AALBORG UNIVERSITY
DENMARK

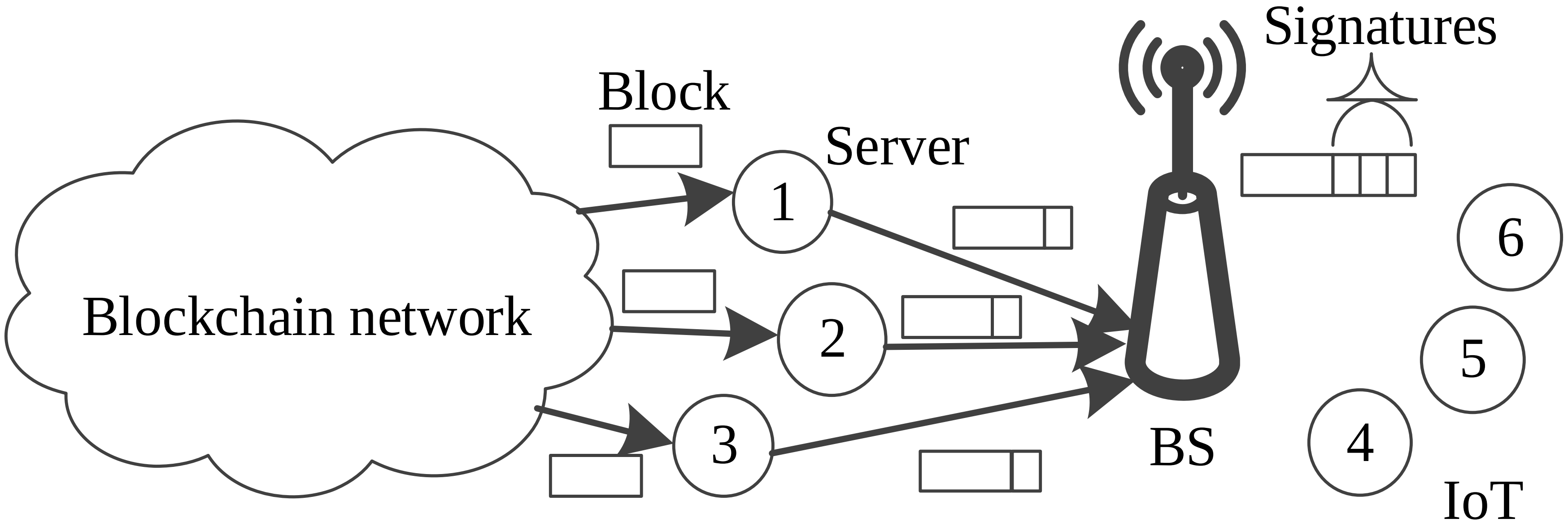
Repeat-Authenticate Scheme for Multicasting of Blockchain Information in IoT Systems

Pietro Danzi, **Anders E. Kalør**, Čedomir Stefanović, Petar Popovski
Aalborg University, Denmark

IEEE GLOBECOM Workshop on Blockchain for Telecommunications
December 2019
Waikoloa, HI, USA

