IP Multicast Security

Abdelmadjid Bouabdallah, Isabelle Chrisment

ING 2004 - Obernai

IP Multicast security

Abdelmadjid BOUABDALLAH[1], Isabelle CHRISMENT[2]

[1]Lab. Heudiasyc, UMR CNRS 6599, UTC, France
bouabdal@utc.fr

[2] ESIAL-UHP, LORIA-Projet MADYNES France
ichris@loria.fr

- Thanks to :
  - Mohamed Salah Bouassida (Loria)
  - Ghassan Chaddoud (Loria)
  - Yacine Challal (UTC)
  - Mounir Kellil (UTC)

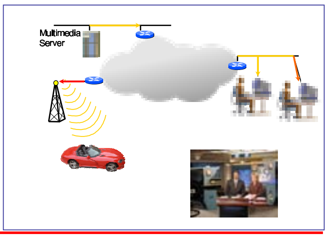
Outline

1. Introduction

IP Multicast

The growth of the Internet is accompanied by the multiplication of new applications :

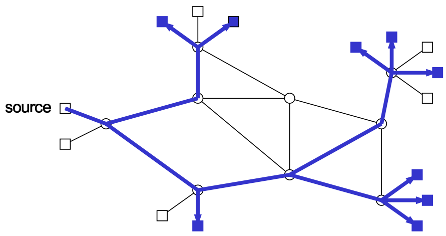
- *Multimedia Conferences,*
- *Pay Per View,*
- *Multiparty Video Games*
- *Military Communications,...*



IP Multicast- (cont.)

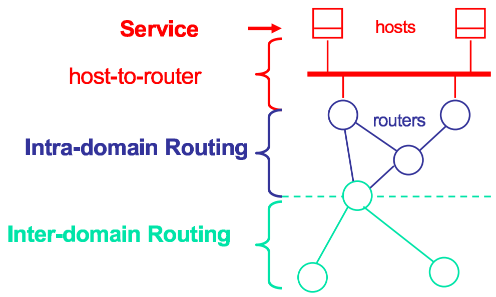
- One or more sources are sending data to multiples receivers
- Multicast aims to send data to a set of receivers (group)
- Multicast router replicates packets only when needed
- Multicast avoids processing overheads associated with replication at the source and the bandwidth overheads

Multicast Architecture



Dynamic Membership : prune/graft

IP Multicast Architecture



Multicast Routing

Multicast Routing Protocols

- **Dense Mode** : [DVMRP, MOSPF, PIM, SSM …]
  Per source trees, Flooding and Prune
- **Spars Mode** : [CBT, PIM-SM, …]
  - Shared Trees, explicite join
- **Inter-Domaine**: [BGMP, PIM-SM/MSDP, …]

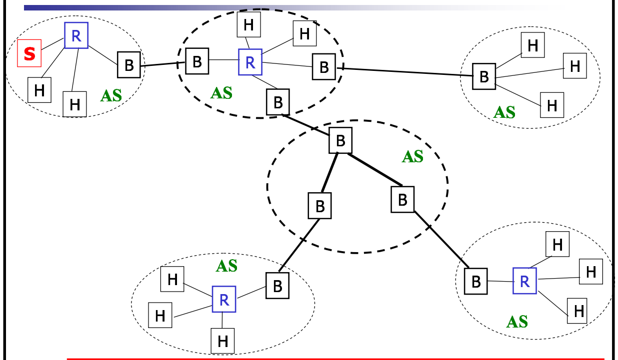
Multicast groupe management

- **Adressing**: SDR, MASC, …
- **Join/Leave**: IGMP,MLD
- …

- A multicast group is identified by an IP address (multicast address)
- A multicast source does not need to maintain a list of receivers
- A receiver initiates the membership request to its local multicast router
- Multicast receivers are allowed the freedom of joining and leaving the multicast session
- One or many delivery trees are built for a single multicast group (i.e shared-tree or per source tree)

- The demand for multicast communications is increasing
- One obstacles to the wider deployment of IP multicast is the lack of security
  - Security for the multicast data being transmitted
  - Security of infrastructure underlying the IP multicast

Problem-Areas in Multicast security



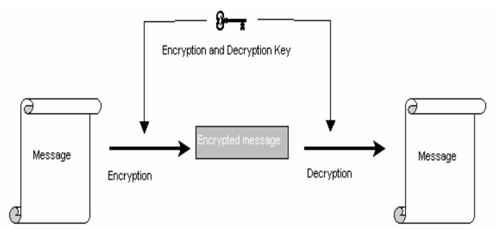
Problem-Areas in Multicast security

- **Core problem area**
  - Methods for multicast data confidentiality/integrity and source authentication
  - Multicast group key management
  - Multicast security policies
- **Infrastructure problem area**
  - Security of multicast routing protocols
  - Security of reliable multicast protocols
- **Applications problem area**
  covers more advanced issues that might be built upon eventual secure multicast infrastructure

2. Security Services

Definitions

- **Confidentiality**: only authorized receivers will get the data.



Definitions- (cont.)

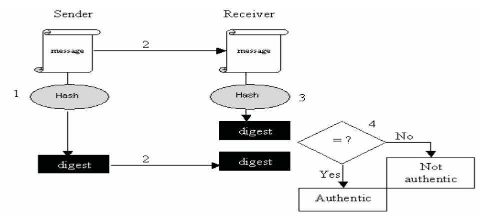
- **One-way function (*f*):** given *x*, it is easy to compute *f(x)*, but given *f(x)* it is hard to deduce *x*.

- **Hash function :** is a one-way function that takes a variable length string and converts it to a fixed length string called **digest**.

- **Message Authentication Code (MAC) :** is a one way hash function with the addition of a secret key

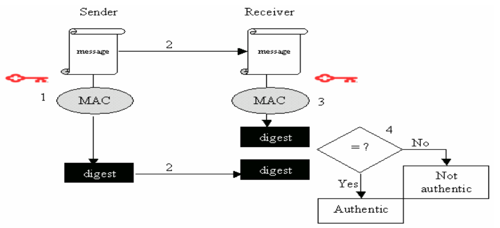
Definitions- authentication (data integrity)

- the message has not been modified during its transmission.
- Generally, we use hash functions to assure message authentication.



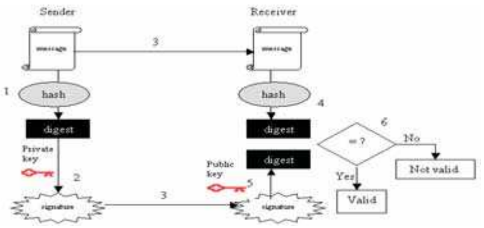
Definitions- authentication

- Consists in assuring that a received message originates from a source having a specific identity.
- Generally, we use MACs to assure source authentication.



Definitions- Non-repudiation

- An authorized receiver can prove to a third party the identity of the data's source.
- Generally, we use digital signatures to assure non-repudiation.



3. Factors in securing IP multicast

The most relevant factors influencing IP multicast security include :

- Multicast application type
- Group size and group dynamics
- Scalability issues
- Trust model

Multicast application type

Application type could be :

- One-to-many
- Many-to-many
- Frequency and rate of data transmission

Group size / Group dynamics

Important factors affecting multicast security :

- group size

- frequency of join and leave

Scalability issues/ Trust model

- **Scalability** is the ability of the mechanisms implementing the security features to be extended :
  - to cover large group of members over large region
  - and offer good performance
- **Trust model** addresses the issues of which entities to be accorded trust to carry-out
  - the generation, distribution and management of cryptographic keys and security policies
  - Source of authority,
  - …

4. Standardization

IRTF : GSEC

- Group GSEC (Group SECurity)
  - Has replaced SMuG group in July 2000
- Chairs :
  - Lakshminath Dondeti (Nortel) and Peter Dinsmore (NAI Labs)
- www.securemulticast.org

IRTF GSEC
Emerging technologies, not ready for standardization

Areas of Interest

1. Group Policy Management :Policy parameters that describe group authorization
2. Decentralized Group Key Management : Design robust and fault tolerant protocols with multiple *Key Distributors* (KDs)
3. Security technologies for *closed* and *open* groups
4. Multiple Senders : denial of service protection, minimize state needed for sender authentication
5. Group Key Management & Wireless Applications : scalability, processing requirements energy usage, storage, and inter-member communications
6. Non-multicast security : Broadcast, Anycast, group key management for ad-hoc networking, etc
7. Reliable Multicast : Relationship between secure multicast and reliable multicast

IETF : MSEC

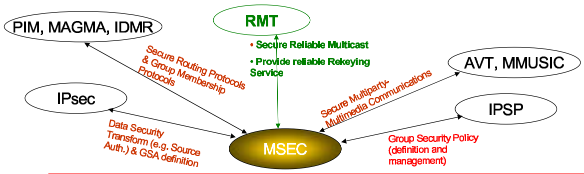
- Group MSEC (Multicast SECurity)
  - Created in march 2000
- Chairs :
  - Thomas Hardjono (Verisign) and Ran Canetti (IBM)
- www.ietf.org
  - Security Area
- www.securemulticast.org

