Options for PTP Security

Doug Arnold, Meinberg-USA

ITSF 2015, Edinburgh UK

Robustness and Options for PTP Security

Doug Arnold, Meinberg-USA

ITSF 2015, Edinburgh UK

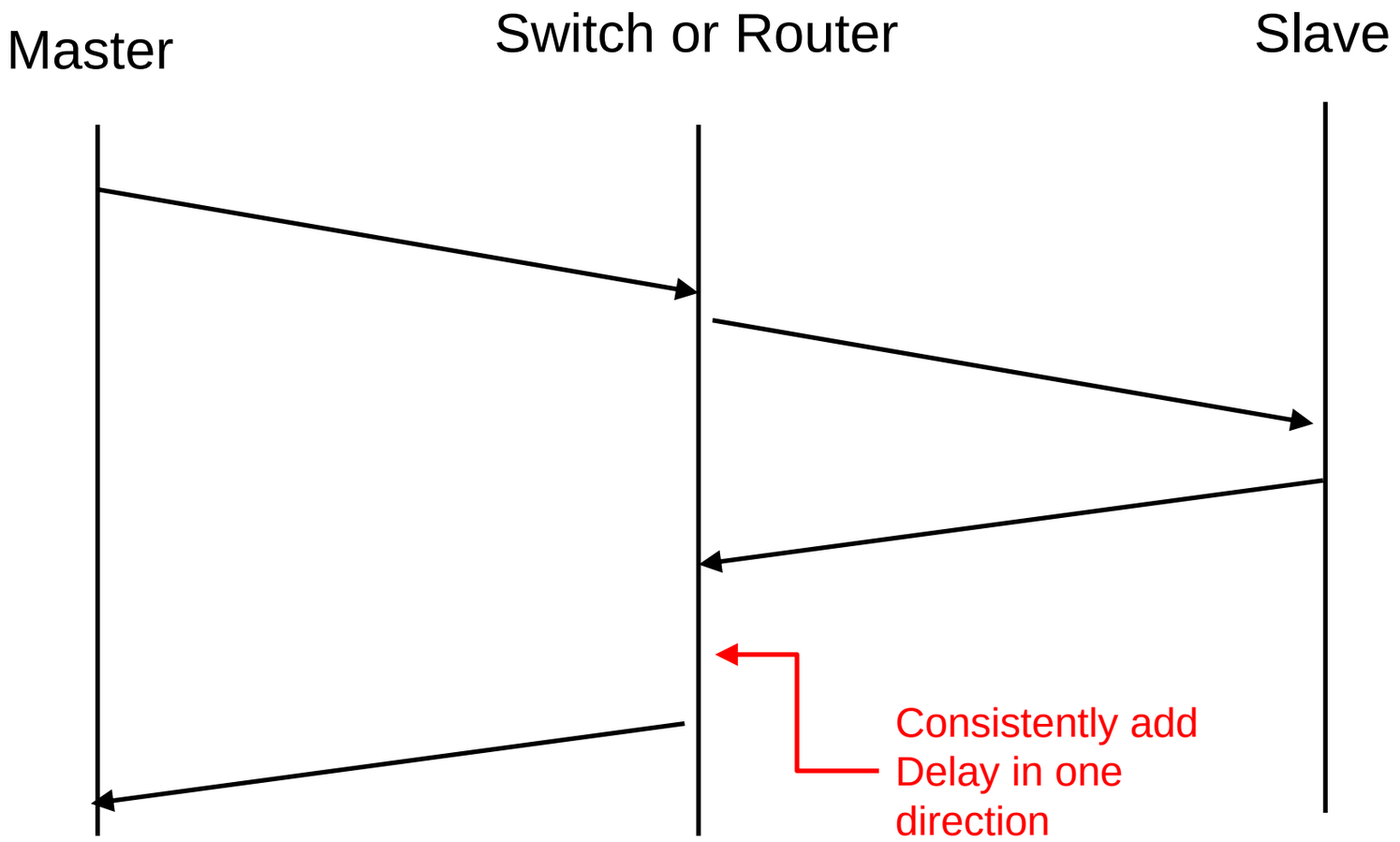
Agenda

1. Time and Security
2. A Weakness in PTP
3. Solutions and limitations
4. Conclusions

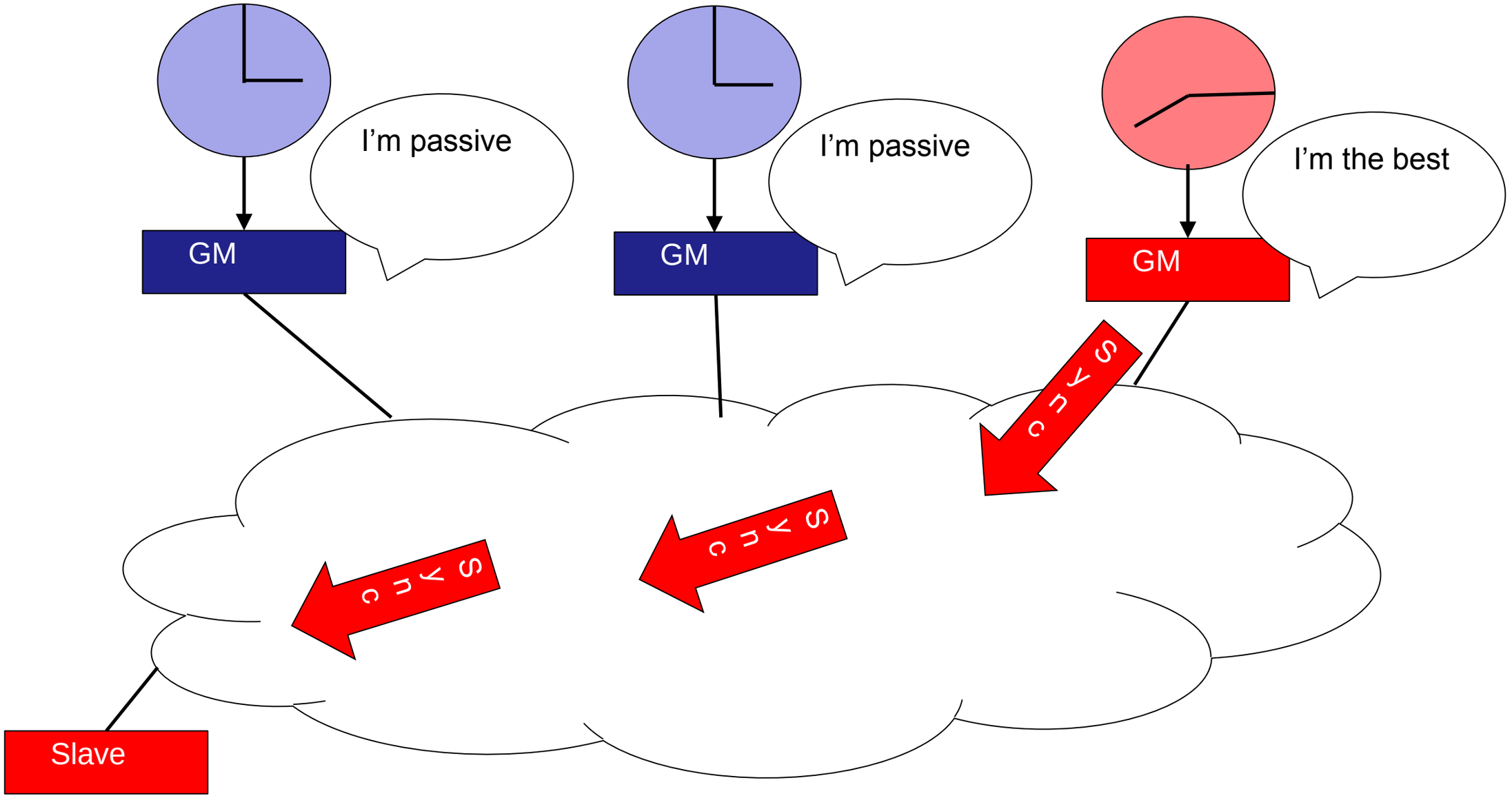
Time and Security

- Time and frequency are not data!
  - Time is not secret
  - Time is not stored in an archive
  - Encryption unimportant
- Time from multiple sources which are slightly different is useful
  - Not usually true of data
- Standard network security mechanism assume time is already distributed to all nodes

