FMKE

(Flat Multicast Key Exchange)
Securing multicast satellite systems

draft-duquer-fmke-00

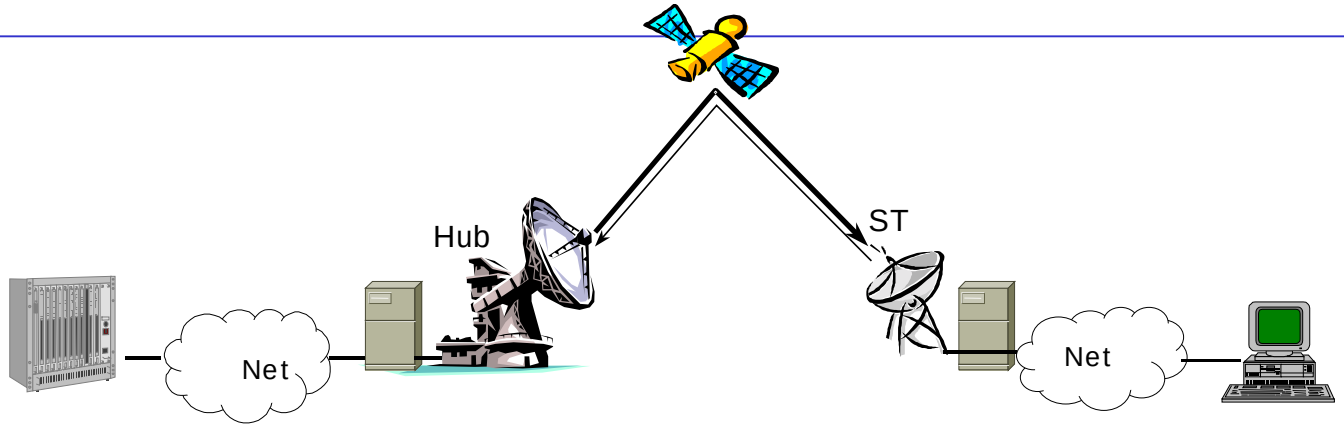
S. Josset, L. Duquerroy / Alcatel Space Industries

Table of content

Satellite systems overview: Satellite Missions

- Observation/Meteo
- Navigation
- Science
- Telecom
  - Architecture: Fixe/Mobile
  - Return link way: Broadcast, light interactivity, full mesh

Satellite systems overview: Satellite System Equipment



- User equipment
  - Phone system (PABX, E1…), Network(ATM, IP interface,...),TV...
- Satellite terminal
  - Network interface, adaptation layer, MAC layer, physical layer, antenna
  - In-door unit, Out-door unit.
- Satellite
  - Transparent (physical layer frequency translation), on board switching (MAC labels)
  - TMTC (Tele-measurements & Tele-commands)
- Hub or Gateway, NCC
  - Hub: Terminal access concentrator
  - NCC: Network Control Center (Terminal authentication, Resources allocation)
- Network
  - Internet, Private network, Video server

Security needs in a Satellite system

- Satellite Network management
  - Equipment (Satellite terminal & Hub, ctlr & mgt)
  - Network data filtering (firewalling)
  - Same needs and solutions as in terrestrial
  - TMTC (Satellite Tele-measurements & Tele-Commands)

- User data plane & Space segment
  - Layer 3 security (IP): Existing protocol modification (IPSec)
  - Layer 2 security (satellite packet): Mainly dedicated protocols (Ctrl & Data plane)
  - Layer 1 security (waveform, frequency agility…): Mainly military only protocols

- Services
  - On demand delivery
  - Satellite resource on demand reservation
  - Secure billing (caller billing)