IETF MSEC -Developing Standard Solutions

Areas of Interest

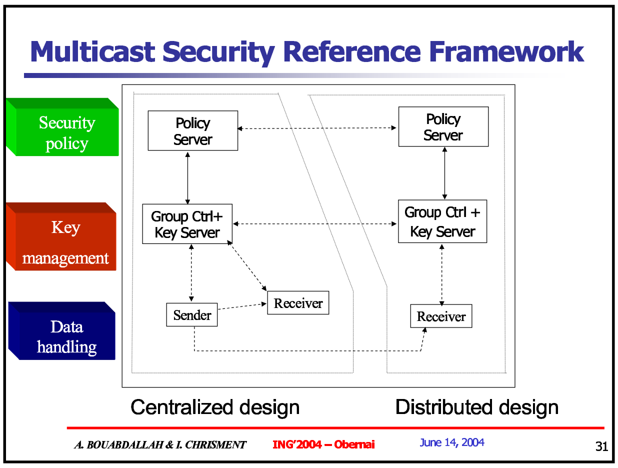
1. Specify a general framework having as main components:
   - Source Authentication protocols
   - Group key management and group security association (GSA)
   - Group policy management mechanisms
2. Protect against denial-of-service attacks, whenever possible
   - E.g. Sender & Receiver Access Control Mechanisms
3. Address the Many-to-Many Security Problem

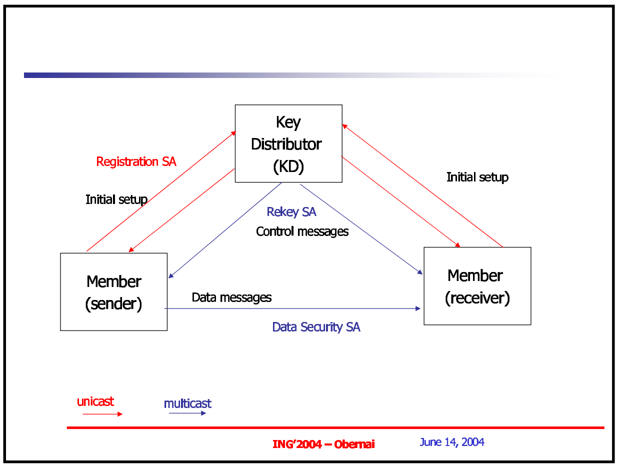
Interaction with Other IETF's WGs

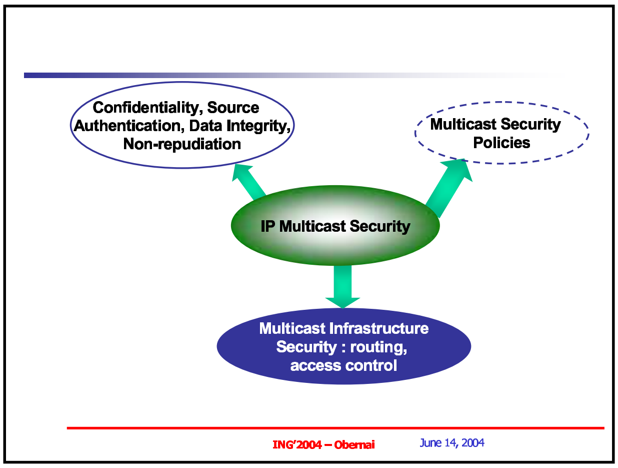


MSEC Architecture

- draft-ietf-msec-arch-05.txt
  - January 2004
  - The Multicast Group Security Architecture
- Presents an overview of the multicast architecture used to secure data packets of large multicast groups
- Defines and explains GSA (Group Security Associations)


Multicast Security Reference Framework
Security policy
Key management
Data handling
Policy Server
Policy Server
Group Ctrl+ Key Server
Group Ctrl + Key Server
Sender
Receiver
Receiver
Centralized design
Distributed design
A. BOUABDALLAH & I. CHRISMENT
ING'2004 – Obernai
June 14, 2004
31


Key Distributor (KD)
Registration SA
Initial setup
Initial setup
Rekey SA
Control messages
Member (sender)
Member (receiver)
Data messages
Data Security SA
unicast
multicast
ING'2004 – Obernai
June 14, 2004


Confidentiality, Source Authentication, Data Integrity, Non-repudiation
Multicast Security Policies
IP Multicast Security
Multicast Infrastructure Security : routing, access control
ING'2004 – Obernai
June 14, 2004

5. Multicast Infrastructure Security

Securing Multicast Routing

- Protecting the routing information from being illegally modified in transit or in storage
- Protecting from bugs or false routing information being injected into the network

⇨ *Routers must be provided with the ability to detect and reject false information*

Multicast Infrastructure security- (cont.)

- In IP multicast model, any host can join a multicast group
- Edge multicast routers do not maintain identification information about the hosts that join the group

Possible attacks :

- A host joins a multicast group without any intention of using the data being delivered to it (receiver attack)
- A non member, simply joins the group causing the tree to expand and the multicast to be forwarded
- Injection of bugs packets with the correct multicast address (sender attack)

⇨ **bandwidth consuming**

Multicast security is more challenging!!

Mobility support

- Mobile IP
- Ad'hoc networks

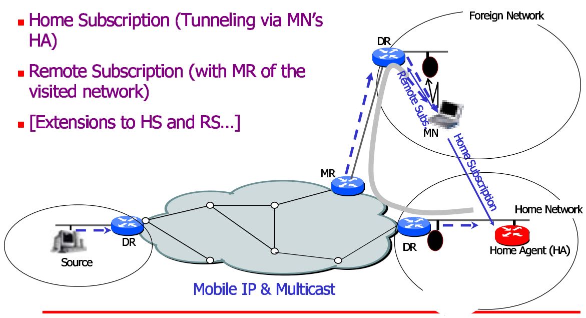
Mobile IP

Motivation : users need to move while working and communicating

- Mobile IP (v4, v6) protocol (IETF)
  - transparency and management of user mobility in the Internet
  - Mobile Node (MN) continue communicating with its Correspondent Node (CN) while changing network location (*Handover*)
- Multicast Support
  - Home Subscription (Tunneling via MN's HA)
  - Remote Subscription (with MR of the visited network)

Mobile IP- (cont.)

- Multicast Support
  - Home Subscription (Tunneling via MN's HA)
  - Remote Subscription (with MR of the visited network)
  - [Extensions to HS and RS…]



Mobile IP & Multicast

Securing Ad hoc routing

Ad Hoc Networks Vulnerabilities

- Attacks by jamming Radio
- Attacks by consumption of batteries
- Perturbation of Ad Hoc Routing due to modifying routing information
- Compromising internal nodes in the network
- Ensuring Dynamicity and Scalability of the security architecture solution

Sender/Receiver Access Control

- Sender access control
- Receiver access control

Sender/Receiver Access Control- (cont.)

- Any host can send its Report messages for any multicast group as a receiver
- Any user can send its traffic to any multicast group as a sender
- Multicast traffic Confidentiality do not resolve the problem

Consequences

- Risk of illegitimate use of multicast router resources
- Risk of Denial of Service (DoS) Attacks on the group scope
  - ✓ Malicious senders
  - ✓ Malicious receivers

Sender/Receiver Access Control- (cont.)

