

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

Seung Yi, Robin Kravets

Department Of Computer Science
University Of Illinois At Urbana-Champaign



PKI in a New Environment

- Most PKI solutions rely on
 - Online CA(s) that is...
 - (Almost) always available
 - Secure
 - Stable connectivity to CA
- *What if all of these nice things go away?*



Trust in an Untrusted Network

- Mobile wireless ad hoc network
 - A network formed with a set of wireless nodes without any infrastructure support including ground wire or base station
 - Packets are forwarded through neighboring nodes to reach out-of-range destinations
- Lack of infrastructure
 - Eases deployment in cost-effective way
 - Implies no pre-existing trust anchor within the network, making an ad hoc network inherently untrusted network



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

3

Target Scenario

- Popular ad hoc network example scenarios
 - Battlefield communication
 - Emergency rescue operations
 - Disaster recovery
- Mission critical applications require strong security
 - Begins at a trust anchor
- Question
 - Can we provide PKI in ad hoc networks without relying on any infrastructure support?



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

4

Requirements for Ad Hoc PKI

- Fault tolerance
 - General purpose mobile nodes are prone to faults
 - PKI should be tolerant to a fraction of faulty nodes
- Security
 - Mobile nodes are more vulnerable to attacks than wired nodes
 - PKI should operate securely even when a fraction of nodes is compromised
- Availability
 - Connectivity is not guaranteed in ad hoc networks
 - CA service should be (always) available to clients



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

5

Naïve Approaches

- Single CA for an ad hoc network
 - Single point of failure
 - Clients may not be able to contact the CA
 - Adversary must locate the single CA to compromise
- Replicated CAs
 - Tolerant to *(number of replicas - 1)* failures
 - Better availability
 - Collapses if one replica is compromised



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

6

A Better Approach : Use Threshold Cryptography

- Parameters
 - m total nodes in the network
 - n nodes share the CA's private key
 - any k out of n can reconstruct the CA's private key
 - $k \ll n \ll m$
- Tolerance
 - up to $(n-k)$ faulty CAs
- Security
 - up to $(k-1)$ compromised CAs



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

7

Threshold Crypto Parameters

- Availability
 - Determined by k
- Security
 - Determined by the gap between n and m
 - Example : Randomly select five nodes to compromise
 - $k=5, n=20, m=100$: with 0.0002 they're all CAs
 - $k=5, n=50, m=100$: with probability 0.028
 - $k=5, n=100, m=100$: with probability 1



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

8

Related Research

- [Zhou99] first suggested using threshold cryptography for distributed CA in ad hoc networks
 - Later extended to COCA
 - Aimed at the Internet, focusing on long-term operation including proactive share update
 - Do not address availability
- [Kong01] makes every mobile nodes to be a distributed CA
 - $n = m$
 - Maximum availability for ubiquitous presence
 - But at the price of weakened security
 - An adversary needs only compromise any k nodes to collapse the system



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

9

MOCA (Mobile Certificate Authority)

- Choosing CA nodes
 - Exploit heterogeneity to select “better” nodes
 - More trustworthy
 - Computationally more powerful
 - Physically more secure
- Configuration
 - (k out of n) threshold cryptography
 - $n \ll m$ for security
 - Client needs to contact k MOCAs
- Availability
 - Efficient communication protocol to guarantee adequate availability



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

10

Certification Protocol

- Goal
 - High success ratio
 - Provide availability of the CA service
 - Acceptable overhead
 - Do not cripple the network
- Naïve approach
 - Flood the ad hoc network with a certification request
 - High success ratio
 - High overhead!

