FMKE

(Flat Multicast Key Exchange)

Securing multicast satellite and other wireless systems transmissions

draft-duquer-fmke-01.txt

François Cosquer / Alcatel , L. Duquerroy, S. Josset / Alcatel Space

Table of content

Introduction

Flat Multicast Key Exchange :

- Group key management protocol
- Derived from GDOI, in order to provide an adapted solution for wireless link securisation in:
  - satellite systems
  - and potentially in any other wireless systems (WIFI, Wimax)

Introduction

- 1st version of the ID (draft-duquer-fmke-00.txt)
  - presented to the MSEC group at the 57th IETF meeting (July 2003,Vienna)
- Draft-duquer-fmke-01.txt : update of the initial ID by taking into account received comments
  - FMKE presented as a use case of GDOI
  - Underlining of the differences between both protocols

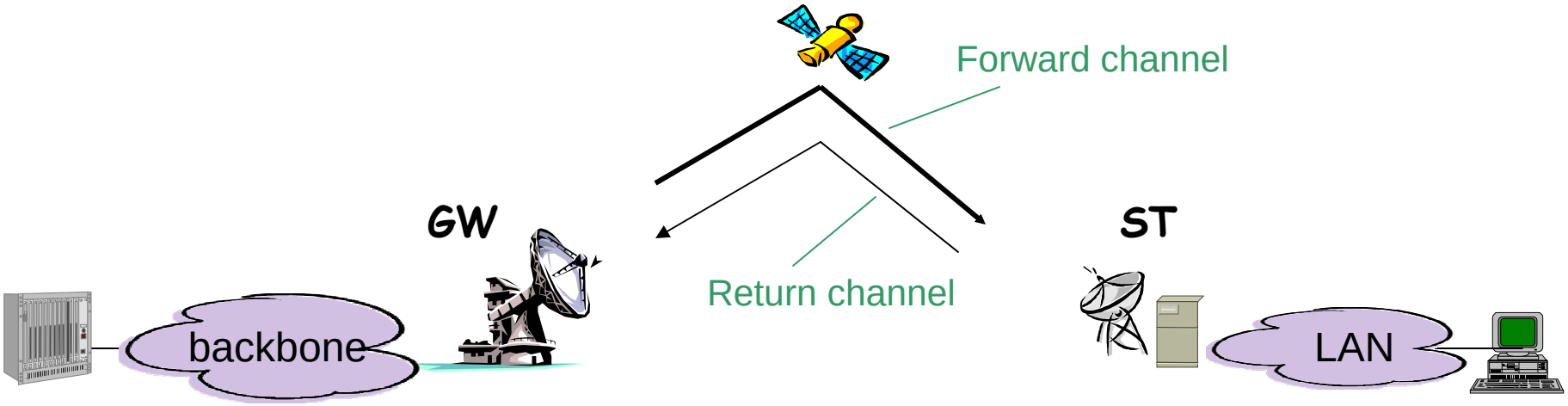
GDOI and FMKE : General comparison

- FMKE : two exchanges derived from GDOI exchanges
  - GDOI GROUPKEY-PULL exchange = = FMKE phase 2
    - protected by a phase 1 ISAKMP SA
    - dedicated to the configuration of a Group member (it receives Rekey-SAs and/or Data-SAs)
  - GDOI GROUPKEY-PUSH exchange = = FMKE phase 3
    - protected by a Re-key SA
    - dedicated to the update of a group , i.e. its group members (update of the Re-key SA and/or creation or update of Data-security SAs)

➔ other mechanisms optimized for wireless application

Specific needs : variety of connectivity & network topology (1/3)

- Satellite systems :



Network
Internet, Private network, Video server...

Gateway or Hub
Terminal access concentrator

Satellite

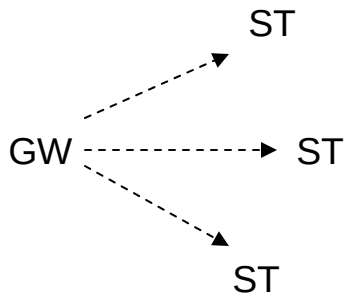
Satellite Terminal

User equipment
PC, LAN, TV, ...

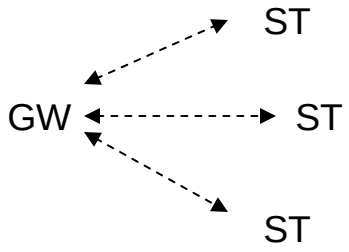
Specific needs : variety of connectivity & network topology (2/3)

- Satellite systems : several topologies

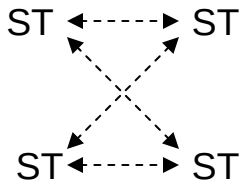
  - Star topology without return channel
    - Unidirectional Communications from GW to STs



  - Star topology with return channel
    - Bi-directional Communications between GW and STs



  - Mesh topology
    - Bi-directional Communications between STs



Specific needs : variety of connectivity & network topology (3/3)

- Need for a group key management protocol able to establish Group SA in any topologies with :
    - group members located in each ST and GW
    - GCKS located in GW in star topologies, and in a ST in mesh topology.