- User Authentication and Authorization
- Based on a *Proof-of-Legitimacy*
  - ✓ Receiver: Securing Group Membership (MLD/IGMP) Report Messages
  - ✓ Sender: Specific mechanisms…

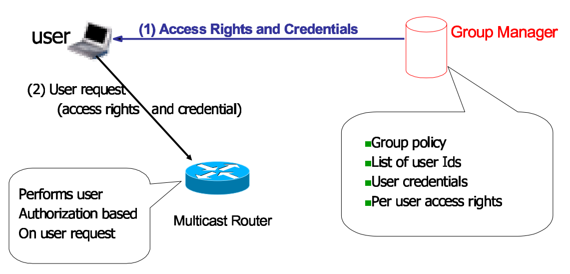
Open/ Current Issues : Reduce DoS attack risks, sender access control, mobility support

Sender/Receiver Access Control Issues

Mobility related-issues

- DR of the visited network *vs.* HA
  - Transmission/reception via HA: issues of the stationary case
  - Transmission/reception via DR of the visited network: concerned with mobility issues
- Failure of the [authentication and] authorization procedure(s)
  - Limited scope of the credential coverage
    - The multicast router authorization (e.g. a DR) of the visited network/domain does not hold the necessary information (e.g. the key) to perform user [authentication and] authorization
    - The multicast router does trust/know the issuer/signer of the credentials
  - Time Information incorrect (e.g. outdated): difference between time zones across domains
    - Time information part of the access rights

Access Control to the multicast delivery tree



Proposed solutions

Sender/Receiver access control solutions

Digital signature based solutions	Shared secret based solutions
•Basic receiver access control •Token based solutions •Gothic •…	•IGMP Authentication •RAC-PIM-SM •MLDA •…

Basic Receiver Access Control

IGMPv3 Security Consideration Section : two solutions are proposed

- report messages are authenticated using single key shared between router and host
  - ⇨Any node having the key can forge the report messages!!
- digital signature : All hosts need to know the public key of all routers, and all routers need to know the public key of all hosts in the subnet.
  - *Advantages*: Simple
  - *Drawbacks:*
    - A large amount of keys both in hosts and routers
    - Processing overhead and DoS attacks at the multicast router side (digital signature)
    - Does not support sender Access Control, user exclusion, [and member mobility]

Token-based Solutions

[Hardjono & Cain, 2000]

- **Receiver access control** based on a one-time token
- Token contains a validity period and a symetric key (*IGMP key)* that is used to authenticate receiver's *Report* messages.
- Token is digitally signed and sent by the *Key Server* to the Multicast routers and authorized hosts.
- Multicast router maintains a list of access tokens
- Receiver : provides its access token to the edge multicast router
- Multicast router side
  - Authenticates (dig. Sig.) then checks the received token (IGMP key and validity period)
  - Authenticates (IGMP key) the Report message then verifies (in the corresponding entry of the access token list) whether the requested multicast address is bound to the IGMP key

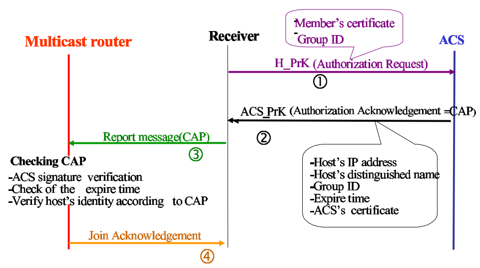
Token-based Solutions- (cont.)

- *Advantages:*
  - Provides user exclusion (token contains a validity period)
- *Drawbacks:*
  - User exclusion (Validity period) may not be efficient in a typically dynamic environment (membership duration unknown, i.e. higher (=>session interruption)/ lower than the validity period + token is not encrypted)
  - Does not address the sender access control problem
  - Vulnerable to *DoS* attacks (multicast router receives fake tokens=> digital signature verifications)
  - Limited performance:
    - Receiver needs a distinct access token for each group, with a distinct IGMP key,
    - Edge multicast router may have a large amount of access tokens.
  - May not work in mobile environment (coverage of access token list+ public key/and trust on key server signature)

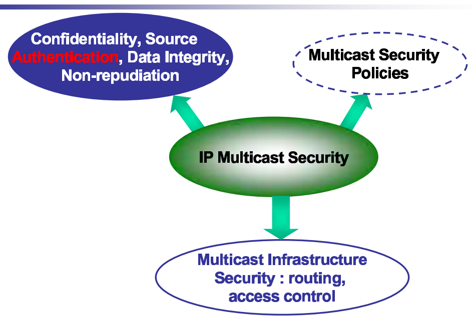
Gothic

- Gothic(Group Access Control architecture for Secure Multicast and Anycast, *Jugge, Ammar, Infocom 2002*)
  - Receiver Access Control
  - *Access control functions:* authentication and authorization of users according to the group policy.
  - *Access Control Server* (ACS): provides to authorized hosts a credential called Capability to enable them participating to particular multicast groups.
  - Group Join: host sends its *Report* message to the multicast router including the capability
  - Check of Capability integrity by the multicast router:
    - ACS signature
    - Authenticate the host, and verifying that host's identity and that included in the capacity match.

Gothic- (cont.)

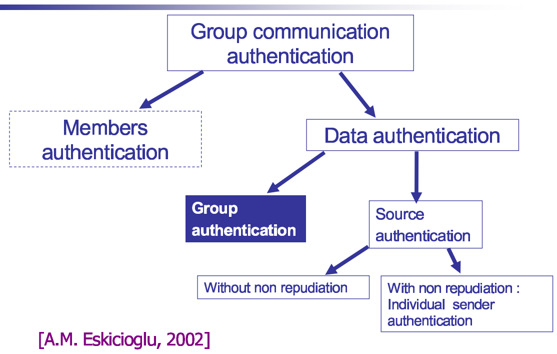


-h_PrK Host's digital signature
ACS_PrK: ACS's digital signature
-CAP: Capability



6. Multicast Authentication

Service Classification



[A.M. Eskicioglu, 2002]

Multicast Data Authentication Requirements

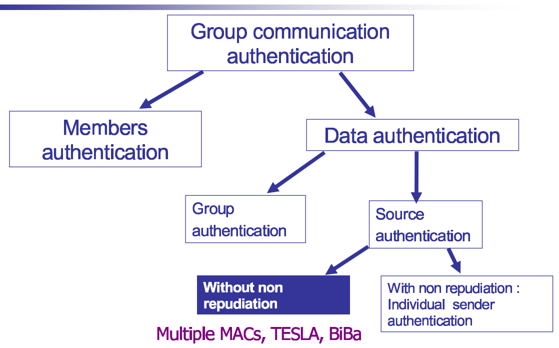
- Security Requirements
- QoS Requirements
  - Bandwidth
  - Latency
  - Packet loss
- Processing Requirements
  - Low computation
  - Low memory overhead at receiver/sender

Data Authentication in Group Communication

- **Group authentication**:
  consists in assuring that the received multicast messages by group members originate from a valid group member (sender or receiver).

⇨ shared key among all members
⇨ group key management issue

Service Classification



Data Authentication in Group Communication

- **Source authentication**:
  consists in assuring that the received multicast messages by group members originate from a source

⇨ shared secret between the sender and receiver
⇨ without non repudiation
  ⇨ MAC-based approaches
  ⇨ One-time signature

Multiple MACs

[Canetti, et al., Infocom'99]

- The sender appends to each multicast message m, L MACs using L different keys.
  - R = <K_1, K_2, …, K_L>
- Each receiver (u) holds a subset (R_u) of keys among the L sender's keys and verifies the authenticity of received messages using its subset of keys.
  If at least, a single MAC is incorrect, the receiver rejects the message.
- To forge a message of the valid sender, an attacker needs to acquire the L keys from a coalition of w receivers

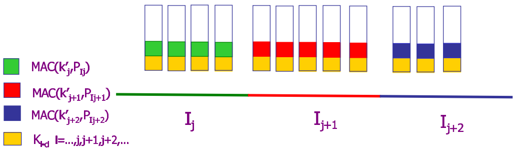
TESLA Protocol

[Perrig, Canetti, et al. draft-ietf-msec-tesla-intro-02.txt, 2002]

- Time Efficient Stream Loss-tolerant Authentication
- To initialize a receiver, the sender transmits a digitally signed packet (time intervals, time synchronization, disclosure delay,…)
- The sender appends to a packet P_i sent in interval I_j a MAC computed with a key k'_j and the key k_{j-d} used to check packets sent in the interval I_{j-d}.
  - d= disclosure delay : time in number of intervals that a receiver needs to wait
- The receiver buffers the packet without being able to authenticate it
- A short time later, the sender discloses the key k and thus allows the receiver to authenticate the received packet

TESLA Protocol- (cont.)

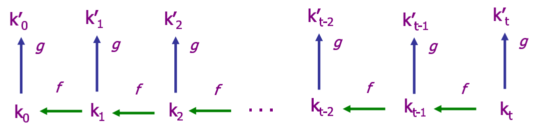
- Time intervals Concept
  - Time is divided into t intervals of duration T_{int} each



Interval = Ij sender side

TESLA Protocol- (cont.)

- MAC keys Concept
  - Sender generates a key chain k_1, k_2,....k_t using a one-way function
  - Sender generates MAC keys k'_1, k'_2,....k'_t using another one-way function



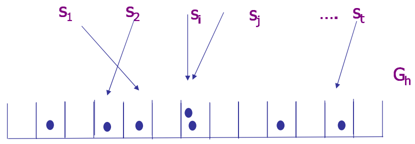
⇨ **Robust against packet loss.**

⇨ **A single MAC per packet**

BiBa : One-time signature

- BiBa (Bins and Balls) [A. Perrig, 2001]
- Signer precomputes values : SEALs (SElf Authenticating vaLues)
  - Random numbers that receivers can authenticate using a public key
  - Given a SEAL s, public key f_s = $F_s(0)$
- Exploits the birthday paradox
  - Signer : high probability to find a signature (many balls)
  - A adversary ; low probability (few balls)

BiBa : One-time signature- (cont.)