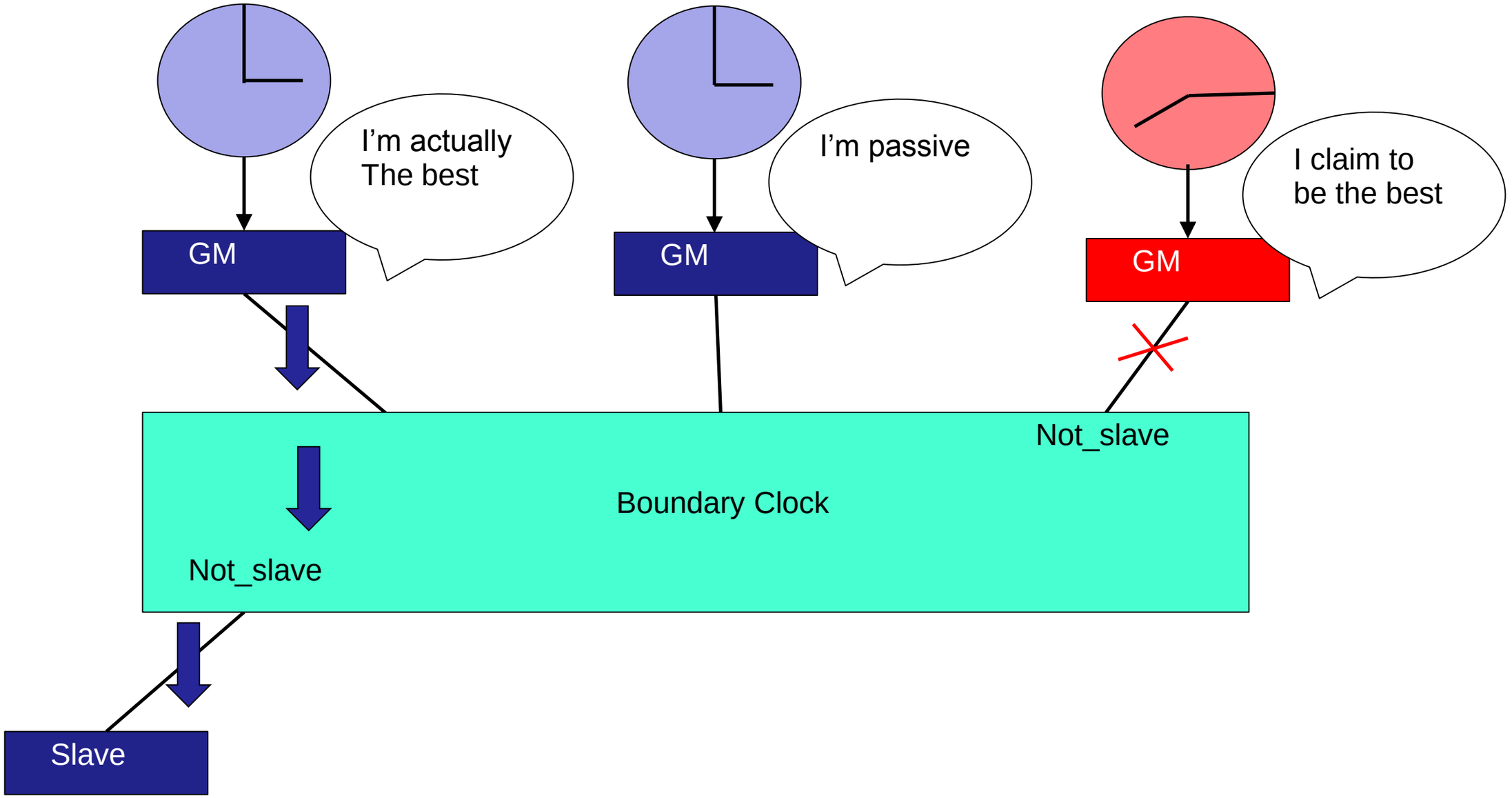
Delay attack



