



# THE SKEMASNET PROJECT

## *SESSION KEY MANAGEMENT IN A SPONTANEOUS NETWORK*

**HGP Team**

**Alauzet Pierre, Park Hyunho , Ricciardi Gianni M.**

# TABLE OF CONTENTS

1. Background & problem definition
2. Design specifications
3. Implementation
4. Comparisons & conclusions

# BACKGROUND

- ❑ In the context of spontaneous networks, we focused on session key management during the merger of two networks and when a user leaves the network
- ❑ Referring to some paper about GKA, we compared this solution to our own and started developing our *Skemasnet* idea
- ❑ Using GKA and *Skemasnet* algorithms, we runned some tests thru ns2 simulator and got some results

# PROBLEM DEFINITION

❑ In the private networks they are using common session keys for secure communication,

- ❑ When merging network(s) it needs to manage session keys.
  - Creating a new session key or choosing one of them for the merged network.
  - Share the new session key to all members.

❑ Related works

- ❑ GKA(Group Key Agreement)-key paper
  - A mechanism to create a common session key for a group of users.
  - Each member provide a public contribution for creating a common session key.
  - It can share a common session key **without** the use of a *secure* channel.

❑ Problem

- ❑ Require creation of a new session key at every times when the network members are changed (join, leave, merge, separating)
- ❑ Requires  $2n$  messages exchanges for creation and distribution of a new session key.
- ❑ Each message for exchange a session key is in size of encrypting  $\text{SizeOfSessionKey} * 2 * n$ 
  - ❑ Ex) if the key size is 256bit, and size of node is 100 $\Rightarrow 256 * 100 * 2 = 51200$  bit = 6.4kbytes.

# DESIGN CASE: MERGING 2 NETWORKS

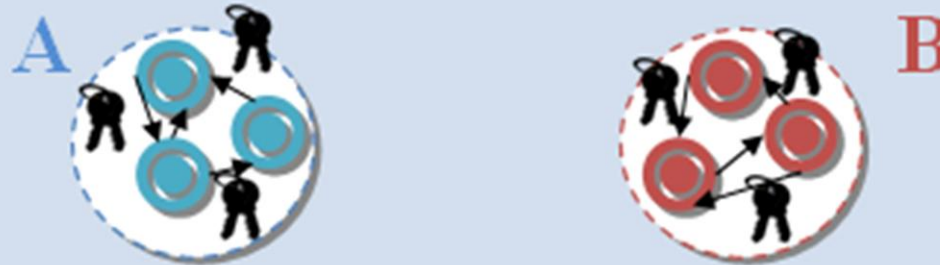
## □ Preface

*Decision making comes from human interaction.  
Two groups meet and decide to merge their networks and then they choose two leaders (one per network).*

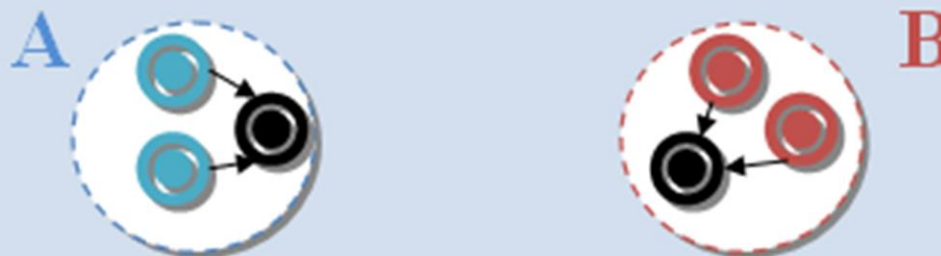
# DESIGN CASE: MERGING 2 NETWORKS (CONT.)

## □ Initial phase

Thanks to the joining procedure, each user has the public key of all other users in the same network



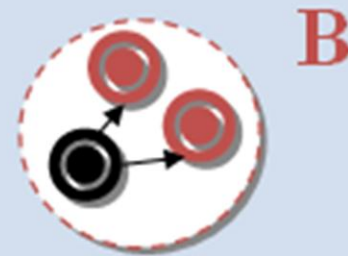
All users of each network, after a *social* agreement, select the leader on the users list.