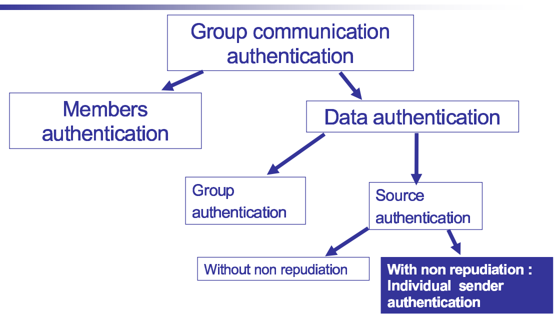


- Signature Generation :
  - compute h = H(m)
  - find a two-way collision $G_h(s_i)=G_h(s_j)$ and $s_i \neq s_j$, **$<s_i,s_j>$ signature**
- Signature Verification :
  - compute h = H(m)
  - check $G_h(si)=G_h(sj)$

BiBa : One-time signature- (cont.)

- To increase security
  - k-way collisions instead 2-way collisions
  - Sender commits to a different set of balls after each period of time
    - Using one-way function chains to construct SEAL
- BiBa
  - tolerates packet loss
  - Not vulnerable to collusion
  - Smaller signature
  - But has a large public key (10Kbytes)

Service Classification



Star and tree chaining,
Simple off-line protocol, EMSS

Data Source Authentication in Group Communication

- **Individual Source authentication**:
  consists in providing assurance of the identity of the sender of a packet

➪ with non repudiation
➪ using digital signature with sender's private key
➪ A naïve approach :
  - ➪ sign all messages
  - ➪ poor performance …

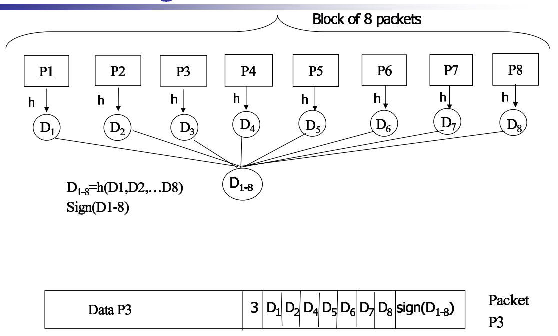
Star chaining

[Wong, et al. Trans. On Net. 1999]

- Block of *m packets*
- *Block digest* is the *message digest* of the *m* packets signed with digital signature
- For authentication, each packet needs its authentication information (packet signature)
- Packet signature consists of : block signature, packet position in the block, the digest of all other packets in the block
- **Verification :** a receiver computes the digest of the received packet and the block digest (using the digest of the other packets)

If the obtained block digest is equal to the block digest received within the block signature, the packet is authentic

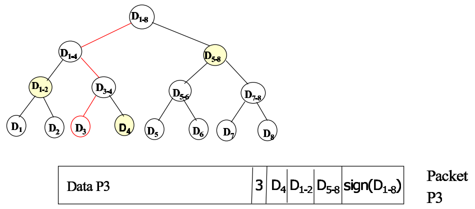
Star chaining



Tree chaining

[Wong, et al., Trans. on Net. 1999]

- hash computation is more complicated
- Communication overhead is reduced



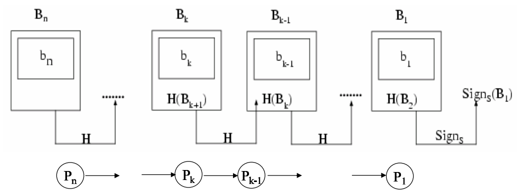
Simple off-line protocol (streaming)

[Guennaro, et al. CRYPTO'1997]

- The sender knows all the stream before transmission (off-line)
- Divide the stream into blocs and embed authentication information
- The authentication information of bloc *i* is used to authenticate bloc *(i+1)*

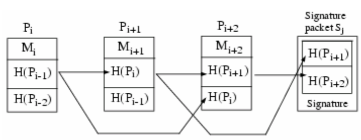
⇨ Does not tolerate packet loss.

⇨ A single hash per packet.



EMSS (streaming)

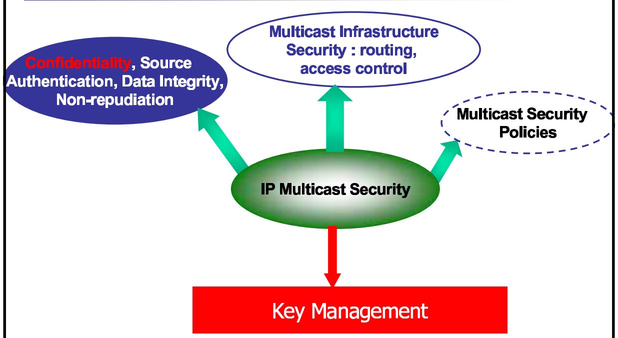
- **Efficient Multi-chained Stream Signature**
- **[Perrig, Canetti, et al., 2000]**
  - Robust against packet loss.
  - (d) hashes per packet + 1 signature periodically.



- Source authentication is a required component in the whole multicast security architecture.
- There is no best solution, but there are good solutions regarding specific requirements and features.
- Many challenges obstruct the design of a source authentication protocol :
  - *Large number of group members.*
  - *Important data volume in streaming.*
  - *Unreliable transport layer + packet loss.*
  - *Limited resources at receivers' side.*
- Other challenges ….

Source Authentication and Ad Hoc Networks

- Multicast security
  - Already a complex multi-faceted problem
  - Even more difficult in ad hoc network where source authentication can be a crucial problem (tactical MANET)
    - Bandwidth limitation
    - Storage limitation
    - Energy constraints
    - Mobility
    - Absence of centralized infrastructure



7. Multicast Key Management

- Encryption is the method commonly used to provide access control to the data :
  - Symmetric cryptography (shared key) is used by the sender/source and the receivers.
  - The shared key is refered as the ***group-key***

  The general problems :
  - method of distributing keys to group members
  - management of the keys (rekeying)

7.1 GKM requirements

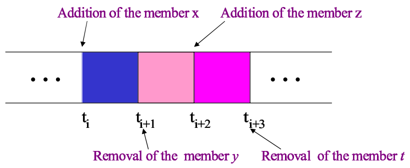
- **Scalability :**

  Group key management operations should :
  - be efficient in resource usage
  - be easily accessible
  - minimize delays within the multicast group

- **Independence :**
  - Group key management must be independent from both unicast and multicast routing

- **Reliability**
  - The delivery of a group-key must be a reliable event
- **Security**
  - Group-key management must be carried out in a secure fashion

Evolution of a secure group



key group updates
$t_i, t_{i+1}, t_{i+2}, t_{i+3}, \ldots$

Key updates

- Key update depends on :
  - Transmission policy
  - Rekey interval
  - Members distribution
  - Members dynamicity

Key updates- (cont.)

- Scalability Problems
  - **1 affects *n*** : when the action of one member affects the entire group ;
  - **1 does not equal *n*** : when the protocol cannot deal with the group as a whole and must consider each member individually.

Member which joins a secure group **backward-secrecy** policy → **1 affects *n***

Member which leaves a secure group **forward-secrecy** policy → { **1 affects *n*** / **1 does not equal *n*** }

Key updates- (cont.)

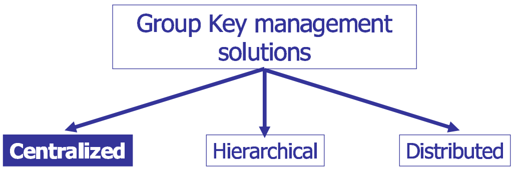
How key updates are carried out?

- **Forward secrecy :** when a member of a group leaves the group, it must be prevented from having further access to the data and the group-keys
- **Backward secrecy :** data communicated within the group before a member joins must remain secret to the new member

Performance parameters

- Time to verify and decrypt data
- Time to encrypt/decrypt data
- Communication bandwidth overhead : *1-affects-n*
- Key set-up and refreshment overhead
- Group set-up and member enrollment time

Key management architectures



GKMP,
LKH, OFT

7. 2 Centralized solutions

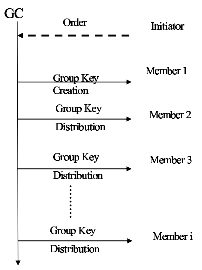
- Only one entity (Key Distribution Centre) controls the whole group
- Drawbacks :
  - Single point of failure
  - Scalability problems

Centralized solutions : GKMP

GKMP : Group Key Management Protocol [Harney et al. 97]

- KDC creates a Group Key Packet (GKP)
- GKP contains a Group Traffic Encryption Key (GTEK) and Group Key Encryption Key (GKEK)
  - Group Key Packet (GKP) = [$GTEK_n$,$GKEK_{n+1}$]
- **Member Join operation :** KDC sends a copy of the GKP to the new member
- **Rekeying operation :** KDC generates a new GKP and encrypt it with the current GKEK

Problem : as all members know the GKEK, the is no forward secrecy!!
Except to recreate the entire group!!



