# draft-lehtovirta-srtp-rcc-01.txt

Rolf Blom
Ericsson Research

# Problem

- ROC is signaled out of band.
- Users may join an already ongoing session.
- Due to packet reordering and the way the ROC is estimated/updated on the receiver side, receiver may not be able to synchronize ROC.

# A Solution

- Carry ROC in the SRTP packets them selves.
- Will lead to immediate and robust synch.
- Leads to 4 octets of wasted bandwidth per packet, so only include ROC in *some* packets.
- ROC needs integrity protection to avoid DoS and SRTP has hooks that allows new integrity transforms. Hence, include ROC in the integrity tag of a new transform (see also draft-mcgrew-srtp-ekt-00.txt for similar usage of the integrity transform hooks).

# Format and processing (1/2)

- Negotiate a constant R, so that every packet with SEQ % R == 0 will carry the ROC, and the others won't.
- Conceptual packet format for SEQ % R == 0:


- Conceptual packet format for SEQ % R != 0:

# Format and processing (2/2)

- Possible to have integrity protection on all packets or only on packets carrying ROC.
- Transform only applicable to SRTP, not to SRTCP.
- This is a new transform and it is not compatible with the default integrity transform without seriously ugly hacks that will impact:
  - future extensibility,
  - interpretation of SRTP policy,
  - and maybe even security.

# Implications for MIKEY

- The draft adds possibility to negotiate different transforms for SRTP and SRTCP in MIKEY via new IANA registrations in the SRTP policy payload
- Also adds necessary registrations to negotiate the ROC transmission rate R in MIKEY.

# Status

- The specification text in the draft is mandatory for 3GPP MBMS and OMA BCAST.
  - This implies that the IANA registrations are necessary to avoid name space collisions.
- The solution can be useful for late joiners to SRTP sessions in general.
  - Therefore it could be good to have the specification in IETF.