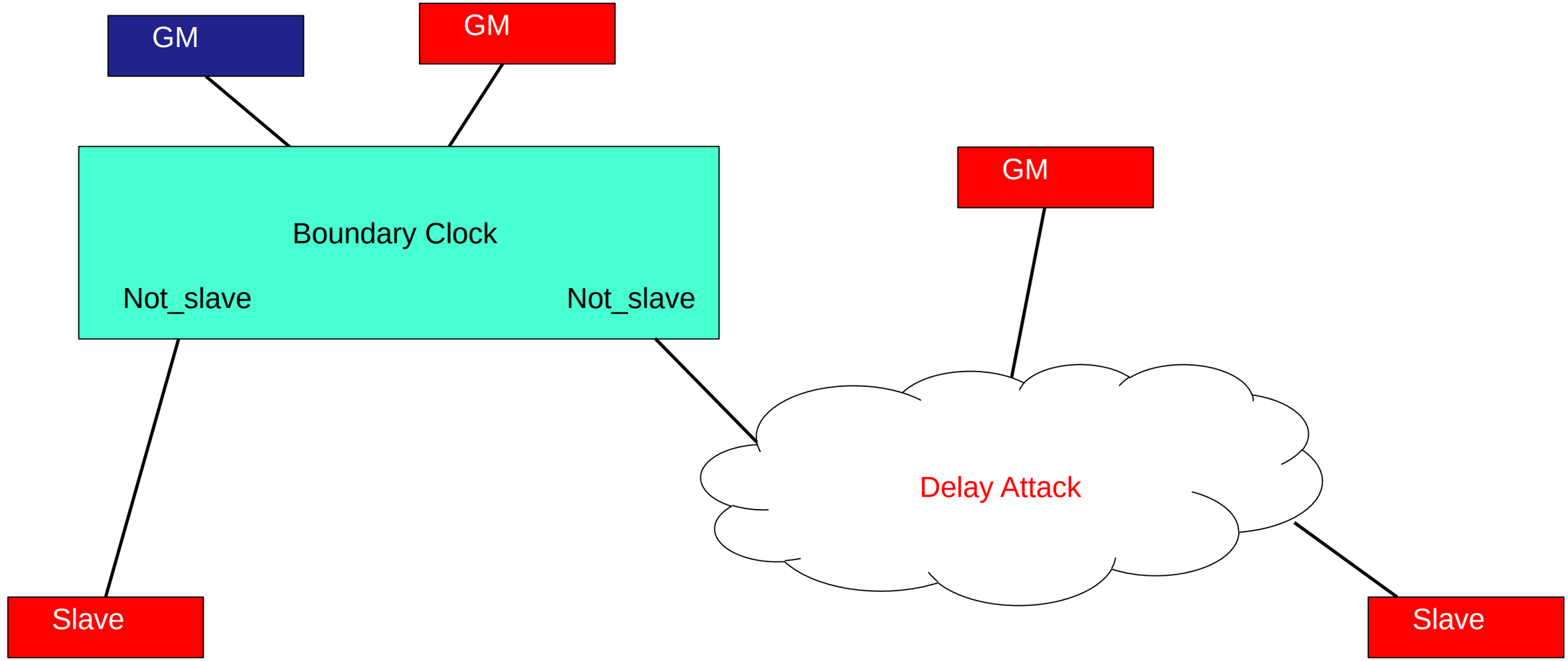
BMCA: A Single Point of Failure!



