THE SKEMASNET PROJECT

SESSION KEY MANAGEMENT IN A SPONTANEOUS NETWORK

HGP Team

Hyunho Park , Gianni M. Ricciardi, Pierre Alauzet

CS642 - Distributed Systems

September 23th, 2009

TABLE OF CONTENTS

INTRODUCTION

- Spontaneous network definition
  - Application oriented network deployed when some users meet together for some common purpose
  - No pre-existing infrastructure (no server or connection point)
  - Features such as address allocation, name resolution, service location, authentication, and so on have to be provided without pre-configuration or centralized services
- Possible spontaneous network examples
  - Interactive presentations
  - Document sharing
  - Collaborative editing
  - Games

SCENARIO

- Spontaneous network merging
  - How can we merge 2 different networks but a same application?
  - Do we keep previous communications & data ?
  - How can we manage the security in merging networks ?

- Spontaneous network separation
  - What is happening when some users leave a spontaneous network ?
  - Do we wish 2 independant spontaneous networks ?
  - How can we maintain the previous shared data, communication, etc.

MOTIVATIONS

- Spontnet: Experiences in Configuring and Sequring Small Ad Hoc Network
  - In paper[5], we found a comprehensive discussion about the setting of a spontaneous network using session keys shared among users, but they don't consider different groups, each one with its own network, desiring to join all together in only one network;
- Network merging at MANET
  - In paper [4], they propose a realistic model about permanent or transient merging of MANET, but from a low level point of view (networking, routing, etc.), without considering session keys management as we propose;

PROBLEM DEFINITION

- We suppose to be in the case of networking established using *spontaneous VPN* (i.e. a VPN among nodes, built using a shared session key).

- A session key is a single-use symmetric key used for encrypting all messages in one communication session

- Normally, keys must be distributed securely before encryption can be established, in order to get a secure network.

PROBLEM DEFINITION (CONT.)

- Merging problems
  - Session key management (security management)
    - Do we create a new session key ?
    - Do we use a proxy node ?
    - …
  - Considering other aspects such as naming, addressing or authentication

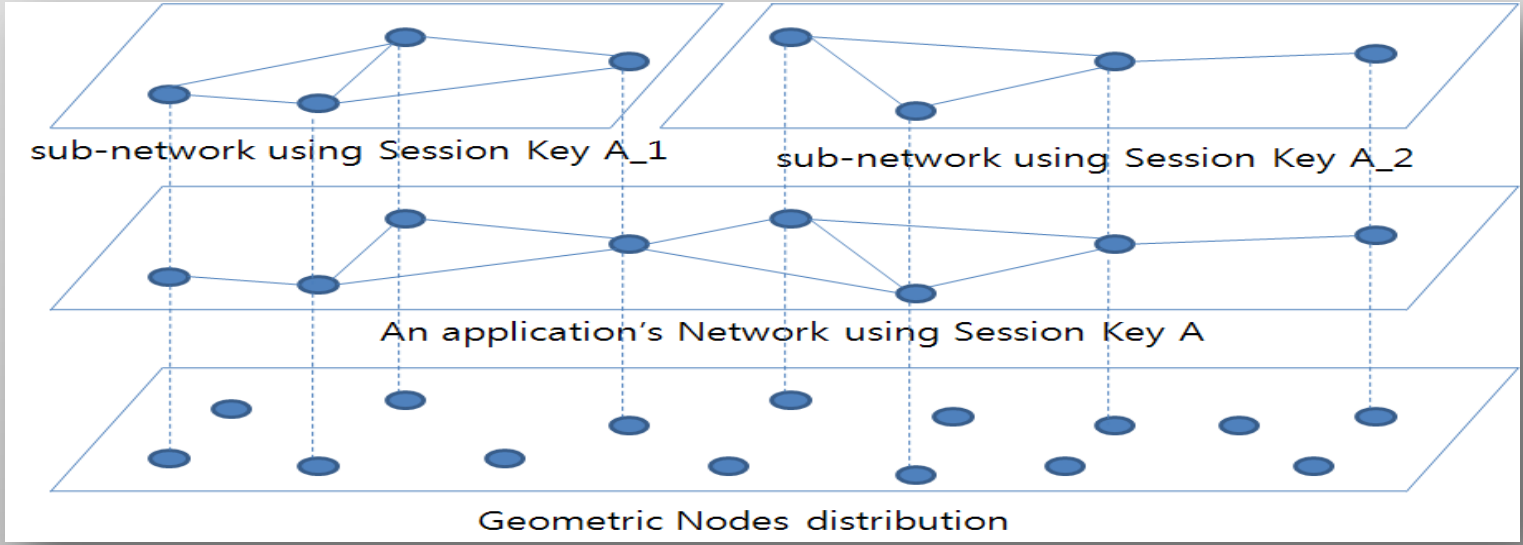
- Separation problems
  - Session key management (security management)
    - Do we use the previous key ?
    - Do we wish to separate independent networks ? In this case, are data, communication, etc. now independent ?

DESIGN CONSIDERATIONS

- How to create session key?
  - Using cryptographic keys as session keys.
  - Advantages
    - Globally unique session key at any time without reference to central authorities.
    - A node's session can be remains valid as long as desired.
    - The node can retain its session key when it moves or the surrounding network topology change.
    - Multiple session keys can be generated simultaneously.
    - Independent of centralized public key infrastructure.
- How to distribute session key?
  - For the initial session key a secure channel have to be used to transfer the key (e.g. IrDa, memory card storing the key, etc.)
  - After the mother spontaneous network has been deployed, to create child ones the required session keys can be shared using the mother network, before this one disappears.

DESIGN CONSIDERATIONS

- How to manage merging and separation?
  - Necessary a key generating algorithm that allows a key to be merged with other key to make a common key that can be used on the merged network.
  - Necessary addressing, naming scheme which support network merging.



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

1. “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)
2. “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)
3. “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)
4. “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)
5. "Spontnet: experiences in configuring and securing small ad hoc networks”, Feeney, L.M.; Ahlgren, B.; Westerlund, A.; Dunkels, A.; Networked Appliances, 2002.