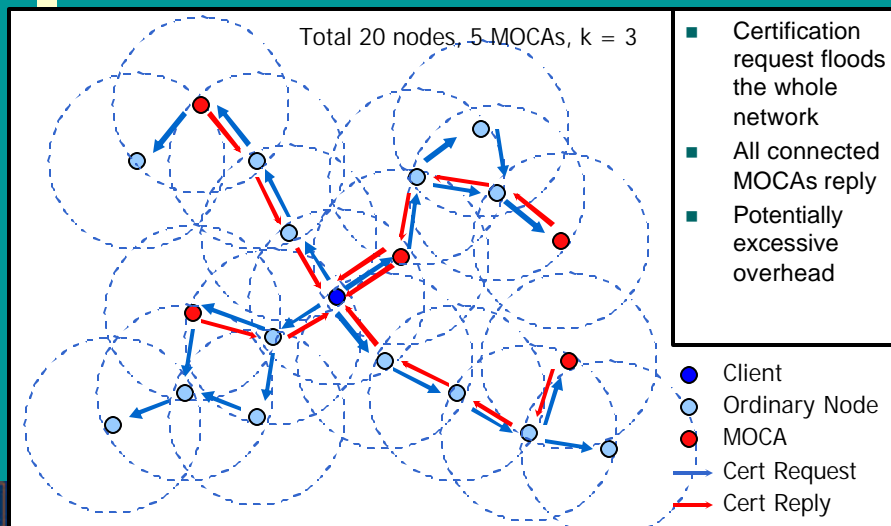


4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

11

Flooding-based Certification Protocol



Wireless Ad Hoc Networks

Reducing Communication Overhead

- Observation
 - New communication pattern
 - “Manycast”
 - Single source
 - Multiple destinations
 - Multiple independent replies
 - Applicable for any threshold-based distributed service
 - (cf. unicast, anycast, multicast, broadcast)
- Goal
 - Efficient support of manycast communication in ad hoc networks



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

13

Certification Protocol Continued

- Two mechanisms
 - Flooding
 - Simplest way with highest overhead
 - Certification request floods the whole network
 - Unicast optimization
 - Once MOCAs are located (and routes cached), use multiple unicast queries

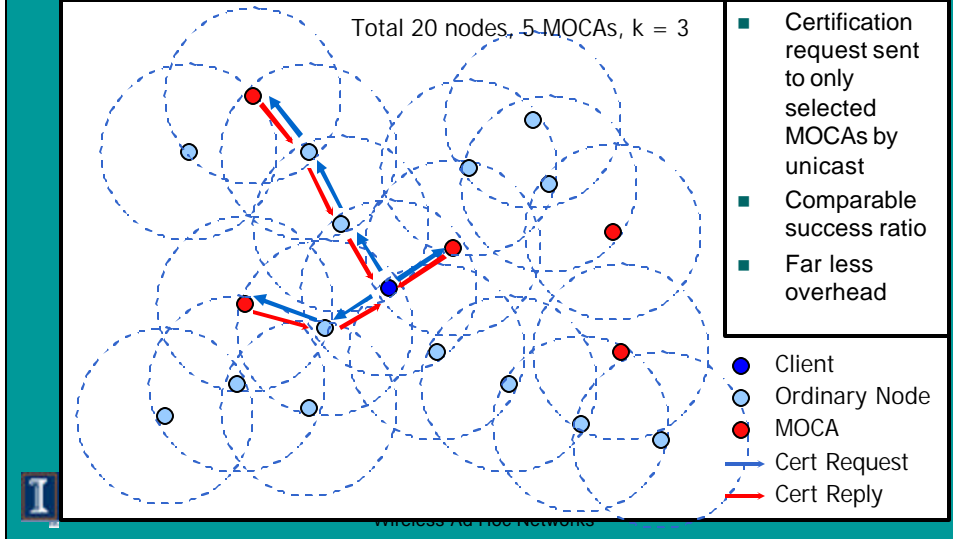


4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

14

Unicast-based Certification Protocol



Making MOCA More Robust

- Problem
 - What if k responses is not enough?
 - Moved or compromised MOCAs
- Safety margin
 - Contact α extra nodes
 - Unicast threshold $b = k + \alpha$
 - b should be set according to perceived network conditions



Evaluation

■ Metrics

- Use of unicast optimizations
- Control overhead
- Success ratio
- Response time