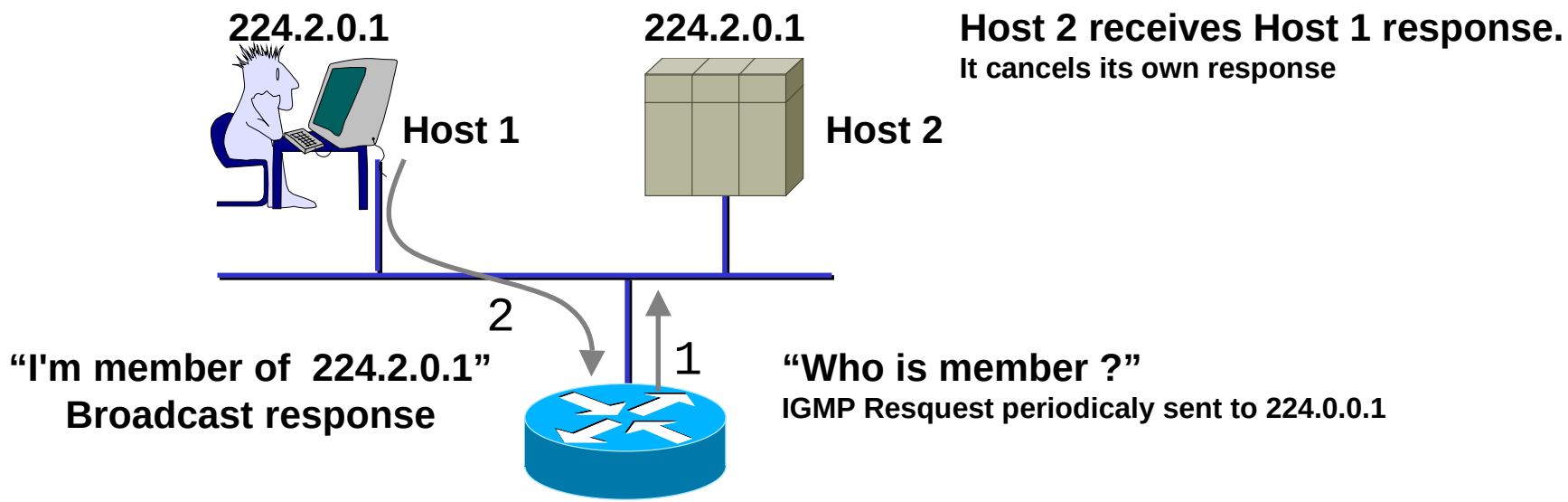
Following slides focus on User Plane & Space segment security

Satellite link specificities

- High delay
  - Geostationary satellite : 250ms transmission delay (baseline for communication missions)
  - Protocols with handshakes & small data windows may be slowed down (TCP)
- Broadcast and multicast capabilities
  - Natural broadcast capability
- Extended coverage
  - Wide footprint (1 spot can cover whole Europe)
  - Thousands of terminals are managed by a single Hub station
  - Local weather condition
- Cost of the link
  - Point to point satellite links are more expensive than terrestrial link.
  - Each data bit must be sold many times (broadcast/multicast) to reduce bit cost.

Satellite link specificities: Impact on IGMP

- Internet Group Management Protocol (IGMP)