# DESIGN CASE: MERGING 2 NETWORKS (CONT.)

## Initial phase (cont.)

When the leader receives a signed *election message* from each user, he assumes the role of leader and sends a signed *confirmation message* to all users



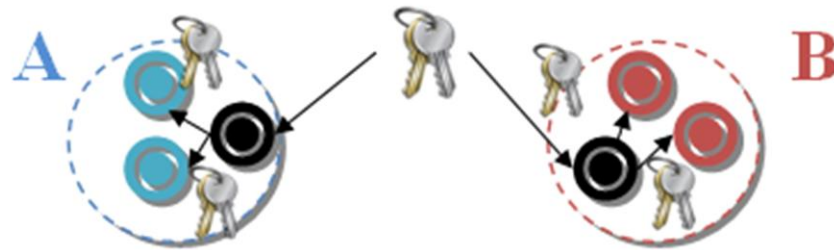
The two leaders meet **face to face** and share a new session key using a *secure side channel*



# DESIGN CASE: MERGING 2 NETWORKS (CONT.)

## □ Propagation phase

Each leader propagates the new key  to his/her members of pre-existing network through the network itself using a signed message.



## □ Communication phase

Users from both original networks can communicate one to each other







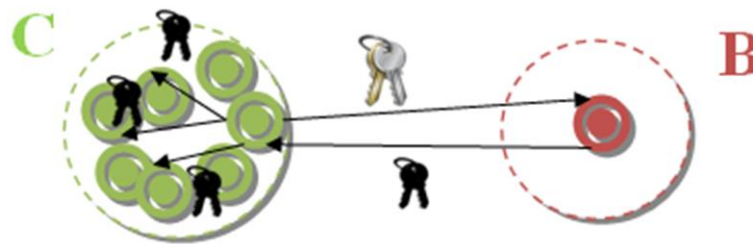
# DESIGN CASE: MERGING 2 NETWORKS (CONT.)

## □ Joining phase

If a new node requests to join the new network, it is performed as a common joining process. Each host owning the new key is able to share it again.

Public key  of the new user is sent to the connected user who broadcasts it to

all other users; the session key  is delivered to joining user.



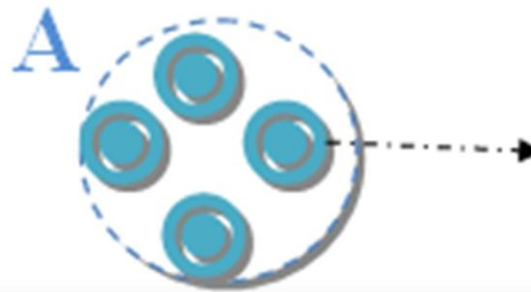
The new node joined the network and communicates with the others.



# DESIGN CASE: LEAVING A NETWORK

## □ Preface

*Decision making comes from human interaction.  
A user decides to leave the network.*



## □ Initial phase

*Idem that for the first design case: merging 2 networks*

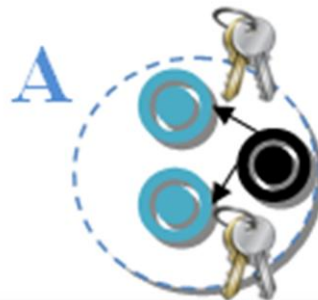
# DESIGN CASE: LEAVING A NETWORK (CONT.)

## □ Propagation phase

The leader creates the new key



and sends it to all other users, encrypting it with their public keys.



## □ Communication phase

Nodes can now communicate once again, in a new secure network that the previous node cannot see anymore



# COMPARISON TO GKA

## □ Number of exchanged messages

	GKA	Skemasnet
Merging Networks	$2*(2N-1)$	$2(N-1) + (N-2)$
Leaving User	$2*(2N-1)$	$2(N-1) + (N-1)$

# COMPARISON TO GKA

- Size of exchanged messages to deliver a new session key

GKA	$\text{SizeOfSessionKey} * 2 * N$
Skemasnet	$\text{SizeOfSessionKey} + \max(N1, N2) * \text{SizeOfPubKey}$

# IMPLEMENTATION REVIEW

- ❑ We use *ns-2* (**N***etwork* **S***imulator version **2***) in order to
  - ❑ **Implement** our *Skemasnet* and the **GKA algorithm**
  - ❑ **Simulate** 3 scenarios: **merging** between 2 networks, the **joining** and the **leaving** of several nodes
  - ❑ **Compare** our implementation with **GKA** in term of **number & size of exchanging messages**
  
- ❑ We did not implement encryption algorithm: our concern is number and size of messages even if current implementation does not reflect this