Centralized solutions : LKH

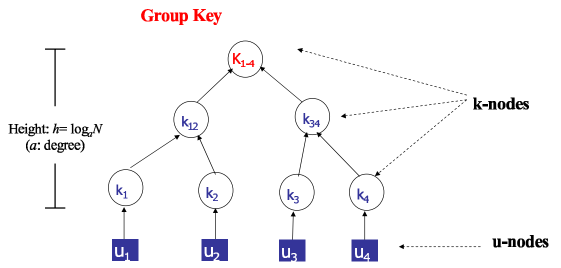
LKH : Logical Key Hierarchy [Wong, et al. 98, Wallner et al. 99]

- KDS maintains a tree of keys
  - « The nodes of the tree hold *Key Encryption Keys* »
  - The leaves correspond to group members
  - Each leaf holds a KEK associated with that one
- Each member receives and maintains :
  - a copy of the KEK associated with its leaf
  - KEK corresponding with each node in the path from its parent leaf to the root
- The root Key is the group Key

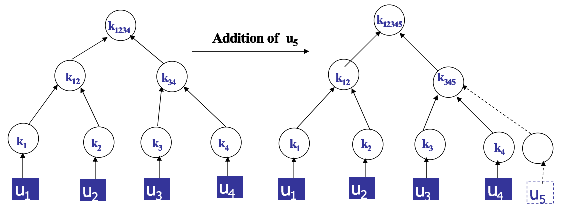
Centralized solutions : LKH- (cont.)

- **Secure group communications using key graphs** [Wong, et al., Sigcomm'98]
  - Secure group: triplet (U,K,R)
    - U: group of users
    - K: group of keys;
    - R: binary relation between U and K, R ⊂ UxK called user-key relation. User u has key k if and only if (u,k) is in R
  - A secure graph specifies a secure group :
    - Each U element is a u-node;
    - Each K element is a k-node;
    - (u,k) is in **R** ⇔ A directed path exists from the u-node u and the k-node k.

Secure group communications using key graphs



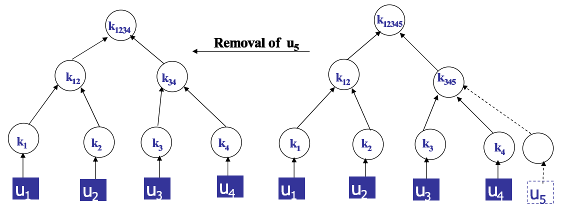
Joining a Tree Key Graph



Group Oriented Rekeying

S --> $\{u_1,u_2,u_3,u_4\}$: $\{K_{12345}\}K_{1234}$, $\{K_{345}\}K_{34}$
S --> $\{u_5\}$: $\{K_{12345}, K_{345}\}K_5$

Leaving a Tree Key Graph



Group Oriented Rekeying

S --> $\{u_1,u_2,u_3,u_4\}$: $\{K_{1234}\}K_{12}$, $\{K_{1234}\}K_{34,}$, $\{K_{34}\}K_3$, $\{K_{34}\}K_4$

Centralized solutions : OFT

OFT : One-way Function Tree [McGrew, et al. 1998]

- A node's KEK is generated rather than just distributed
- The KEK held by a node is resulted from using a one-way function and mixed using a mixing function :

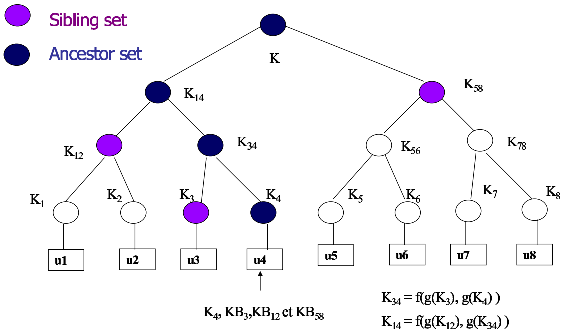
$$k_i = f(g(k_{left(i)}), g(k_{right(i)}))$$

- *left(i)* and *right(i)* are the left and the right children of node *i*
- *g* is a one-way function and *f* is a mixing function known the group members
- A node has two keys K_i, KB_i
  - $KB_i = g(K_i)$; and KB_i is called a blinded key

One-way Function Tree

- **Ancestor set** of a node are those nodes in the path from its parent node to the root
- **Sibling set** is the set of siblings of the nodes in the ancestor set
- Each member receives :
  - its key
  - its sibling's key
  - The keys corresponding to each node in its sibling set
- Applying these information to the formula , a member is able to generate all keys in its *ancestor set*

One-way Function Tree- (cont.)

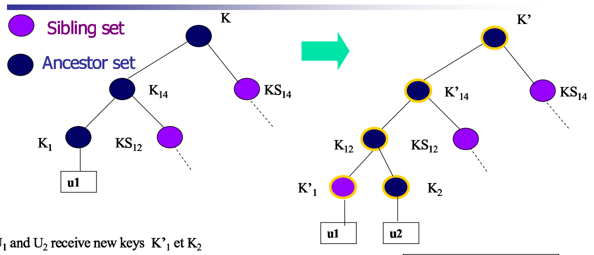


$K_{34} = f(g(K_3), g(K_4))$

$K_{14} = f(g(K_{12}), g(K_{34}))$

$K = f(g(K_{14}), g(K_{58}))$

One-way Function Tree
Addition of a member



U_1 and U_2 receive new keys K'$_1$ et K_2

K_2, KB'$_1$, KBS_{12} and KBS_{14} are sent to U_2 by GC via a secure channel

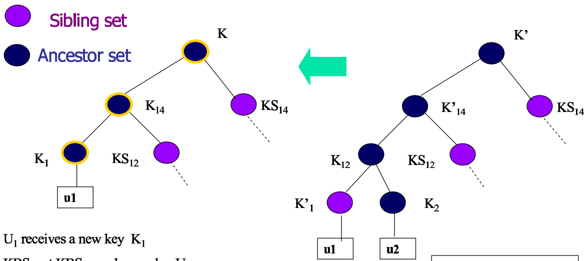
{K'$_1$, KB_2}K_1, {KB_{12}}KS_{12} et {KB'$_{14}$}KS_{14} are broadcast

$K_{12} = f(g(K'_1), g(K_2))$

$K'_{14} = f(g(K_{12}), g(KS_{12}))$

$K' = f(g(K'_{14}), g(KS_{14}))$

One-way Function Tree
Removal of a member



U_1 receives a new key K_1
KBS_{12} et KBS_{14} are known by U_1
$\{K_1\}K'_1$, $\{KB_1\}KS_{12}$ et $\{KB_{14}\}KS_{14}$
are broadcast

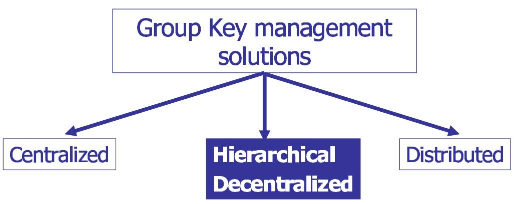
$K_{14} = f(\, g(K_1), g(KS_{12}))$
$K = f(\, g(K_{14}), g(KS_{14}))$

LKH and OFT: Comparison

- Both have a tree structure
  - The height of the tree determines user storage and key update communication related to as $O(\log N)$
- Keys on LKH are independent, while keys on OFT are related by one-way function
  - The GC storage
    - LKH: all the keys of a tree are stored
    - OFT: *N*, only the leaf keys are stored; The storage is independent of the tree degree *a*
  - Key update communication
    - OFT trades user computation for the reduction in rekey messages when compared with LKH

Slide of Mingyan LI Radha Poovendran (IRTF, GSEC,2001)

Key management architectures



SMKD,
Iolus, Baal
Hybrid (AKMP, SAKM)

7.3 Decentralized solutions

- The large group is split into subgroups
- Different controllers are used to manage each subgroup

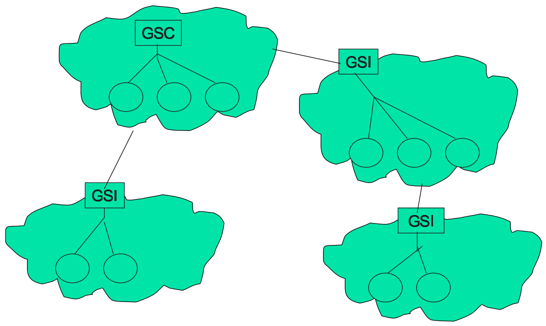
Scalable Multicast Key Distribution [Ballardie, 96]

- Uses the CBT multicast tree to deliver keys to a multicast group
- No forward secrecy

