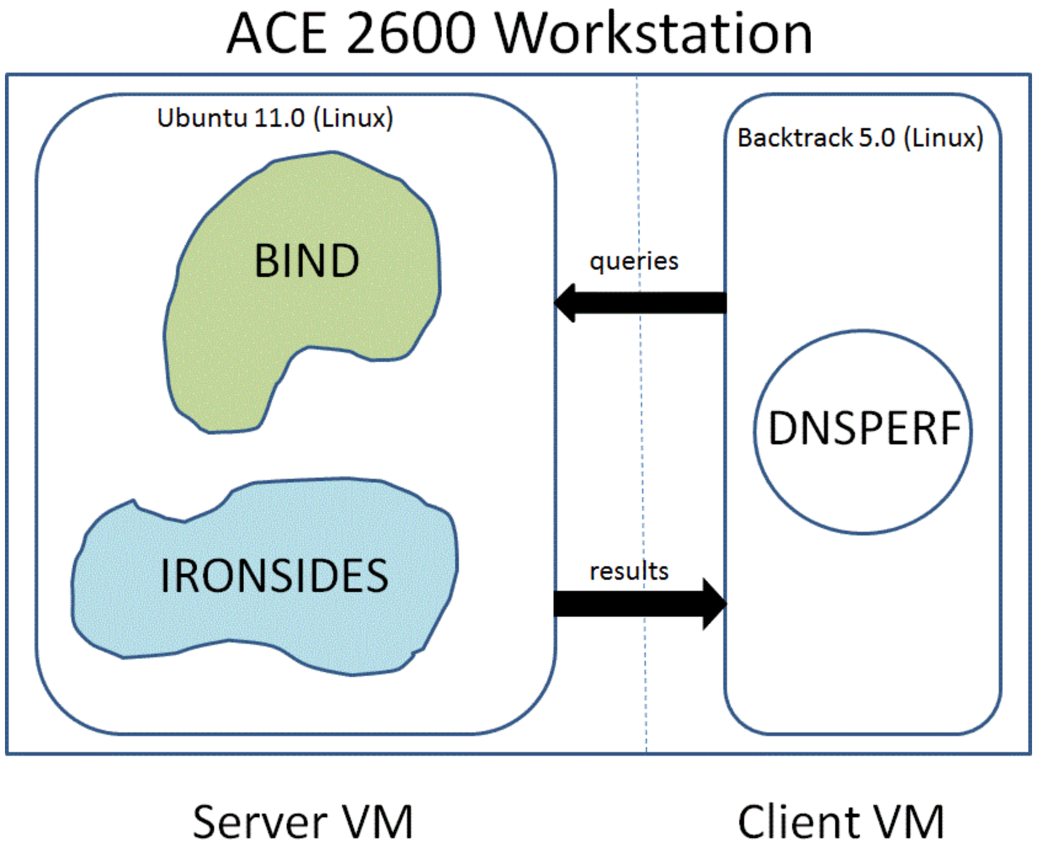
DNS is both important and implemented poorly.

IRONSIDES is an Ada/SPARK DNS implementation intended as proof-of-concept:

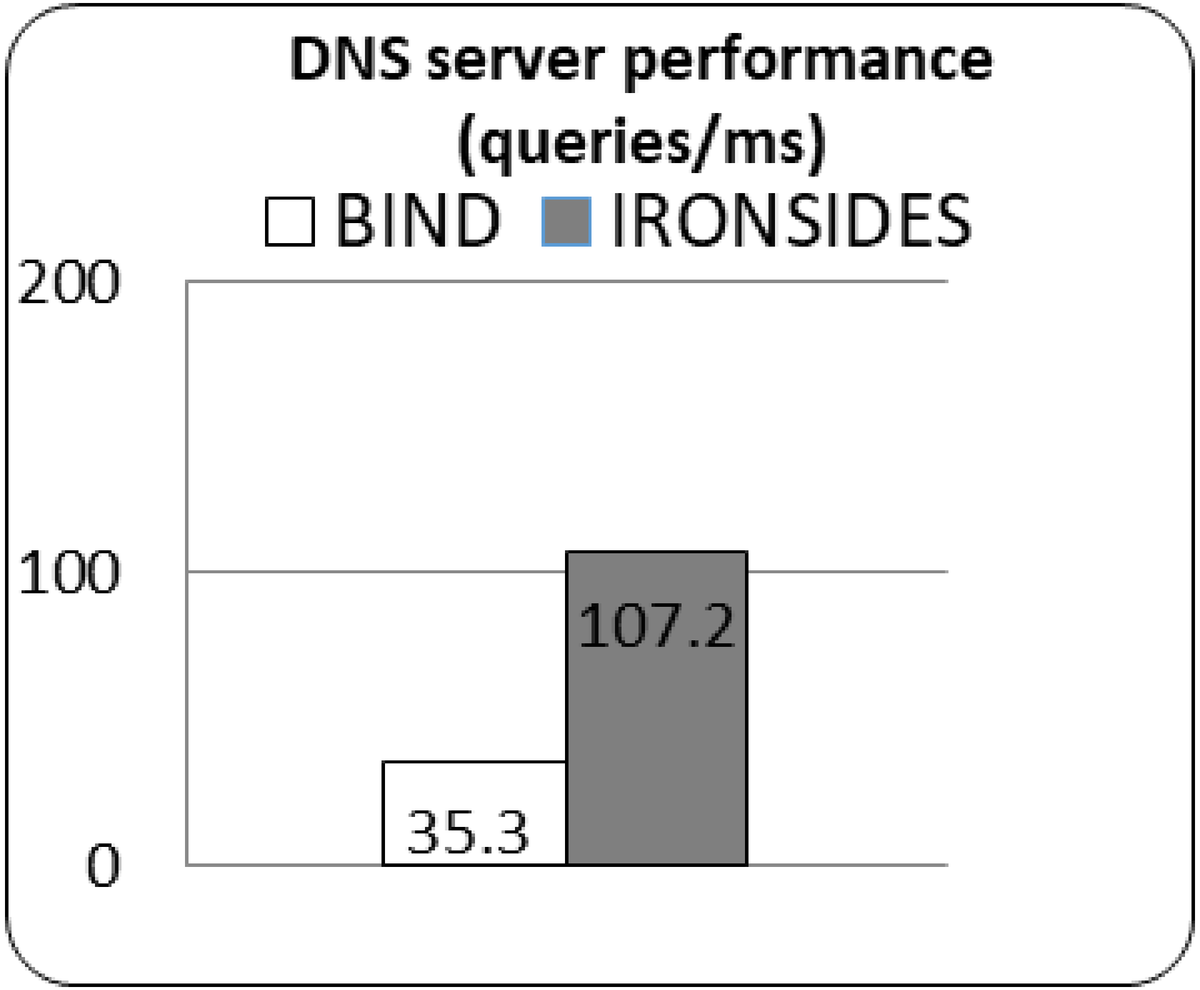
Can DNS server be implementation on a modest (!!!) development budget with provable security properties?