Solution: BC Not_slave port



BC Not_slave port limitations

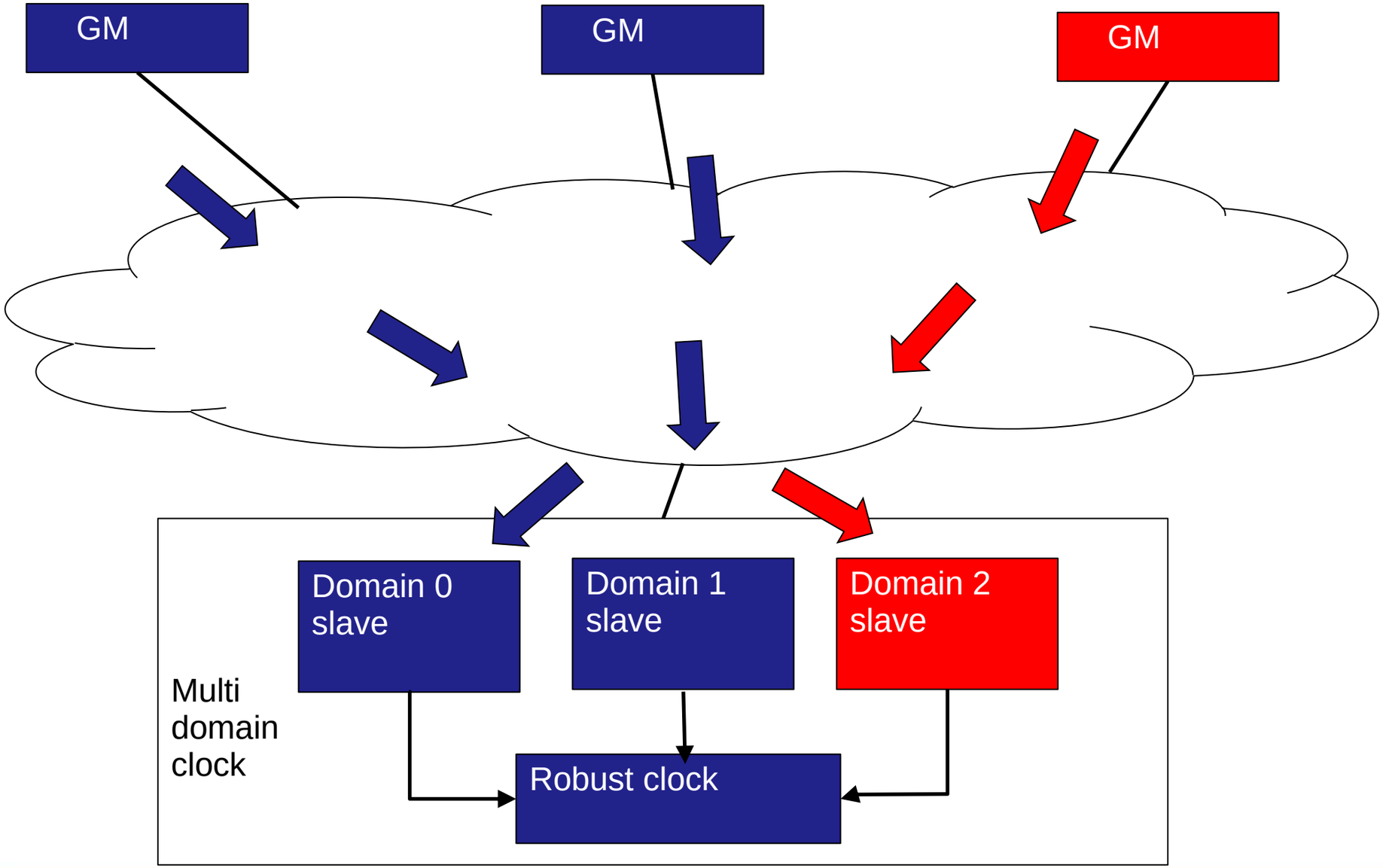


Partial Assisted GPS BC