# SCENARIO

## ❑ Merging

- ❑ 2 networks with the same number of nodes: **10 to 50 nodes / network**

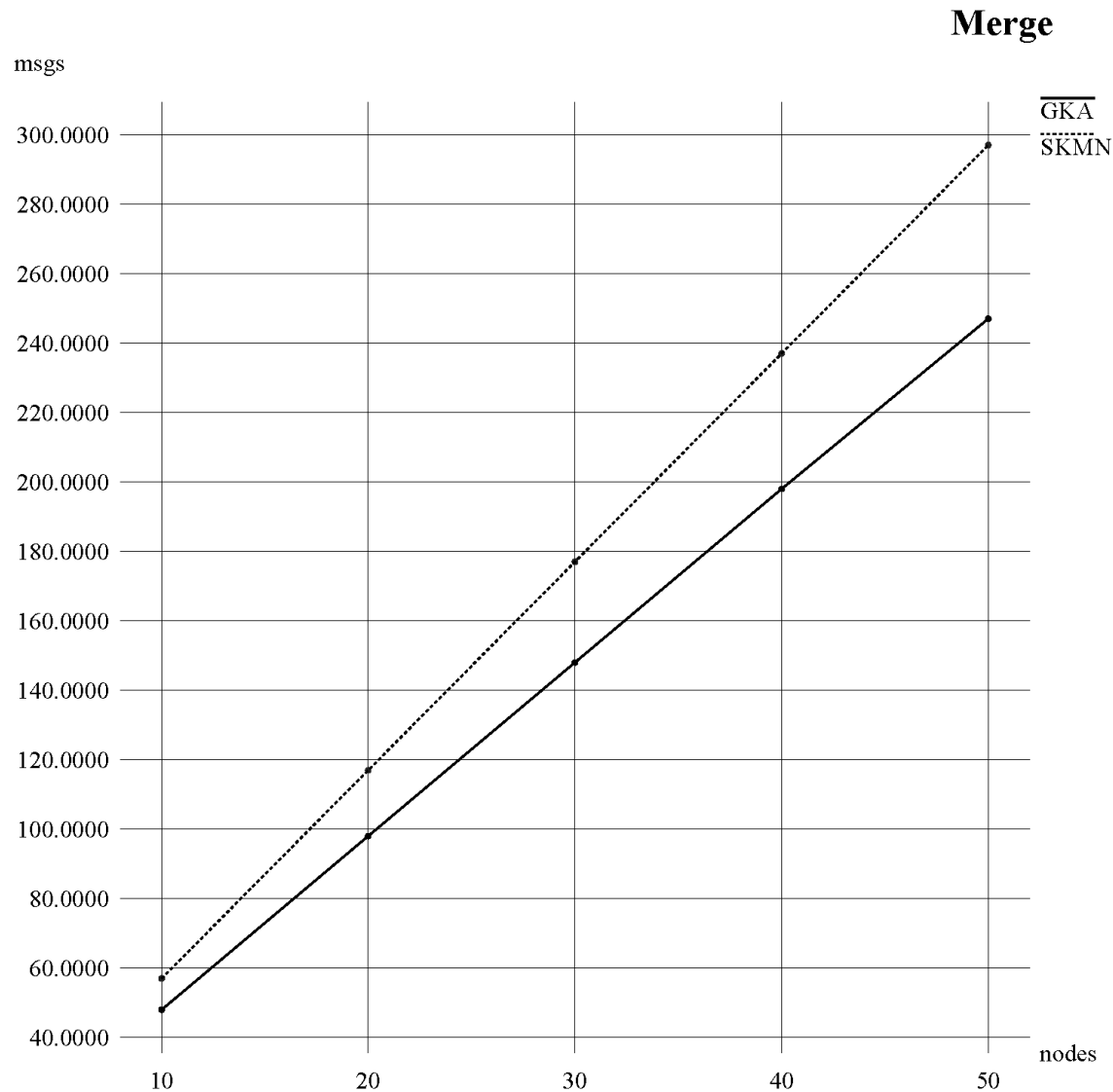
## ❑ Joining

- ❑ Considering