Multipath TCP improvements

Q. De Coninck, M. Jadin, O. Bonaventure
UCLouvain

Agenda

- Improving Multipath TCP on smartphones
- Multipath TCP Secure

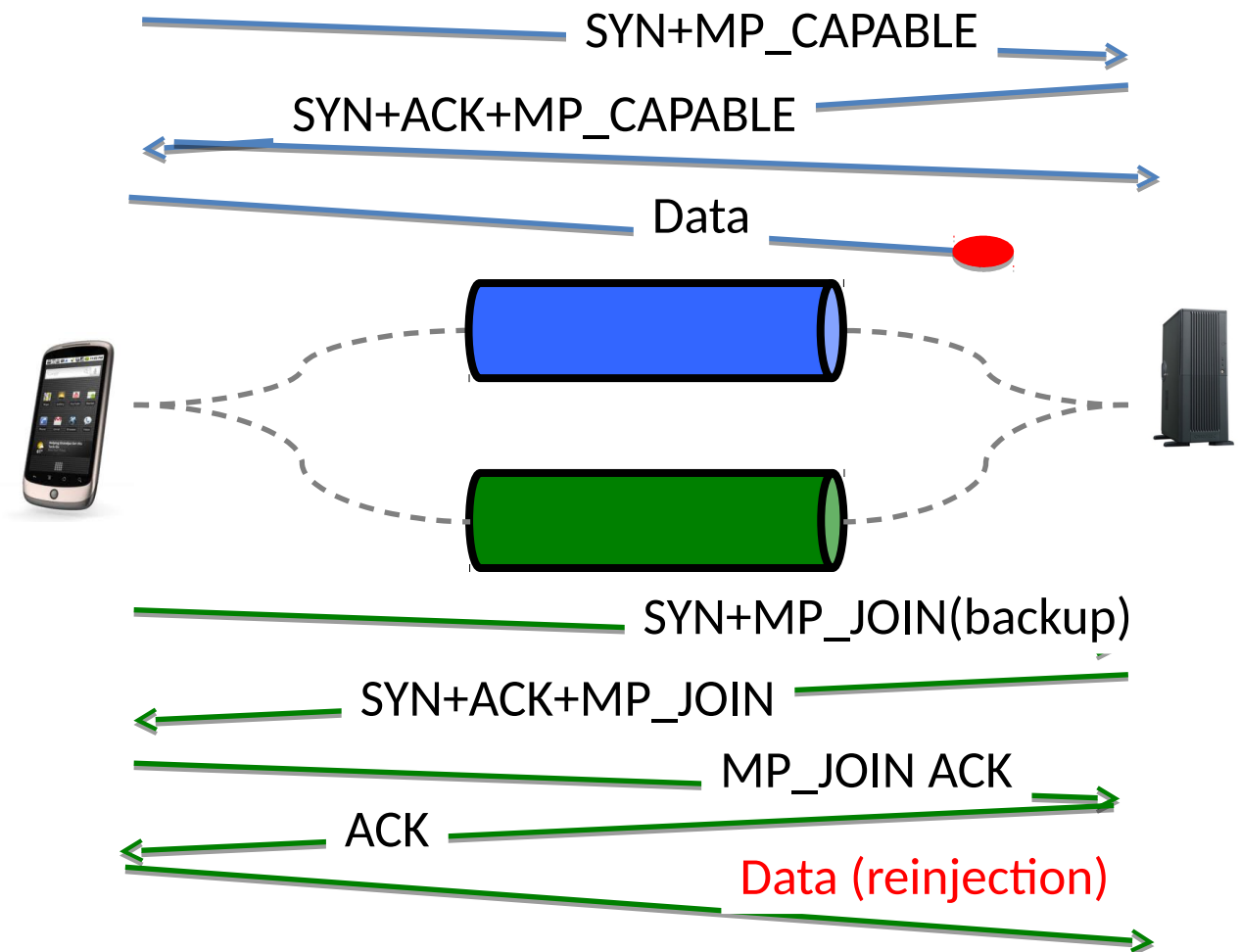
Multipath TCP on smartphones

- What are the benefits of using Multipath TCP on smartphones ?
  - Higher bandwidth by bonding WiFi and LTE
    - Very few applications require this feature

      See Q. De Coninck et al., A First Analysis of Multipath TCP on Smartphones, PAM2016, https://inl.info.ucl.ac.be/publications/first-analysis-multipath-tcp-smartphones
  - Faster handovers between WiFi and LTE
    - This is the main reason why Siri uses Multipath TCP

