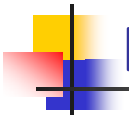
Scalable Secure Group Communication over IP Multicast

Authors:Suman Banerjee, Bobby Bhattacharjee

Speaker: Kun Sun

Contents

- Introduction
- Related Work
- Secure multicast using clustering
- Spatial Clustering
- Simulation Experiment
- Conclusions



Introduction(1/2)

- If assuming the network infrastructure is insecure :
  - Non-members can eavesdrop on the multicast group and store encrypted messages
  - The members who have left the group can continue to decrypt messages
  - New members can decrypt messages they had stored previously

  ➡ Need the “Group re-keying” during each membership change

Introduction(2/2)

- Point-to-point ➡ Point-to-multipoint
  - Scalability problem of key management
- This paper’s algorithm
  - Does not require router support
  - Completely end-host based

Related Works(1/3)

- Group Key Management Protocol (GKMP)
  - Group Key Controller generates group keys.
- Scalable Multicast Key Distribution (SMKD)
  - It requires explicit router support, not scalably solve the problem of group re-keying.

Related Works(2/3)

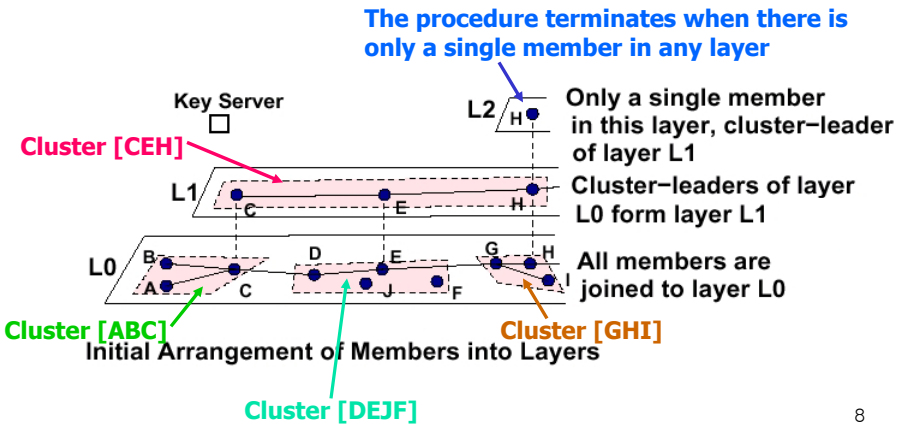
- Iolus
  - Divide the secure multicast group into multiple sub-groups, which is managed by Group Security Agent (GSA).
  - Not define size bound of subgroup
- MARKS
  - Assume the duration that a member stays in the group known apriori.

Related Works(3/3)

- Key Graphs scheme
  - Use a tree hierarchy of keys distributed between members.
- Boolean Minimization
  - Use virtual hierarchy of keys
  - More scalably than Key Graphs scheme i n bulk membership changes

Secure Multicast using Clustering

- Member hierarchy for Key distribution

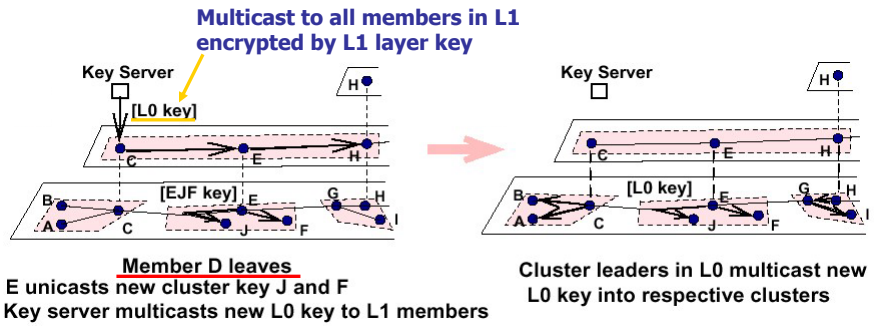


Secure Multicast using Clustering

- Layer Keys and Cluster Keys :
  - Layer key
    - Possessed by the group members in that specific layer
    - Generated, on-demand, by a key-server
  - Cluster key
    - The leader of each cluster is responsible for generating the cluster key for that cluster
    - A pair-wise key is shared between the cluster-leader and each member