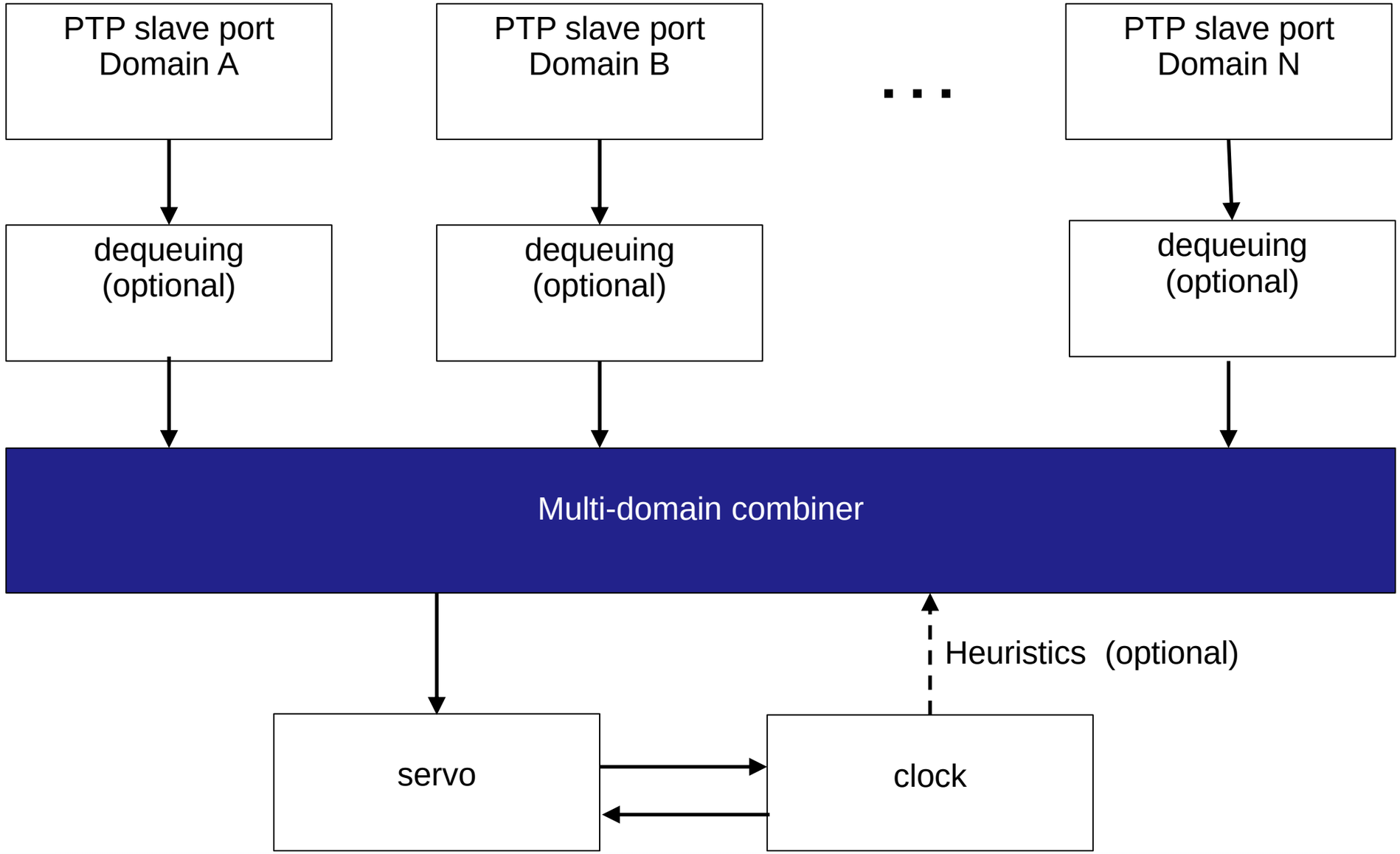
- Compare GPS and (asymmetry corrected) PTP
  - Could identify PTP ramp, step errors due to bad GM