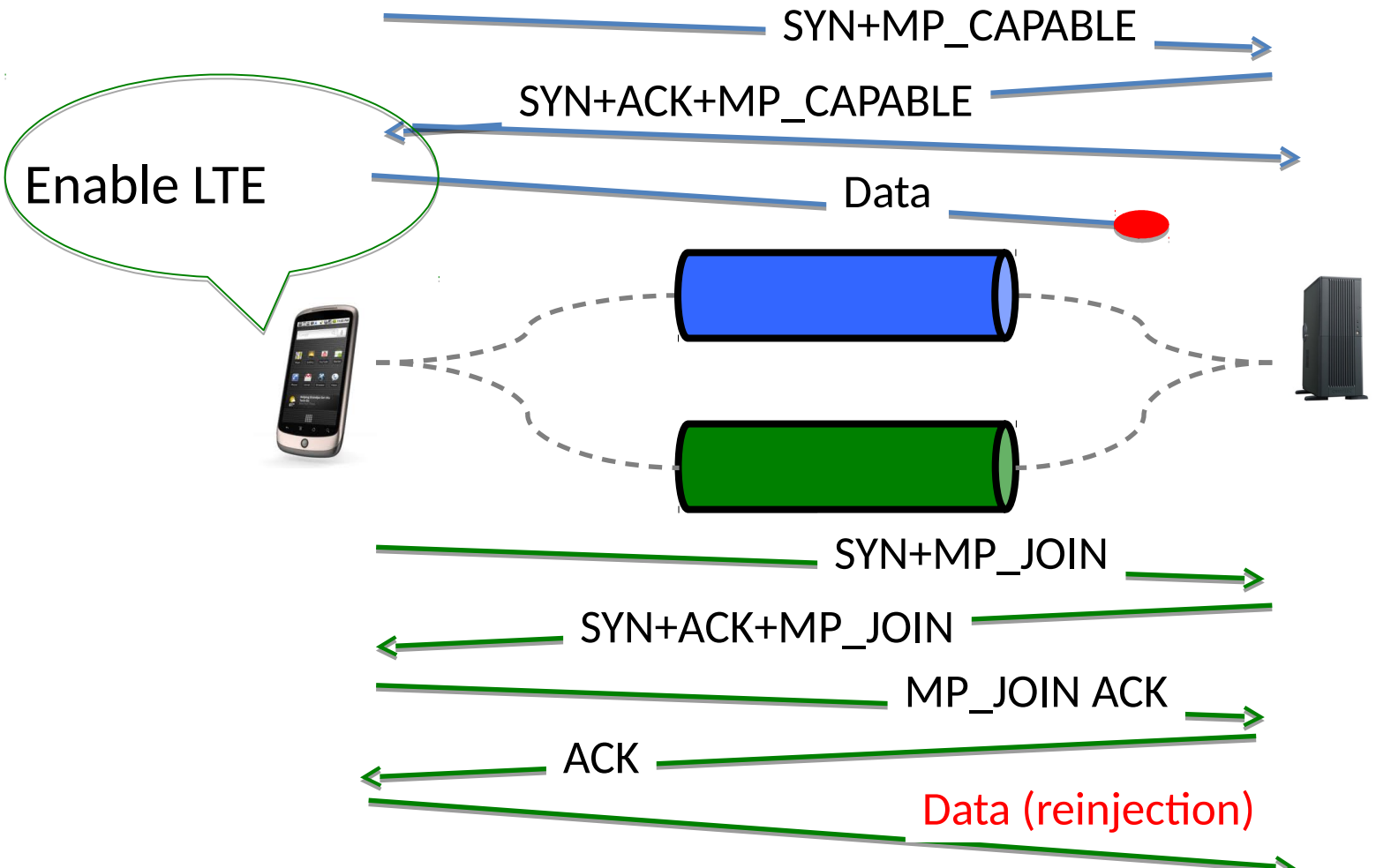
Multipath TCP on smartphones

- Both LTE and WiFi active



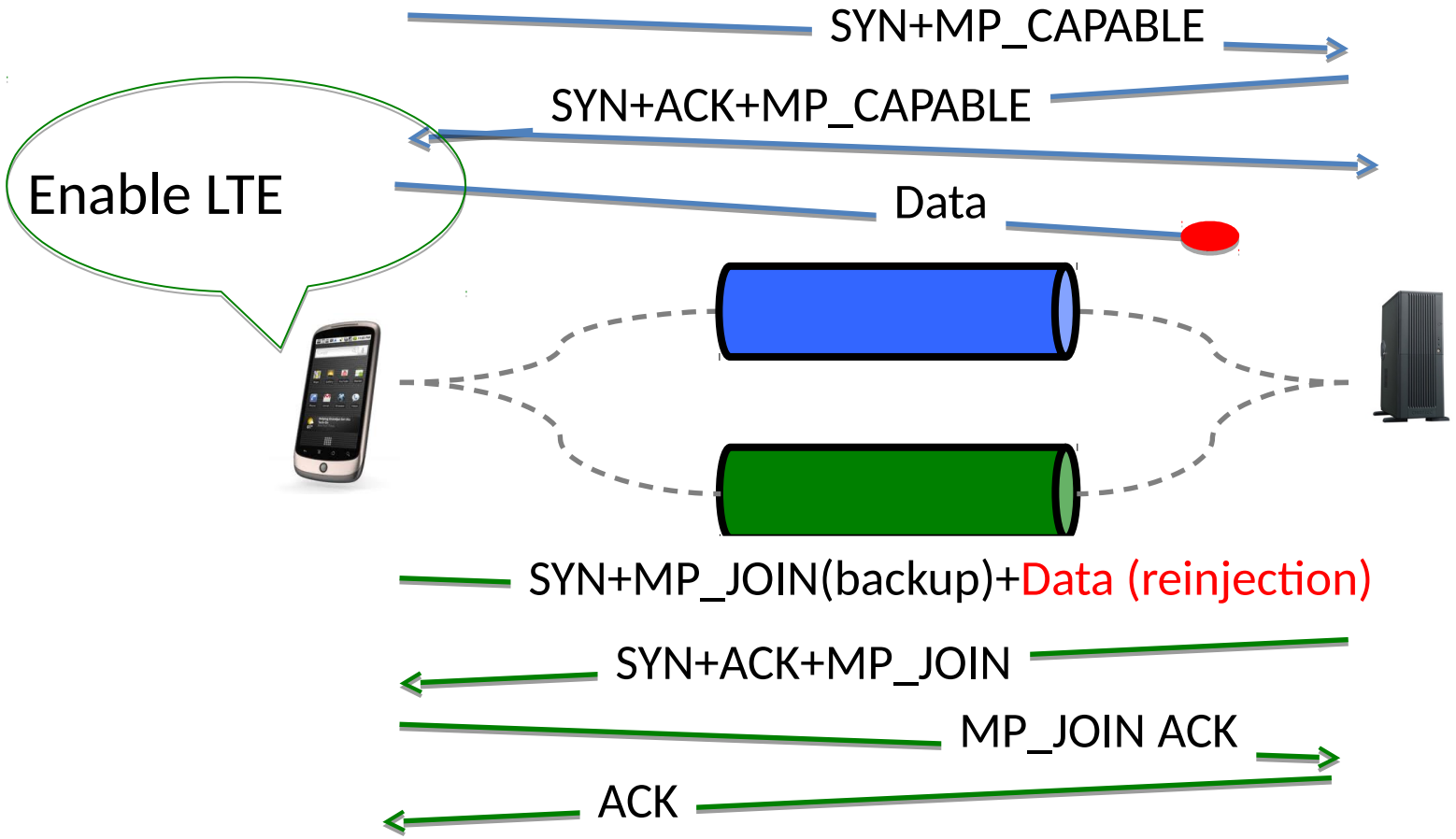
Multipath TCP on smartphones

- To minimise energy consumption, WiFi only



Improving handovers on smartphones

- Ideally, smartphones would like to do



Faster handovers

- In RFC6824, we opted for a four-way handshake to establish the additional subflow
  - This is fine for bandwidth aggregation, but far too long for fast handovers on smartphones
- RFC6824bis should revisit this assumption by
  - Analysing the security threats caused by the transmission of data inside SYN+MP_JOIN
  - Devise a solution that allows to transmit/reinject data inside SYN+MP_JOIN