What does adding provable security properties do to performance?

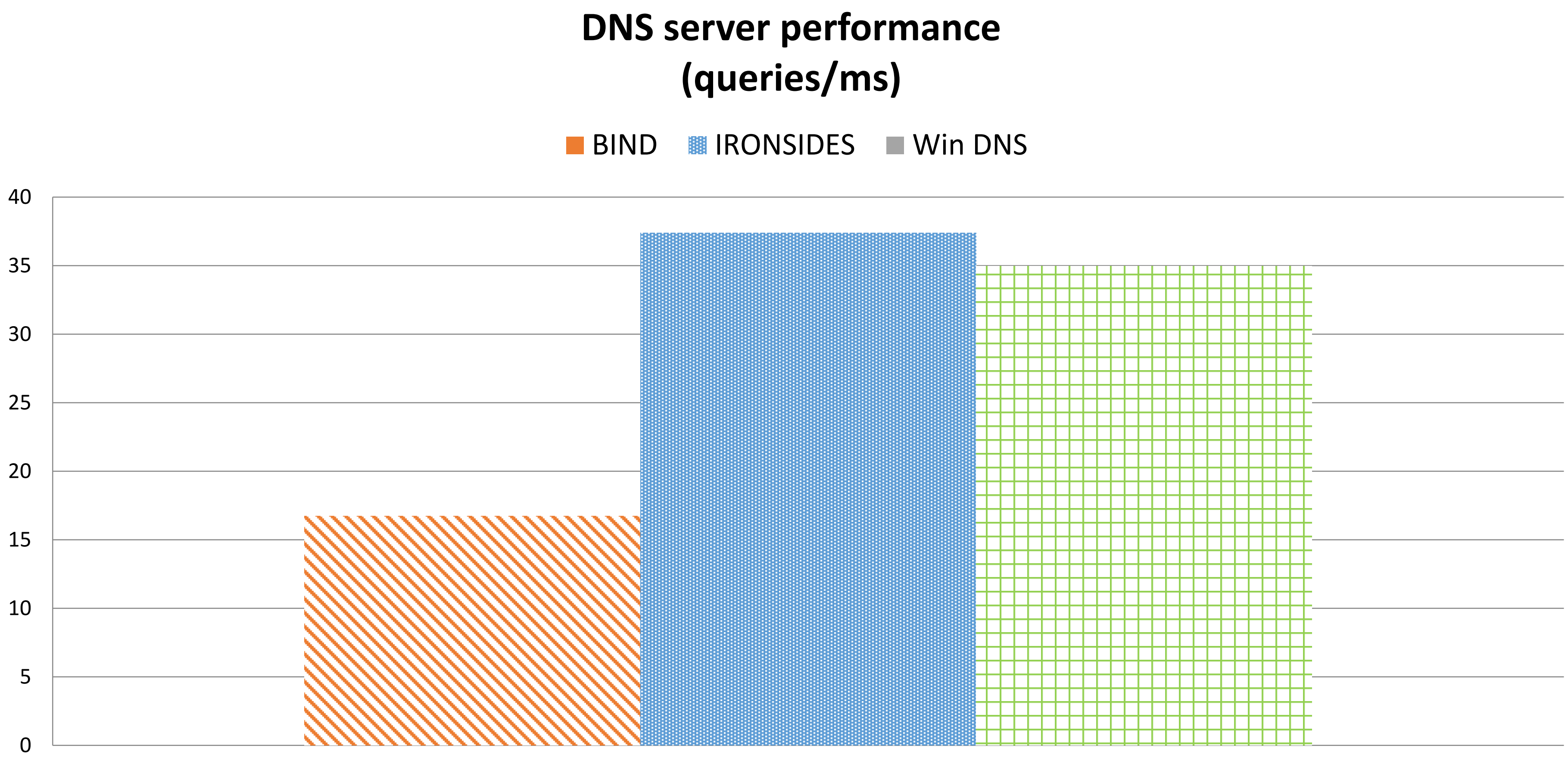
Milestone 1: Authoritative server on Linux [2012]



