Securing Ad-Hoc Networks
Lidong Zhou and Zygmunt J. Haas

Denial of Service in Sensor Networks
Anthony D. Wood and John A. Stankovic

Presented by
Nipoon Malhotra

Why security in sensor networks

- Military applications
  - Hostile environments
  - Adversary may gain physical access to nodes
- Disaster management/relief and rescue
  - Protect casualties in terrorist attack
- Public safety
  - False alarms
  - Disabling sensors before attack
- Home and Heathcare
  - Privacy

Goals of Security Policy

- Availability
- Confidentiality
- Integrity
- Authentication
- Nonrepudiation

Challenges

- Wireless links
  - Jamming
  - Eavesdropping
- Hostile environments
  - Nodes can be compromised
- Dynamic networks
  - Topology
  - Size
  - Trust relationships
- Scalability
DOS Attacks

“A Denial of Service attack is any event that diminishes or eliminates a network’s capability to perform its expected function.”

Attacks can be by an intelligent, determined and resourceful adversary
– Fault tolerance based on independent and sparse error model may not be adequate

<table>
<thead>
<tr>
<th>Network layer</th>
<th>Attacks</th>
<th>Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Jamming</td>
<td>Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change</td>
</tr>
<tr>
<td>Link</td>
<td>Collision</td>
<td>Error-correcting codes</td>
</tr>
<tr>
<td></td>
<td>Link-layer</td>
<td>Rate limitation</td>
</tr>
<tr>
<td></td>
<td>Link-layer</td>
<td>Link misuse</td>
</tr>
<tr>
<td>Network and routing</td>
<td>Network-layer</td>
<td>Redundancy, probing</td>
</tr>
<tr>
<td></td>
<td>Routing</td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Routing</td>
<td>Misdirection</td>
</tr>
<tr>
<td>Transport</td>
<td>Flooding</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Denial of service</td>
<td>Authentication</td>
</tr>
</tbody>
</table>
Physical layer

• Tampering
  – Tamper-proofing
  – Camouflaging
  – Self destruct if removed from intended environment

Link Layer

• Collision
  – Attacker requires less energy than jamming
  – Can block access to medium

• Defense
  – ECC
  – Collision detection

Link Layer

• