Security in Ad Hoc Networks Attacks

Nie Pin

niepin(at)cc.hut.fi

T-79.5401
Special Course in Mobility Management: Ad hoc networks

Agenda

- Objectives of attacks
- Target selection
- Classifications of attacks
- Passive & Active
- Analysis of layers
- Detection and countermeasure
- Ideas and suggestions

Objectives of attacks

- Computer Network Attack
  - Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or themselves.
- Groups and features
  - Camouflage and pretending (invalid/illegal access)
    - impersonation, masquerading, spoofing
  - Stealing
    - Target at the content (information & data)
    - Eavesdropping, snooping, interception
  - Destroying
    - Target at the content (virus, fabricating/forging, replay stale msg)
    - Target at the resources (DoS, Worm, Overflow)

Target selection

- Traffic load analysis
  - Frequent appeared nodes (address)
  - Frequent appeared packets (protocol, type)
- Responses evaluation
  - Services available on the node (capability)
  - Status of the node (membership)
  - Topology of the network
- Distribution of functions
  - Importance of the functions (pro-studied)
  - Weakness of the functions (pre-studied)

Classifications of attacks

- Passive and Active
  - By operations
- MAC layer, Network Layer, Transport Layer, Application Layer
  - By carriers and underlying services
- Intentions
  - Disable functions (DoS, Overflow, Sleep deprivation)
  - Limited disturb (blackhole, byzantine, impersonating)
  - Invalid access (eavesdropping, hijack)

Passive & Active

- Passive
  - No altering to the data and network
  - Hard to detect
  - Information disclosure and followed by active attacks
- Active
  - Violation of the consistency or availability
  - Perceptable but hard to track
  - Malfunction of the services or the network
- Man-in-the-middle attack
  - Malicious intermediate node, on the relay path
  - Passive + Active

Analysis of layers

- MAC layer
  - Jamming, backoff attack (RTS/CTS handshake), interferences
- Network layer
  - Routing and resources (bandwidth, memory, battery)
- Transport layer
  - Session and data (content) interception
- Application layer
  - Repudiation, privacy, invalid access services

Detection and countermeasure

- Key management
  - Minimal requirement for secure communication
  - Threshold cryptography
- Watchdog (fault tolerance)
  - Persistent monitoring
- Periodic security refresh
  - Session timeout, node configuration, key pair (share) exchange
- Redundancy and non-repudiation
  - Multi-path routing (diversity coding)
  - Non-repudiation provides the evidence of intentions (signature)
- Intrusion Detection System
  - Tracing and sharing (P2P), collective determination, EWS
- Standardization
  - Standards-compliant, knowledge threshold

Secure Routing

- Routing table
  - Overflow, poisoning
  - Signature, roof limits
- Routing packets
  - Replication, flooding
  - Signature, sequence number, IDS
- Trust model
  - Friends, encounter, polling, knowledge-based
- Backup channels
  - Advantages of the redundancy
  - How to store and update backup routes

Ideas and suggestions

- Overheads of prevention should be low
  - Service-oriented, fast deployment and function is required
  - Lifetime of ad hoc applications used to be short
- Detection and responses of attacks should be quick and persistent
  - Attack-aware VS Security-aware (self-adjust)
  - Benefits of randomness (frequent changes)
- Knowledge based
  - Local database of the last encounter
  - Whitelist and blacklist (internal state tracking)
- Multi-configurations for different situations
  - “tolerable attacks”
  - Security-binding services (hidden security parameters)
- The resurrecting duckling model
  - Secure transient association of a device with multiple serialized owners

Resources

- *Ad Hoc Wireless Networks: Architectures and Protocols*, C. Siva Ram Murthy and B. S. Manoj
- *Standardization Areas for Securing Ad hoc Networks*, Rajesh Talpade and Anthony McAuley
- *Secure Ad Hoc Networking*, Panagiotis Papadimitratos
- *Securing Ad Hoc Networks*, Lidong Zhou and Zygmunt J. Haas
- *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*, Frank Stajano and Ross Anderson
- *Security within Ad hoc Networks*, Preetida Vinayakray-Jani
- *Mobility Helps Security in Ad Hoc Networks*, Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan

Questions