the join of each user: **10 to 50 nodes / network**

## ❑ Leaving

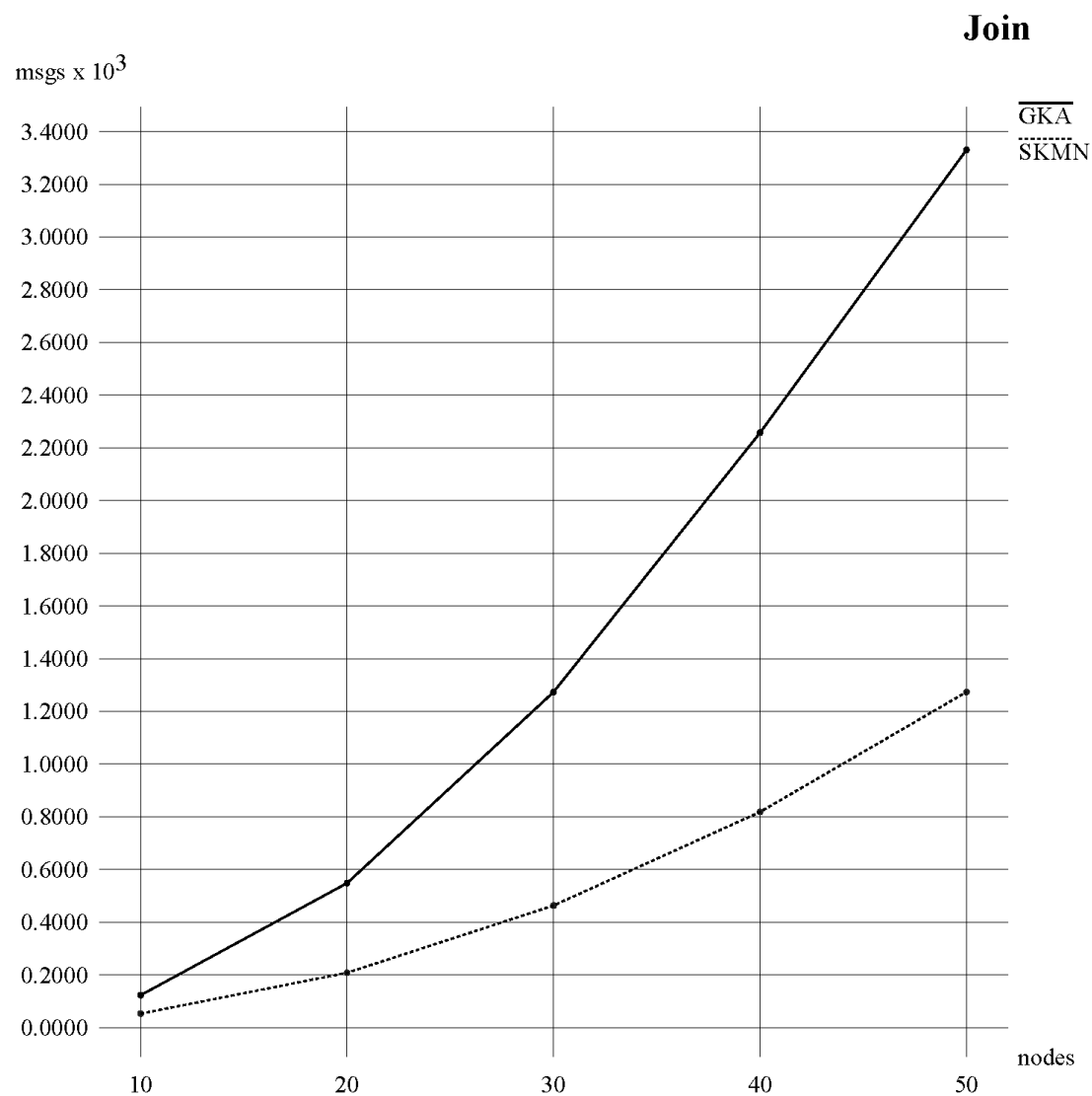
- ❑ Considering one leaving user in a network of **10 to 50 nodes**