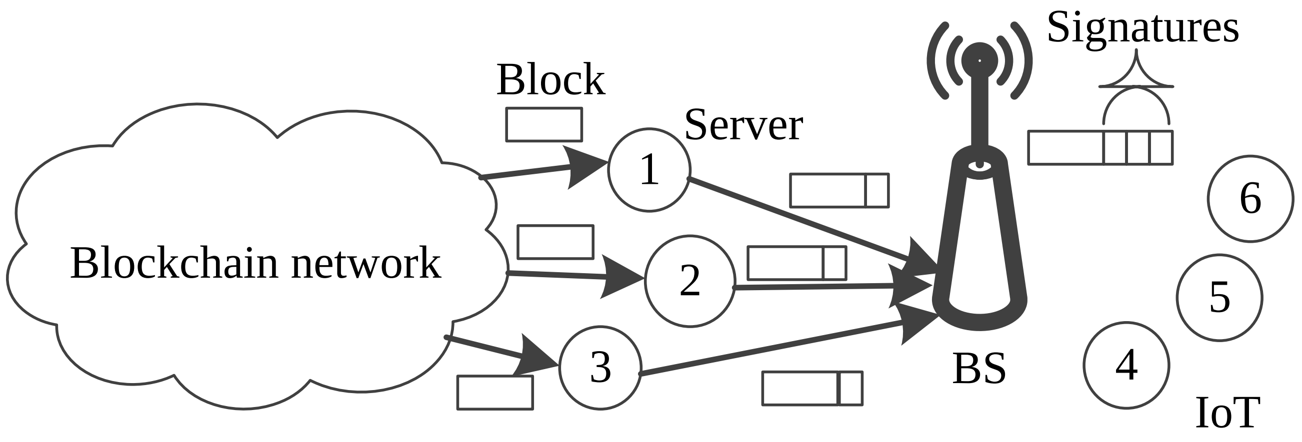
General Scenario: Light Clients

- IoT devices want to receive block headers from a global blockchain
- Devices trust a subset of the servers in the blockchain network
  - The IoT devices need signatures from trusted servers
- Base station aggregates blocks and signatures

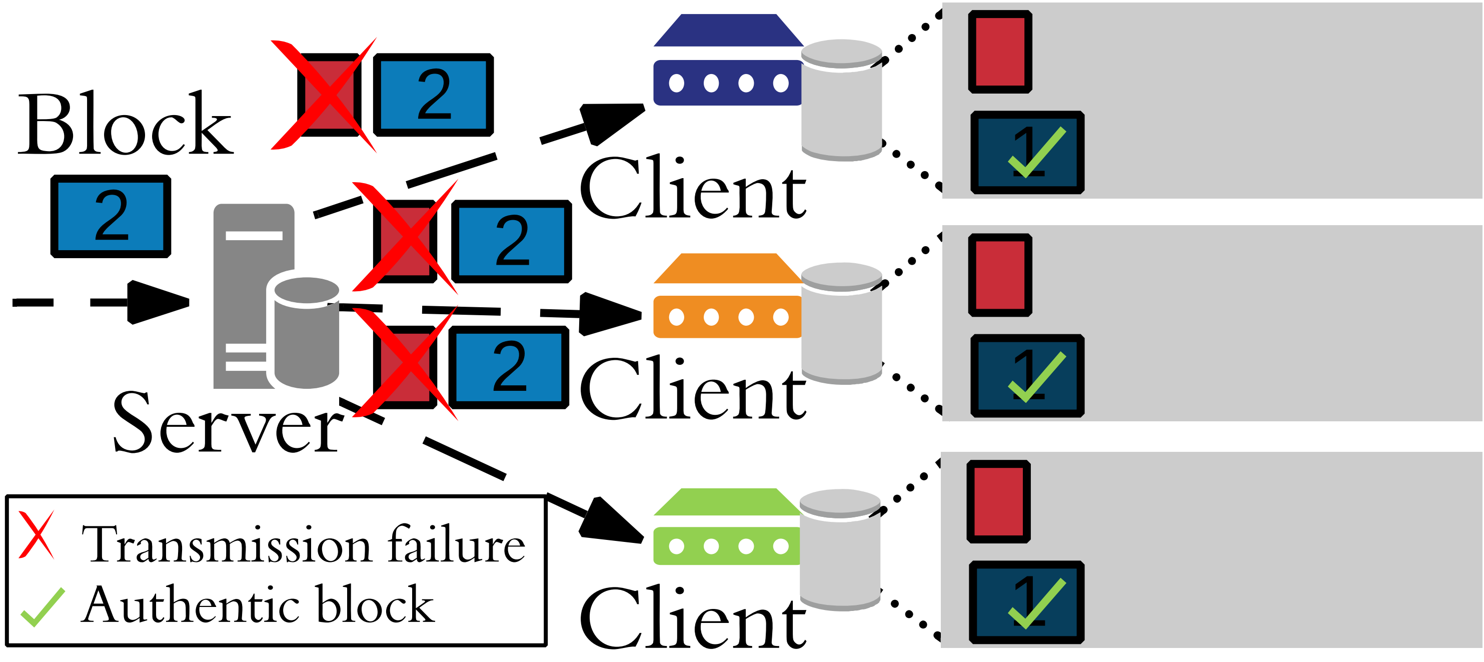


Motivation

- IoT devices are communication constrained (LoRaWAN, Sigfox, etc.)
- Exploit broadcast nature of wireless channel:
  - Most of the information to the IoT devices is the same (block headers)
  - Signatures are different

