Group key management architecture

<draft-ietf-msec-gkmarch-03.txt>

Mark Baugher, Cisco

Ran Canetti, IBM

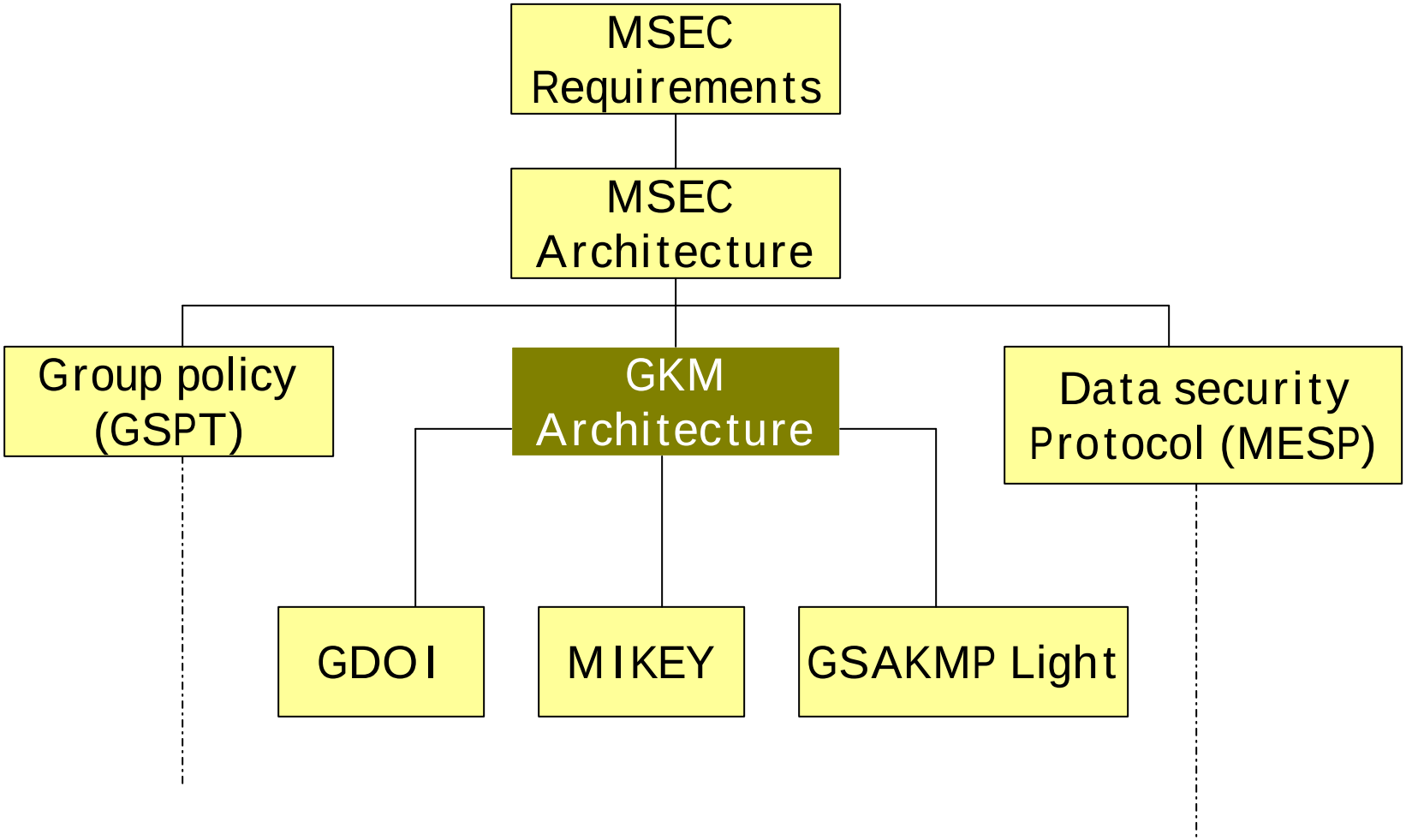
Lakshminath Dondeti, Nortel

Fredrik Lindholm, Ericsson

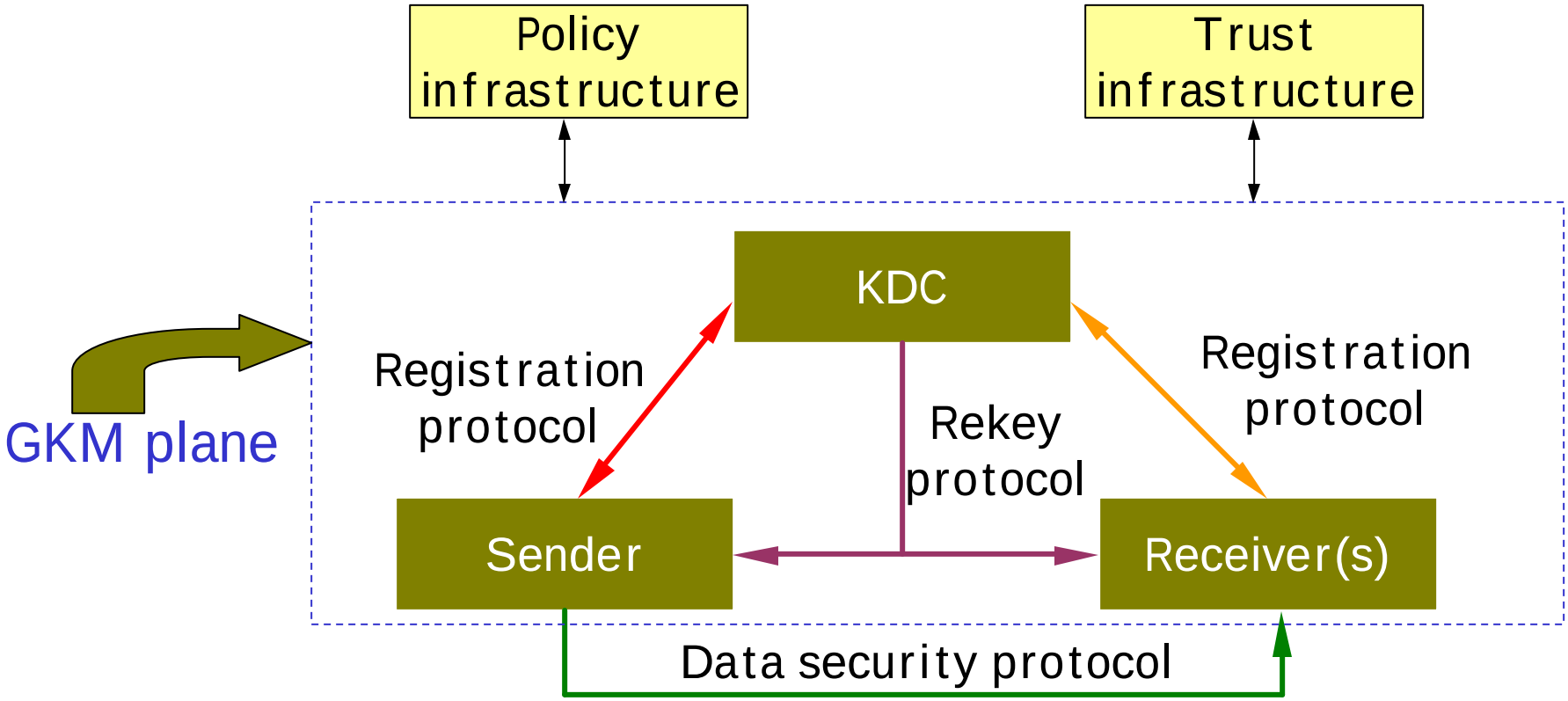
Overview of this talk

- Introduction to GKMArch
  - Relative positioning in MSEC I-Ds
- Focus of this talk
  - Reliable transport of rekey messages
  - SA synchronization
  - Results from **Sanjeev Setia** et. al (GMU)
- Conclusion

GKMArch as part of MSEC IDs



GKM entities and protocols



Outstanding issues in rekeying

- Reliable transport of rekey messages
  - feedback implosion
- GSA Synchronization
- Incorporating GKMAs into rekey msgs
  - Stateful and stateless rekeying
    - Different reliability requirements
- Interoperability of GKMA
  - e.g. Different LKH implementations

Reliable transport of rekey messages

- In periodic (batched) rekeying, number of rekey packets can be large.
  - e.g.: Group Size = 64 K, No. of leaves = 512 (0.7%)
    - 170 packets in rekey payload (assuming 40 keys fit in one packet)
- Scalable reliable multicast protocols
  - require infrastructure support
  - introduce new security problems