# MERGING SCENARIO: MESSAGE NUMBER

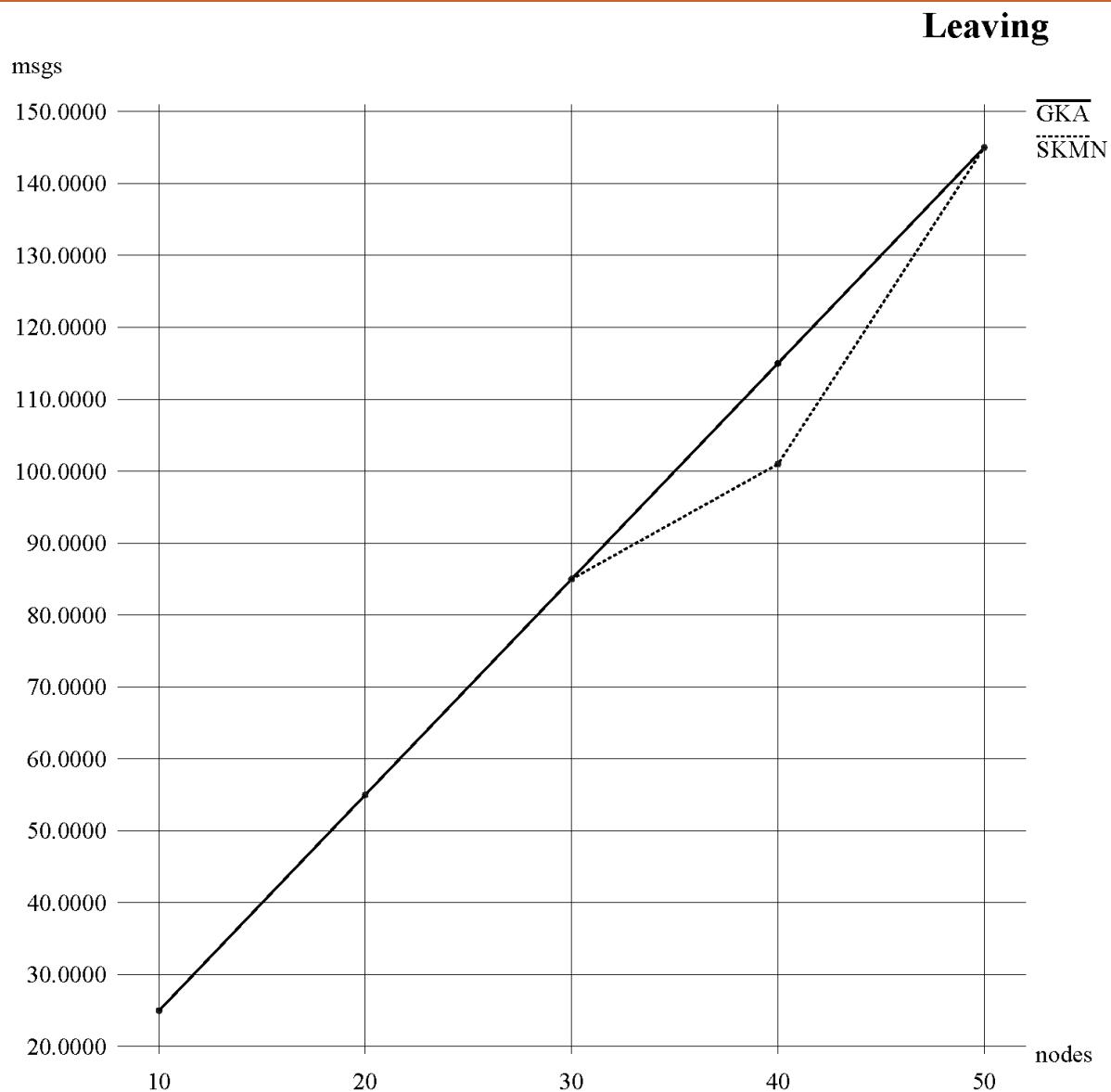




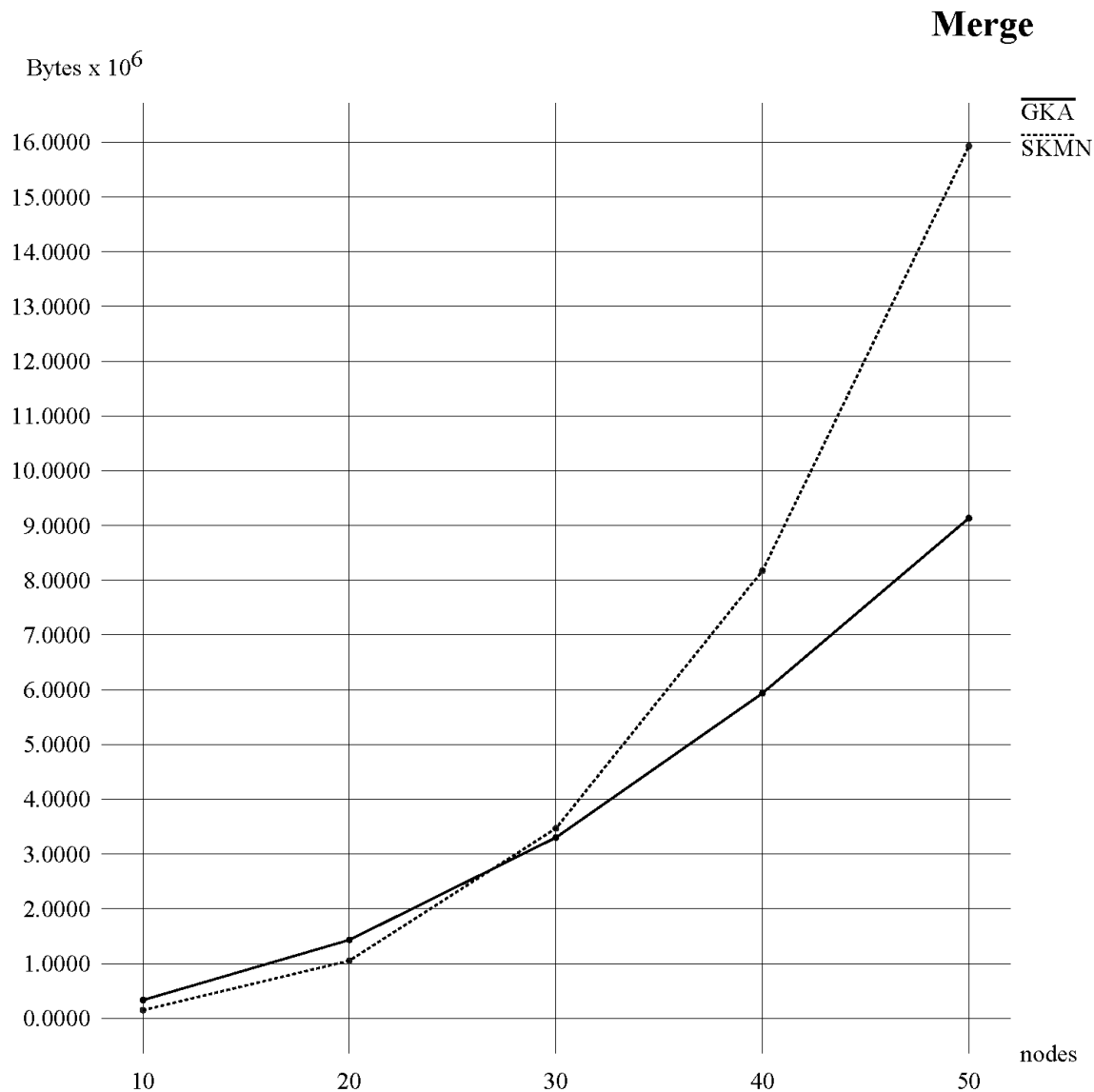
# JOINING SCENARIO: MESSAGE NUMBER



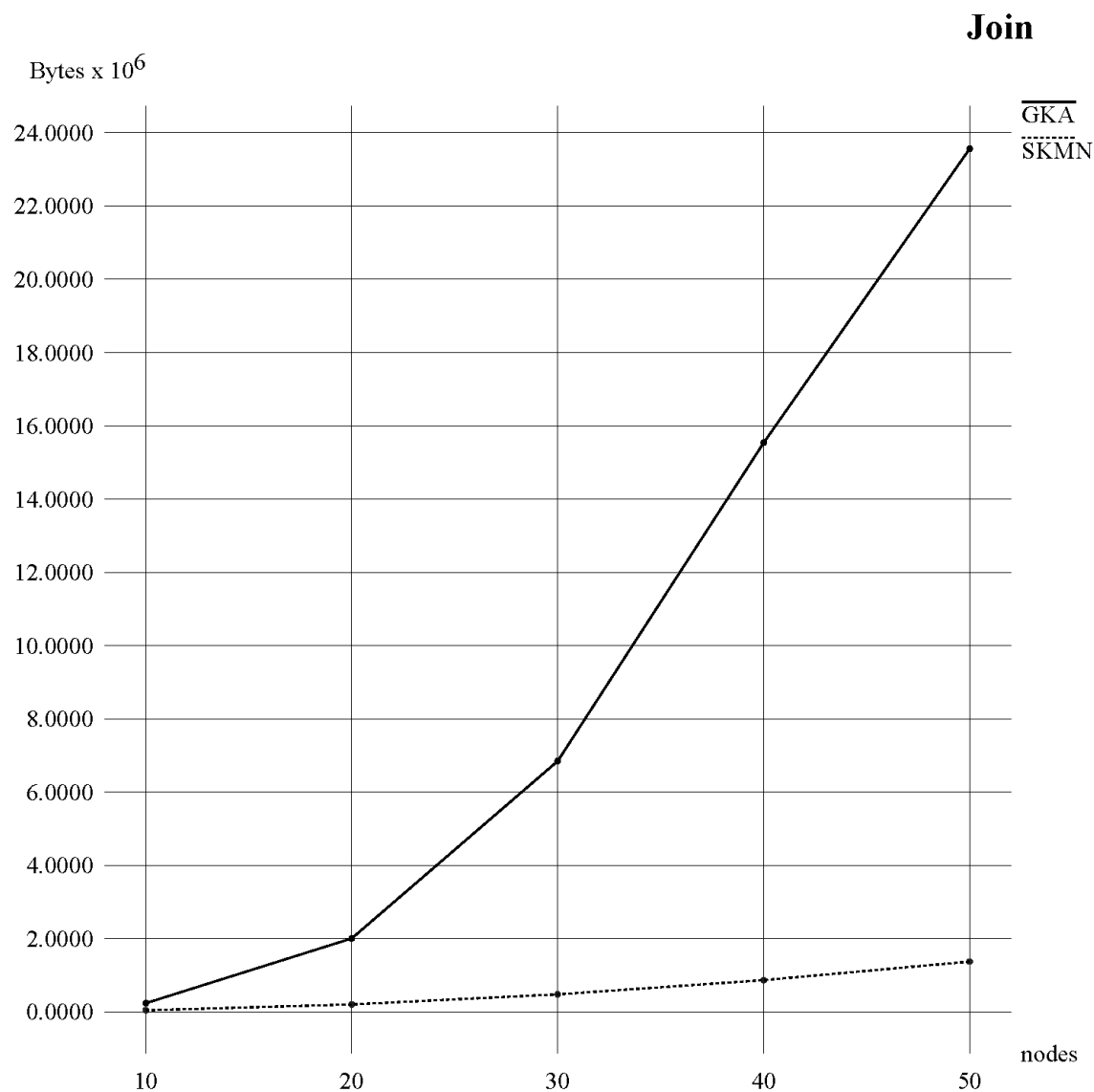
# LEAVING SCENARIO: MESSAGE NUMBER



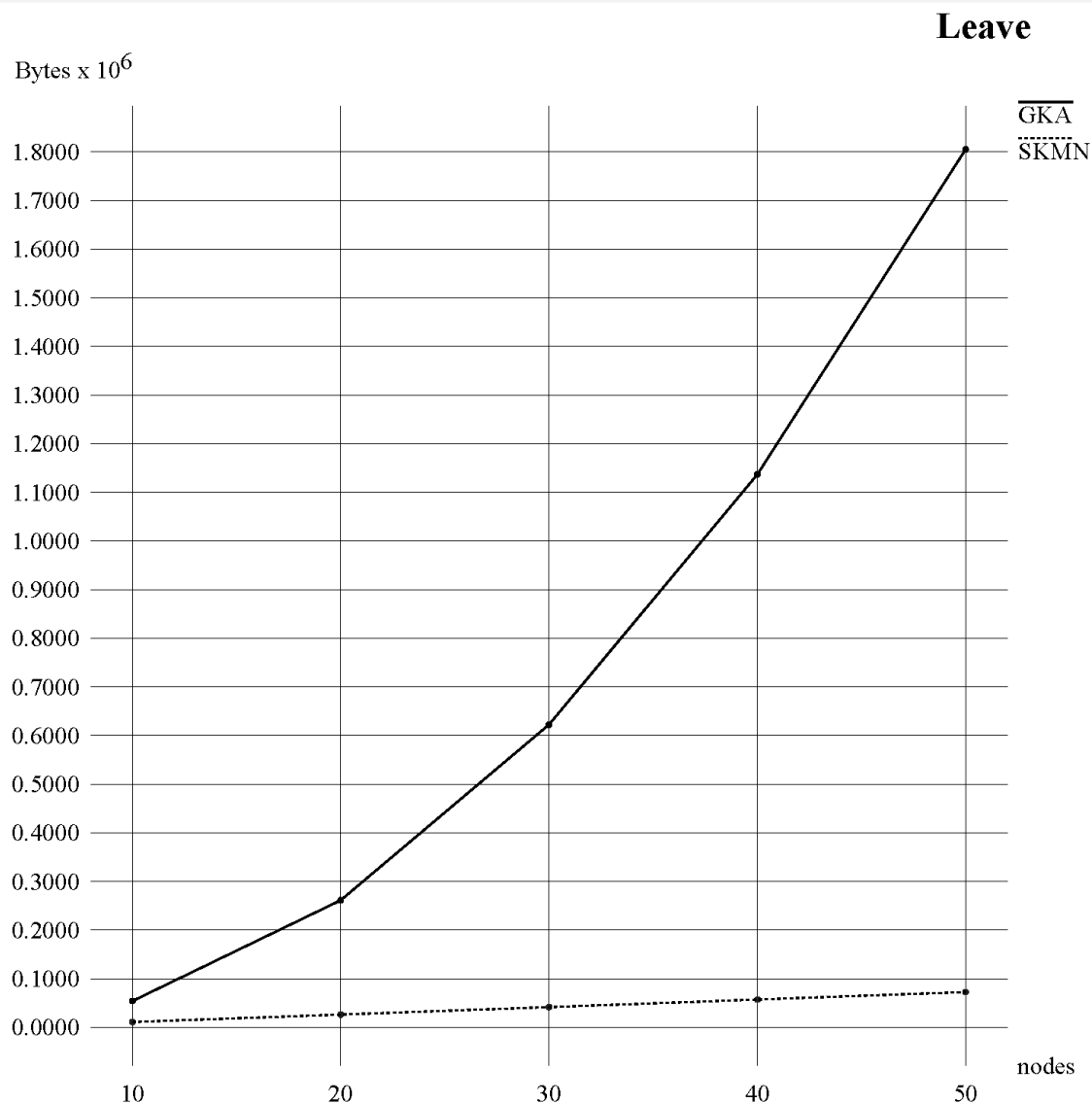
# MERGING SCENARIO: MESSAGE SIZE



# JOINING SCENARIO: MESSAGE SIZE



# LEAVING SCENARIO: MESSAGE SIZE



# RESULTS EVALUATION

- ❑ Goods results in Skemasnet scheme
  - ❑ Using smaller messages
  - ❑ Using less messages
  
- ❑ Skemasnet algorithm can be applied to specific cases
  - ❑ Considering social face to face agreement and trust (security)
  - ❑ Small number of nodes (<150)
  