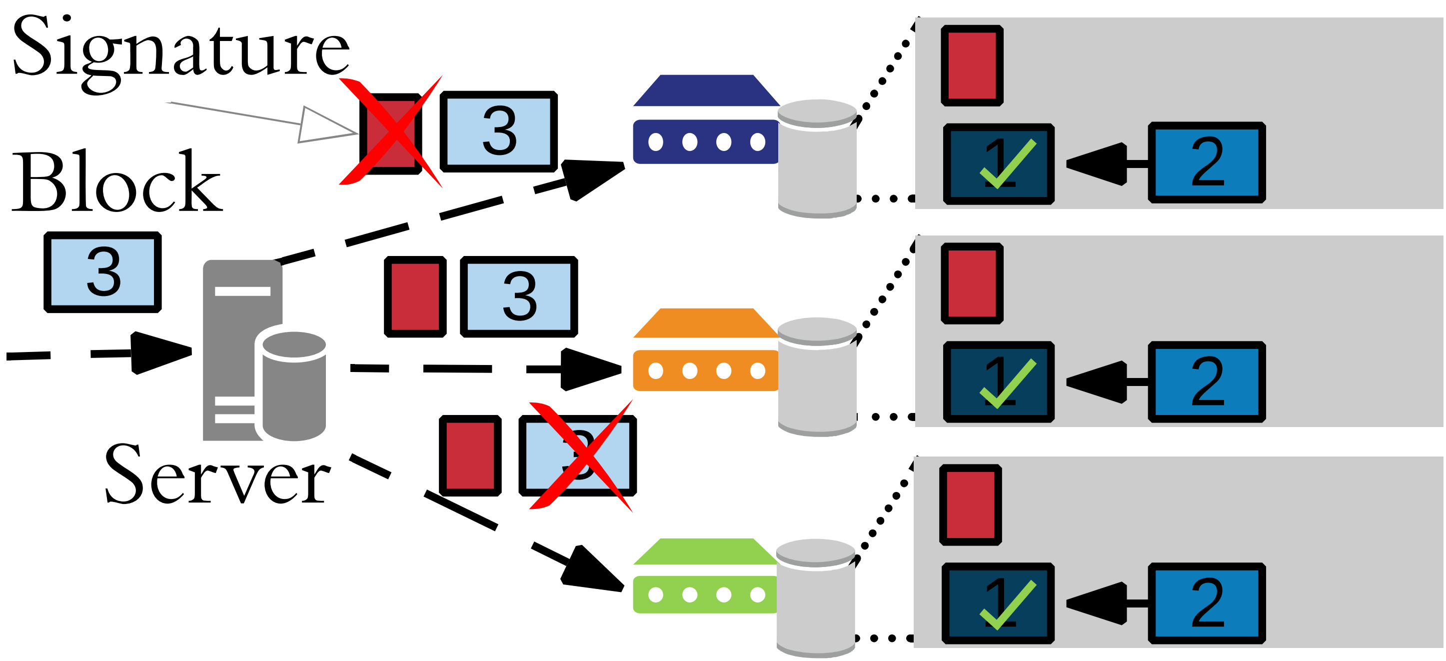


Motivating Example



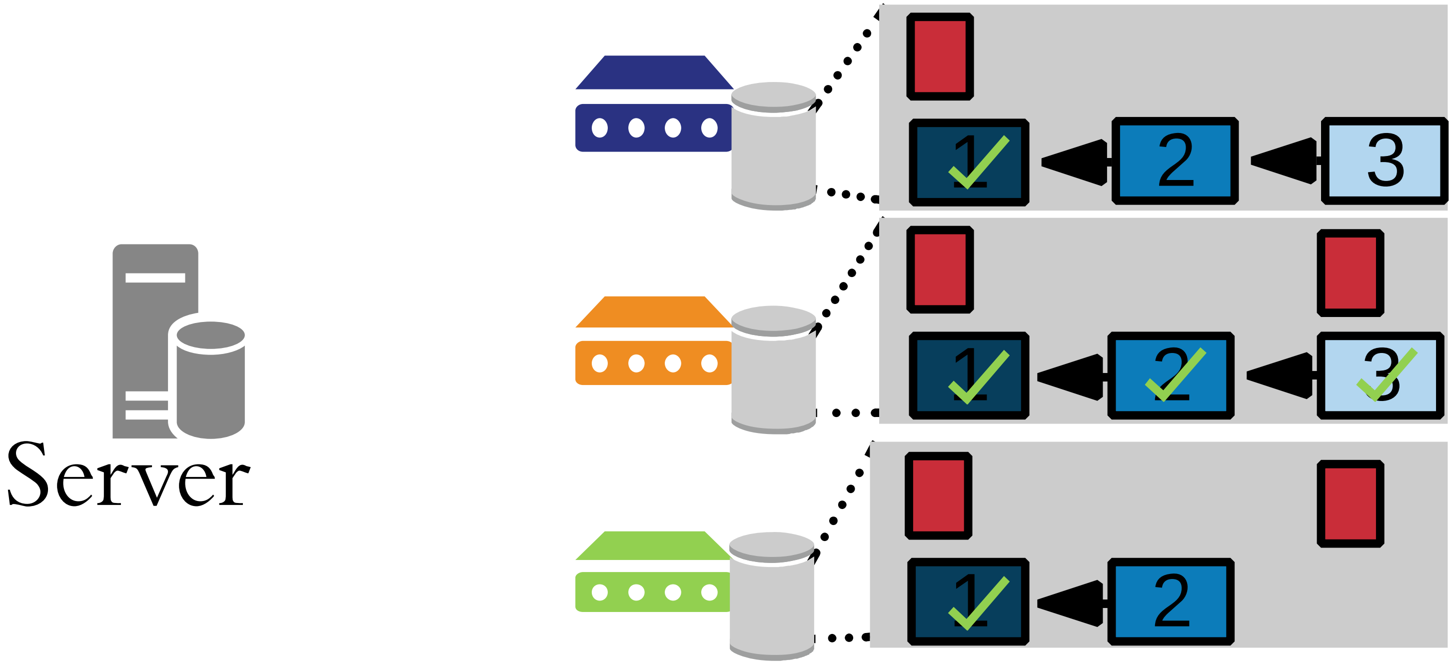
- Clients are initially synchronized
- Signature transmissions fail for block 2

Motivating Example



- Signature transmission fails again for blue client
- Block header transmission fails for green client

Motivating Example



- Blue and green clients are synchronized to block 1
- Orange client is synchronized to block 3 (by *signature amortization*)

