Self Organizing Trust Establishment
&
Cooperation Enforcement

Refik Molva, Melek Önen, Abdullatif Shikfa

EURECOM

Security Challenges in self-organizing networks

- Self-organizing
  - No (or limited) infrastructure
  - Lack of organization
    - No security server
- Wireless & Mobile
  - Scarcity of Resources
  - Limited Energy
  - Lack of physical security

- Comm. Security
- Trust establishment
- Cooperation Enforcement
- Key management

Security issues in HAGGLE – WP4

- Trusted Communities & Secure Communications
  - Task 4.1: Trust & Cooperation
    - Build trust among parties
    - Enforce cooperation
  - Task 4.2: Secure communication mechanisms
    - confidentiality, integrity, availability
    - requirements due to forwarding
  - Task 4.3: Integration of trust & cooperation with Communication security
    - Solve potential conflicts between security and communication functions

Agenda

- Task 4.1: Trust &Cooperation
  - Security Requirements
  - Existing solutions
  - Potential directions

Trust Establishment

- Managed environment
  - A-priori trust
  - Authentication $\Rightarrow$ trustworthiness
  - But:
    - requirement for infrastructure
    - scarcity of computing resources (sensors)
    - lack of connectivity (sensors, ad hoc nw)
- Open environment
  - No a-priori trust
  - authentication does not guarantee correct operation

Self Organizing trust establishment

- Requirement: trust establishment from scratch
  - No infrastructure for Communication or Security
  - No a-priori trust relationship
- Trust establishment protocols
  - e-cash
    - One-time credentials: use of money in case of malwareness [Bussard et al'04]
  - History based trust establishment
    - Use of different credentials based on history

Trust establishment & key management

Authentication ⇒ Key Management

- **Public key certificates**
  - Self organized CA : based on threshold cryptography
    [Bechler et al'04], etc.
    - Share distribution during bootstrap phase, network density
  - Web of Trust (PGP) : no centralized TTP
    [Hubaux, et al.'01]
    - Initialization, storage, transitivity of trust
- **Certificate-less**
  - Crypto-based IDs: ID = h(PK)
    SPKI, SUCV-based, [Rivest], [Montenegro et al'05]
    - Generation of bogus IDs
  - ID based crypto: PK= h(ID)
    [Boneh, Franklin'01],[Khalili et al.'03]
    - SK computed by TTP, distribution of initial shares

Potential directions

- Trust establishment without identities
  - Attribute certificate vs. ID certificate
  - Sticky policy using ID-based crypto
- Opportunistic networking ⇔optimistic security protocols
  - without TTP : very difficult and often costly
  - with TTP: minimum interaction, only required in case of litigation
- Key management with symmetric techniques
  - Key pre-distribution

Cooperation enforcement

- No infrastructure for communication
  - Collaboration among parties is a MUST
- Selfish behavior
  - Optimal resource usage
  - Need for cooperation enforcement

Cooperation enforcement schemes

- Schemes based on virtual money
  - Nugglets [Buttyan et al'01]
  - SPRITE [Zhong et al'03]
- Reputation based schemes
  - CORE [Michiardi et al'02]
  - CONFIDANT [Buchegger et al'02]
- etc.

Potential directions

- Definition of hybrid schemes
  - combining the use of virtual money with reputation
  - fair exchange protocols
- Dedicated schemes
  - Network coding: coding operations at each node
  - No cooperation $\Rightarrow$ no decoding

Summary & Conclusion

- New paradigms for self-organizing networks
  - Trust establishment
    - Attribute certificates, sticky policies with IBC, optimistic protocols
  - Cooperation enforcement
    - Hybrid schemes (money + reputation)
    - Dedicated schemes (e.g.: network coding)

- Other security issues
  - Key management (Task 4.1, 4.2 and 4.3)
    - Lack of organization: no security server
      - key pre-distribution protocols, id-based crypto,..
  - Communication security (Task 4.2)
    - Confidentiality, authentication, secure routing/forwarding
      - homomorphic cryptographic algorithms

References

- *History-based Trust Establishment Protocols,* Bussard, Molva, Roudier, in PerCom'04 and iTrust'04
- *Analysis of Coalition Formation and Cooperation Strategies in Mobile Ad hoc Networks*, Michiardi, Molva, in Ad Hoc Networks Journal – Volume 3, Issue 2 , March 2005, Pages 193-219
- *Policy-based Cryptography ,* Bagga, Molva, Financial Cryptography 2005, Dominica, February 2005.
- Other papers on http://www.eurecom.fr/ce/researchce/nsteam.fr.htm
- *HAGGLE: www.haggleproject.org*

THANK YOU