Certificate Management for Mobile Ad Hoc Networks

2003.12.12

林佑青

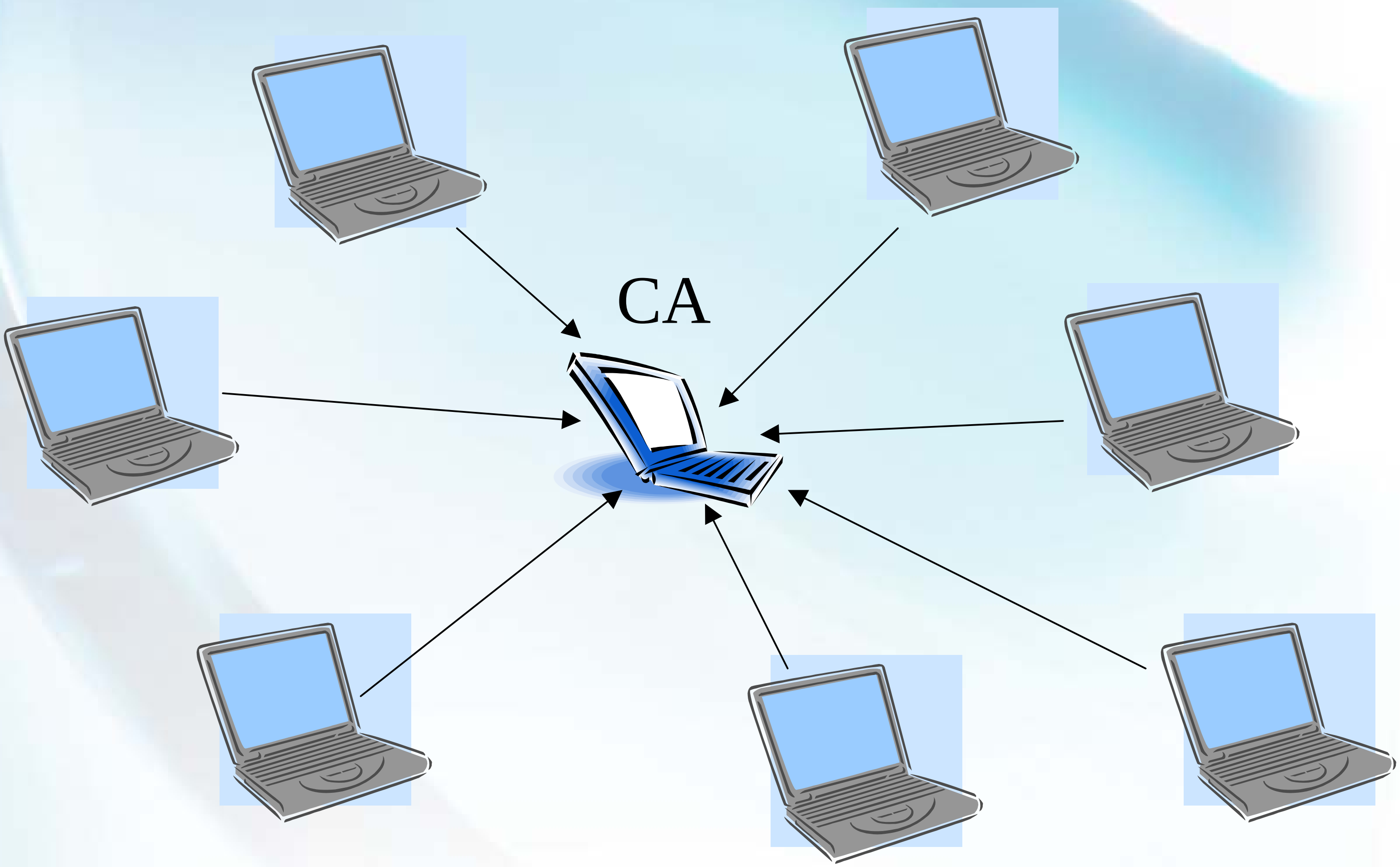
Outline

- Introduction
- Key management protocols
  - Centralized
  - Partially distribution
  - Fully distribution
- MOCA：Mobile Certificate Authority
  - Secret sharing
- Self-organized public-key management
  - PGP extension
- Secure Key Exchange
- Performance
- Conclusion