Reveals tradeoff between transmission of blocks and signatures

System Model

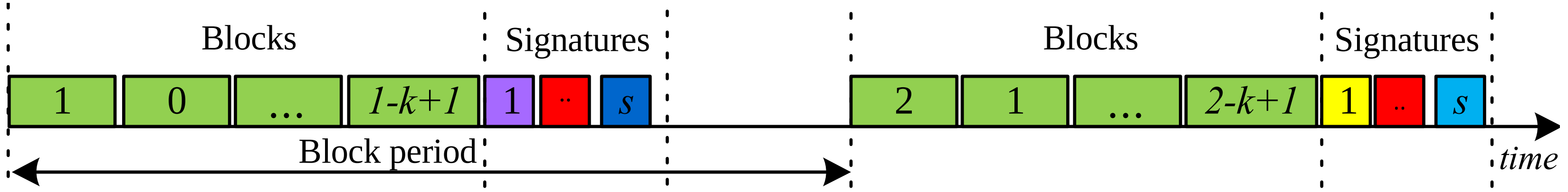
- *V* servers, *U* clients
- Each client trusts a subset of the servers
- No forks (achieved by delaying transmissions)
- Devices can tolerate a delay of at most *d* blocks
  - If more than *d* blocks are missing the device requests reliable unicast transmission of missing blocks
- Bit error with probability P_{bit} (fixed rate transmission)