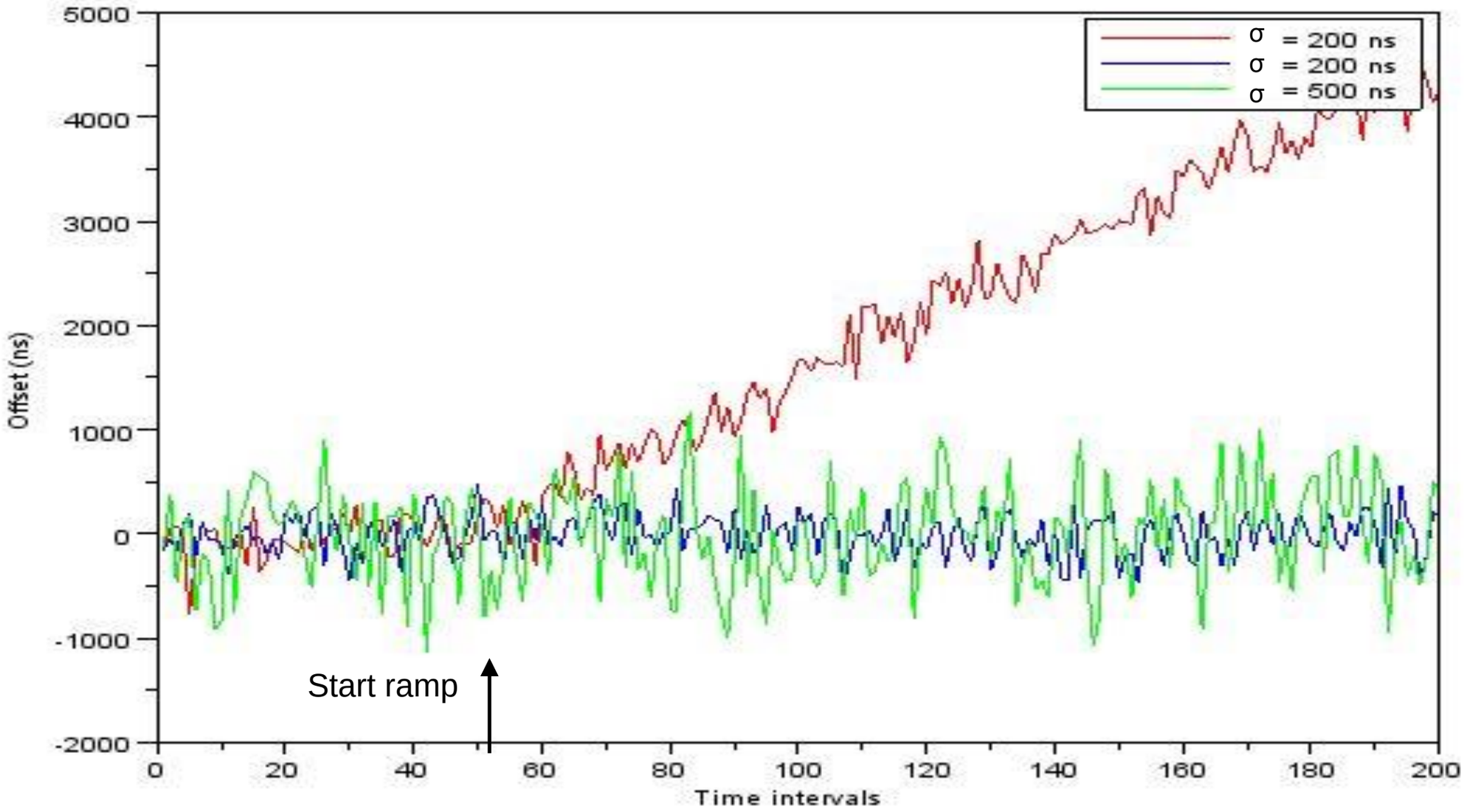
- Vulnerabilities
  - GPS Jamming
  - Spoofing
  - GPS jamming/spoofing combined with bad GM
  - Does not protect against bad GM inserted downstream