Agenda

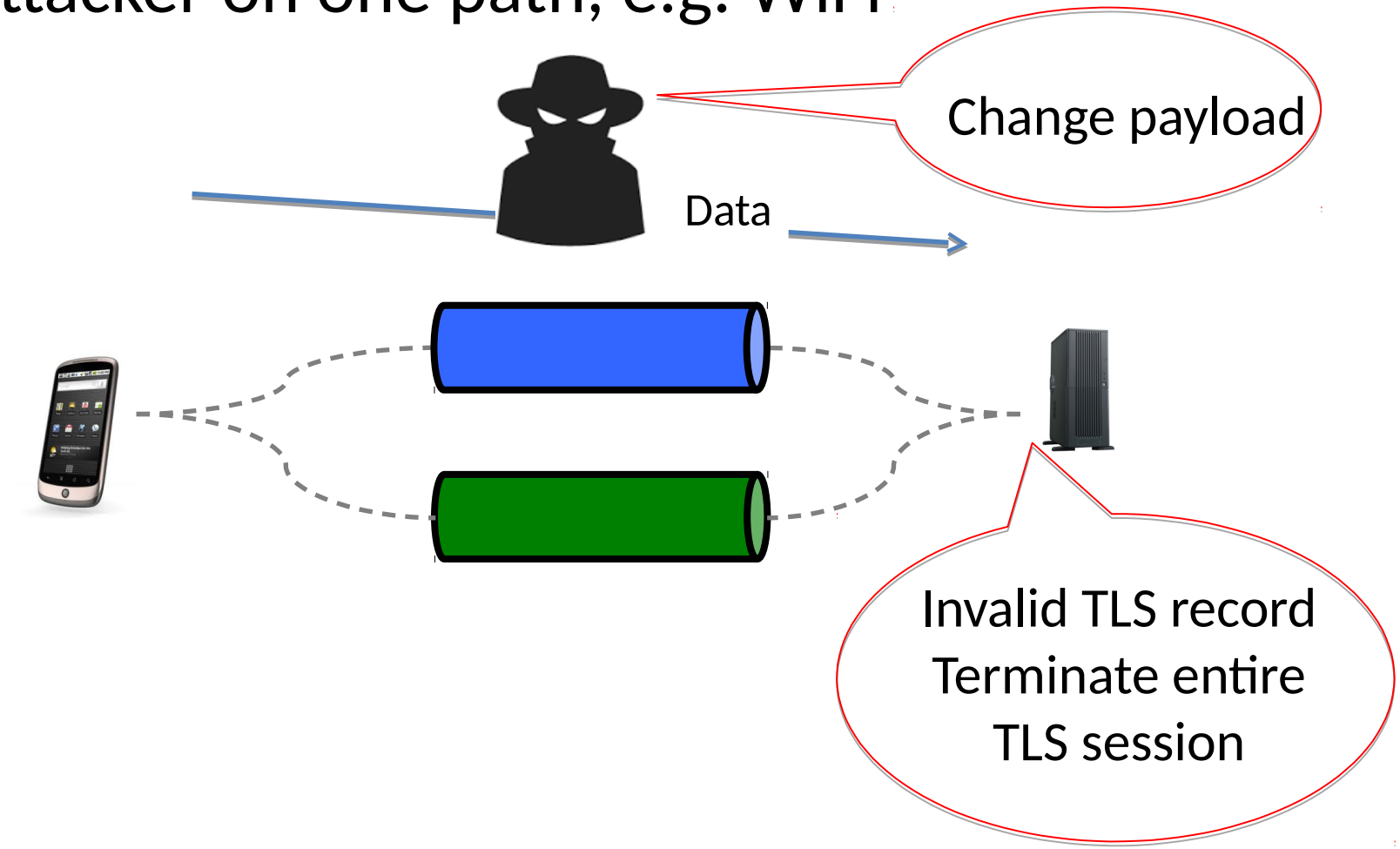
- Improving Multipath TCP on smartphones
- Multipath TCP Secure

Multipath TCP Secure

- TLS over Multipath TCP
  - Works out of the box, but attackers could cause denial of service by
    - Changing TCP headers or MPTCP options
    - Injecting/modifying data
- Multipath TCP Secure's design objective
  - Preserve connectivity when attacker is not active on all paths