Repeat-Authenticate Scheme

- BS multicasts packets containing:
  - *k* most recent blocks (each of size l_b bits)
  - *s* signatures (each of size l_s bits)
- Packets have fixed length b bits, so large *k* implies small *s*

$$s = \left\lfloor \frac{b - k\, l_b}{l_s} \right\rfloor$$

- Signatures are chosen uniformly at random among V servers

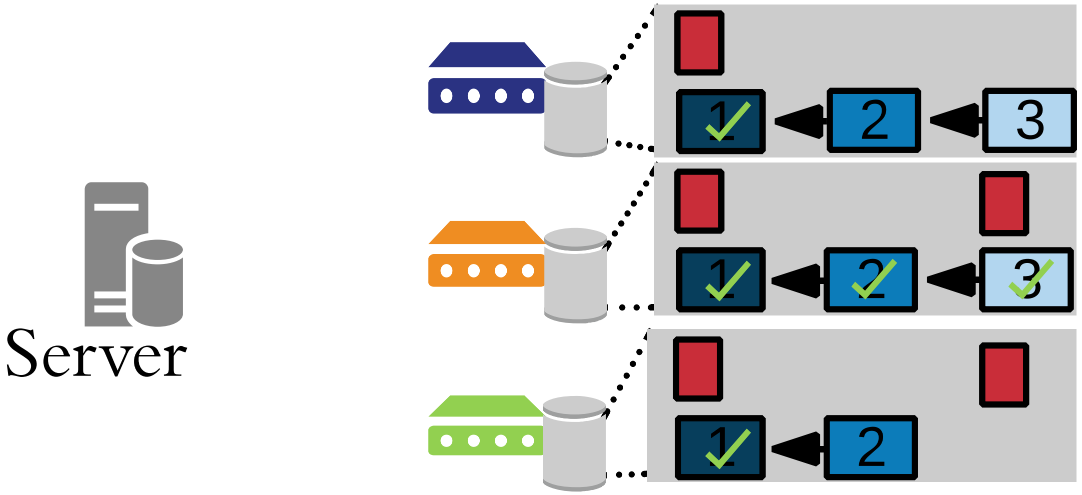


Analysis Methodology

We are interested in how often the devices need to request unicast transmission, i.e. their block delay exceeds *d*

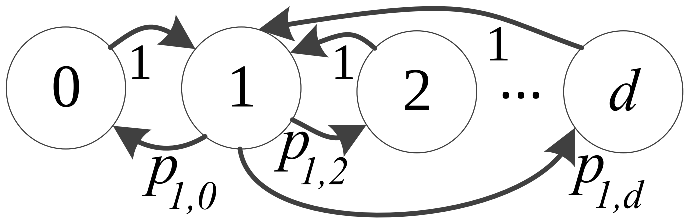
Recall that a block is successfully authenticated if either:

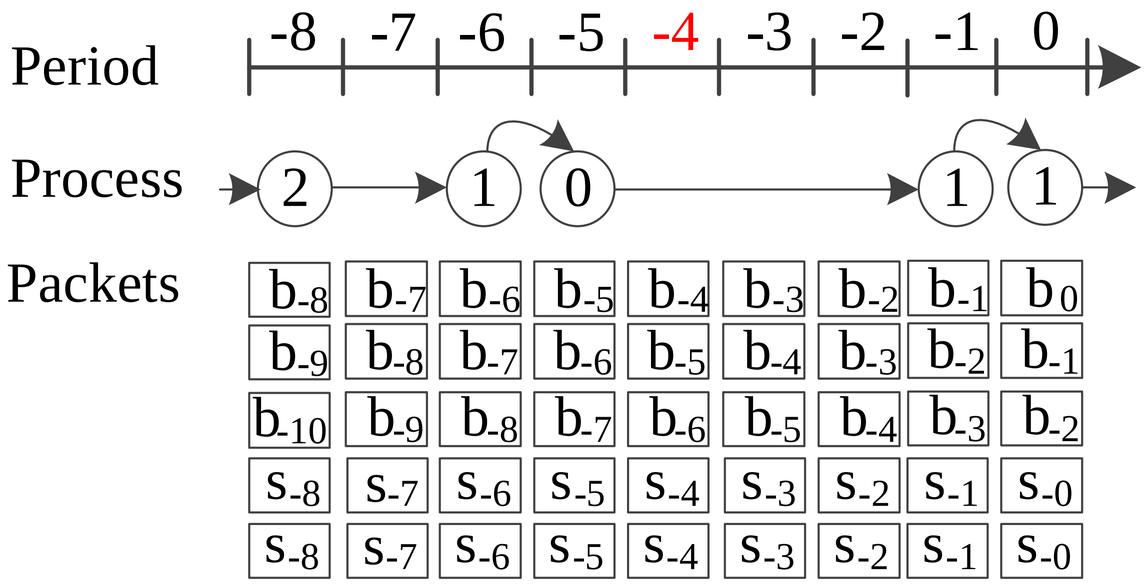
- The block and its signature is received from a trusted server
- The block is received without signature, but blocks and signatures of more recent blocks have been received (without disconnecting in the chain)