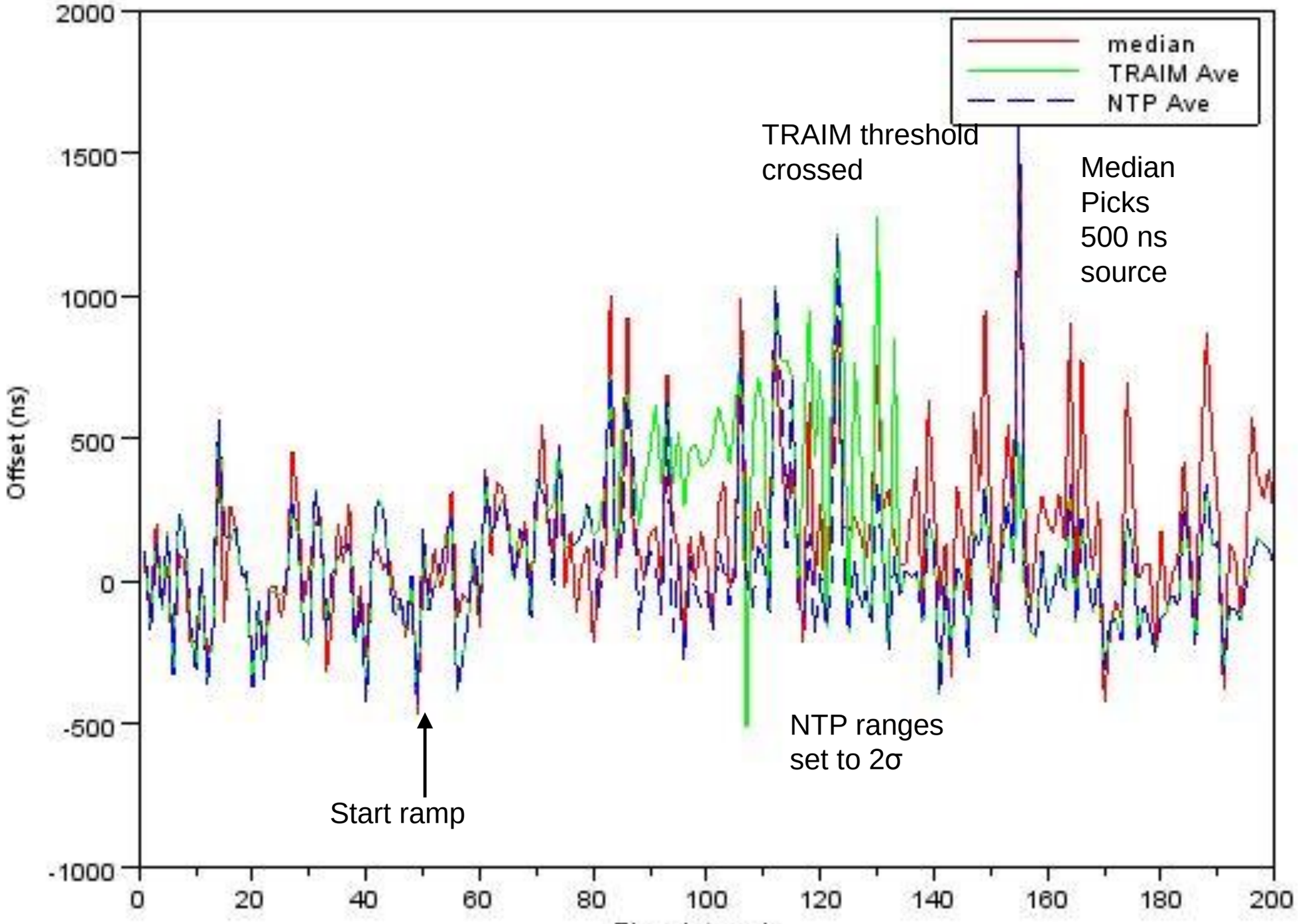
Proposal in IEEE 1588 Working Group



Robust Clock




σ = 200 ns
σ = 200 ns
σ = 500 ns
Offset (ns)
5000
4000
3000
2000
1000
0
-1000
-2000
0
20
40
60
80
100
120
140
160
180
200
Time intervals
Start ramp


median
TRAIM Ave
NTP Ave
TRAIM threshold crossed
Median Picks 500 ns source
NTP ranges set to 2σ
Start ramp
Offset (ns)
2000
1500
1000
500
0
-500
-1000
0
20
40
60
80
100
120
140
160
180
200

Defeating Multi-master PTP

- Multicast:
  - Inject announce and sync from False PTP master in every domain
- Unicast:
  - Capture a switch
  - Alter sync messages or impersonate GMs
- Solution:
  - Authenticate messages from masters cryptographically

Under discussion in 1588 WG

- External Security mechanisms
  - PTP over IPsec
  - PTP over MACsec
- Monitoring of sync “quality” throughout network
  - PTP nodes report standard metrics
  - Management node can detect anomalies
- Security TLV:
  - Append to all messages from master
  - Hash code for message integrity checking and master verification

Network Time Security with TESLA

- Under development in IETF for NTP
  - Similar solution for PTP expected in P1588
- Security robustness of asymmetric key cryptography
- Computational efficiency of symmetric key cryptography
- Keys are distributed after they are no longer valid
  - Slaves hold PTP messages and authenticate when key is received
  - Slaves must be able to coast until key distributed
- Warning: cryptography can’t stop delay attacks!

Conclusion: What should we do?

- Things you can do now:
  - Use BCs with not_slave ports configured
  - Compare GPS and PTP from other masters
- Future development
  - Monitoring PTP metrics in the network
  - Multi-master PTP
  - Cryptography – master authentication, message integrity checking
- Combine cryptography with multiple time sources

Thank you for your attention

Doug Arnold

doug.arnold@meinberg-usa.com

+1-707-303-5559