- In star topology without return channel
    - IKE phase 1 SA configured manually in each member and GCKS
    - GDOI GROUPKEY-PULL not possible, as group member has to request to get access to each group

- A change in GROUPKEY-PULL philosophy is required :
    - Group member directly configured by the GCKS
    - No request

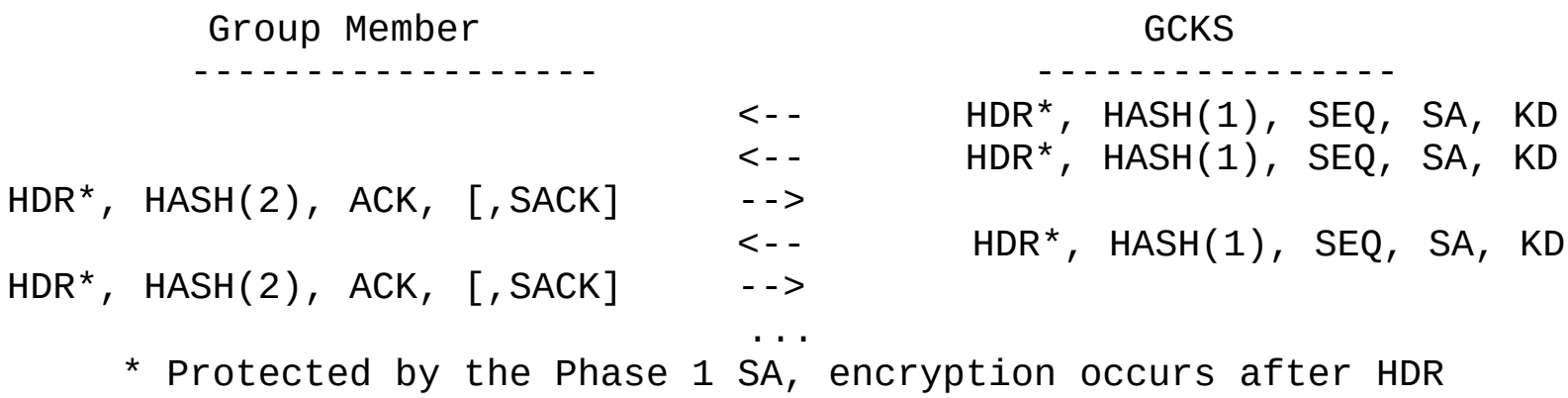
Specific needs : bandwidth utilization efficiency(1/2)

- GDOI GROUPKEY-PULL exchange :
  - For a member : as many GROUPKEY-PULL exchanges as the number of groups it belongs to.

```
Initiator (Member)                          Responder (GCKS)
------------------                          ----------------
HDR*, HASH(1), Ni, ID       -->
                            <--       HDR*, HASH(2), Nr, SA
HDR*, HASH(3) [,KE_I]       -->
   [,CERT] [,POP_I]
                            <--       HDR*, HASH(4),[KE_R,][SEQ,]
                                        KD [,CERT] [,POP_R]
```

Specific needs : bandwidth utilization efficiency(2/2)

- FMKE phase 2 :
  - One phase 2 exchange per member, lasting all its session
  - GCKS transmits directly all Data-Security SAs and Re-key SAs (no request for each group)
  - A GCKS message can contain SAs from several groups.



  - Possibility to transmit point-to-point SA too.

Specific needs : reliability (1/2)

- FMKE phase 2 (unicast)
  - The group member is configured by the GCKS
    - group member does not send any request
    - reliability based on Acknowledgements (ACK) & Selective Acknowledgements (SACK) *
  - The GCKS manages a message window.
  - Each message contains a sequence number (SEQ payload).
  - The group member sends periodically a message containing an ACK payload, and some optional SACK payloads
- Ex:
  - First sequence number =1
  - Sequence numbers of Msg received by the member : 1 2 3 4 . 6 7 . 9
  - Acknowledgement message sent : ACK: 4, SACK 6-7, SACK 9-9
    (triggering the retransmission of messages 5 & 8)