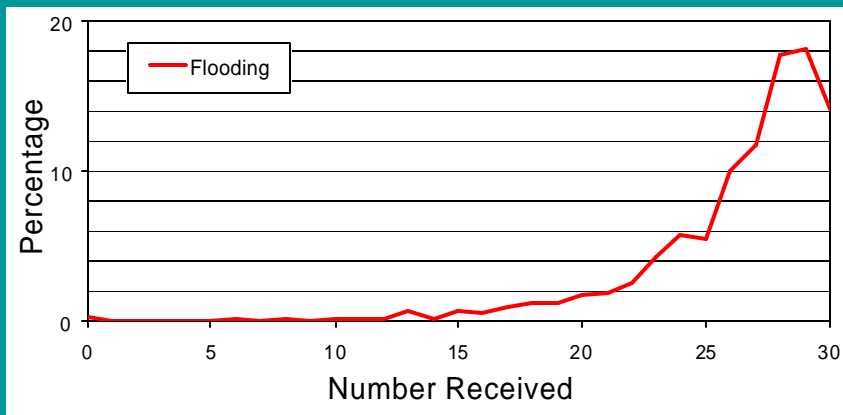


4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

17

Flooding Vs. Unicast

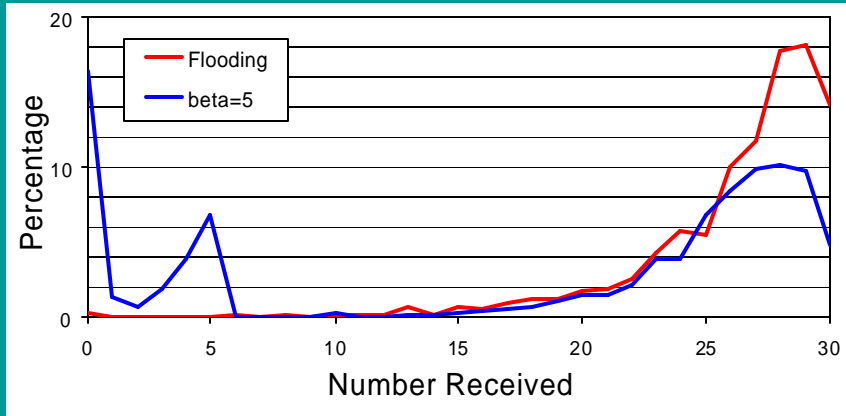


4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

18

Flooding Vs. Unicast

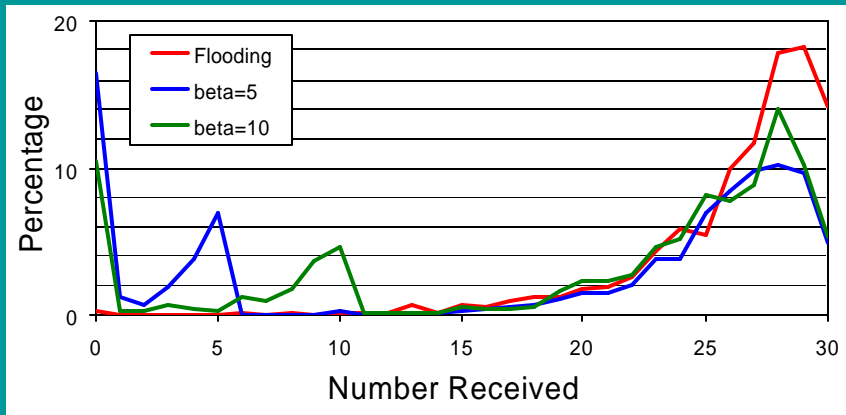


4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

19

Flooding Vs. Unicast

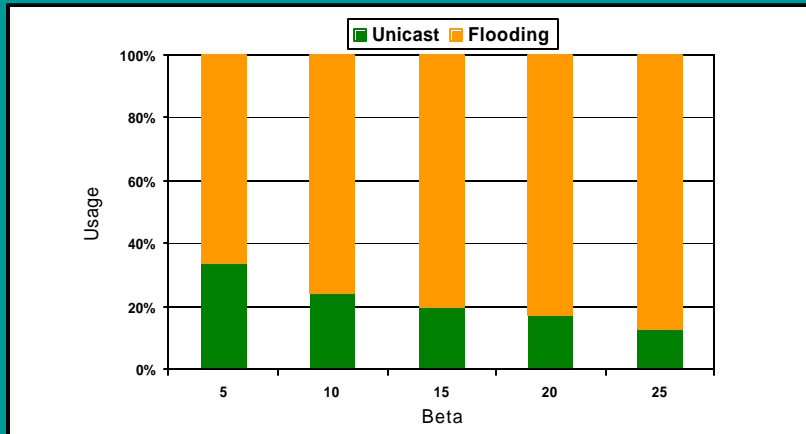


4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

20

Unicast Usage

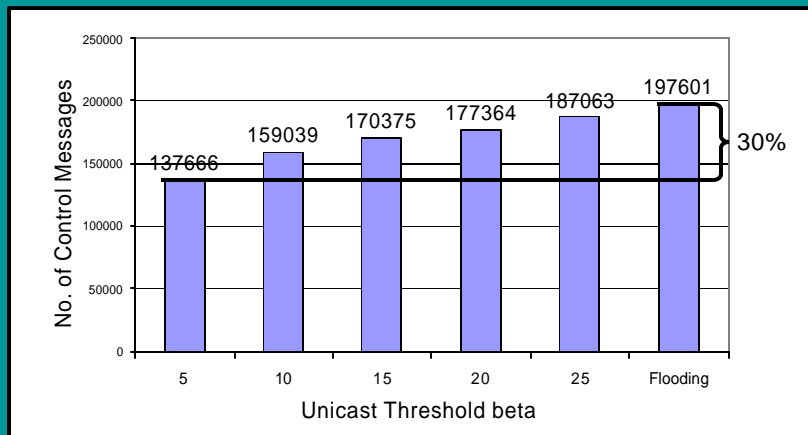


4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

21

Overhead

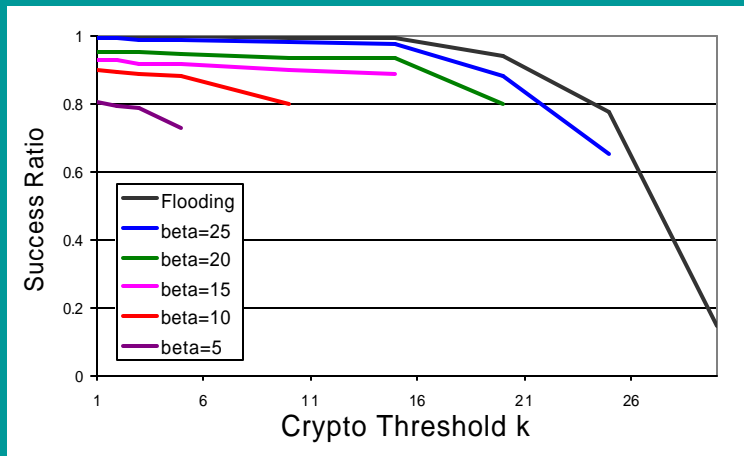


4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

22

Success Ratio

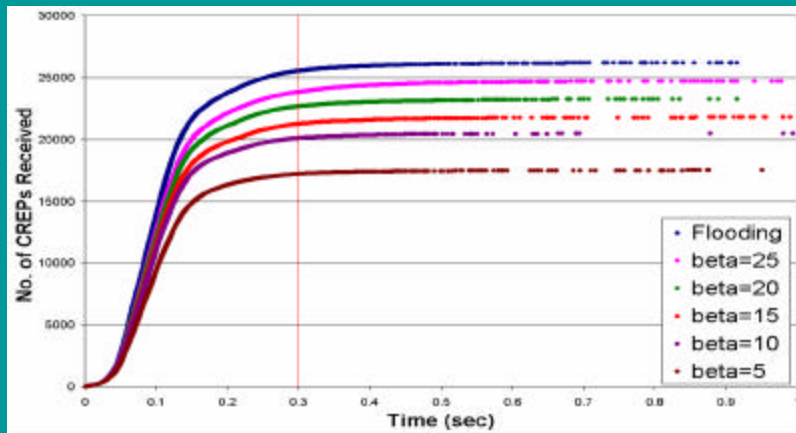


4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

23

Response Timeliness



4/29/2003

MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks

24

Evaluation Summary

- Implemented in ns-2 network simulator
- High success ratio
 - Flooding achieves 99% success ratio for most time
 - With unicast-based optimization, success ratio is between 75% and 97%
- Reduced overhead
 - Unicast optimization saves up to 30% of control packets
- Certification delay is acceptable



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

25

Future Work

- Extended MOCA
 - Need a way to handle temporary network partition or harsh network condition where k MOCAs are not reachable
 - Use a limited and regulated PGP-type certificate chaining [Hubaux01] from any certified node to extend the reach
 - Certificates issued by chaining is short-lived and should be used only until the network is reconnected



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

26

Conclusion

- PKI support in ad hoc networks is feasible
 - Intelligent choice of CA nodes based on node heterogeneity
 - Secure usage of threshold cryptography
 - Support for a new communication pattern in routing layer to provide maximum availability without sacrificing security



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

27

Contact Information

“MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks”

- Seung Yi:
seungyi@cs.uiuc.edu
<http://www.uiuc.edu/~seungyi>
- Mobius Group at UIUC:
<http://mobius.cs.uiuc.edu>



4/29/2003

MOCA: Mobile Certificate Authority for
Wireless Ad Hoc Networks

28