Markov Chain Analysis

- Indexed by time instances at which there is potential failure
- State represents the oldest signed block chained to the most recent block
- Unicast transmission are requested in state 0

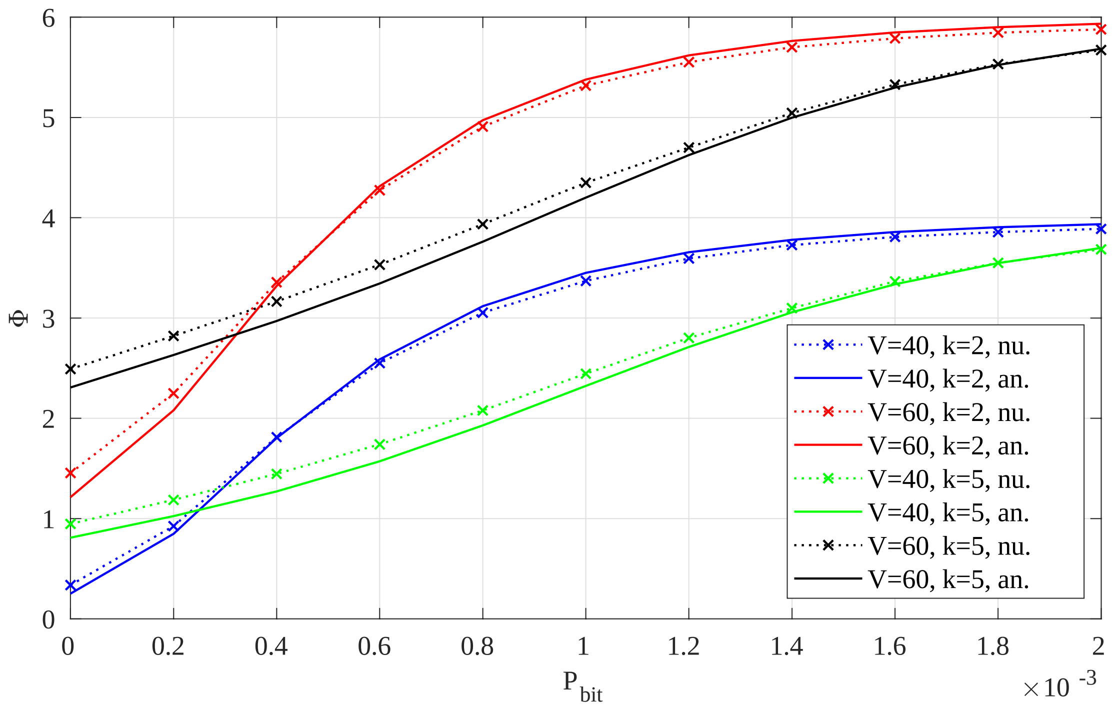




Results (Markov Chain Analysis)

Average number of users that fail (i.e. must request unicast tx)