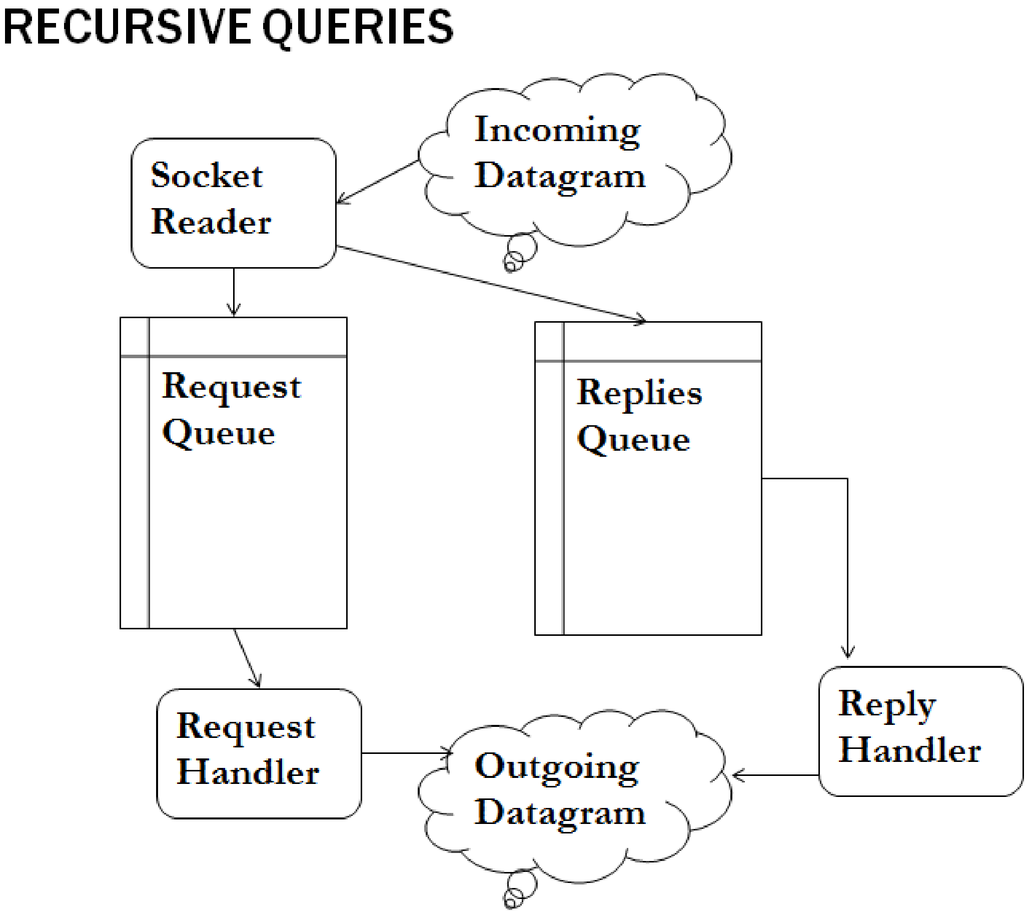
BIND and IRONSIDES performance -- Linux



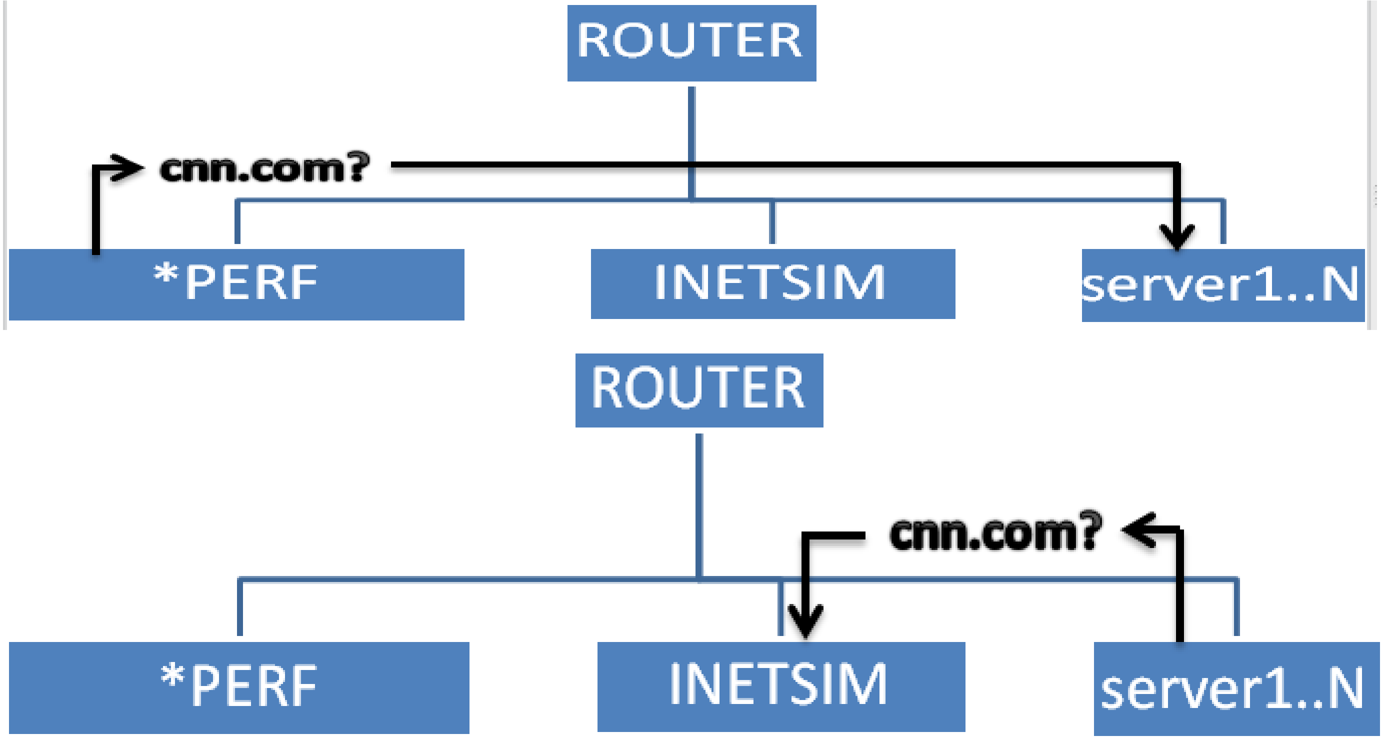
Milestone 2: Authoritative server under Windows (2013)



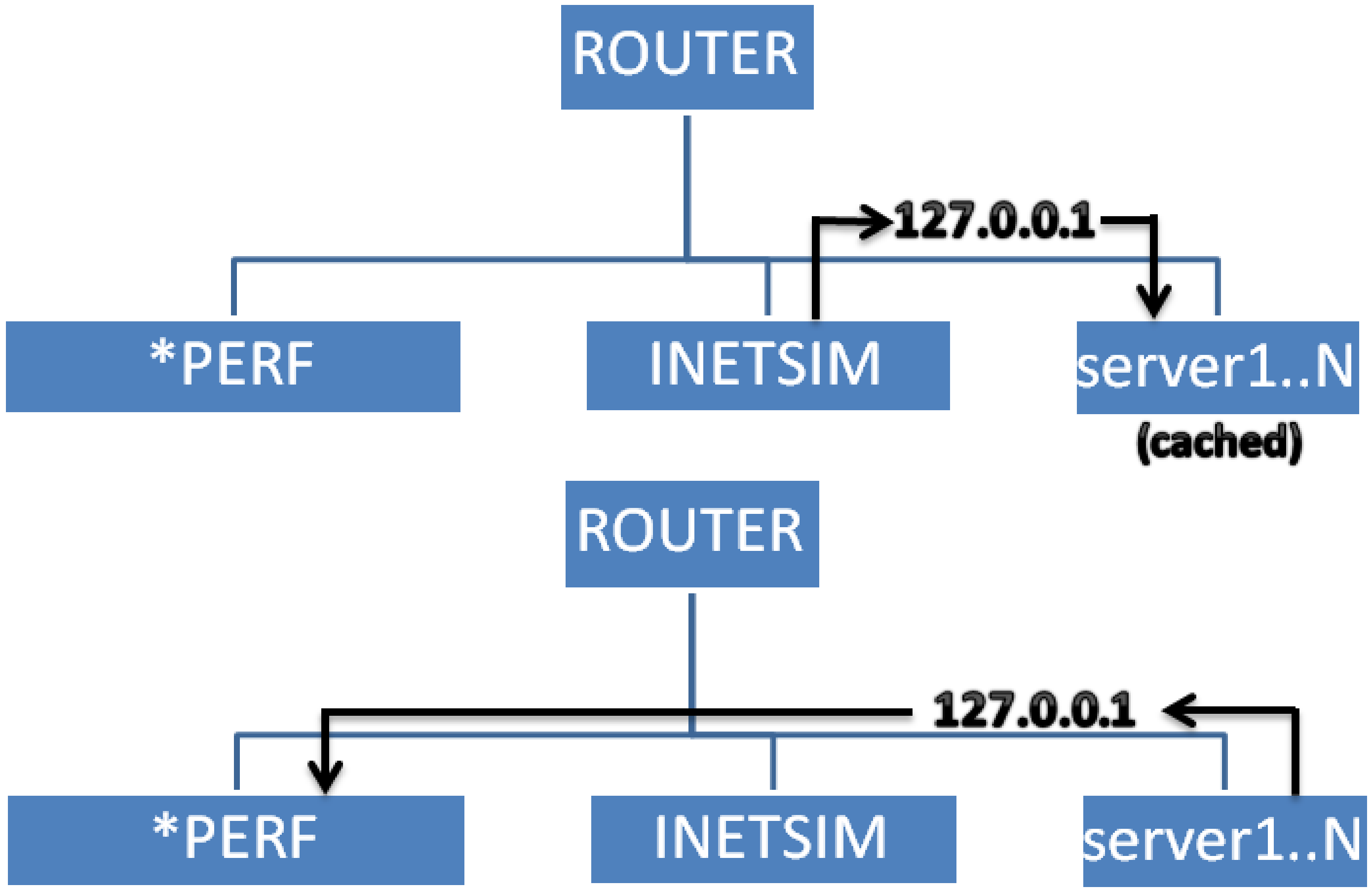
Milestone 3: Recursive server, performance comparisons (2017)