* in one-way systems, acknowledgement not enabled in group members

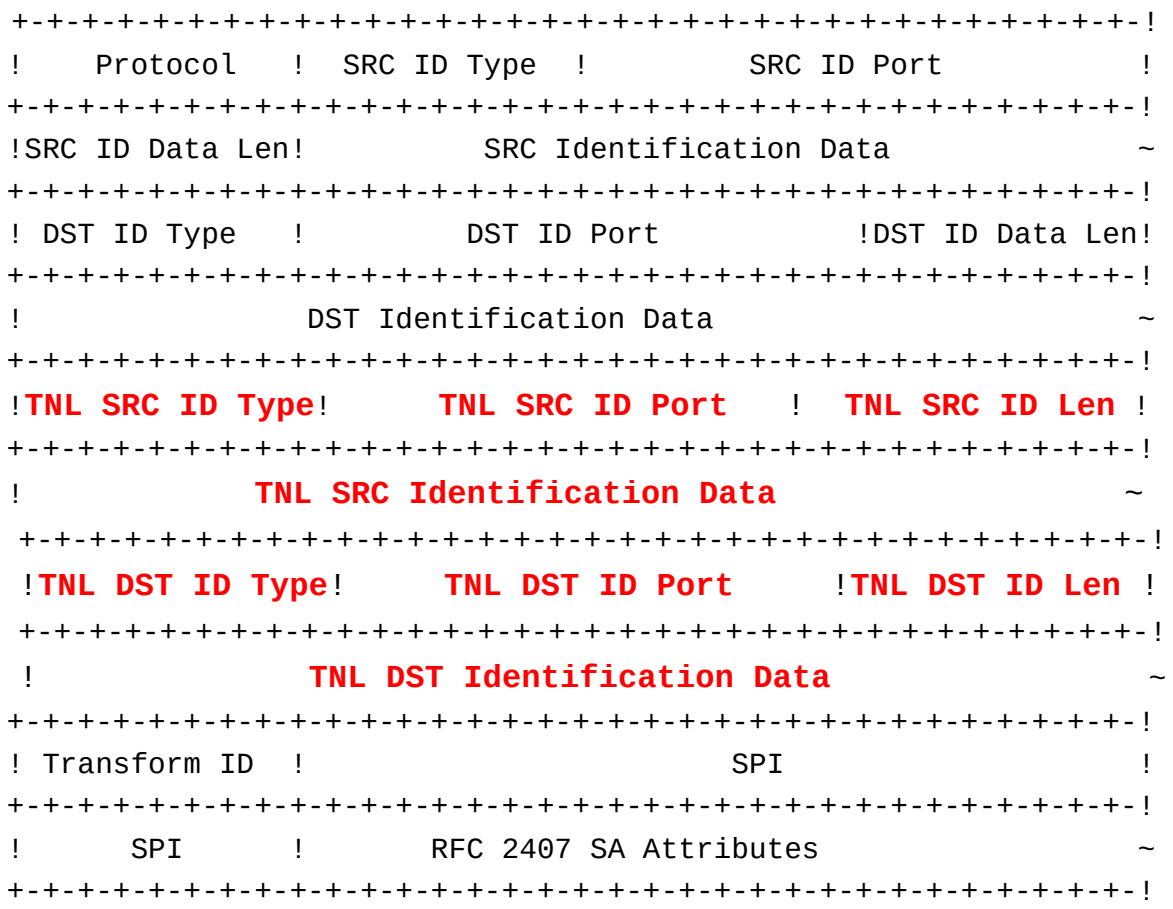
Specific needs : reliability (2/2)

- FMKE : phase 3 (multicast)
  - Configuration and update of group members by the GCKS
    - Reliability based on Negative Acknowledgements (NACK)
  - The GCKS manages a message window
  - Each message contains a sequence number (SEQ payload)
  - The GCKS sends regularly the Last Sequence number used (LSEQ payload)
  - When a member determines that one message is missing, it sends a Nack message after a variable delay, containing one or several NACK payloads.
  - This delay is optimised to avoid massive NACK flood in case of message loss.
- Ex:
  - Next sequence number (configuration) = 5
  - Sequence numbers of Msg received by a member : . 6 7 . 9
  - Negative Acknowledgement sent: Nack: 5-5, Nack 8-8
    - triggering the retransmission of messages 5 & 8 in multicast

* in one-way systems, negative acknowledgement not enabled in group members

Specific needs : dataplane in tunnel mode

- Satellite networks : end-users distinct from group members
  - group members shall encapsulate data in tunnels
  - Data-Security SA : additional information for tunnel definition



TEK Protocol-Specific payload for ESP

Implementation

- Project

  – IST (European) SatIP6 project (http://satip6.tilab.com)

  – Military DVB-RCS demonstrator

  – FMKE phase 1 (IKE) and phase 2 + IPSec ESP dataplane implemented

Conclusion

- Proposition of M. Baugher (GDOI writer) :
  - to minimize the FMKE changes, fold them into GDOI if it is possible, and publish a new version of GDOI

If any questions...

Laurence Duquerroy
Alcatel Space
26 avenue J-F. Champollion
BP 1187
31037 Toulouse Cedex 1
France

laurence.duquerroy@space.alcatel.fr

sebastien.josset@space.alcatel.fr