- ❑ Skemasnet may become a good alternative to GKA in specific situations, but cannot replace general schemes like this one

Thank you for your attention !

Any question ?



# THE SKEMASNET PROJECT

## *SESSION KEY MANAGEMENT IN A SPONTANEOUS NETWORK*

**HGP Team**

**Hyunho Park , Gianni M. Ricciardi, Pierre Alauzet**

# REFERENCES

“Establishing trust in pure ad-hoc networks”, Asad Amir Pirzada, Chris McDonald January 2004 ACSC '04: Proceedings of the 27th Australasian conference on Computer science - Volume 26 , Volume 26 (ACM Portal)

“Spontaneous networks: Trust in a world of equals”, Gilaberte, R.L.; Herrero, L.P.; Networking and Services, 2006. ICNS '06. International conference on 16-18 July 2006 Page(s):42 - 42 (IEEE Xplore)

“Security management for ad-hoc networked resource-limited mobile devices” Sedov, I.; Speicher, S.; Cap, C.; Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th Volume 5, 26-29 Sept. 2004 Page(s):3262 - 3266 Vol. 5 (IEEE Xplore)

“Implicit merging of overlapping spontaneous networks [mobile ad hoc networks]”, Legendre, F.; de Amorim, M.D.; Fdida, S.; Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th Volume 4, 26-29 Sept. 2004 Page(s):3050 - 3054 Vol. 4 (IEEE Xplore)

"Spontnet: experiences in configuring and securing small ad hoc networks", Feeney, L.M.; Ahlgren, B.; Westerlund, A.; Dunkels, A.; Networked Appliances, 2002.

Johann Van Der Merwe, Dawoud Dawoud, and Stephen McDonald

*A Survey on Peer-to-Peer Key Management for Mobile Ad Hoc Networks*

Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong

*Talking To Strangers: Authentication in Ad-Hoc Wireless Networks*

Michael Steiner, Gene Tsudik, Michael Waidner

*Diffie-Hellman Key Distribution Extended to Group Communication*

Daniel Augot, Raghav Bhaskar, Valerie Issarny and Daniele Sacchetti

*An Efficient Group Key Agreement Protocol for Ad hoc Network*

<http://www.isi.edu/nsnam/ns/>

Official website of ns-2 simulator, accessed on November 29th 2009