Test bed

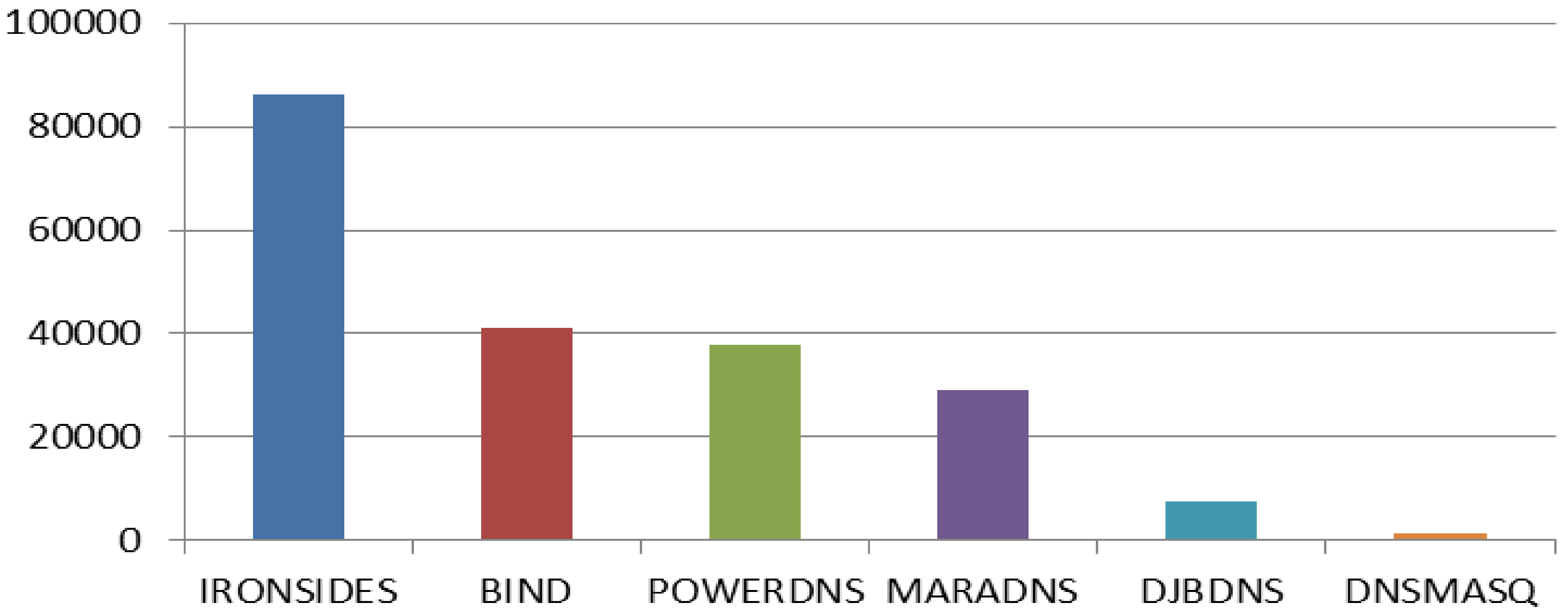

ROUTER
cnn.com?
*PERF
INETSIM
server1..N
ROUTER
cnn.com?
*PERF
INETSIM
server1..N

Test bed



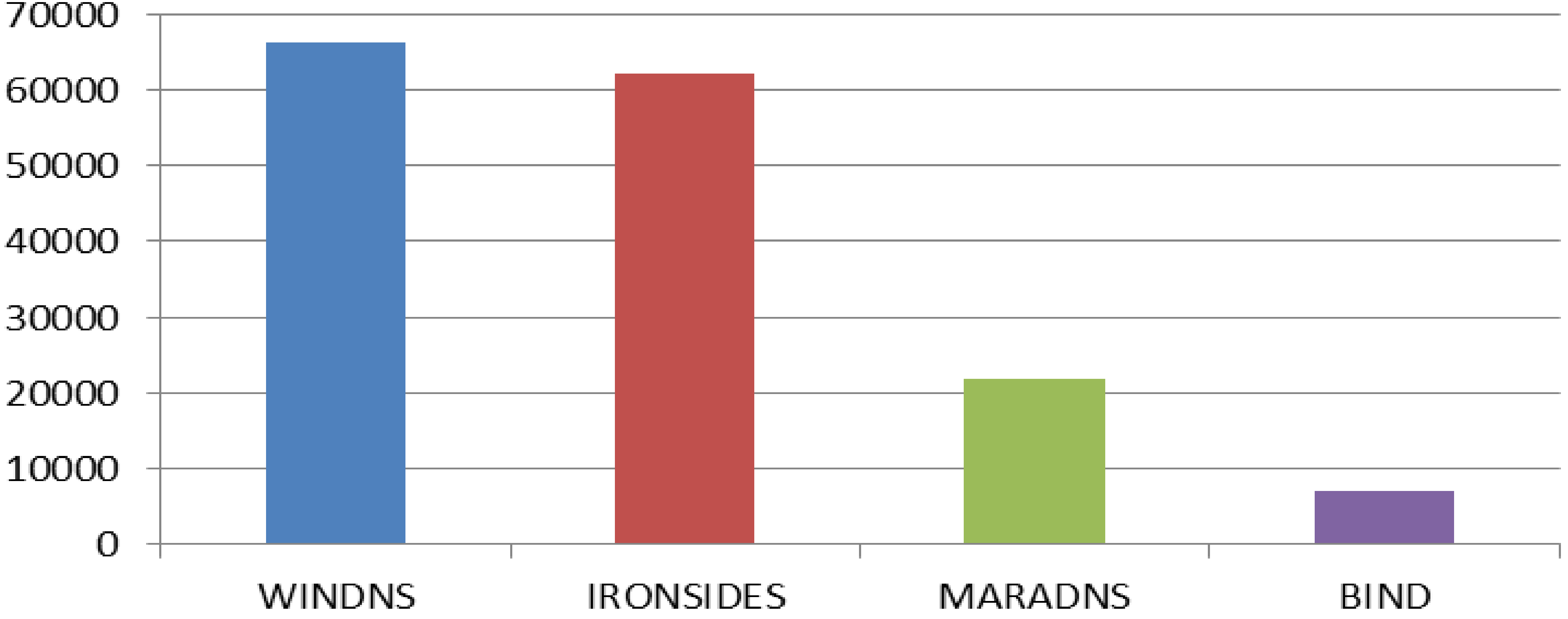
ROUTER
127.0.0.1
*PERF
INETSIM
server1..N
(cached)
ROUTER
127.0.0.1
*PERF
INETSIM
server1..N