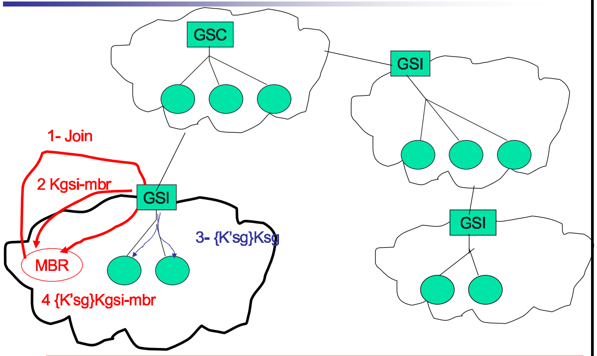
Decentralized solutions : Iolus

- A Framework for Scalable Secure Multicasting
  - [S. Mittra, Sigcomm'97]
- A large group is split into subgroups linked via GSI (Group Security Intermediaries)
- A Group Security Agent (GSA) manages each subgroup
- The whole group is managed by a GCS (Group Security Controller

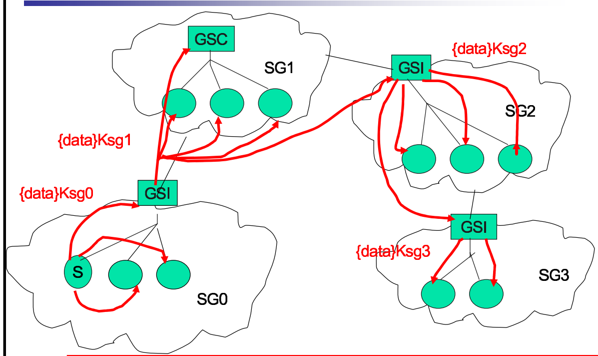
Iolus- (cont.)



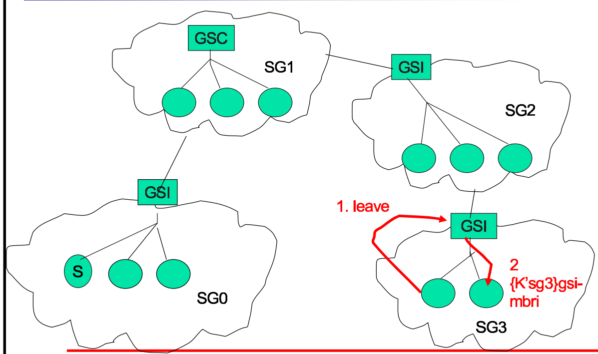
Iolus : Joining a group



Iolus : Multicasting data



Iolus : Leaving a group

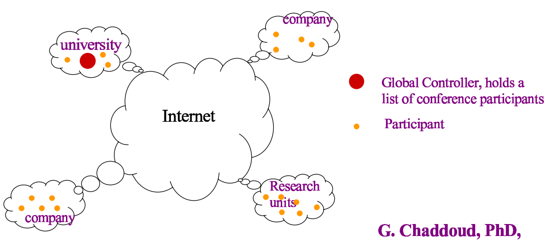


- Iolus uses independent keys for each subgroup
- Each membership change in a subgroup is treated locally without affecting other subgroups
- More fault-tolerant (absence of a general controller)

Drawback : translation

Decentralized solution : Baal

Motivation :



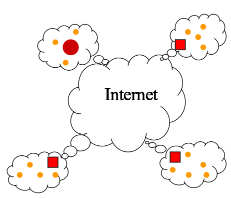
G. Chaddoud, PhD, 2002

Ex : Virtual Conference via Internet

Baal : architecture

Distributed Key Management :

Local Controller : entity delegated by CG if there are any join/leave within their domain.



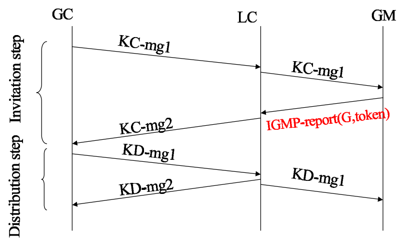
α coefficient of participation : average of the number of participants per domain.

● : Global Controller, GC

■ : Local Controller, LC

• : Group Member, GM

Baal : Group Initialization

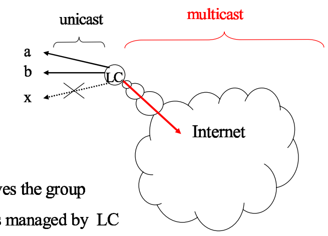


MG ➔ IGMP-report (G, token)

token ≡ @ du récepteur, timestamp, nonce

GC : Global Controller
LC : Local Controller
GM : Group Member

Baal : Eviction of a member



- member x leaves the group
- a, b : members managed by LC
- LC : IGMPv3-multicast router

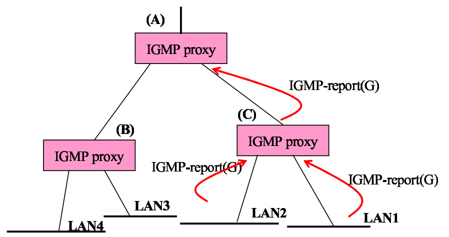
Analysis and comparaison

	Baal	SKDC	LKH	OFT
Transmission size (initialization)	*(n/α).k*	*nk*	*2nk + h*	*2nk + h*
Transmission size (rekeying)	*k*	*nk*	*2hk +h*	*hk+h*

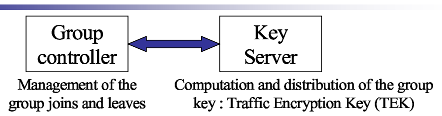
➔ 1 affects n problem

n : group size
h : height = log *n*
k : key size

➢ Based on IGMP proxing

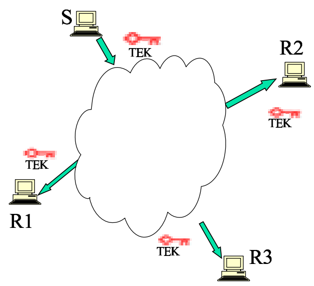


7.4 Hybrid Group Key Management



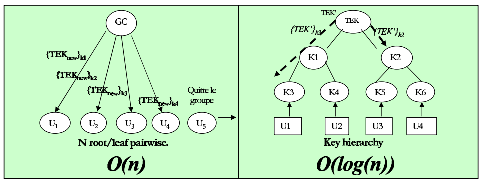
- **Two approaches to manage group keys**
  - Approach A : Sharing a single TEK among group members
  - Approach B : Subdivision of the group into many sub-groups with independent local TEKs.
- **Performances**
  - The required number of messages to update the TEK
  - « 1 affects n »
  - The required number of decryption/re-encryption operations to send the multicast messages to all the members.

Key Management : Approach A



Key management : Approach A

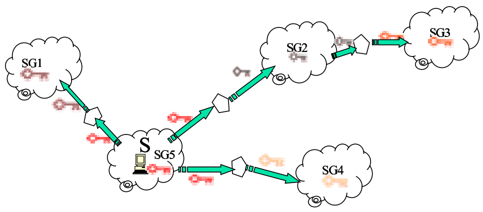
- Sharing a single TEK
  - Centralized management *(single point of failure, bottlenecks)*
  - Distributed management *(scalability, fault tolerance)*



•Advantage : **a single decryption/encryption.**

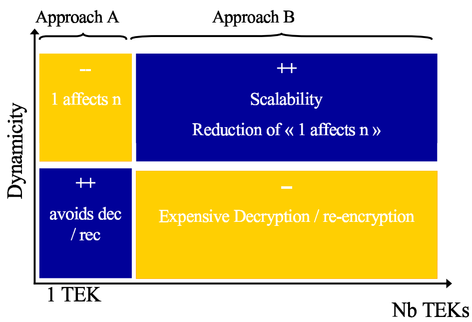
•Disadvantage : **« 1 affects n ».**

Key management : Approach B



- Iolus, KHIP…
- Advantages : **scalability, reduction of « 1 affects n »**
- Disadvantage : **high number of decryption / re-encryption.**

Key Management : Summary



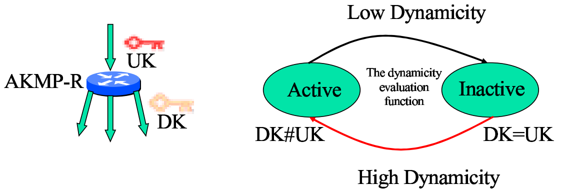
Adaptive Key Management Protocol (AKMP)

[H. Bettaha, et al. ICCCN'02]

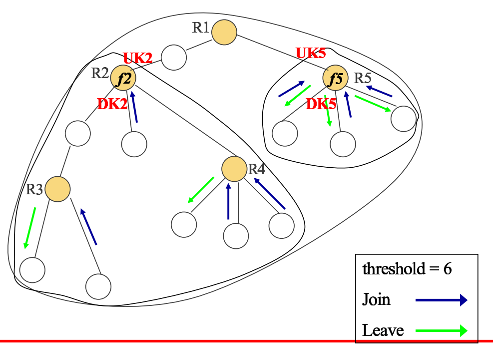
- A new approach which adapts automatically to the group dynamicity
- The subgroups are created and destroyed according to the dynamicity
- The size and the lifetime of each subgroup depends on the scope and the duration of the dynamicity.