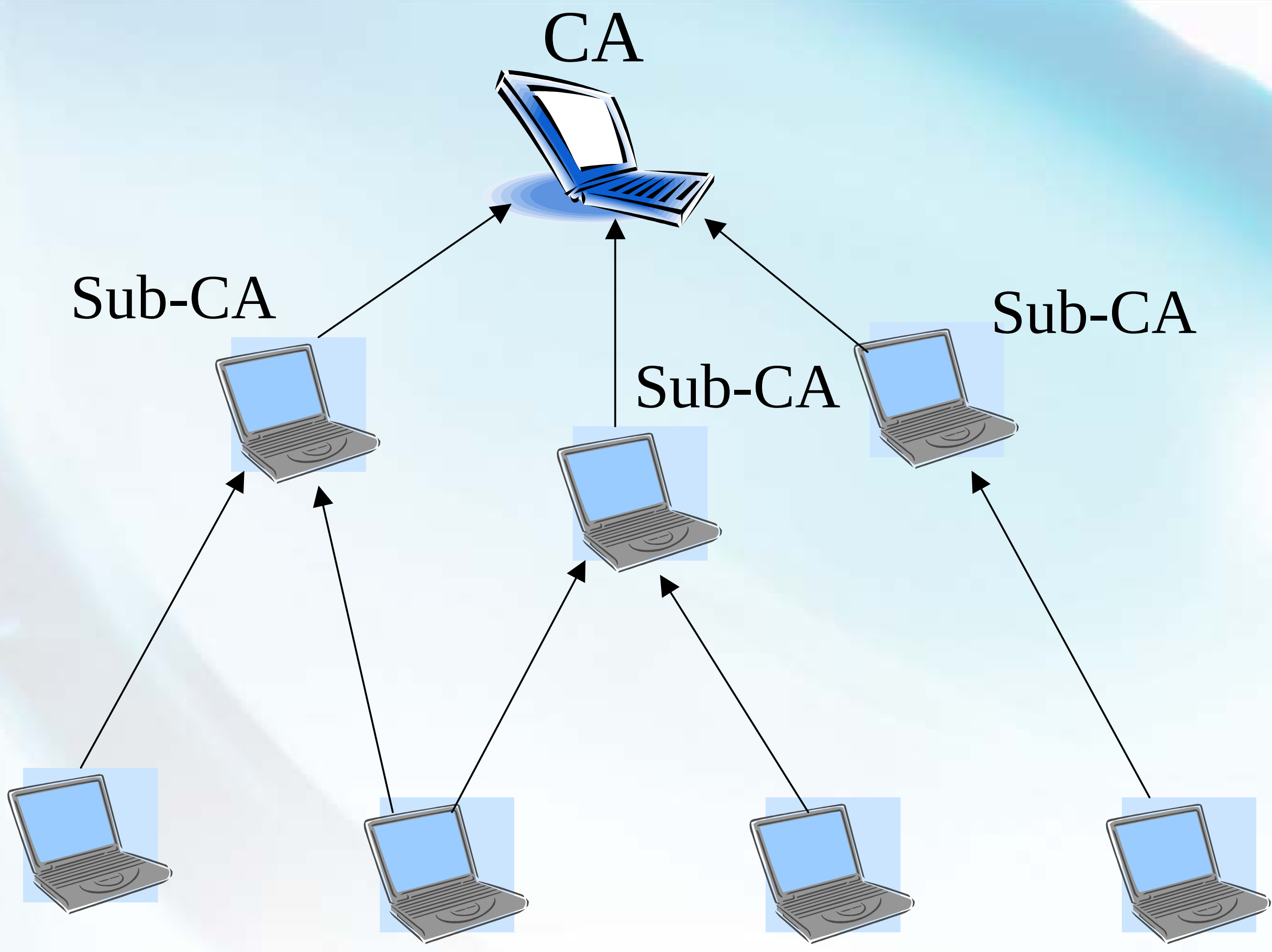
Introduction

- PKI has been recognized as one of the most effective tools for providing security for dynamic networks.
- It is a challenging task to provide such an infrastructure in ad hoc networks due to their infrastructure-less nature.
- Distributed CAs instead of using single trusted authority.