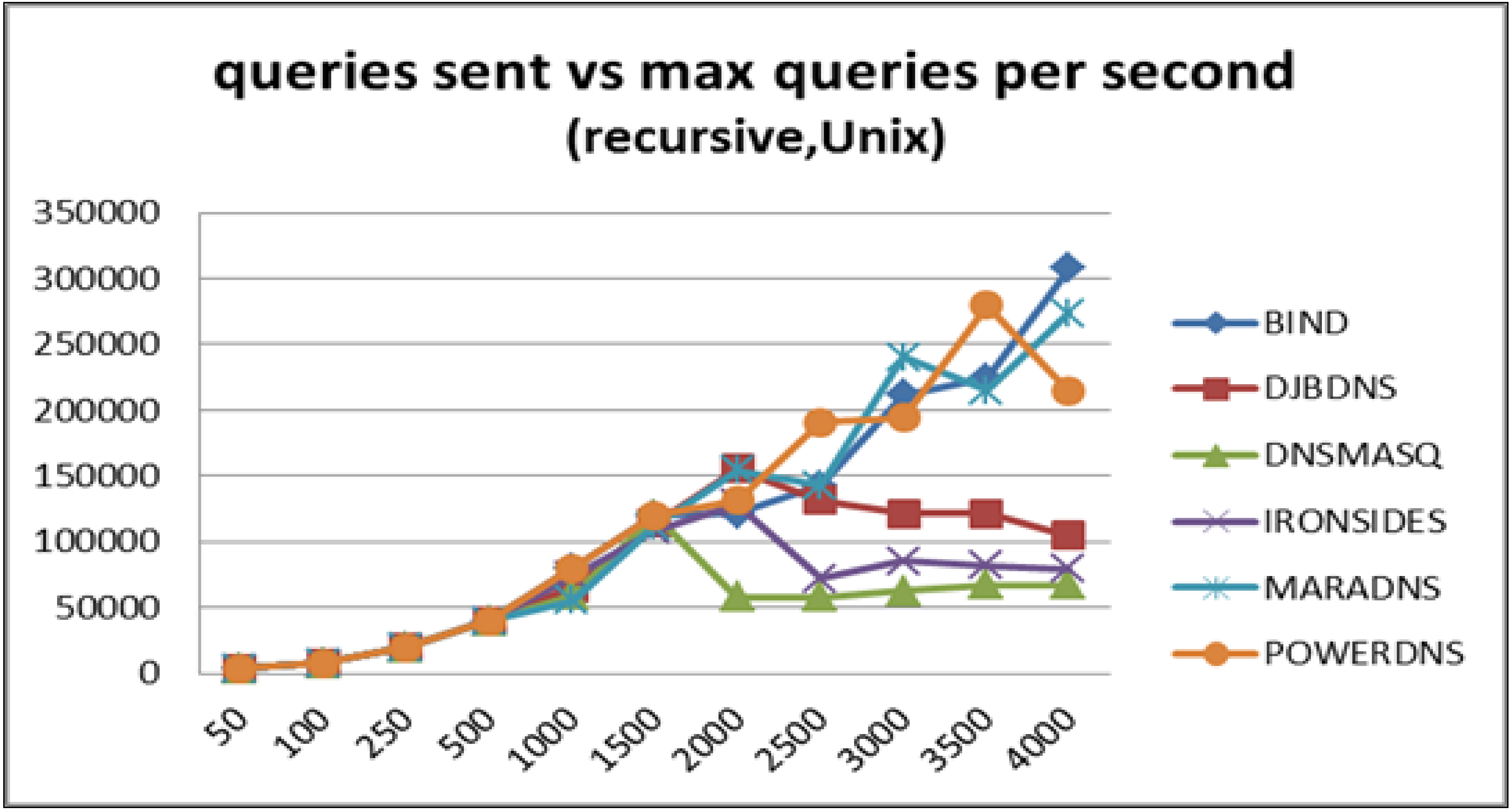
max queries per second
(authoritative, Unix)