AKMP

- AKMP routers
- The dynamicity evaluation function
- Each AKMP-R maintains two keys :
  - Upstream Key (UK)
  - Downstream Key (DK)



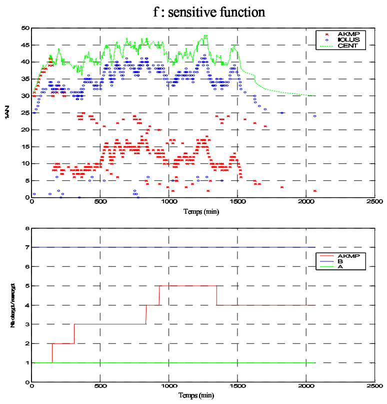
AKMP (Example)



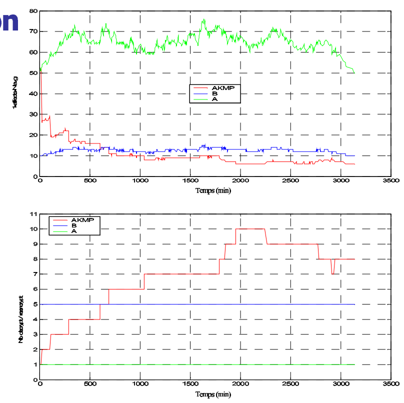
AKMP : Simulation

- **AKMP :**
  - 250 nodes (the graph is generated with Waxman algorithm). Among them, 30 nodes are AKMP nodes.
- « join / leave » according to Almeroth models.
- **Approach A :** centralized solution.
- **Approach B :** Iolus with 7 subgroups.
- **Measure of :**
  - « 1 affects n ».
  - Number of the required decryption/re-encryption operations

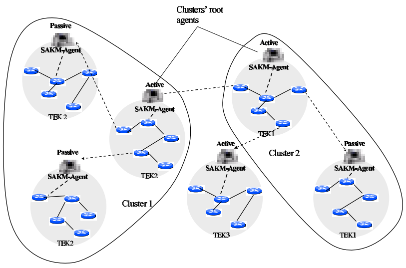
Simulation



Simulation



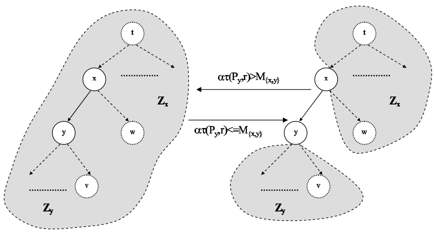
SAKM: Concepts and Architecture



Issues:

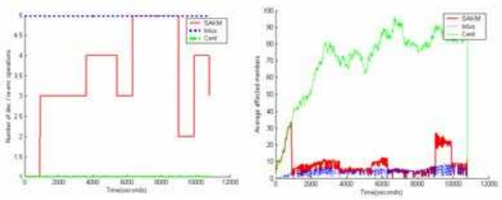
- Evaluating the overhead induced by clustering;
- Finding the partition which minimizes this overhead.

SAKM : Heuristic



- Periodically, each two adjacent agents (x,y) exchange the dynamism information: (λ_x, μ_x) (λ_y, μ_y)

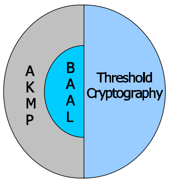
SAKM : Simulation : scenario 1



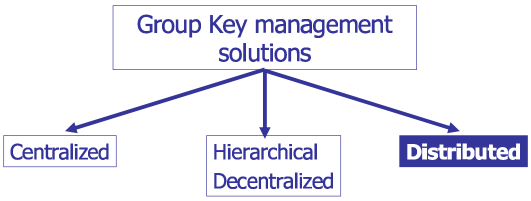
- α : favorize splitting.

An Enhanced hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks

- [M. Bouassida, et al. , Networking 04]
- New Approach :
  - Based on BAAL
  - More dynamic
    - event frequency and members group number
    - dynamic decomposition of the group in clusters
  - More scalable
    - attenuating the "1 Affects n" phenomenon
    - limiting the overhead due to encryption/decryption process
  - More secured
    - using the Threshold Cryptography



Key management architectures

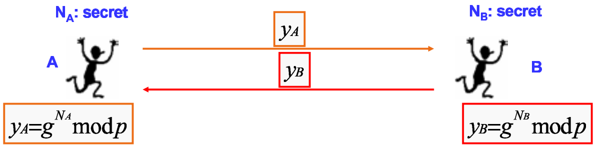


7.5 Distributed solutions

- No group controller
- All group members contribute in the generation of the group key
- Processing time and communication requirements increase in term of the number of members
- The efficiency of contributory protocols is evaluated by :
  - *Number of rounds*
  - *Number of messages*
  - *Processing during setup*

Distributed solutions- (cont.)

Diffie-Hellman [1976]



$$clé = (y_A)^{N_B} = (y_B)^{N_A} = g^{N_A N_B} \bmod p$$

p, g: pair of primes

Distributed solutions- (cont)

Group Diffie-Hellman key Exchange [Steiner, et al.,96]

- Extension of the basic Diffie-Hellman key agreement protocol
- The group agrees on a pair of primes (p et g)
- The first member M1 computes the first value (g^{N1}) and passes it to the next member M2
- M2 computes and sends to M3 : $\{g^{N2}, g^{N1}, g^{N1N2}\}$
- M3 computes and sends to M4 : $\{g^{N2N3}, g^{N1N3}, g^{N1N2}, g^{N1N2N3}\}$

- Each subsequent member receives the set of intermediary values and raise them using its own secret number generating a new set.
- The set generated by the i^{th} member will have :
  - *i intermediate values with i-1 exponents and*
  - *A cardinal containing all exponents*

Distributed solutions- (cont.) GDH

Example : the fourth member receives

$\{g^{N2N3}, g^{N1N3}, g^{N1N2}, g^{N1N2N3}\}$

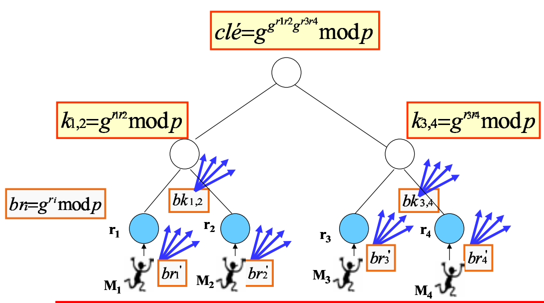
and generates the set :

$\{g^{N2N3N4}, g^{N1N3N4}, g^{N1N2N4}, g^{N1N2N3}, g^{N1N2N3N4}\}$

- The *cardinal* is $g^{N1N2N3N4}$
- The last member (n) computes k from the *cardinal* value
  $k = g^{N1...Nn} \bmod p$
- Member (n) raises all intermediate values to its secret value and multicast the hole set
- Each member extracts its respective intermediate value and computes k

Distributed solutions (cont.)

Perrig et al. protocol,2000



8. Fault-tolerance and Key Management

- Failure : fail-stop, byzantin, temporarly
- Fault detection
- Fault recovery

Existing Solutions

- Synchronous systems
- Multi-round protocols with no fault tolerance support
- Network partitions : (key agreement protocol) each partition sets up a new key
- **Lost key updates:**
  - **Retransmission :** explicitly request the lost message
  - **Replication :** multisend key update messages
  - **Error correction codes :** split up each key update packet into *n* packets such that a receiver that gets any *m* packets (*m*<*n*) can reconstruct the original message.

- Motivations
- Group characteristics
- Key management with group characteristics
- Solutions
- Evaluation
- Conclusion

Motivations

- Different multicast groups :
  - Centralized key distribution for large groups
  - Cooperative key management for autonomous groups

But ...

... Independent from group characteristics !!!

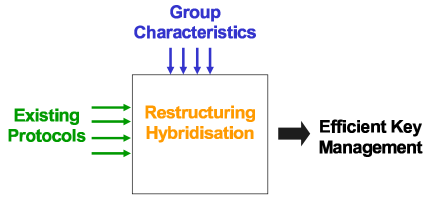
  - Only the type of the application (one-to-many or any-to-any) : Centralized/cooperative key management
  - No other group characteristics is considered in key management approaches.

Group characteristics

- Group size
- Group communication
- Routing protocol (shared tree, source tree, multi-core tree)
- Group dynamism
- Volume and traffic type : heavy volume of communication, real-time communication, allowed latency ?
- Trust consideration : members trust each other, single trusted entity, several trusted entities
- Session duration : permanent, periodic, temporary
- Heterogeneity of characteristics within the same group, etc, ...