- IGMP is designed for ethernet network with small delay
  - The server sends an IGMP query
  - Every multicast subscriber host prepares a response
  - Every host receives the first answer, and then cancels its own.



Satellite link specificities: Impact on IGMP

- Satellite = Extended coverage & High delay
  - In a satellite system, the transmission delay is about 250ms.
  - Every user terminal behind a host broadcast a response, and 2*250ms later (terminal to Hub, Hub to terminal) receives every responses.
  - Thousands of terminals sending an IGMP response every 5 seconds is an incredible waste of bandwidth, with possible DoS at server side.

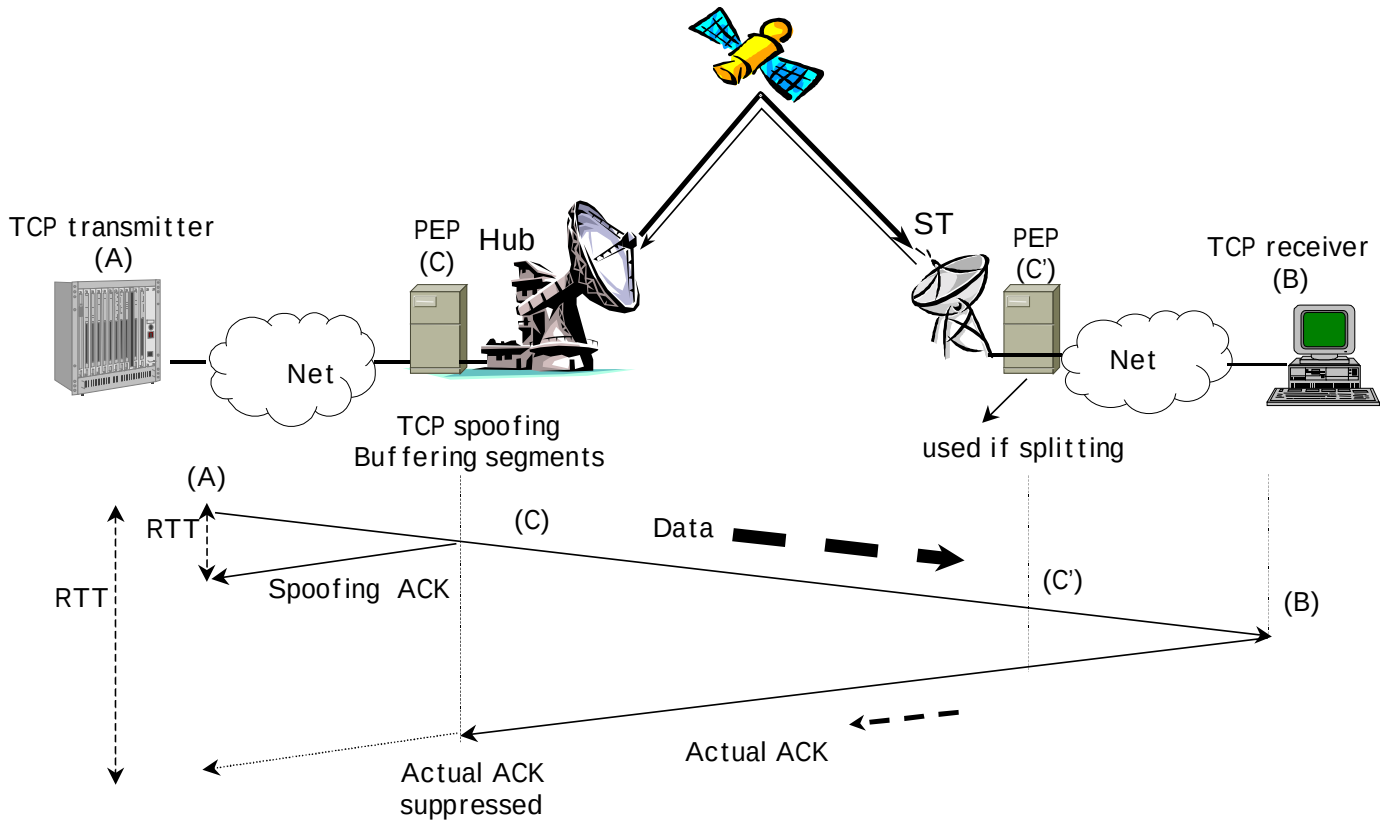
- IGMP adaptation for satellite
  - IGMP proxying (The satellite terminal sends only one response)
  - IGMP electing (Only elected terminal sends the response)