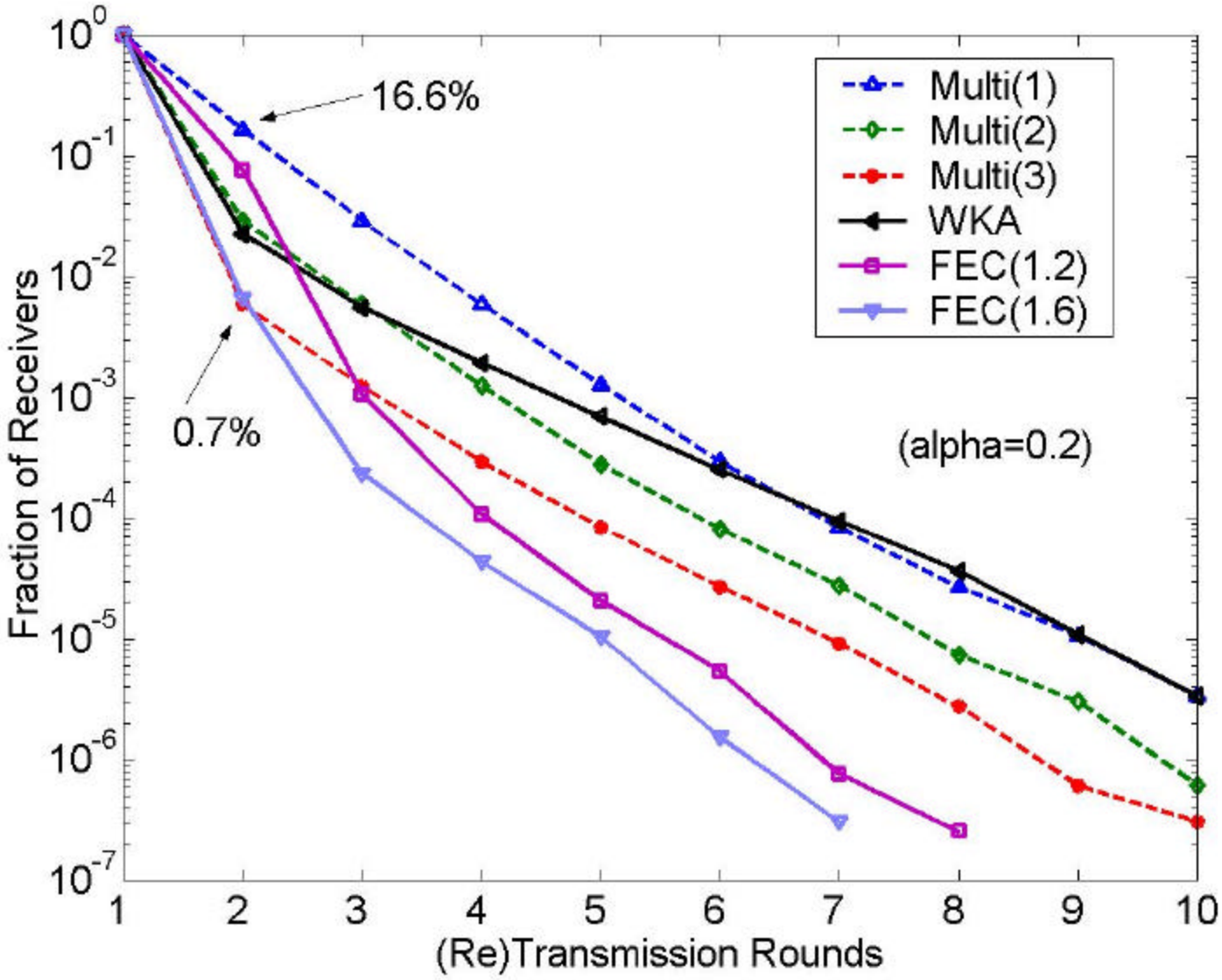
Previous work on reliable key delivery

- Transmit rekey message multiple times
- proactive FEC with NACKs
  - Key packets + parity packets multicast to group
- Perrig et. al. proposed ELK
  - "Hints" embedded in data stream that allow receivers to recover keys
- Weighted key assignment (WKA)

Weighted key assignment

- Customized for LKH
  - Should work for OFT, SDR etc.
- Proactive redundancy
  - Based on KEKs' positions in the key tree
- Feedback-based
  - NACKs determine weight of keys in next rekey message
  - Only keys that a receiver needs

Results: Latency



What next?

- Still would like to see what we can achieve without NACKs?
- NACKs require O(n) secure channels at GCKS
  - There may be a way to use the GSA
- WKA may not need changes to rekey protocol (FEC-based scheme might)

Many-to-one secure transport of NACKs

- Two layers of integrity protection
  - Outer using group authentication key
  - Inner using one-to-one authentication key
    - Processing is no more complex than at receivers
  - Scalability issues: implosion of NACKs
- Replay protection using SEQ numbers
  - No new per-member state required

Conclusion

- Rekey protocol: outstanding issues
  - GSA synchronization
  - Reliable transport and sync req implosion
  - Method to securely send NACKs
  - Interoperability of GKMAs
    - Standardize LKH, OFT, Subset difference etc.