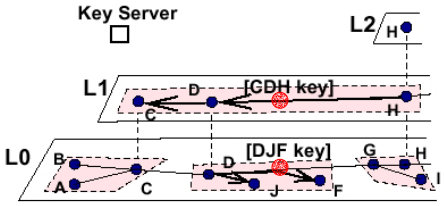
Secure Multicast using Clustering

- Key Distribution Protocol (Example 1)
  - Assuming the cluster size : 3~5



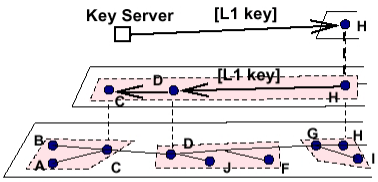
Secure Multicast using Clustering

- Key Distribution Protocol (Example 2)

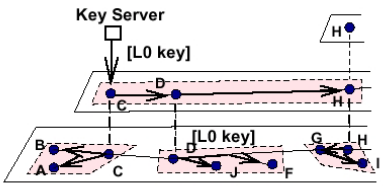


Member E leaves from initial configuration
It was part of layers L0 and L1
D replaces E as cluster-leader in the L0 cluster (DJF)
D unicasts new cluster key in DJF cluster
D joins layer L1, and the cluster CDH
H unicasts new cluster key in CDH cluster

- Example 2 cont.



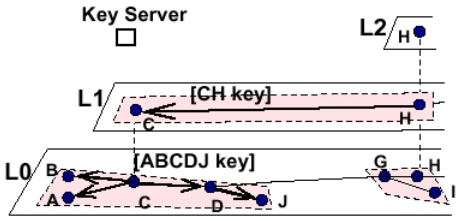
Key server multicast the new L1 key to L2 members
L2 members (cluster-leaders of L1) multicasts this new L1 key into respective L1 clusters



New L0 key is multicast by key server to L1 members as before. It is encrypted using the new L1 key.
They are distributed as before into L0 clusters

Secure Multicast using Clustering

- Key Distribution Protocol (Example 2)



Member F leaves from the configuration in 3.
Two clusters merge in layer L0
D drops out of L1.
New cluster keys are generated for L0 cluster ABCDJ and the L1 cluster CH, by cluster leaders C and H.

Spatial Clustering

- Clustering algorithm
  - Member discovery protocol
  - Clustering protocol

Spatial clustering

- Member discovery protocol
  - Defines **parent-child relationships** among the different members of the multicast tree
  - Focus on network layer multicast scheme that creates shared bi-directional trees (e.g.CBT)
  - $d(x,y)$: distance between the members x and y, in router hops, then,
    y is considered to be **parent** of x, if and only if
    - $d(S,y) \le d(S,x)$ (where, S is source)
    - $\forall z$ that satisfy $d(y,x) \le d(z,x)$

Spatial Clustering

- Member discovery protocol (Cont.)

