

# Three-Tier Satellite Multicast Security Protocol Based on ECMQV and IMC Methods

Attila Altay YAVUZ,  
Fatih ALAGÖZ,  
Emin ANARIM

Presented by Gökçen Arslan



# Outline

---

- Motivations
- Key Management Problems in Multicast Systems
- Key Management Protocols(Flat , LKH , ELK . . .)
- Cryptographic Methods Used in Multicast Protocols
  - RSA, DLP Based( El-Gamal-Diffie-Hellmann), GAP Diffie-Hellmann Type Solutions, ECC and its advantages, other Issues.
- Our Contribution for Cryptographic Method Aspect.
  - ECMQV (Elliptic Curve Menezes-Qu-Vanstone)
    - A novel approach for key exchange in multicast security.
    - Properties and Advantages of ECMQV.
  - IMC (Improved Merkle Cryptosystem)
    - A novel cryptographic method for use in key exchange protocols.
- Our Contribution for Protocol Aspect : A Novel Approach
  - Three-Tier independent Key Distribution Layer ( 3-LHK).
  - Integrated mechanisms covering GEO, LEO-MEO satellites and ticketing mechanism.
  - Significant Performance Gain.
- Advantages and Performance Comparison of Our Protocol
  - Cryptographic Aspect
  - Key Management and Architectural Aspect
- Conclusion



# Motivations

---

- Satellite multicast applications become more **important and prevalent** such as TV, multimedia video and audio distribution, pay-use applications, file transfer applications in current trend.
- **Providing security in satellite multicast systems is one of the most challenging problems in wireless communication.**
  - Naturally Broadcast, easy eavesdropping and active attacks.
  - Resource Constraint system.
  - Packet loss and delay problems are much severe.
- Problems becomes much severe for satellite multicast system having very **large number of members and high member join-leave frequency**.
- Unfortunately, existing security models **cause massive workload** on all of the system components.
- **We propose a novel three-tier satellite multicast security protocol that significantly reduces communication and cryptographic workload especially suitable for very large and highly dynamic satellite multicast systems (SSMS).**



# Problems of Multicast Security Systems

---

- Multicast security protocols suffers from cryptographic workload resulting from **rekeying to provide cryptographic goals**:
  - Confidentiality
  - Authentication
  - Integrity
  - Unforgeability.
- Generally, due to performance issue, some of the mentioned cryptographic goals are neglected .
- Most costly cryptographic goals are **forward and backward security** requirements.
- Every group member shares the same Group Key(GK) to encrypt/decrypt multicast data.
- GK has to be updated whenever there is a change in membership (join/leave event). This is done to provide forward and backward security.



