Security Issues in Ad hoc Networks

Navid Nikaein and Pietro Michiardi
Institut Eurecom
http://manet.eurecom.fr
http://www.eurecom.fr/~nsteam

Security Issues

- Security Attacks
- Security Services
- Security Mechanisms

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Security Attacks

- Passive attack → Selfish Node
  - No intention to damage the network
  - Stealing information or eavesdropping communication
  - Lack of cooperation with the purpose of saving resources
  - E.g. passive DoS, black hole, idle status, traffic monitoring
- Active attack → Compromised or Malicious Node
  - Intention to damage network
  - Misbehavioring with resource utilization to perform a thread
  - External attack:
    - Committed by parties that are not part of the network (not authenticated)
    - E.g. jam the communication of an ad hoc network
  - Internal attacks:
    - Intention to damage the network → not easy to prevent
    - Sourced from inside a particular network threading the functional efficiency of the entire network
  - E.g. DoS, traffic subversion, attacks on routing mechanism

Security Services

- Availability
- Secrecy
- Access Control
- Authentication
- Confidentiality
- Integrity
- Non-repudiation

Availability and Secrecy Services

- Availability
  - Authorized access by authorized users must always be
- Secrecy
  - Information must not be disclosed or made accessible to a non-authorized user, process, or system

Access Control Service

- Prevent non-authorized use of resources
  - Information
  - Entities
  - Links
  - Domains
  - Service

Authentication Service

- Verify that the remote party is who he claims to be
  - Peer entity authentication or identification
  - Data origin authentication to the recipient
- Without authentication
  - A malicious node can masquerade a node and gain unauthorized transmission or reception
- Note: Requires the integrity of identification information

Data Confidentiality Service

- Prevent from non-authorized disclosure of
  - Information
  - traffic

Data Integrity Service

- Prevent form accidental or malicious modification of data
  - Information must not be altered or destroyed by a non-authorized user of in a non-authorized way
  - Modification can be also caused by radio propagation impairments
  - E.g. the integrity of routing information is a key factor of the proper functionality of the network
- Integrity does not assure confidentiality

Non-repudiation Service

- Confirm the fact that a subject has performed an operation despite the possibility of denial by the subject
  - Non-repudiation with proof of origin
    - Provide the proof of data origin to the recipient
  - Non-repudiation with proof of delivery
    - Provide the proof of data delivery to the sender

- Notes: for some application privacy of location, data, existence, or identity is important

Services vs. Layers

Layer / Services	PHY	MAC	Network	Transport	App.
Authentication		x	x	x	x
Access control		x	x	x	x
Confidentiality	x	x	x	x	x
Secrecy	x		x		x
Integrity		x	x	x	x
Non-repudiation					x

To protect application data, the lowest layer for security is Transport

To protect communication infrastructure, the highest layer for security is Network

Security Mechanisms

- Security services implemented by one or several security mechanisms
  - Data confidentiality mechanisms
  - Data integrity mechanisms
  - Digital signature
  - …
- Security mechanisms rely on security primitives:
  - Encryption algorithms
  - Hash functions
  - Pseudo random number generators

Trust in MANET

- Infrastructured environment
  - A-priori trust
  - Entity authentication → correct operation
  - But requires:
    - authentication infrastructure
    - Tamper-proof hardware

- Ad Hoc environment
  - No a-priori trust
  - Authentication does not guarantee correct operation
  - *New security paradigm*

MANET Requirements

- Wireless & Mobile
  - Limited energy
  - Lack of physical security
- Ad hoc
  - No infrastructure
  - Lack of organization

- Cooperation enforcement
- Secure Routing
- Key Management

Outline

- Secure routing
- Key management
- Cooperation enforcement
  - only applies to selfish nodes

Routing Vulnerabilities

- Modification
  - Compromises routing information integrity
  - Traffic subversion, DOS
- Impersonation or Spoofing
  - Misrepresenting the identity
  - Routing table inconsistency, loops, and inefficiency
- Fabrication
  - Generating false routing messages
  - Routing failure
- Wormhole attack
  - Create a shortcut (tunnel) to route messages to another malicious through a private network
  - Routing malfunctioning
- Lack of cooperation
  - Do not participate in network operation

Secure Routing - Objectives

- Authentication (Integrity) of routing information
- Entity authentication
  - Source
  - Destination
  - Intermediate node
- Correct behavior (of algorithm, if any)
- Asymmetric vs. Symmetric Crypto
- Pro-active vs. Reactive routing protocols

Secure Routing Proposals for MANET

- ARIADNE [Hu, et al.]
  - Shared secret known by (src, dst)
  - Prerequisite: distribution of authenticated TESLA keys
- Secure Routing Protocol [Papadimitriou, Haas]
  - Security associations between source and destination only
- ARAN [Dahill, et al.]
  - PK certificates for IP @
- SEAD [Hu, et al.]
  - Proactive routing authenticated hash chains
- TESLA with instant key disclosure (TIK)
  - Cope with wormhole attack
- All solutions rely on some key set-up prior to secure routing operation

Key Management Requirements

- Secure routing
- Basic security services
  - Authentication
  - Confidentiality
  - Integrity
  - Non-repudiation
- Symmetric or Asymmetric Keys

Key Management Challenges

- Lack of (or limited)
  - Security infrastructure
    - Key servers (KDC, CA, RA)
  - Organization (a priori trust)
    - p2p
    - Authentication is not sufficient to build trust

Key Management Approaches

- Symmetric crypto: key pre-distribution
- Asymmetric crypto: (ID, PK) binding
  - PK Certificate = $(ID,PK)_{CA}$
    - Self-organized CA
    - Web of trust(PGP)
  - No certificate
    - Crypto-based IDs: ID = h(PK)
    - ID-based Crypto: PK = f(ID)
- Context awareness
  - Location-limited channels
  - Shared passwords
  - Distance bounding protocols

Cooperation Enforcement in MANET

- Routing and Packet Forwarding cost energy
- Selfish node saves energy for itself
- Without any incentive for cooperation network performance can be severely degraded.

[Michiardi, Molva EW'02]

Cooperation enforcement mechanisms

- Token-based [Yang,Meng,Lu] — Threshold cryptography
- Nuglets [Buttyan,Hubaux]
- SPRITE [Zhong, Chen, Yang] — Micro-payment
- CONFIDANT [Buchegger,Le Boudec]
- CORE [Michiardi,Molva]
- Beta-Reputation [Josang,Ismail] — Reputation-based

Validation of Cooperation Enforcement Mechanisms

- Mechanisms based on reputation difficult to validate
  - Simulation
  - Game theory

- How to tackle with monitoring errors?