Quality of Authentication in Ad Hoc Networks

Seung Yi, Robin Kravets  {seungyi,rhk}@cs.uiuc.edu

Quality of Authentication
- Problem: Quality of authentication (QoA) may vary depending on network situations
  - How confident can you be with an authentication?
- Solution: Provide QoA information to end users
  - QoA depends on trust relationships among mobile nodes
    - Security level of CA in PKI
    - Shape and density of trust relationships among mobile nodes in certificate chaining
  - End users apply metrics of authentication to reason about given authentication instances

Conclusions
- Quality of Authentication
  - Enables end users to measure confidence in authentication instances
  - Enables comprehensive evaluation of key management frameworks
- Future directions
  - More intuitive way to express changing conditions
  - Incorporate multiple chain confidence values

Calculating Quality of Authentication
- Combine confidence values of certificates in a certificate chain
  - Multiply all confidence values
- Apply attenuation factor to the chain confidence value
  - Compensate for compromised nodes
- Incorporate all chain confidence values
  - Choose one: highest, lowest, median
  - Combine: sum or average

Measuring Quality of Authentication

Comparison of Distributed PKI Approaches

Comparison of Certificate Chaining Approaches

Composite Key Management