# Problems of Multicast Security Systems

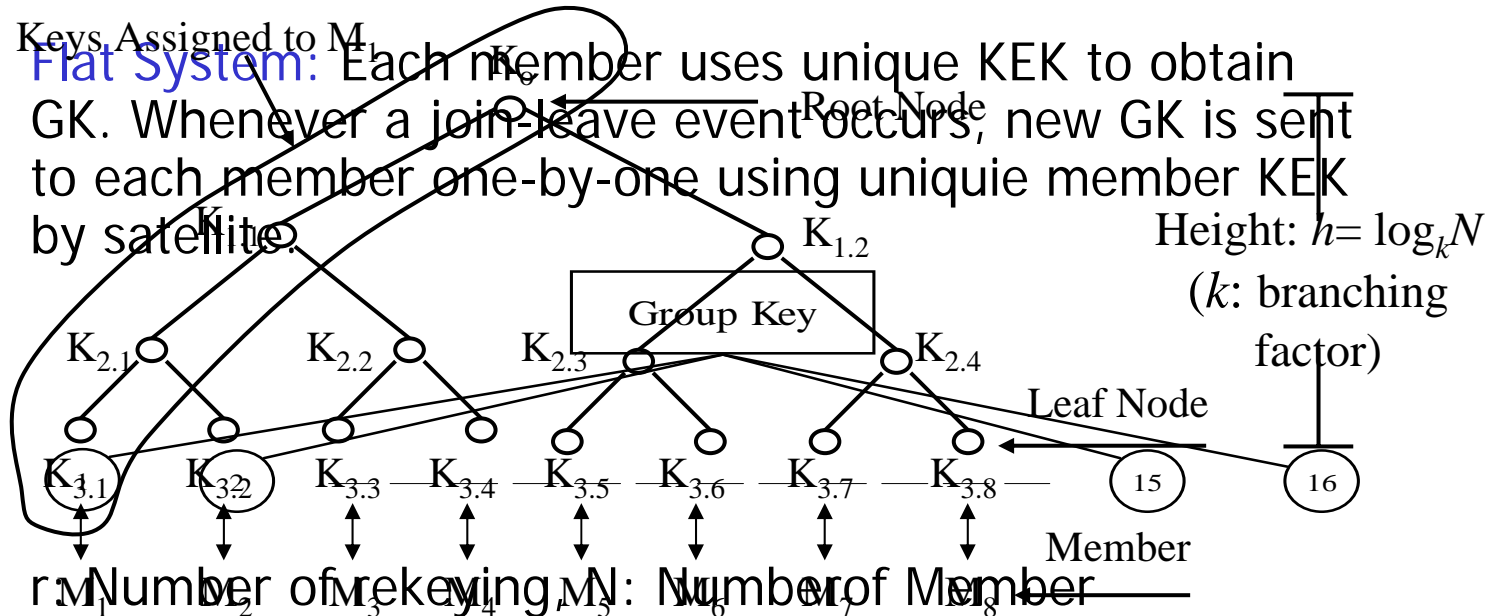
---

- **Forward Security:** If a member leaves from multicast system, GK should be updated. Else, member will be able to decrypt multicast data and reach information even if he/she is not a member of the multicast system.
- **Backward Security:** If a member joins the multicast system, GK should be updated. Else, a member can store previous multicasted data and using newly obtained GK, he/she can decrypt and obtain information even if he/she was not a member of the multicast system.
- **Key management problem :** How to distribute KEKs (Key Encryption Key) so that all valid members can be securely reached and updated with the new GK.
- Various protocols have been proposed to solve these problems. The solution approaches include:
  - **Group based hierarchy** (Flat (Iolus))
  - **Key based hierarchy** (LKH, OFT, ELK)
  - **Hybrid approach** (Our paper).

# Flat and LKH(Logical Key Hierarchy)

## Logical Key Hierarchy (LKH) (with 8 members)

- **Flat System:** Each member uses unique KEK to obtain GK. Whenever a join-leave event occurs, new GK is sent to each member one-by-one using unique member KEK by satellite.



- **Storage of KEKs:**
  - Workload of Satellite:  $r * O(N) = 10^9$
  - Storage load of Satellites:  $O(N) = 10^6$
  - Group controller (Satellite): For moderate or large  $N$ , Flat system becomes infeasible:
  - Member: Each member is uniquely assigned to a leaf node
  - Update Comm.:  $r * (k \log N - 1) = r * 21 \log 10^6 \approx 42000 \ll 10^6$  (Flat)



# Cryptographic Methods for Multicast Protocols

---

- Distributing GK with KEK requires hybrid cryptography approaches.
- Satellite executes key agreement protocols with members ( in key management protocol) using some PKC routines. However, no all major cryptographic goals are **generally provided**.
- RSA, DLP(Discrete Logarithm Problem) based El-Gamal and its variants, and especially Diffie-Hellman Key Exchange(DH) variants are frequently used. Also for group key exchange, GAP Diffie-Hellman variants are used.
- However, DH and GAP-DH based approach can not provide all active security properties and major cryptographic goals together efficiently.

# Our Contribution for Cryptographic Aspect

Advantages of EC over Factorization Based and Classical DLP Based Cryptosystem with comparison of Symmetric Cryptosystem

- **Problem:** DSA variants create message expansions. If message is small, then signature creates significant workload.