Scenario: Each server is trusted by exactly one client



Small P_{bit} → better to transmit many blocks

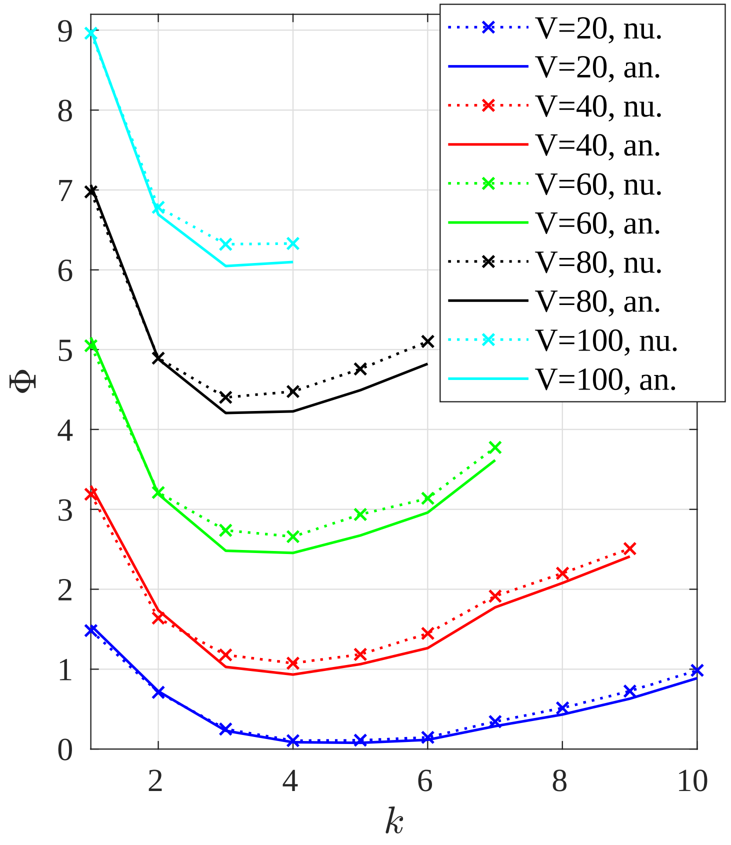
Large P_{bit} → better to transmit many signatures

Block size: 640 bits (Bitcoin)

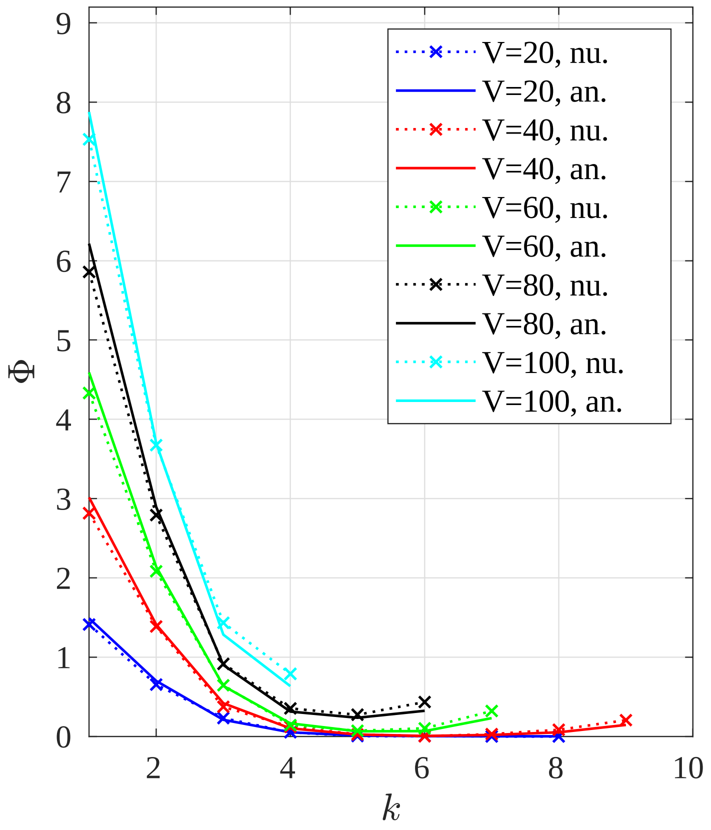
Signature size: 512 bits

Results (Markov Chain Analysis)

Each client trusts one server



Each client trusts five server



Block size: 640 bits (Bitcoin)

Signature size: 512 bits

Conclusions

- Separation of block headers and signatures is a promising strategy for transmission over wireless channels
- Tradeoff between transmission of block headers and signatures
- Future work:
  - Studying the tradeoff for blockchains with dissimilar block header and signature sizes
  - Exploring more advanced coding schemes

AALBORG UNIVERSITY
DENMARK

Thank you!