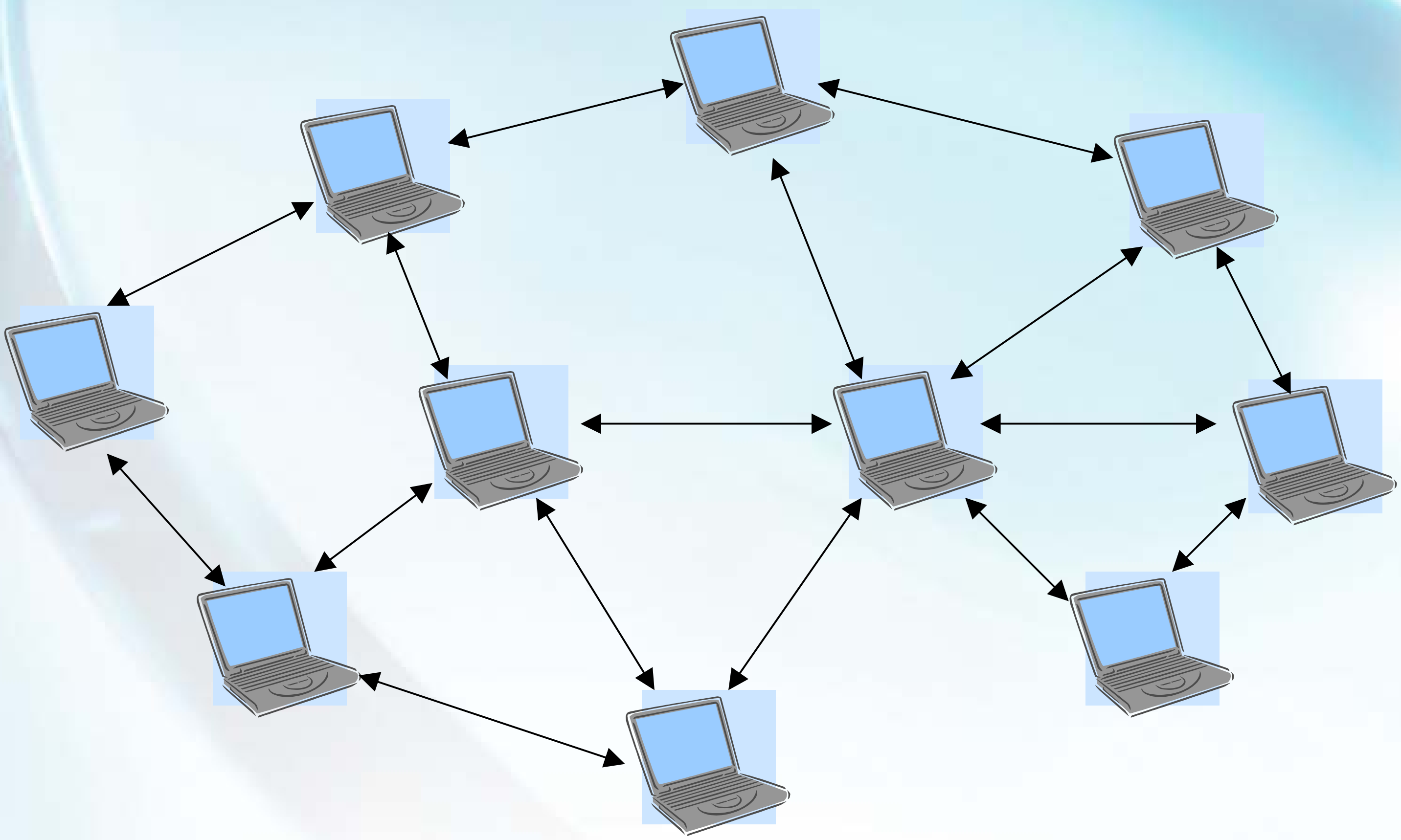
Centralized



Partially distribution



Fully distribution



Threshold Cryptography

- (n,k) threshold scheme
  - Divide a secret key (D) into n pieces, D_1、D_2 ……、Dn
  - Distribute the pieces to n nodes in a group
  - Collect any k pieces (k<n) to reconstruct the full secret

How to share a secret

- Shamir's (k, n) secret sharing scheme
- Split secret *D*
  - Randomly pick a *k-1* degree polynomial $f(x)=D+a_1x^1+\ldots+a_{k-1}x^{k-1}$
  - Evaluate $D_1=f(1),\ldots,D_i=f(i),\ldots,D_n=f(n)$
  - Each node x_i gets his share $y_i = f(x_i)$ for n nodes
  - Given k shares, the polynomial is determined

Example

- (2,3) threshold scheme
  - Secret D=7
  - Random pick 1 degree polynomial
    - f(x)=7+2x
    - Shares D_1=9, D_2=11, D_3=13
- Recovery: provided {D_1=9, D_2=11}

  $D_1 = f(1) = D + a_1 = 9$

  $D_2 = f(2) = D + 2a_1 = 11$

  - Then we have a_1=2 and D=7

MOCA：Mobile Certificate Authority

- Selected n MOCA nodes.
  - Physically more secure
  - Computationally more powerful
- MOCA nodes provide the functionality of a CA.
- n MOCAs share the CA's private key and any set of k MOCAs can reconstruct the full CA key.
- Use secret sharing protocol.