■ ECC is a projection of DLP problem over EC with finite field arithmetic and point multiplication arithmetic faster than vector arithmetic. For this reason, we have preferred ECC based cryptographic methods in our protocol.

■ As a novel approach, we utilize ECMQV (Elliptic Curve Menezes-Qu-Vanstone) authentic key exchange protocol in our three-tier satellite security protocol.

■ ECMQV is one of the most efficient authentic key exchange schemes in current PKC algorithms. It has been suggested as "Top-Level" security algorithm by NSA for government critic key exchange duties.

■ ECMQV is the projection of MQV key exchange scheme to EC domain. Thus, ECMQV provides all computational and storage advantages of ECC and keeps security properties of MQV.

Symmetric	ECC	DH/DSA/RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Table 1. Equal Security Level Bit Length



## Our Contribution for Cryptographic Aspect

---

- ECMQV achieves major cryptographic goals such as confidentiality, authentication, integrity and unforgeability more efficiently than its counterpart algorithms.
- Also, different from classical approaches, ECMQV provides security against some active attacks such as:
  - KK-S (Known Key Security)
  - FS (Forward Secrecy)
  - KCI-R (Key-Compromise Impersonation Resilience) under assumption of intractability of ECDLP.
- We use ECMQV to transmit group keys and group key seeds among satellite layers. Using these keys, bulk data multicast can be realized using symmetric key cryptography.
- As far as our concern, ECMQV has not been used for this purpose before.



## Our Contribution for Cryptographic Aspect

---

- Apart from ECMQV, we propose to use a novel cryptographic method, IMC (Improved Merkle Cryptosystem) in our three-tier satellite multicast security protocol.
- MC (Merkle Cryptosystem) is the first cryptosystem that provides secure communication over insecure channel. MC uses puzzle structure to provide public key properties in his system. In IMC, we have improved MC for both security and performance aspects.
- In IMC, cryptographic hash functions and a new puzzle structure are used together in order to increase the security of MC and VMC (Variant of MC). The key agreement value, which is sent as clear text in VMC, is hidden using a cryptographic hash function in IMC. Also, in order to increase the security of the key agreement value, auxiliary keys are used.
- Notice that, IMC inherently has significant storage requirement of MC. Thus, generally we prefer using ECMQV in our protocol. However, NTS (Non-Trusted Servers) help to solve this problem for IMC. Also, they facilitate key management for ECMQV.
- In addition to ECMQV and IMC, we use ECPVSS (Elliptic Curve Pintsov-Vanstone Signature Scheme) in the third layer of our protocol. Since ECPVSS is a Message Recovery type algorithm, it also provides many advantages for both computational and storage aspects.



# Contribution for Protocol Aspect

---

- Main idea behind of our design approach is to provide modularity and independency of the layers. Thus, workload of the individual satellite is significantly reduced. Moreover, number of keys that are stored in the satellite is significantly reduced.
- In addition to these, we propose three-tier independent key distribution layer, utilizing existing hierarchy among satellites in satellite network. In our protocol, GK and KEKs are generated by GEO satellites (top level of the hierarchy) and distributed to lower layers using appropriate cryptographic algorithms.
- We use main principle of TTPVSS (Two-Tier Pintsov-Vanstone Signature Scheme), that is hybrid key management approach utilizing multi-LKH layer and Iolus type key management protocol in integrated manner.
- This approach eliminates single point of failure problem in pure centralized approach. Also, independency of layer with centralized key management approach reduces the cost of pure decentralized approach. In this way, we can utilize advantages of both logical key tree based approaches and Iolus type decentralized approaches together.