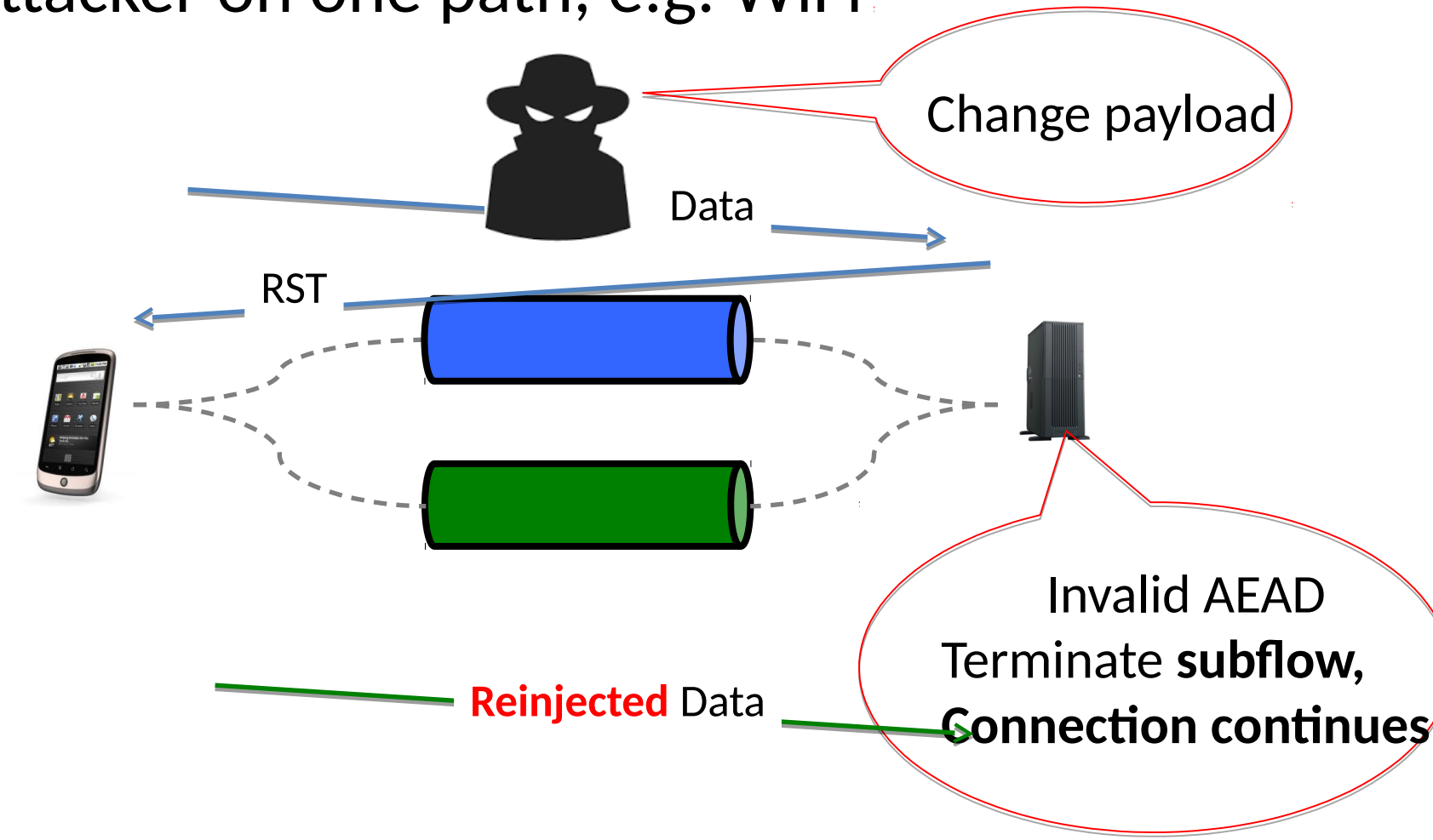
Attack scenario
TLS over Multipath TCP

- Attacker on one path, e.g. WiFi



Attack scenario
Multipath TCP Secure

- Attacker on one path, e.g. WiFi



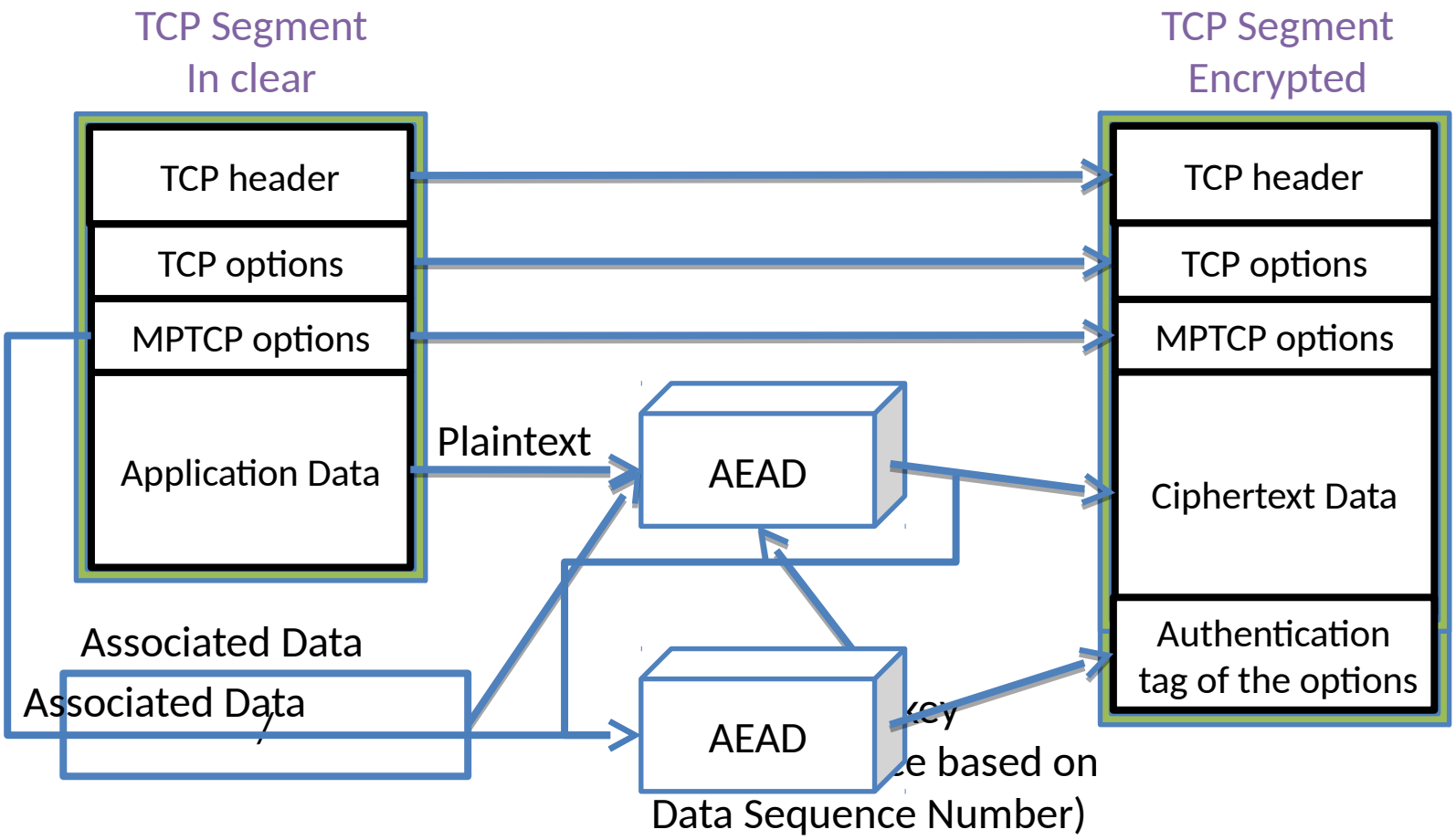
Building blocks

- A secure handshake allows to negotiate keys
  - TLS 1.3 for example
- AEAD : Authenticated Encryption with Additional Data
  - Used to securely encrypt and authenticate both data and key Multipath TCP options

Authentication information

- Where should we place the authentication information ?
  - As an extension of Multipath TCP options
    - Not enough space inside TCP extended header
  - Inside the payload
    - Authentication information is added at the end of each mapped data

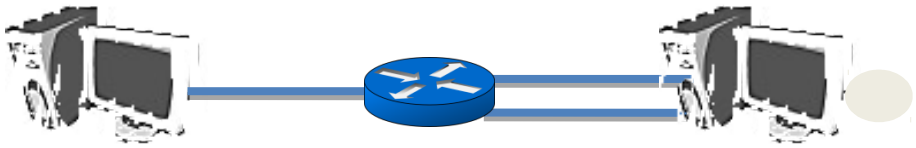
Authenticating data and options



Implementation status

- Linux Kernel v.4.1, inside the MPTCP code
- Use of the Linux/GNU CryptoAPI
- Regular MPTCP still negotiable
- ~5000 lines of diff
- https://bitbucket.org/mptcpsecteam/mptcpsec

