THE PPSP PEER PROTOCOL (PPSPP)

Arno Bakker
Riccardo Petrocco (TU Delft)
Victor Grishchenko (Citrea LLC)

VU UNIVERSITY AMSTERDAM

LOOKING FURTHER

OVERVIEW

- Updates since IETF 87:
- -08:
  - Responded to all points of AD Review

-08 CHANGES

Addressed last open issues from AD Review:

- No formal protocol message definition
  - Bit-based ASCII art added
- Removed in-protocol NAT hole punching.
- Removed compatibility between chunk addressing schemes.
- Reformatted IANA Considerations.
- Clarified what constitutes minimal swarm metadata.

-08 CHANGES (CONT'D)

Processed other feedback:

- Elliptic curve support for live streaming
  - To get small swarm IDs.
  - ECDSAP256SHA256 (default) and ECDSAP384SHA384.
- Peer SHOULD NOT send HAVEs to seeder
- IETF 87 remark about MTU
  - Added paragraph on Path MTU Discovery
  - Use 512 byte chunks and probe packets made of multiple DATA messages
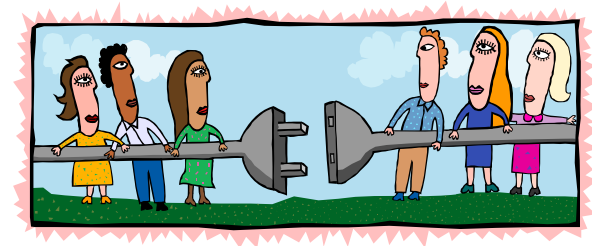 - Optional

FUTURE

- Responded to all points of AD Review
  - See -07 Revision History at end of draft.
- Ready to start discussion whether satisfactory

REFRESH: PPSPP MESSAGES

- Basic unit of communication: Message
  - HANDSHAKE
  - HAVE: convey chunk availability
  - REQUEST: request chunks
  - DATA: actual chunk
  - INTEGRITY: hashes to enable integrity verification
  - …
- Messages are multiplexed together when sent over the wire.

EXAMPLE PPSPP ON THE WIRE

- Peer A and B both have some chunks:

	HANDSHAKE + HAVE	
A		B

HANDSHAKE + HAVE

HANDSHAKE + HAVE + REQUEST

REQUEST + INTEGRITY + DATA

REQUEST + INTEGRITY + DATA
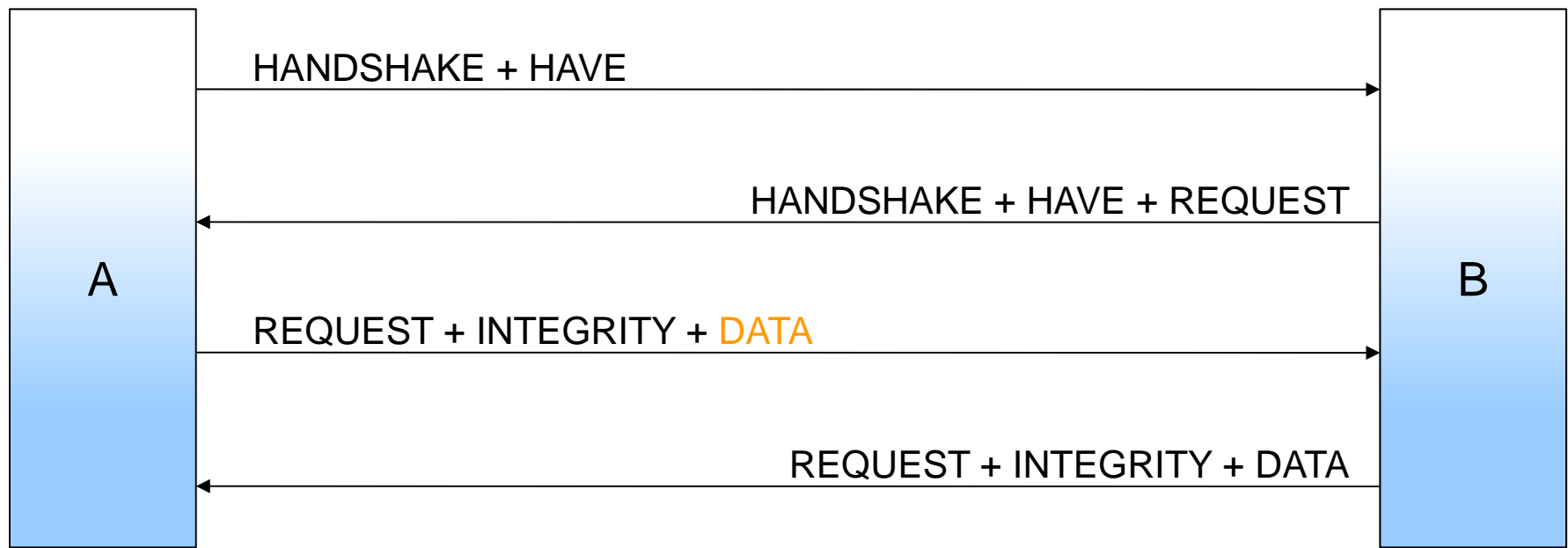
- Note: low latency, data transfer already in 3rd datagram.