## Contribution for Protocol Part

---

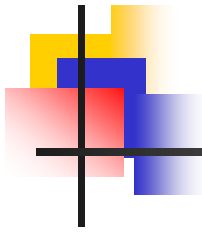
- Two Major problem: Depth of the tree, spreading effect of the modification, on which performed any point of the tree to the root of the tree. Our solution:
- **Three Independent LKH Key Distribution Layers are used.** These layers are:
  - GEO satellite layer
  - LEO-MEO satellite layer
  - Terrestrial Unit (TU)-Members Layer.
- **Most important contribution is: Join-Leave operation of one member does not affect any other group or Satellites in the multicast system. For this reason workload of satellites significantly is reduced.**



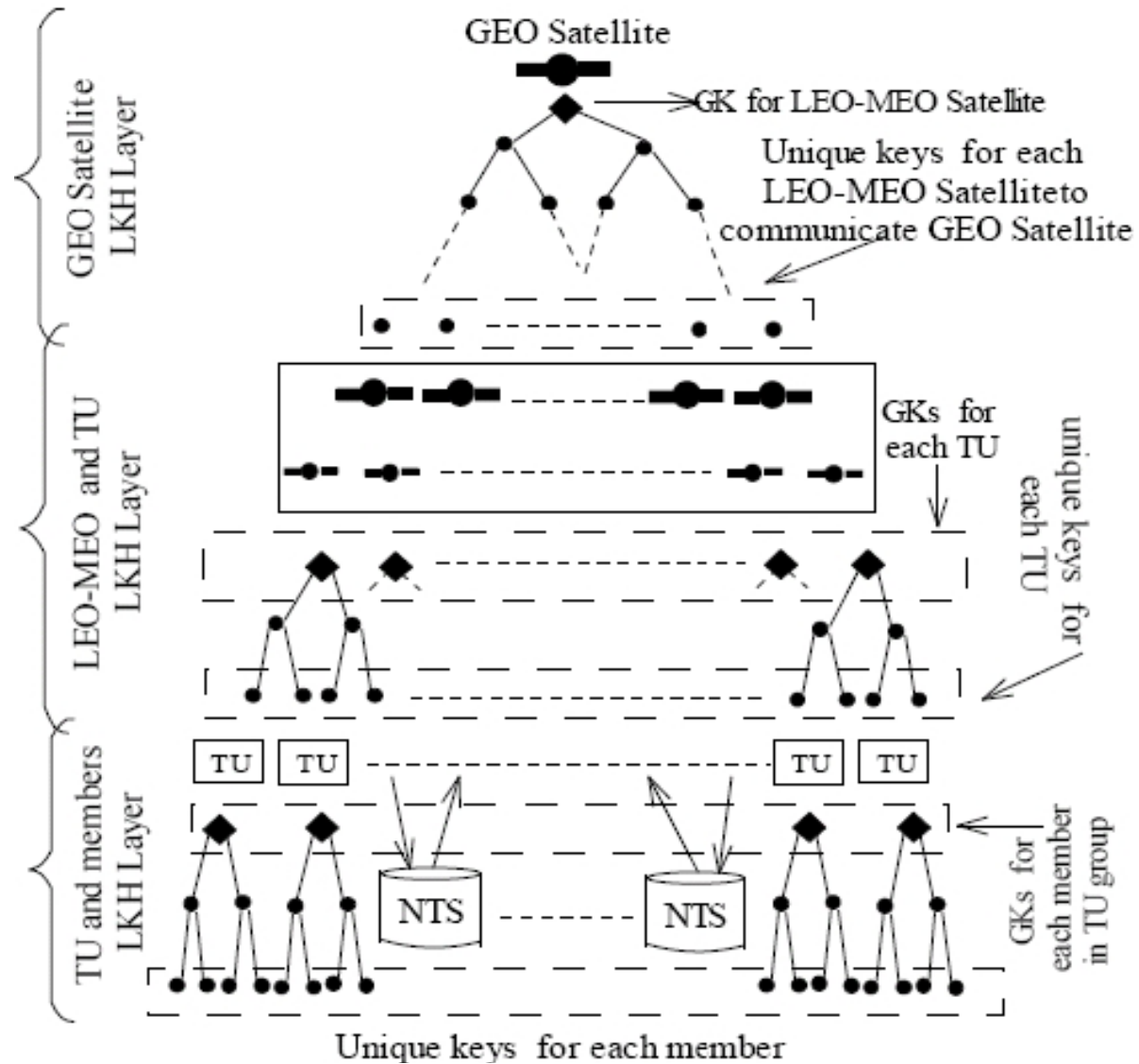
# GEO Satellite Layer

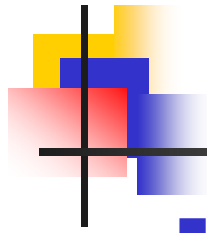
---

- GEO satellite layer is responsible for general key management of the overall multicast system. The group keys, which are generated by the GEO satellite, are transmitted to each layer in encrypted form.
- In this protocol, group keys of the lower layer are known by only the upper layers and keys are only determined by the GEO satellite. This way, the GEO satellite can always control and manage the overall multicast system.
- Firstly, the GEO satellite(s) realizes ECMQV key exchange to transmit group keys and seeds to the LEO-MEO satellite layer. Secondly, it generates and transmits group key seeds, which will be used between the LEO-MEO satellite and TUs, to the LEO-MEO satellite layer. Thirdly, it generates and transmits group key seeds that will be used between TUs and members to realize a secure communication.
- These session keys and seeds should be generated by a CPRNG (Cryptographic PRNG) like Blum- Blum-Shub because they will be used for long term security as a principle of batch keying. Also, as an option, if needed, the GEO satellite may involve data multicast.



# Architecture of Our Protocol

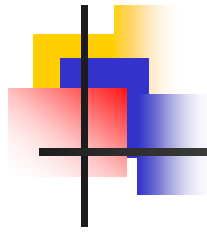




# LEO-MEO Satellite Layer

---

- This layer is mainly responsible for bulk data multicast to TUs and distributing group keys to the TUs and NTS. LEO-MEO satellites obtain shared secret keys from the GEO satellite.