Benchmarks

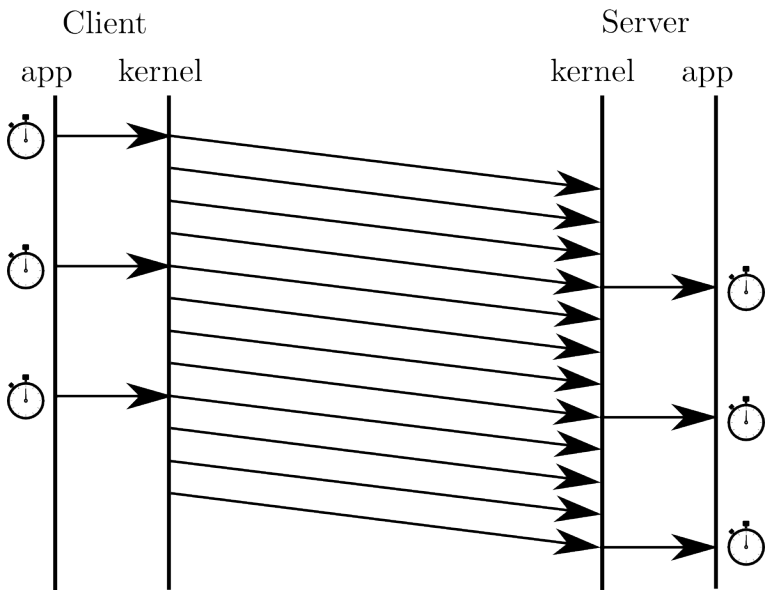


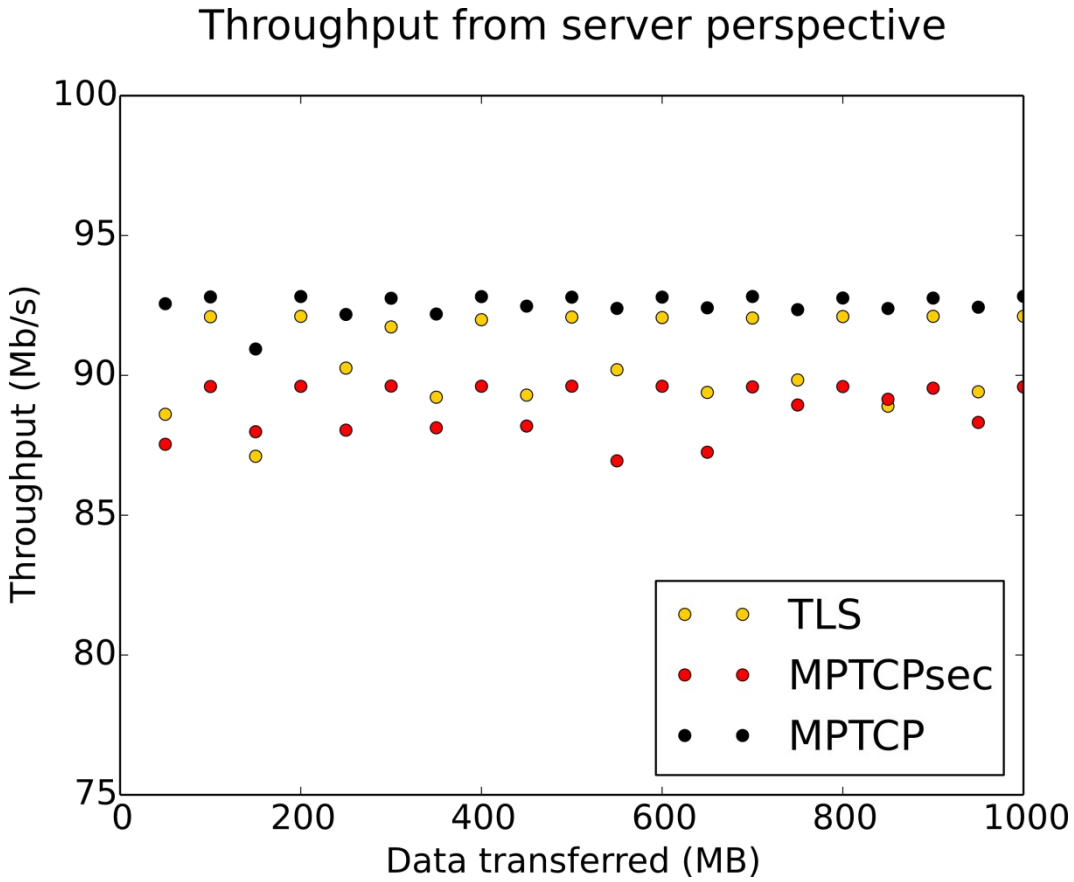
Client Router Server

	Client	Server
RAM	4 GB	2 GB
CPUs	Intel i5	Intel Core 2

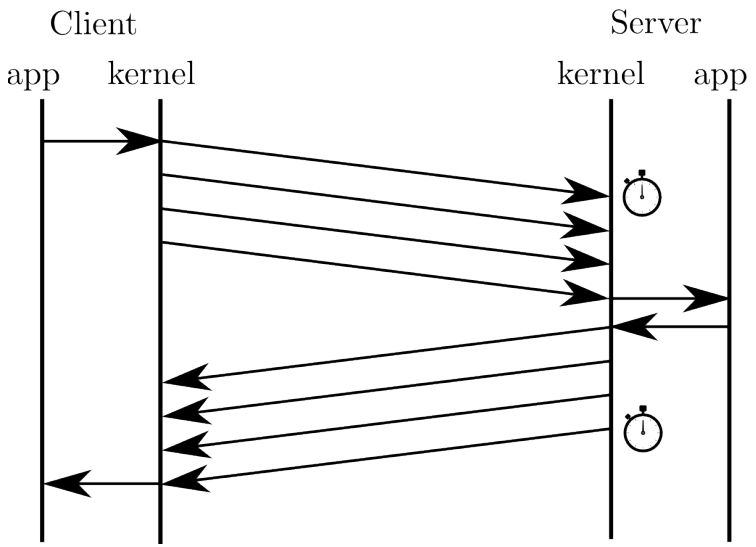
	Client eth0	Server eth0	Server eth1
Speed (Mb/s)	100	100	100
MTU (bytes)	1500	1500	1500
Offloading	off	off	off

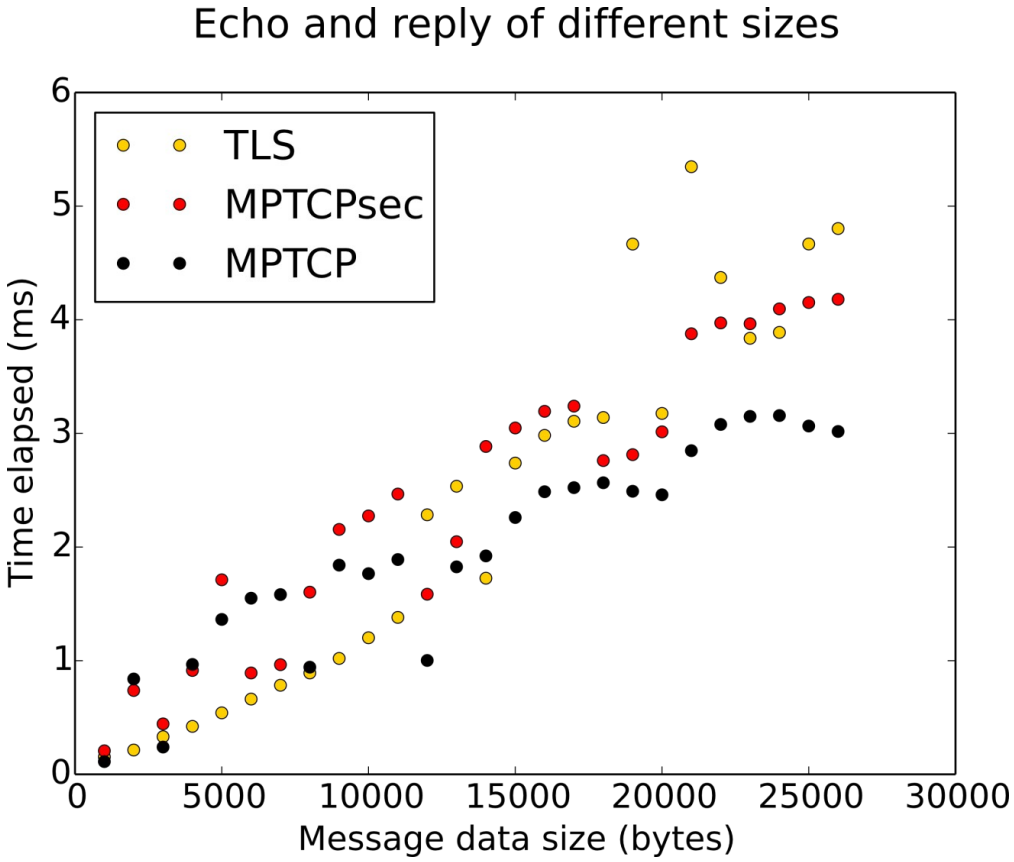
Benchmarks : goodput





Benchmarks : request/response





Conclusion

- Multipath TCP on smartphones
  - RFC6824bis should include solutions to reduce handover times
- Multipath TCP secure
  - First step towards a version of Multipath TCP that can cope with on-path attackers
  - More details in
    M. Jadin et al. "Securing Multipath TCP : Design and implementation", to appear, INFOCOM'17
    https://inl.info.ucl.ac.be/publications/secure-multipath-tcp-design-impementation