Key Management for Secure Multicast in Hybrid Satellite Networks

Ayan Roy-Chowdhury, Nalini Bharatula, John S. Baras

Problem Statement

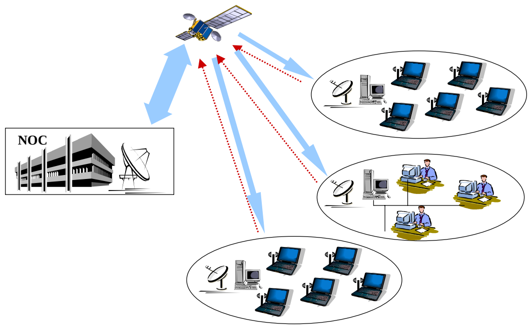
To design a framework for multicast key management in hybrid satellite networks.
• Satellites are attractive media for group data delivery, due to wide coverage and broadcast capabilities. Expected to be major component of future wide-area broadband multicast.
• Commercial viability of broadband multicast applications require that the data be accessible only to authorized receivers – achieved by data encryption.
• Encryption requires secure and efficient methods to distribute the encryption/ decryption keys to all the group members. Existing group key management protocols do not scale well when applied as is to large dynamic groups in wide-area networks.

We analyze current group key management protocols and design a framework for secure and scalable key management for hybrid satellite networks that have terrestrial Ethernet LANs interconnected by ATM-based satellite channels.

Key Management Review

• *Key management* refers to the generation, distribution and update of group encryption/decryption keys.
• A secure group key management protocol should ensure *key confidentiality*, *forward* and *backward access control*, and *key independence*.
• Protocols should be scalable, robust, have low overhead in communication, processing and storage.
• Proposed designs for group key management are either:
  • centralized - schemes requiring a group controller (GC) for key generation, such as KPS, Broadcast Encryption, Secure Lock, GKMP, CAS, LKH, or,
  • distributed – group members collaborate to generate the keys: GDH, Iolus.
Some designs are combinations of both – HFK, variations of LKH.

Network Topology



• Multiple terrestrial LANs that have one or more satellite terminals connected to them; satellite has ATM switching functionality, no IP.
• Proposed a multicast routing framework for the hybrid satellite network [1]. PIM-SM is used for IP multicast in the terrestrial Ethernet LANs; ATM with MARS architecture for multicast over the satellite links.
• One or more satellite terminals in each terrestrial LAN act as Rendezvous Point (RP) for the multicast groups within its LAN; the MARS is located at the NOC.

Proposed Framework

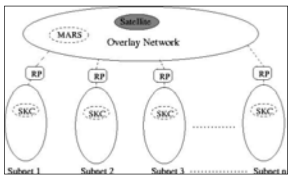
Security Considerations

• Requirement: data privacy for multicast groups in the satellite network.
• Groups varying widely in size, high member dynamics.
• Independent domains with different security policies.
• Simultaneous reliable delivery to all domains an issue - channel errors due to rain fade in geostationary satellite.
• Objective: ensure keys are delivered correctly to maximum members possible.
• Primary metric: Communication overhead, due to high latency in satellite links.

Therefore: design a framework that minimizes communication over the satellite links, to reduce delay in group initialization and key updates and error conditions.

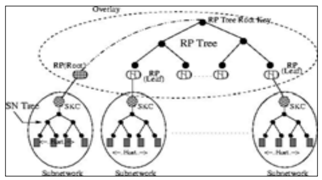
Solution: Tiered Tree Framework

• Hierarchical network topology – *independent* terrestrial subnetworks/domains, with the satellite channels forming an *overlay*.
• Divide key management into two levels. Use logical key trees in each level.
• Global RP Tree in overlay, local SN Tree in each subnetwork.



Logical Grouping

=>



Tiered Tree Framework

Trust Model

• MARS – Performs access control for domains, maintains database of member domains, Certificate Authority. Not authorized to read data traffic.
• RP – securely transmits/receives multicast traffic. Not trusted to read data traffic.
• Hosts: encrypt/decrypt application data.
• Subnetwork Key Controller (SKC): manages group keys in subnet. Performs access control for subnet members.

RP Tree

• RPs are at the leaves of the RP tree.
• Root RP dynamically selected by MARS based on group policy – *earliest to join*.
• Security additions to MARS messages, MARS table.
• At no point does MARS obtain the traffic.

SN Tree

• LAN hosts are leaves of SN Tree - stores all keys on path from its leaf to root.
• Each host also given long-term *datahiding key*, common to all group members across all subnets.
• Local RP gets only the session key from the SKC.

Secure Data Transmission

• Source encrypts twice: datahiding key + local session key.
• RP partially decrypts using local session key. Cannot decrypt further without the datahiding key. Re-encrypts using the RP Tree session key; transmits to remote subnets over satellite links.
• Remote RP decrypts partially using RP Tree key. Re-encrypts with local session key and forwards along local multicast tree.

Communication/Storage Cost

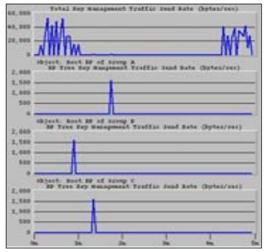
	Total Cost
Tree setup	$(n_1-1)k_p + \frac{d_1(n_1-1)}{d_1-1}k_s + n_1\left(\left(n_2+\frac{d_2(n_2-1)}{d_2-1}+1\right)k_s\right)$
Member join to existing group in subnet	$(d_2h_2+2)k_s$
Adding a subnet to existing group	$k_p+(d_1h_1+1)k_s+\lceil\left(n_2+\frac{d_2(n_2-1)}{d_2-1}+1\right)k_s\rceil$
Removing a member from subnet	$(d_2h_2-1)k_s$
Removing a subnet	$(d_1h_1-1)k_s$

Total Communication Cost

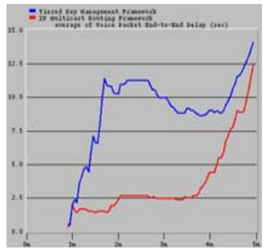
RP root	SKC	RP	Member
$\lceil\frac{(d_1n_1-1)}{d_1-1}k_s+n_1k_p\rceil$	$\lceil\frac{(d_2n_2-1)}{d_2-1}k_s+2\rceil$	$\lceil h_1+2\rceil$	$\lceil h_2+2\rceil$

Total Storage Cost

Simulation



Many-to-Many: Savings in Satellite Links



Many-to-Many: End-to-end Delay Comparison

Conclusion

• Proposed a hierarchical scheme that attempts to minimize control overhead in satellite links.
• Hides dynamism of join/leave in a subnet from other subnets.
• Attempts to mitigate the effect of root failure at the overlay level.
• Assumes minimal trust in the satellite infrastructure.
• "Fuses" key management at the application level (host) with management at the network level (RP).
• Essentially a generic design – different algorithms can be applied in each logical group depending on group dynamics.
• Future Work:
  • Fine-tuning of the mechanism for hiding the multicast data from the RPs.
  • Mechanisms for collusion resistance.
  • Source authentication of the multicast data.

Reference

1. A. Roy-Chowdhury. "IP Routing and Key Management for Secure Multicast in Satellite ATM Networks". Master's Thesis, University of Maryland College Park, 2003.

Acknowledgement

This work is sponsored in part by Lockheed Martin Global Telecommunications under the MIPS grant #123456789.