- Each LEO-MEO satellite uses these shared secret keys to obtain the related group key to communicate with the upper layer.
- The group key seeds are used to generate group keys. Then, they distribute the group keys and session key seeds to the TU using either ECMQV or IMC protocol also involving NTS if necessary.



## TU – Member Layer

---

- In this layer, TUs are responsible for decrypting the data coming from the LEO-MEO satellite layer and multicasting it after encrypting it with required group keys. TUs obtain and use group keys to realize secure communication with the LEO-MEO satellite layer using either ECMQV or IMC protocol also involving NTS if necessary.
- TUs use seeds to generate group keys that will be used for secure bulk data multicast.
- TUs send GK to members using ECPVSS different from other layers. The reason is that, computational and storage possibilities of members are lower than satellites and TUs. Thus, ECC-MRDS type algorithm is more suitable.



## Performance Comparison(Cryptography Aspect)

---

- In our proposed protocol, ECPVSS, ECMQV and alternatively IMC algorithms are used. We show comparison of these algorithms and other prevalently used approaches in key exchange methods.
- DH-ECDH protocols are frequently used for key exchange. **However, pure implementation of these protocols is insecure.** Man-in-the-middle attack is the most well-known attack used against these protocols.
- **Also, these protocols do not provide KK-S, FS and KCI-R security properties.** Notice that for signature variants and ECPVSS, KK-S, FS and KCI-R are not compared because signature variants and ECPVSS are not key exchange protocols.
- Taking into consideration the properties of algorithms, we show whether the algorithm provides the mentioned property (authentication, integrity, unforgeability) or not.
- Also, for three criteria, bandwidth efficiency, computational effort and confidentiality, VL (very low), L (low), M (moderate), H (High) and VH (very high) levels are assigned.
- **As we see, ECMQV and ECPVSS are the most efficient and secure algorithms among the mentioned alternatives.**



