Security in Wireless Ad Hoc Networks

Ahn Young- Ah
August 20, 2003

Theory and Formal Methods Lab.
Korea University
Traditional wireless networks

- Infrastructure
  - base stations
  - high speed backbone
  - on-line servers

- Network operators
  - operate and maintain the system
  - determine policies

- Single-hop wireless communication
Wireless ad hoc networks

- no infrastructure
  - no base stations
  - no backbone
  - no servers (\(\rightarrow\) P2P)
- no network operators
  - self-organization
  - self-configuration
  - self-healing
- multi-hop wireless communication
Applications of ad hoc networking technology

- battlefield
- rescue operations
- sensor networks
- spontaneous networks of personal devices
  - e.g., conferences, meetings
- car networks
- pervasive computing
  - connecting embedded computers
  - e.g., connecting personal gadgets or household devices
Hybrid networks (multi-hop cellular)

- **Advantages**
  - Fewer base stations / larger coverage
  - Reduced total energy consumption of mobile stations
  - Reduced interference

- **Disadvantages**
  - Synchronization?
  - Routing?
  - QoS?
Security challenges

- well-known security problems (authentication, session key establishment, ...) must be solved under new assumptions
  - set of assumptions depends on the envisaged application of the network, but usually...
  - no central authority can be assumed
  - no access to on-line servers can be assumed
  - network may be very dynamic (mobility, link failures, broken routes, ...)
  - network lifetime may be short (transient associations)
  - capacity of nodes may be limited (energy constraints, peanut CPU, small memory, limited communication in space and in time)
  - nodes can be captured and compromised (no tamper resistance)
Security challenges

- new security problems specific to ad hoc networks
  - selfishness, non-cooperative behavior
  - new forms of DoS attacks (e.g., battery exhaustion)
Securing wireless Ad hoc networks

- Vulnerability of channels
- Vulnerability of nodes
- Absence of infrastructure
- Dynamically changing topology
Four session

- Trust and key management
- Secure routing and intrusion detection
- Availability
- Cryptographic protocols
Trust and key management

- Distributed Trust in Ah Hoc Networks
- Network Performance Centric Security Design in MANET
- Self-Organized Public Key Management for Mobile Ad Hoc Networks
- Admission Control in Collaborative Groups
“Distributed Trust in Ah Hoc Networks”
Lidong Zhou, Microsoft 2002

- Distributed trust
- Distributed secure services
- Threshold cryptography
- Share refreshing
- Secure routing
“Network Performance Centric Security Design in MANET”, Hao Yang, UCLA, 2002

- Network performance centric

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Centralized</th>
<th>Peer-to-Peer</th>
<th>Localized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>Bad</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Availability</td>
<td>Bad</td>
<td>Uncertain</td>
<td>Good</td>
</tr>
<tr>
<td>Robustness</td>
<td>Bad</td>
<td>Uncertain</td>
<td>Good</td>
</tr>
<tr>
<td>Communication</td>
<td>Centralized</td>
<td>Distributed</td>
<td>Localized</td>
</tr>
<tr>
<td>Computation</td>
<td>Undertaken solely by the servers</td>
<td>Shared by the nodes</td>
<td>Shared by the nodes</td>
</tr>
</tbody>
</table>
“Self-Organized Public Key Management for Mobile Ad Hoc Networks”, Srdjan Capkun, EPFL, 2002

- Fully self-organized
- Local certificate repository
- Certificate graph
- Maximum degree algorithm
- Shortcut certificates
- Shortcut Hunter Algorithms
“Admission Control in Collaborative Groups”, Yongdae Kim, University of Minnesota, 2002

- Peer group
- Group charter
- Group authority
- Group lifetime
- Group admission control
- Voting process
Secure routing and intrusion detection (1/2)

- Secure Routing for Mobile Ad Hoc Networks
- Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks
- Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks
Secure routing and intrusion detection (2/2)

- Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks
- Authenticated Routing for Ad Hoc Networks
- Dynamic and Secure Group Membership in Ad Hoc and Peer-to-Peer Networks
- Intrusion Detection
Secure Routing for Mobile Ad Hoc Networks, Panagiotis Papadimitratos, Cornell University, 2002

- SRP: Secure Routing Protocol
- IP header + basic routing protocol packet + SRP header
- SRP header = type + Reserved + Query Identifier + Query Sequence Number + SRP MAC
- Geometry
- Tunnel
“Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, Yih-Chun Hu, Rice University, 2002

- Wormhole attack
- Packet leashes
- Temporal leashes
- Geographical leashes
“Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks”, Yih-Chun Hu, Rice University, 2002

- Sequence number
- One-way hash function
- Distance Vector Routing
- Hash chains
- Authenticating Routing Update

- Symmetric cryptography
- Basic Ariadne Route Discovery
- Target authenticate ROUTE REQUESTs
- Per-hop hashing
- Basic Ariadne Route Maintenance
- Avoiding Routing Misbehavior
“Authenticated Routing for Ad Hoc Networks”, Kimaya Sanzgiri, UCSB, 2002

- Managed-open environment
- RDP: Route Discovery Packet
- $S \rightarrow \text{broadcast}: [\text{RDP}, IP_D, cert_S, N_S, t]K_S$
"Dynamic and Secure Group Membership in Ad Hoc and Peer-to-Peer Networks", Claude Castelluccia, INRIA Rhone-Alpes, 2002

- Secure Node identity
- CBID : Crypto-Based Identifier
Current research directions

- decentralized public-key management schemes
  - using threshold cryptography
  - PGP-like approach*
  - exploiting mobility and secure side channels*

- secure ad hoc routing
  - various schemes for authenticating routing information that is distributed or exchanged among the nodes
Current research directions

- incentives for cooperation
  - micro-payment based schemes*
  - reputation based schemes
- low cost cryptographic primitives (algorithms and protocols)*
- anonymity, intrusion detection, ...