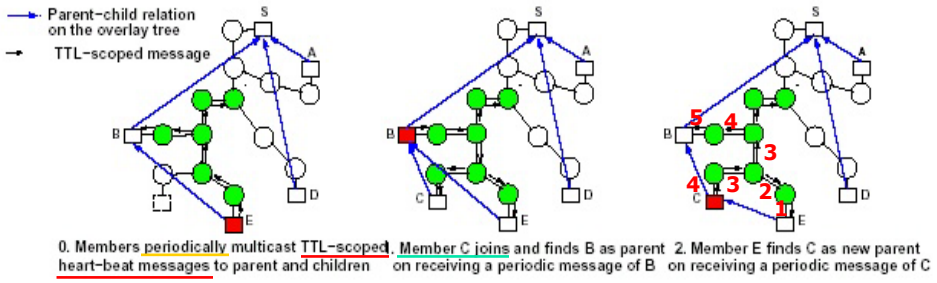
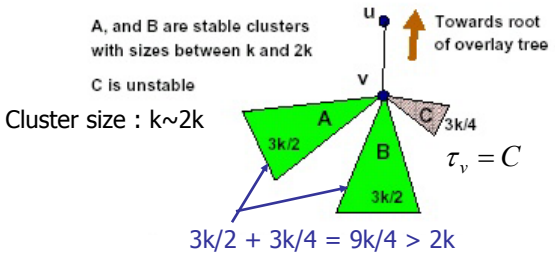


Fig. 3. Member discovery protocol example

Spatial Clustering



- τ_v : subtree rooted at some node v, which cannot be joined to any cluster rooted at v, and has to be joined to a cluster that is rooted at a node upstream of node v

  ➡ *Unstable subtree*

Spatial Clustering

- Clustering protocol (Cont.)

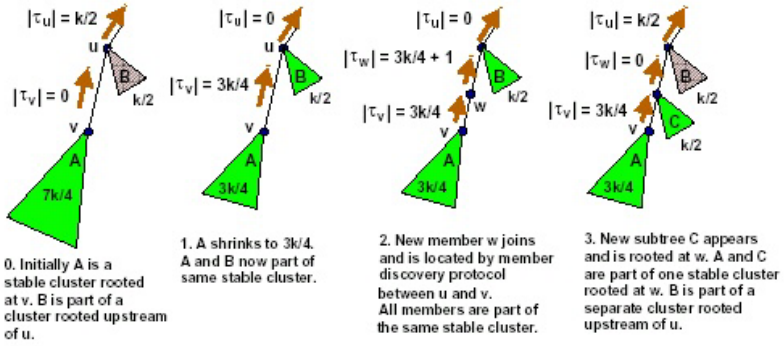


Fig. 7. Clustering protocol example

Simulation Experiment

- Experiment setup
  - Simulated network infrastructures that
    - do support **directed multicast**
      → sender can multicast a packet to individual subtree(s) rooted at a specific router on the multicast delivery tree
    - do **not** support directed multicast
      → using a different multicast address
      → Instead, using TTL-scoping :
      scoped multicast

Simulation Experiment

- Experimental methodology
  - *Key-normalized byte count*
    - The network overhead for re-keying at a single router assuming unit(1 byte) key size
  - *Packet load*
    - A counter of the # of packets processed by the routers on the multicast tree
  - *Storage and Processing Overhead*
    - The # of keys stored at each node and the # of cryptographic operation at each node

Simulation Experiment

Scheme	Single member leaves (varying group size) 3000	6000	12000	24000	48000	96000	1% of group leave (varying group size) 3000	6000	12000	24000	48000	96000
KG-sequential	4.9	5.6	5.0	6.0	5.3	6.3	23.2	32.8	36.3	49.5	57.1	76.8
KG-spatial	1.9	2.1	**1.6**	2.0	**1.5**	**1.8**	10.3	13.7	14.9	18.7	20.8	27.0
Spatial clustering	**1.6**	**1.6**	1.7	**1.7**	1.7	**1.8**	**3.2**	**3.3**	**3.4**	**3.4**	**3.5**	**3.6**

TABLE II Comparison of key normalized byte count per router on a directed multicast-capable network.