Satellite link specificities: Impact on TCP

- TCP windows
  - The standard max TCP windows is 64kbyte.
  - The round trip time delay is about 500ms.
  - The theoretical maximum delay is 1Mbit, even on an expensive 10 Mbit link.
  - Measurements done during IST Brahms project show that the real maximum throughput is about 500kbit/s on recent IP stacks with standard configuration (windows NT/2000, Linux 2.2, 2.4) (error free link).
- Satellite Errors
  - In terrestrial network, packet loss means congestion
  - In satellite network it often means transmission error.
- IETF TCPSat
  - Many TCP extensions such as SACK, or scalable windows have been standardized.
  - Both TCP sender and receiver must implement TCPSat options

Performance Enhancement Proxies (PEP)

- TCP Spoofer/Splitter
  - Spoofers modify the TCP normal behaviour
  - Need to access/modify TCP header
  - Not compatible with IPSec



Satellite segment only Layer 2/3 security

- Satellite link
  - The satellite link is a weak point in a transmission (everybody can listen)
  - Satellite segment only security may be enough for operators

- Security at IP layer
  - Multicast is a strong requirement.
  - Multicast ESP could be used.
  - Implies to put IP Multicast router at Edge
  - IP Multicast Routers is harly managed by satellite Operator

- Security at Layer 2
  - Layer 2 security easily managed by satellite Operator

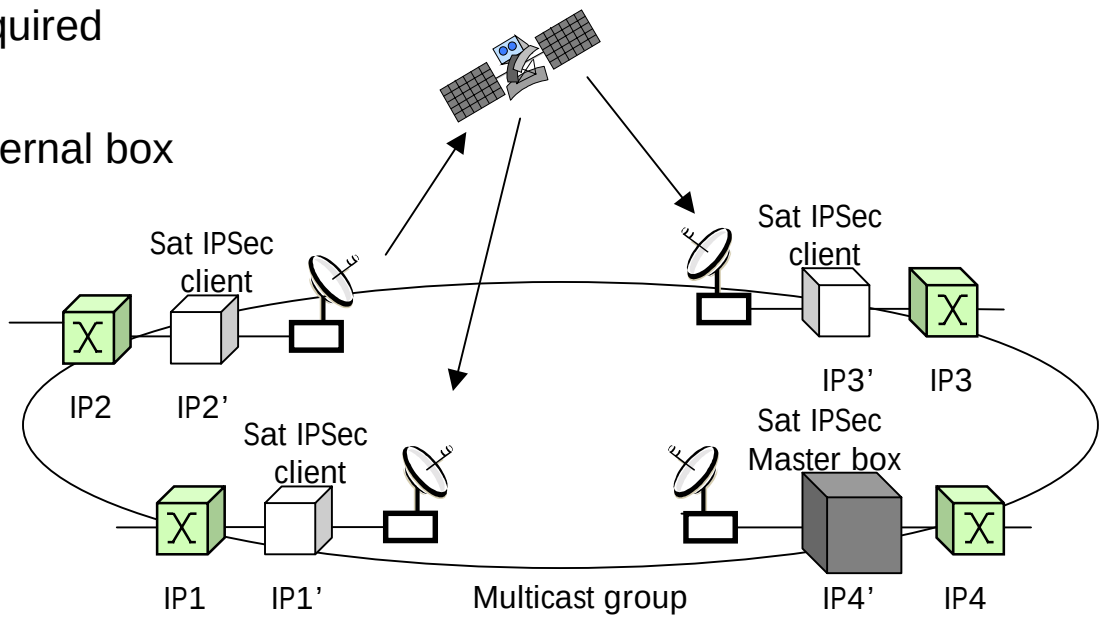
SatIPSec project

- Project:
  - Internal Study: Oct 2001
  - IST SatIP6 Project: March 2002
- Targeted system:
  - Telecom systems for Fixed and Mobile
  - Existing return channel
- Security:
  - IP layer, Terrestrial layer 2 (Ethernet), Satellite layer 2 (Mpeg2-TS, ATM)
  - Based on msec work: Mainly draft-ietf-msec-gdoi-01.txt
- Modifications:
  - Adapted to our needs
  - Added Reliability

Satellite Security: Requirements

- Centralised control & management
  - One control box
  - Possible interaction with external Conditionnal Access system

- Satellite terminal
  - Inbound/Outbound packets are ciphered/deciphered
  - Configured & Controlled by the Server
  - Mutual authentication required
  - Reliability required
  - Embedded Security / External box



FMKE /GDOI Protocol differences

- GDOI
  - IKE Phase 1
  - Groupkey-Pull : The client requests some configuration
  - Groupkey-Push (multicast): Push: The server update a group of clients

- Sat IP Sec
  - Phase 1: Control plane securing between a client and the server : IKE
  - Phase 2 (unicast): The client is configured by the server
    - No request
    - Reliability
  - Phase 3 (multicast): Configuration of Clients maintained by the server
    - Reliability

- Change in the Groupkey-Pull Philosophy
- Reliability
- FMKE is GDOI compatible

-> FMKE is a GDOI Use case with lightweight extensions

FMKE /GDOI Reliability

- GDOI
  - Phase 1: IKE :
    - 1 Question/1 response : Timeout & retransmission
  - Phase 2 (unicast): Pull: The client request some configuration
    - 1 Question/1 response : Timeout & retransmission
  - Phase 3 (multicast): Push: The server update a group of clients
    - Need for external reliability mechanism

- Sat IP Sec
  - Phase 1: Control plane securing between a client and the server : IKE
  - Phase 2 (unicast): The client is configured by the server
    - Client sends No request, Need for another reliability mechanism
    - Ack based
    - Need to manage a windows at server side
  - Phase 3 (multicast): Configuration of Clients maintained by the server
    - Timer+Nack based
    - Avoid massive Nack flood
    - Need to manage a windows at server side

FMKE Protocol: Reliability

- Phase 1
  - Messages are sent one by one.
  - The message order is fixed.
  - Each message is protected by a timer
  - IKE..

FMKE Protocol: Reliability

- Phase 2 (unicast)
  - The server manages a message window.
  - Each message contains a sequence field (SEQ).
  - The client sends periodically a message containing a ACK field, and some optional SACK fields
  - SEQ
  - LSEQ
  - ACK
  - SACK
- Ex:
  - Config unicast: Msg Id start=1
  - Msg Id Rcv: 1 2 3 4 . 6 7 . 9
  - Msg Snd : Ack: 4, Sack 6-7, Sack 9-9

FMKE Protocol: Reliability

- Phase 3 (multicast)
  - The server manages a message window.
  - Each message contains a sequence field (SEQ).
  - When a message is missing, the client sends a NACK message after a variable delay.
  - The variable delay is optimised to avoid massive NACK flood in case of message loss.

  - SEQ
  - NACK

- Ex:
  - Config multicast: Msg Id start=5
  - Msg Id Rcv: . 6 7 . 9
  - Msg Snd : Nack: 5-5, Nack 8-8

Implementation

- Projects
  - Alcatel Space internal project (L3 secure data plane)
  - IST SatIP6 project (Layer 2 secure data plane) (http://satip6.tilab.com)
  - First tests November 2003

- Target
  - DVB-RCS system
  - FMKE over IP
  - IPSec configuration
  - DVB-RCS Layer 2 Security configuration

If any questions...

Sébastien Josset
Alcatel Space Industries
26 avenue J-F. Champollion
BP 1187
31037 Toulouse Cedex 1
France

sebastien.josset@space.alcatel.fr

laurence.duquerroy@space.alcatel.fr