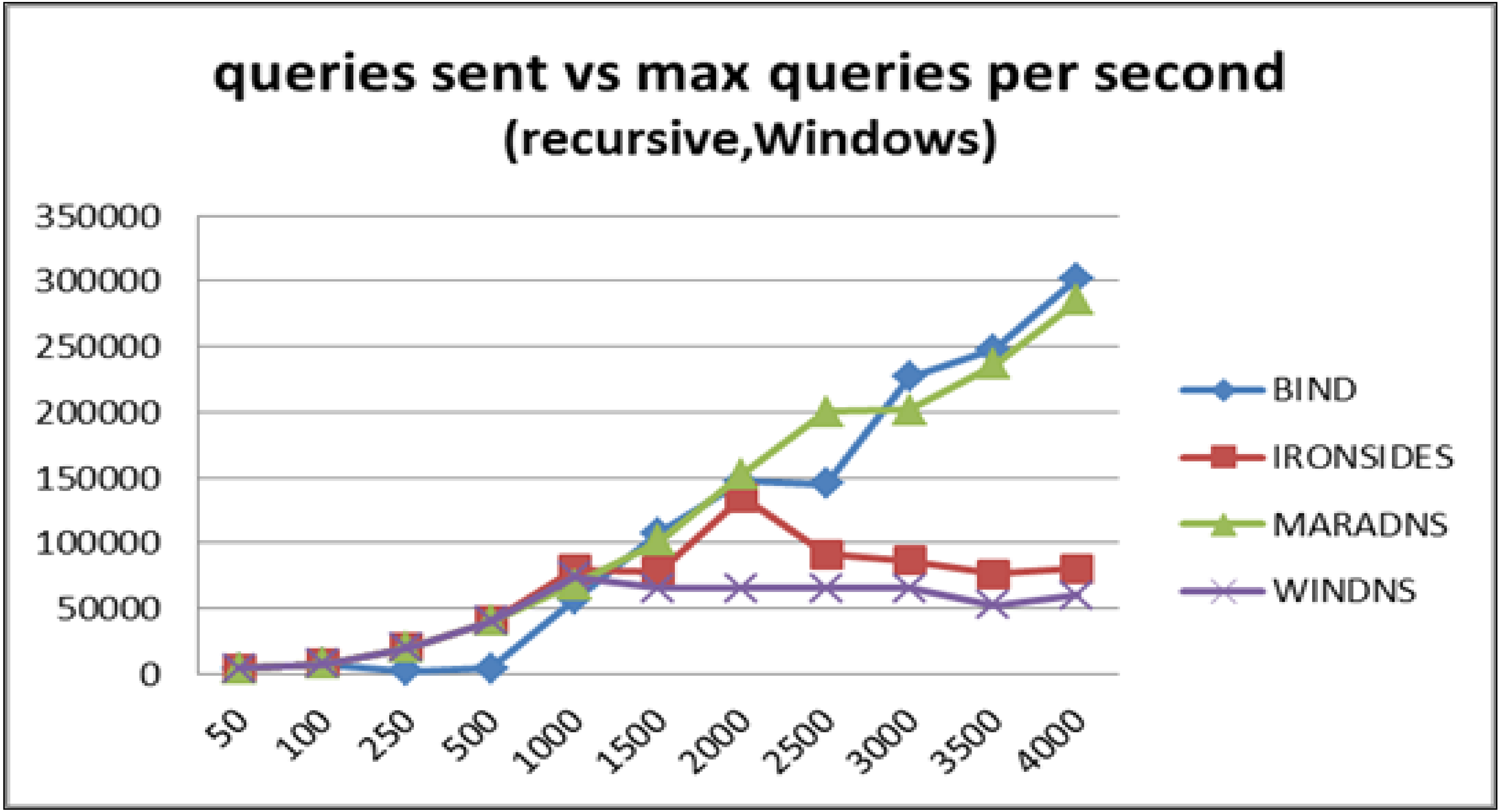


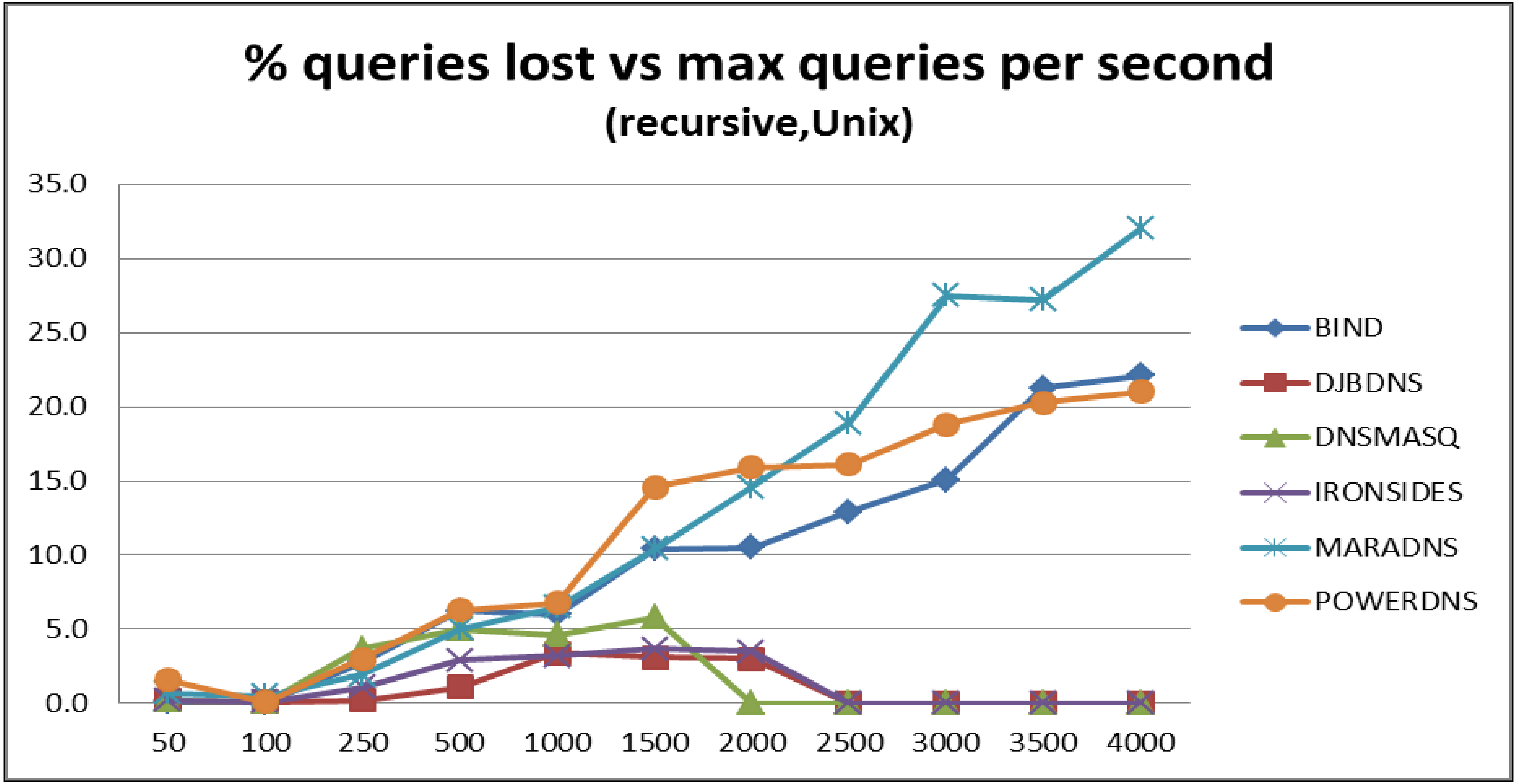