Scheme	Single member leaves (varying group size) 3000	6000	12000	24000	48000	96000	1% of group leave (varying group size) 3000	6000	12000	24000	48000	96000
Key graphs	22.2	23.9	26.8	28.5	31.0	32.4	394.2	792.7	1578.2	3092.7	6222.7	12609.6
Boolean minimization	11.0	12.3	13.5	14.2	15.0	16.2	53.5	94.8	169.9	302.6	567.3	1077.0
Spatial-1	162.5	125.7	121.1	117.5	130.0	117.7	296.4	221.4	190.8	191.2	198.1	208.1
Spatial-16	8.7	11.0	13.9	16.5	19.3	20.6	10.3	12.8	16.2	19.1	22.4	24.1
Spatial-24	6.3	8.1	10.5	12.1	14.4	15.3	8.2	10.3	12.5	14.7	17.1	18.5
Spatial-directed	1.6	1.6	1.7	1.7	1.7	1.8	3.2	3.3	3.4	3.4	3.5	3.6

Spill over

TABLE III Comparison of normalized byte load per router for the different schemes using scoped multicast.

Spatial-i : *i* different multicast addresses

→ a simple decentralized address assignment scheme
: each cluster picks one multicast address at random, independent of each other

Simulation Experiment

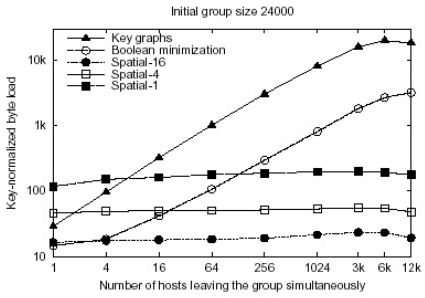


Fig. 8. Varying the number of simultaneously leaving members (Scoped multicast)

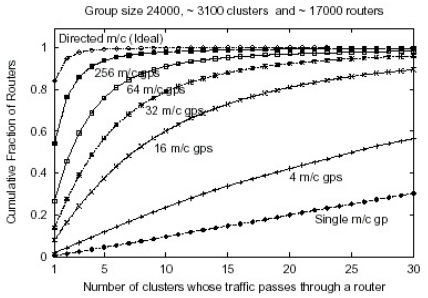


Fig. 9. Cumulative distribution of the routers that handle cluster traffic for different number of clusters

<Impact of batched updates>

<using multiple multicast addresses>

Simulation Experiment

Scheme	A single member leaves		1% of group leaves		10% of group leaves		25% of group leaves	
	KBytes	Packets	KBytes	Packets	KBytes	Packets	KBytes	Packets
Key graphs	1.8	4	197.9	370	905.2	1689	1273.1	2376
Boolean minimization	**1.0**	**2**	12.2	37	100.2	187	184.3	344
Spatial-1	7.5	118	12.2	191	12.8	200	12.3	193
Spatial-16	**1.0**	17	**1.2**	**19**	**1.5**	**23**	**1.5**	**23**
Spatial-directed	0.1	2	0.2	4	0.5	8	0.5	8

TABLE IV Comparison for key-normalized byte and packet loads per router (Group size: 24000 initial members).

Scheme	Number of Keys		Processing at members			Processing at key server		
	Member	Key server	Single leave	1% leaves	10% leaves	Single leave	1% leaves	10% leaves
Key graphs	9	32002	1.7	5.5	6.4	28.0	3095.3	14310.5
Boolean minimization	15	31	**1.0**	**1.0**	**1.0**	15.0	302.9	1583.5
Spatial clustering	**3**	**6**	1.2	1.5	2.4	**1.3**	**3.5**	**4.0**

TABLE V Comparison of storage and processing costs for the different schemes for a group of 24,000 initial members

Conclusions

- This paper's algorithm
  - Does not require router support
  - Completely end-host based
    ➡ efficient in practice
- Directed multicast is an useful primitive for implementing many secure multicast schemes

References

- Suman Banerjee, Bobby Bhattacharjee,Scalable Secure Group Communication over IP Multicast
- I. Chang, R. Engel, D. Kandlur, D. Pendarakis, and D. Saha, Key management for secure internet multicast using boolean function minimization techniques. In Proceedings of Infocom, New York, March 1999
- C.K. Wong, M. Gouda, and S. Lam. Secure group communications using key graphs. Proceedings of SIGCOMM, September 1998