Key management with group characteristics

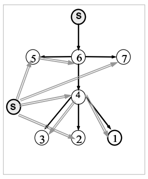
Framework for key management considering group characteristics



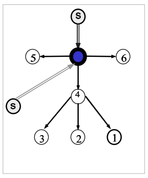
Case 1 : multiple-cores

Two types of multicast trees:

Single Source Shortest-Path Tree



Shared Tree



- core
- source
- group member

Case 1: Multiple cores- (cont.)

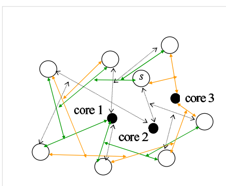
- Shared trees are interesting BUT:
  - *Higher data transmission delay*
  - *Central point of failure*
  - *Traffic concentration at the level of the core*

REPLICATION

< multiple cores >

Members -to-all multiple-core tree

- Several cores
- Each core is the root of its own multicast tree
- Each source transmit data to only one core



Example with three cores

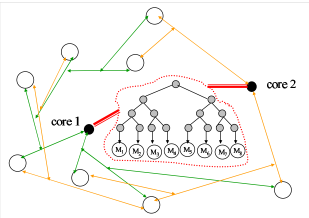
Use in key distribution

Key distribution with logical key trees
Use The Cores as key server

The key tree is maintained by all the cores (passive replication)

Each core maintains its own key tree (active replication)

Key tree maintained by all the cores



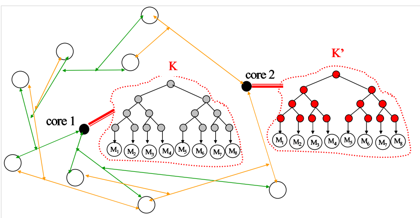
Failure of one core

The second core is active
(≈ rekey the tree)

•Synchronization delay
•Rekey delay

•Synchronization of rekey operations
•Maintaining traffic state with each core
•Choose the least loaded core

Separate Key trees



Failure of one core

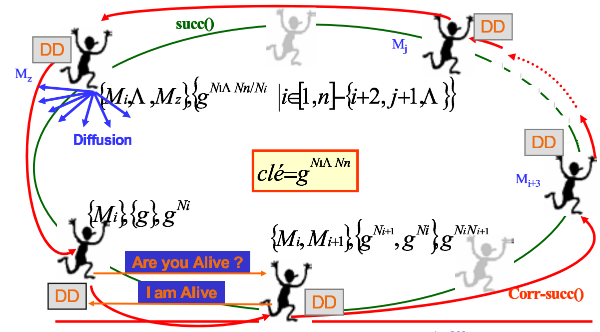
No delay to recover a key

- Each member maintains 2 sets of keys
- Join or leave: rekey 2 trees
- Communicate indifferently with each of the 2 group keys

Storage overhead
Rekey overhead

A fault-tolerant key agreement protocol

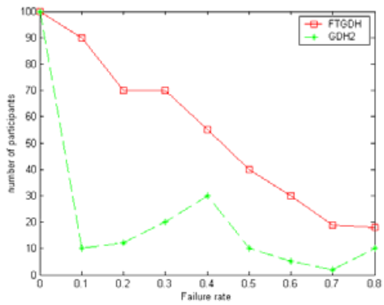
Dynamic construction of a logical ring by the failure detectors



A fault-tolerant key agreement protocol

Simulation

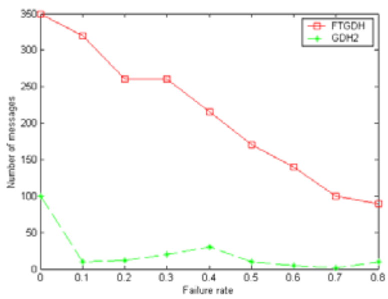
- Number of participants according to failure



A fault-tolerant key agreement protocol

Simulation

- Number of exchanged messages



Conclusion

Multicast security is a huge research area !!

Mobile IP, Ad'hoc, Privacy, secure routing,…

Thanks !!

Projets labellisés en 2004

SAFECAST

Objectifs

Les services de sécurité font intervenir une ou plusieurs clés.

La gestion de ces clés est à la base de toutes les applications sécurisées mais les solutions actuelles ne remplissent pas l'ensemble des exigences liées aux spécificités des applications et des environnements.

Safecast va définir et développer une architecture globale de sécurité de la communication multipoint dans un environnement ouvert.

Retombées attendues

Définition d'une architecture de sécurisation des communications de groupe adaptée à un environnement ouvert ou tout membre du groupe pouvant être simultanément émetteur et récepteur.

L'architecture définie et développée au travers du projet permettra de répondre à des contraintes fortes de sécurité telle que celles présentes dans les réseaux de sécurité publique.

Partenaires

Safecast et le principe de la sécurité des communications

- SP1 — Les besoins
- SP2 — Le modèle de confiance
- SP3 — Architecture et protocoles de gestion de groupe sécurisé
- SP4 — Test et validation

Some References

- [1] Multicast and group security. T. Hardjono and L.R. Dondeti. Artech House. 2003
- [2] A taxonomy of multicast source authentication : issues and solutions. Y. Challal, H. Bettahar and A. Bouabdallah. Under Revision for Publications in IEEE Communication Surveys and Tutorials. 2004
- [3] Méthodes d'authentification pour les communications de groupe : taxonomie et évaluation dans un environnement Ad Hoc. M.S. Bouassida, I. Chrisment et O.Festor. SAR'2004
- [4] Multicast security : a taxonomy and some efficient constructions. R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas. Infocom'99.
- [5] Multimedia security in group communications : recent progress in wired and wireless networks. A.M. Eskicioglu. Conference on communication and Computer Network. 2002.
- [6] TESLA : Multicast Source Authentication Transform Introduction. Draft-ietf-msec-tesla-intro-02.txt. 2004
- [7] BiBa (Bins and Balls) A. Perrig. ACM Conf. Computer Communications Security. 2001
- [8] Digital signatures for flows and multicasts. C.K. Wong and S.S Lam. IEEE/ACM Trans. On Networking. August 1999.

Some References- (cont.)

- [9] How to sign digital streams. R. Gennaro and P. Rohatgi. CRYPTO'97.
- [10] Efficient authentication and signing of multicast streams over lossy channels. A. Perrig and R. Canetti and J. Tygar and D. Song. IEEE Symposium on Security and Privacy. 2000.
- [11] Group key management protocol (GKMP). Architecture. RFC 2094. 1997
- [12] Secure group communication using key graphs. C.K. Wong, M. Gouda and S.S Lam. Sigcomm'98.
- [13] Key management for multicast : issues and architectures. D. Wallner, E. harder and R. Agee. RFC 2627. 1999
- [14] Key establishment in large dynamic groups using one-way function trees. D.A. McGrew, A.T. Sherman. Technical Report. 1998
- [15] Scalable multicast key distribution. T. Ballardie. RFC 1949. 1996.
- [16] Iolus : a framework for scalable secure multicasting. S.Mittra. Sigcomm'97
- [17] Sécurisation de communication de groupes dynamiques. G. Chaddoud. Thèse de doctorat, Université Henry Poincaré - Nancy 1. Août 2002.

Some References- (cont.)

- [18] An enhanced hybrid Key management protocol for secure multicast in Ad Hoc networks. M.S Bouassida, I. Chrisment and O. Festor. Networking'2004.
- [19] Gestion de clés et sécurité multipoint : étude et perspectives. H. Seba, A. Bouabdallah, N. Badache, H. Bettahar et D. Tandjaoui. Annales des Télécommunications. 2003.
- [20] AKMP : an adaptive key management protocol for secure multicast . H. Bettahar A. Bouabdallah, Y. Challal. ICCCN'02.
- [21] A scalable and adaptive key management protocol for group communication. Y. Challal, H. Bettahar and A. Bouabdallah. WWIC'04.
- [22] Collecting and modelling the join-leave behaviour of multicast group members in the Mbone. K. Almeroth et M. Ammar. Symposium on High Performance Distributed Computing. 1996.
- [23] Increasing the robustness of initial key agreement with failure detectors. H. Seba, A. Bouabdallah, N. Badache, IEEE Globecom'2003.
- [24] Mobile multicast communications : challenges and solutions. I. Romdhani, M. Kellil, H.Y. Lach, A. Bouabdallah, H. Bettahar, IEEE Communications surveys and Tutorials, 2004.
- [25] Sender and receiver access control to the multicast delivery tree in mobile environnement: a survey. I. Romdhani, M. Kellil, H.Y. Lach, A. Bouabdallah, H. Bettahar, under revision for publication in IEEE Communications surveys and Tutorials.