max queries per second

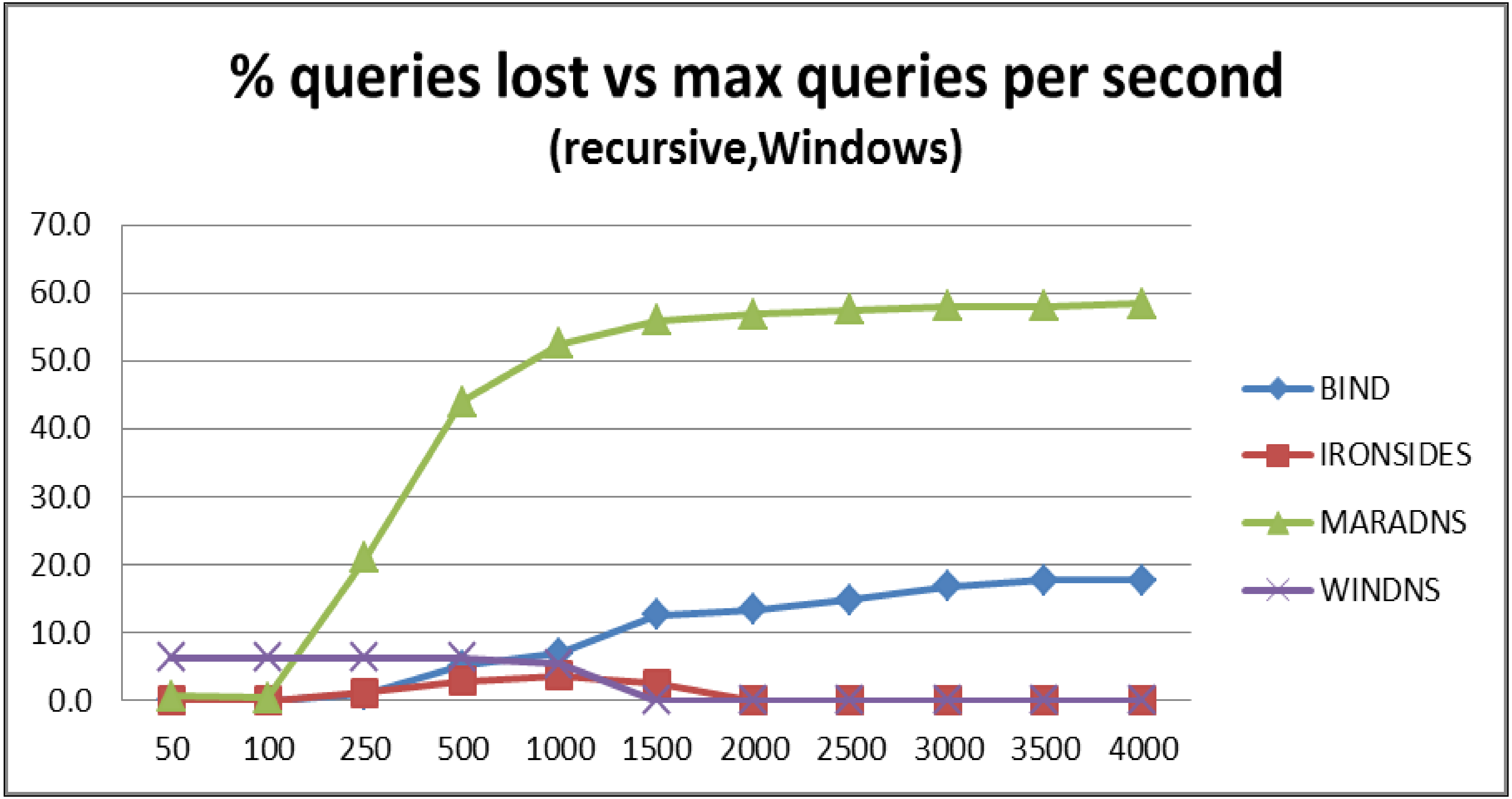
(authoritative, Windows)