## Performance Comparison(Cryptography Aspect)

Comparison of cryptographic protocols with regard to nine essential criteria. RSA-S denotes RSA Signatures and DSA-V denotes DSA Variants

	DH	ECDH	RSA-S & DSA-V	ECPVSS	IMC Based	ECMQV
Authentication	No	No	Yes	Yes	Yes	Yes
Unforgeability	No	No	Yes	Yes	Yes	Yes
Integrity	No	No	Yes	Yes	Yes	Yes
KK-S	No	No	-	-	Yes	Yes
FS	No	No	-	-	Yes	Yes
KCI-R	No	No	-	-	Yes	Yes
BW Efficiency	M	H	L	VH	VL	H
Computational Efficiency	M	H	M	VH	M	H
Confidentiality	H	H	H	H	VH	H



## Performance Comparison (Protocol Aspect)

---

- We show performance comparison of our protocol to Flat, LKH and TTPVSS. The comparison is based on five major criteria: **Rekeying workload for satellite layer and TU, number of keys stored in satellite layer, in TUs and members on the average.**
- The most important criterion is the average rekeying workload of the satellite layer. Since the most resource limited part of the satellite multicast system is the satellite layer, we aim to minimize rekeying workload of this part. **For this criterion, among the compared protocols, the most efficient one is our proposed protocol.**
- Notice that, for average number of keys stored in the satellites, our protocol also provides significant advantages to pure implementation of some of the well-known protocols.

# Performance Comparison (Protocol Aspect)

Performance comparison of our protocol to Flat, LKH and our previous protocol (TTPVSS) is given for five major criteria. Avg. rekeying workload and number of keys in satellite layer (SL) only applicable to our protocol for GEO and LEO-MEO SL.

$$N \geq 10^6, r \approx 10^5, l = (500 - 1000), n_l = N/n_s \geq 2048, n_s \approx 100, m_2 > m_1, q = l/n_s$$

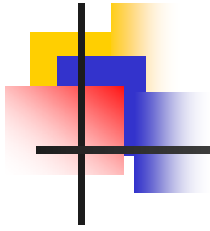
	Avg. rekeying workload for SL	Avg. # keys stored in SL	Avg. rekeying workload for TU	Avg. # keys stored in TU	Avg. # keys stored in member
Flat	$N \cdot r$	$N$	-	-	1
LKH	$(k \log_k N) \cdot r$	$N$	-	-	$\log_k N$
Previous Protocol	$(k \log_k l) / m_1$	$l$	$\log_k n_l$	$n_l + \log_k l$	$\log_k n_l$
Proposed Protocol	$(k \log_k q) / m_2$	$6n_l + l + 1 \approx 2l$	$\log_k n_l$	$n_l + \log_k l$	$\log_k n_l$
GEO	$k \log_k n_s \leq 10$	$6n_l + l + 1 \approx 2l$			
MEO-LEO	$(k \log_k q) / m_2$	$q < l$			



# Conclusion

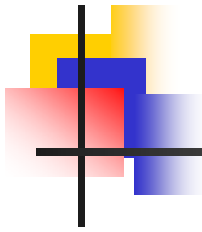
---

- A novel three-tier satellite multicast security protocol has been proposed that significantly reduces the workload of the satellites and provides high security.
- Protocol is especially designed for very large number of member size and highly dynamic groups. Provided advantages make possible to use proposed protocol for secure satellite multicast applications that can not be realized with some classical protocol.
- Three independent LKH-Iolus hybrid key management layer is a novel approach that provides significant performance gain and can be accepted as a general method for different key management protocol integration.
- Using ECMQV, ECPVSS and IMC for KEK and GK transmission is a novel approach that significantly reduces network workload. Moreover, this approach provides many cryptographic goals together efficiently that can not be provided with classical key exchange protocols.
- Batch keying and ticketing mechanisms additionally reduces the cryptographic workload of SSMS.



THANK YOU FOR LISTENING

---



# TTPVSS Architecture

