CS-6910: Advanced Computer and Information Security (ACIS) 
FALL – 2006 
Project # 14B 

Authentication of Helper Candidates in Oppnet Environments 

Durga Koka 
Sowmya Chittineni 
Subhashini Pulimamidi 

Department of Computer Science 
Western Michigan University 
Instructor: Prof. Leszek T. Lilien 
15-Minute Project Presentation Presented on 10/03/06
Topics covered

- What are MANETs.
- Security issues in MANETs.
- Role of Authentication in MANETs
- Locality Driven Key Management Architecture
- How can this be used in OPPNETs
MANETs...

- MANETs is one of the types of Ad Hoc networks.
- Ad Hoc networks are infrastructure less mobile networks
- These are characterized by a collection of hosts that form a network “On-the-fly”
Vulnerabilities of MANETs

• Easy theft of nodes and Tampering
• Limited Resources
• Transient nature of services and Devices
• Wireless vulnerabilities and limited physical security
• Modification, Fabrication and Impersonation attacks
Role of Authentication!!

- Process of determining whether some one something, in fact, who or what it is declared to be.
- Authentication is the cornerstone service, since other services such as Confidentiality, Integrity depend on the authentication of communication entities.
- Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information.
What is PKI?

- PKI is a security architecture, which provides an increased level of security for exchanging information over a network.
- PKI can also be used to deliver cryptographic keys between users securely.
Advantages of PKI

- Certainty of the quality of information sent and received electronically
- Certainty of the source and destination of that information
- Certainty of privacy of that information
Components of PKI

- Certification Authority (CA):
  It is responsible for identifying the correctness of identity of the person asking for a certificate to be issued.
  Responsibilities include:
    - Generating key pairs
    - Issuing certificates
    - Verifying certificates
Contd...

- **Revocation**: Deleting the certificates from the database when validity expires.

- **Registration Authority (RA)**: A CA may use a third party – a Registration Authority (RA) to perform necessary checks on the person or company requesting the certificate.
Locality Driven Key Management Architecture in MANETs

- Although Public key, Digital Signatures are already mature in the Internet applications, providing public key based authentication is still very challenging in mobile ad-hoc networks.
- The reason is, the entire network is world-accessible via wireless channel, the environment is highly volatile and infrastructure less and there is lack of trust in the system.
• Locality driven key management architecture achieves robust key authentication and facilitates timely and efficient establishment of distributed trust.

• The architecture reflects our application oriented view of MANET and is based on threshold cryptography to achieve high fault tolerance against network partition and malicious nodes.

• Envision MANETs from application angle as a group of interacting networks. Different MANETs can communicate with each other for any task.
Contd...

- Here, the concept of locality of trust is used. (Eg. Cars traveling in the same direction takes help from the adjacent car for directions)

- In the architecture, certificate authorities are established only within a neighborhood using threshold cryptography and different certificate authorities maintain trust relationships, called trust chains for cross-CA authentication.
Key Management Architecture:

- Certificate Authority
  -- CA Bootstrap
  -- CA Certificate Generation
  -- CA Certificate revocation

- Trust Chain
  -- Trust Chain Definition
  -- Trust Chain maintenance
Contd...

- The architecture is composed of a group of Certificate authorities (CAs), each of which provides public key authentication service to its own community.

- CAs rely on the trust relationships with others to authenticate “foreign” certificates issued by other CAs.

Figure 1. Conceptual Architecture
Contd...

- CA Bootstrap
  - Each node will generate the public/private key pair and verify signatures.
  - There exists a node d (dealer) trusted by the nodes.

In threshold Cryptography, d will have its own public key PK_d which is known to all nodes.

CA is initialized by d and generate the key pair (PK,SK) and chooses the nodes N to serve as servers.
Contd...

-- After choosing N nodes, d generates the partial keys SK: SK1, SK2, .... SKn and signed by d’s private key.

-- K servers can generate a valid CA signatures by combining partial signatures (K > S/2)
Contd...

- **CA Certificate Generation**
  a node x can request a certificate (public key PKx) from CA signed with SK of CA
  x submits the PKx to one of the N servers say Sp and Sp calls other servers to sign PKx with the partial keys
  Partial keys are gathered for full signature.
  If any of N servers not trust the x, send a denial message.
Contd...

- CA Certificate Revocation
  CA keeps a list of revocation CRL that it signs
  A node y send a request to CA for verifying its validity.
  CA checks CRL and if finds y, it sends a denial message otherwise it again authenticate it and issues new certificate.
Trust Chain

Trust Chain Definition

A principal A trusts another Principal B if and only if

1) A can authenticate B
2) A believes in the authenticity of any valid certificate signed by B

- Direct Trust  $P_{n-1} \rightarrow P_n$
- Indirect Trust  $P_0 ==> P_n$
Security policy:

- Even if any of the server becomes malicious, the architecture guarantees that a single or even up to K-1 malicious servers cannot subvert the authentication.
- The architecture provides support for authenticate foreign certificates in a lower cost and timely fashion.
In OPPNETs

- Our idea is that the Locality driven key management architecture can be used in Oppnets. The nodes (devices, agents...) get connected on-the-fly and the authentication can be done using the above mentioned architecture. Security can be achieved this way.
- If there is any malicious node, the architecture guarantees that a single or even up to K-1 malicious servers cannot subvert the authentication and the network.
Contd..

Architecture in oppnets
References