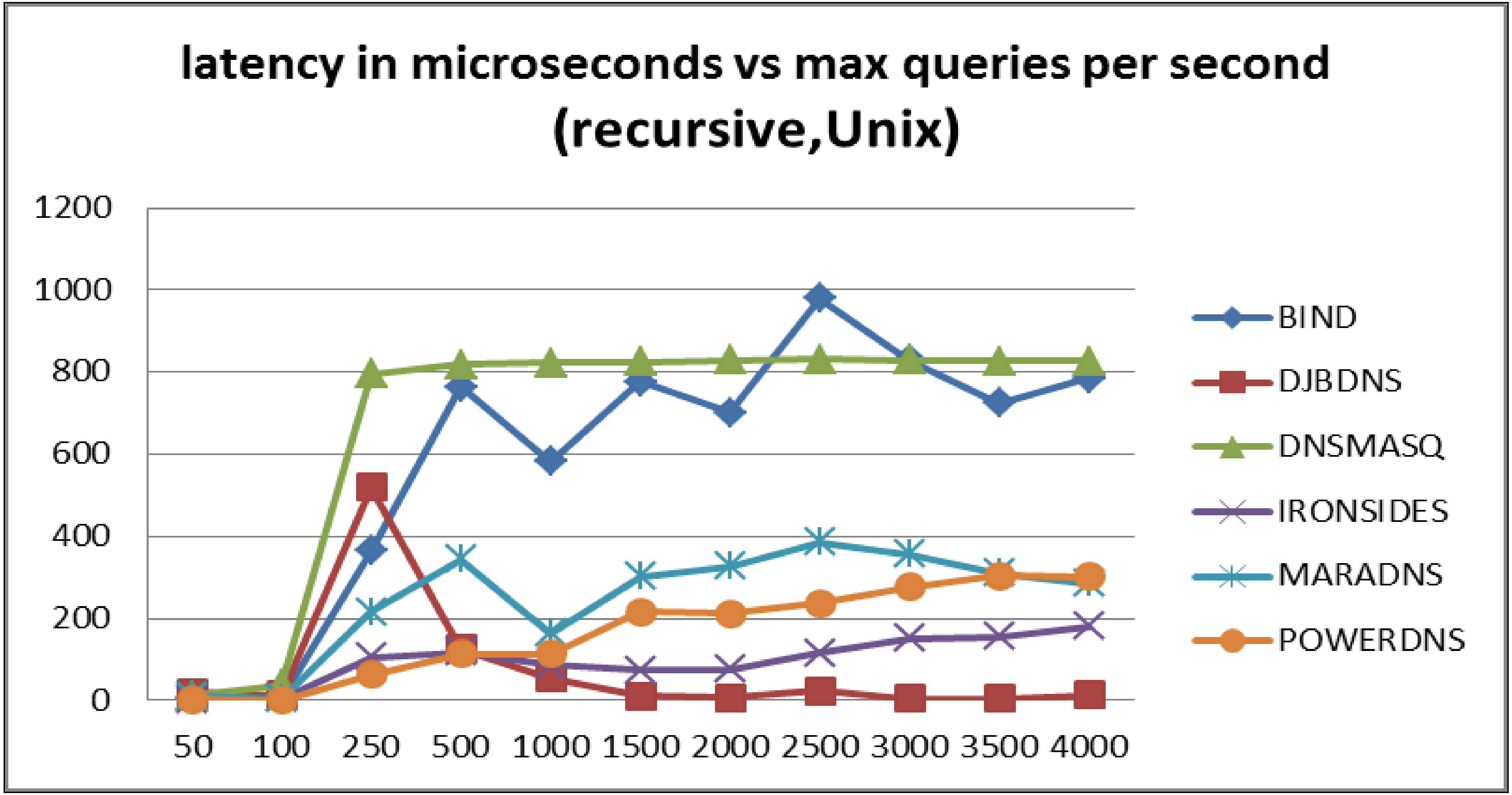


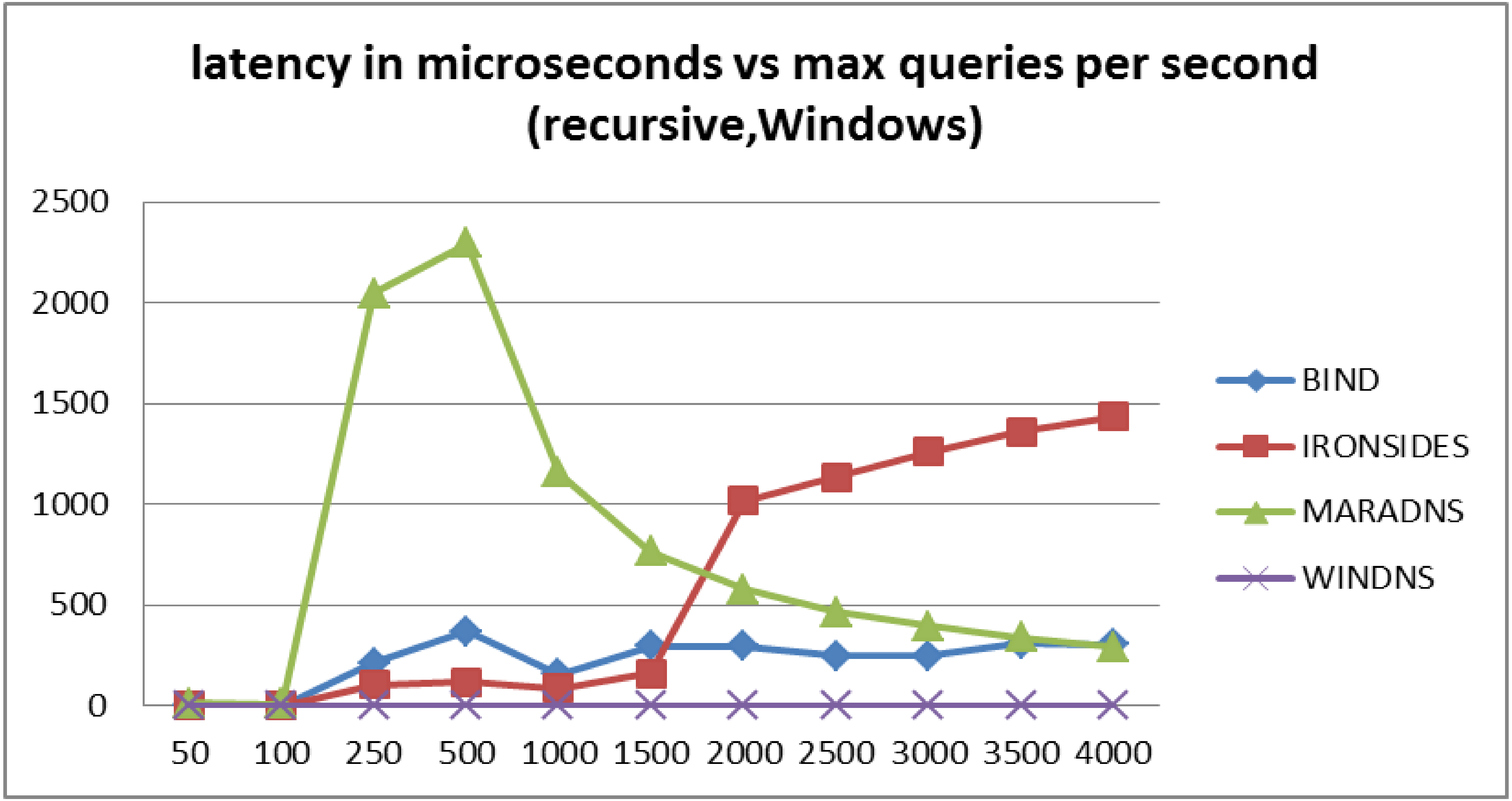

queries sent vs max queries per second
(recursive,Unix)
350000
300000
250000
200000
150000
100000
50000
0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
DJBDNS
DNSMASQ
IRONSIDES
MARADNS
POWERDNS


queries sent vs max queries per second
(recursive,Windows)
350000
300000
250000
200000
150000
100000
50000
0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
IRONSIDES
MARADNS
WINDNS


% queries lost vs max queries per second
(recursive,Unix)
35.0
30.0
25.0
20.0
15.0
10.0
5.0
0.0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
DJBDNS
DNSMASQ
IRONSIDES
MARADNS
POWERDNS


% queries lost vs max queries per second
(recursive,Windows)
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
IRONSIDES
MARADNS
WINDNS


latency in microseconds vs max queries per second (recursive,Unix)
1200
1000
800
600
400
200
0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
DJBDNS
DNSMASQ
IRONSIDES
MARADNS
POWERDNS


latency in microseconds vs max queries per second (recursive,Windows)
2500
2000
1500
1000
500
0
50
100
250
500
1000
1500
2000
2500
3000
3500
4000
BIND
IRONSIDES
MARADNS
WINDNS

Insights from experience

Performance doesn’t need to be sacrificed to improve security. In fact, there are instances where SPARK and formal methods make faster code.

Conversely, instances where SPARK requirements slow things down, must use manual overrides.

Role of compiler important!

Tools are impressive and humbling.

Provable security properties in IRONSIDES

- No classic buffer overflow
- No incorrect calculation of buffer size
- No improper initialization
- No ineffective statements
- No integer overflow/wraparound
- No information leakage
- All input validated
- No allocation w/o limits (no resource exhaustion)

Provable security properties in IRONSIDES

- No improper array indexing
- No null pointer dereferencing
- No expired pointer dereferencing (use after free)
- No type confusion
- No race conditions
- No incorrect conversions
- No uncontrolled format strings
- All loops guaranteed to terminate

Conclusions

- Comparable performance
- Far fewer resources, lower development costs
- Why similar approaches not more widely adopted?
- Upgrade IRONSIDES to more current version of SPARK
- Develop web server with similar properties
- Formal methods and SCADA, performance