Partially Distribution (1)

- Certificate authority has a public/private key pair
  - Public key is known by everybody
  - Private key is shared between the n servers
- Each Server
  - Knows the public key of every node
  - Sign partial certificates using his share of the signing key
- Each Client
  - Equipped with MOCA certification protocol

Partially Distribution (2)

- Initialization
  - Clients flood the network with Certification Request (CREQ) and wait for at least k Certification Replies (CERP).
- Certificate retrieval
  - Each server sends a partial certificate signed with his share of the system’s signing key
  - The client can then verify it using the system’s public key.

Partially Distribution (3)

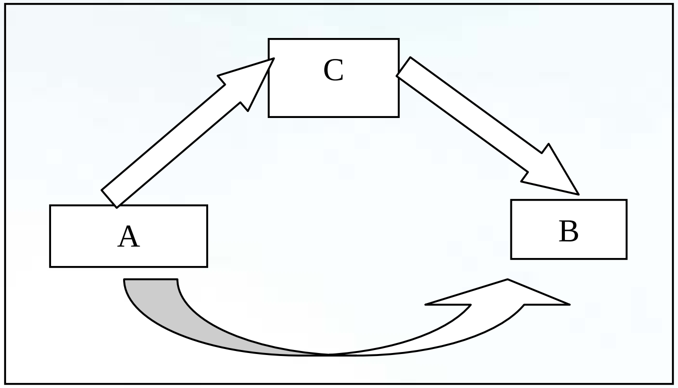
- The MOCA can handles the lack of server infrastructure by distributing the CA.
- Availability relies on:
  - The choice of the threshold parameters (k,n)
  - The choice of the servers nodes
- High overhead due to its flooding nature.

Fully Distribution (1)

- Self-Issued Certificates: Extension of PGP
- No need for an authority
- Each node creates his public / private key pair
- Certificate Issuing
  - Users are able to issue certificates to others
  - Based on trust (Secure channel), certificate received by a trusted user.
- Each node maintains a repository
  - The certificate he has issued
  - The certificates other users have issued to him

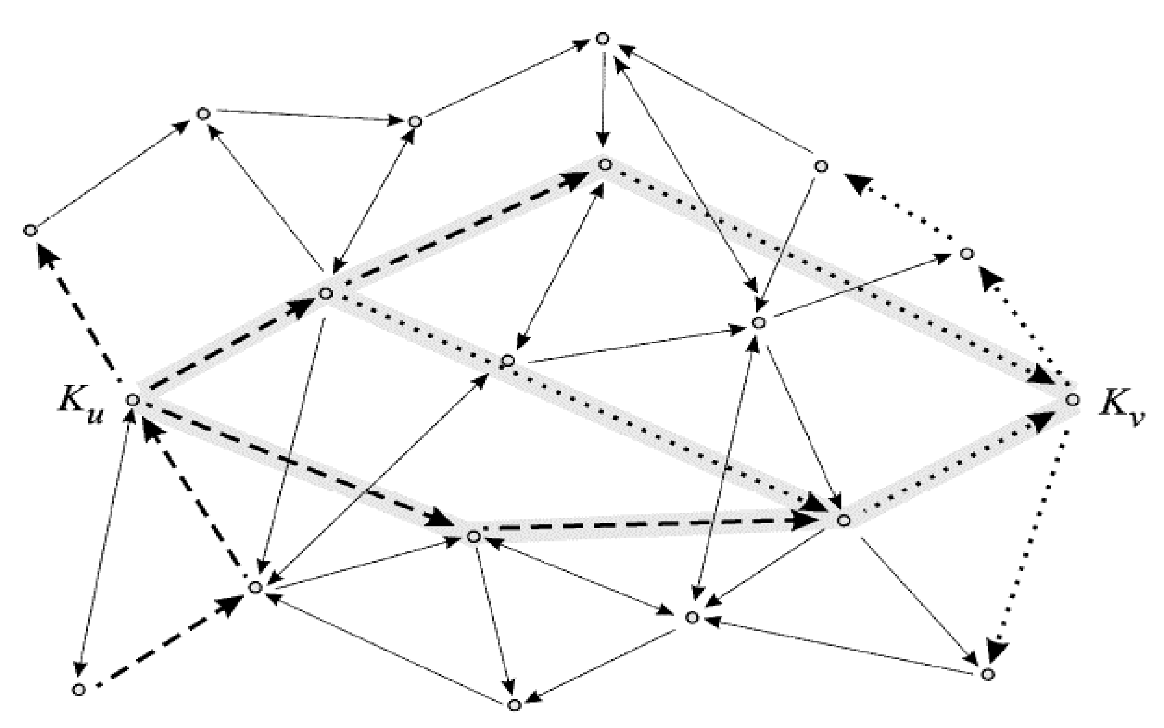
Fully Distribution (2)

- When a user A wants to obtain the public key of another user B, A acquires a chain of valid public-key of user B：
- Certification Chain between two users
  - A wants B’s certificate
  - But A only has C’s certificate and A trusts C
  - C has B’s certificate
  - Chain from A to B through C



Fully Distribution (3)

- System represented as a oriented graph
- Certificate verification
  - Users merge their repositories
- Certificate Chain = Directed path from u to v



Fully Distribution (4)

- A fully self-organized public-key management system for mobile ad hoc networks.
- Key authentication based only on their local information.
- Availability - don't need any authority
- Entirely relies on mutual trust between users.

Fully Distribution (5)

- Provides availability
- Higher communication overhead
- Large computation

Secure Key Exchange (1)

- The idea underpinning the solution is extremely straightforward, as it simply mimics human behavior.
- Exchange sensitive information over a secure channel (location-limited channel)
- Location-limited channel
  - Separate from the main wireless link
  - Infrared, bluetooth ……

Secure Key Exchange (2)

- Doesn't require neither authority, nor prior relationship between users.
- Pre-authentication phase
  - A device can "touch" the device he wants to authenticate
  - Location-limited channel
  - Exchange public information
    - Public key
    - Digital certificate
  - Confidentiality is not required

Secure Key Exchange (3)

- Provide an intuitive way to identify and authenticate communicating entities
- Doesn’t rely on any authority
- Formation of self-configured networks
- Not scalable when there are a lot of devices
- Requires devices to have location-limited channels

Performance (1)

Scheme	Centralized	Partially distributed	Fully distributed
Node increases	92%→22%	88%	96%
Traffic load increases	80%→45%	85%	95%
Channel error rate increases	80%→50%	85%→82%	95%→93%

Performance (2)

Scheme	Centralized	Partially distributed	Fully distributed
Scalability	Bad	Good	Good
Availability	Bad	Medium	Good
Robustness	Bad	Medium	Good
Communication	Centralized	Distributed	Localized
Computation	Server	Shared	Shared

Conclusion

- Solutions to provide security mechanisms and key management with different approaches.
  - Distribution of certificate authority
  - Self-organized ad hoc networks
- Traffic overhead, computation, power consumption
  - Solutions based on public-key cryptography and certificates are expensive
  - Reduce the communication overhead.

References

[1] Seung Yi, Robin Kravets, *MOCA：Mobile Certificate Authority for Wireless Ad Hoc Networks*, 2nd Annual PKI Research Workshop Program (PKI 03).

[2] Seung. Yi and Robin. Kravets, *Key Management for Heterogeneous Ad Hoc Wireless Networks*, IEEE ICNP’02.

[3] A. Khalili, J. Katz and W.A. Arbaugh, *Towards Secure Key Distribution in Truly Ad Hoc Networks*; University of Maryland

[4] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. *Self-securing Ad Hoc Wireless Networks*, IEEE ISCC 2002.

[5] JP Hubaux, L. Buttyan and S. Capkun, *Self-organized Public-Key Management for Mobile Ad hoc Networks*, IEEE Transactions on Mobile Computing, Jan. 2003.

[6] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi Wong, *Talking to Strangers: Authentication in Ad hoc Wireless Networks*, Conference Proceeding of NDSS Conference 2002.

[7] Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttyan, *Mobility Helps Security in Ad Hoc Networks*. ACM MobiHoc 2003.

[8] M.C. Morogan, S. Muftic, *Certificate Management in Ad Hoc Networks*. IEEE SAINT’03

[9] H.Yang, G. Zhong, S. Lu, Network Performance Centric Security Design in MANET. IEEE Mobile Computing and Communication Review.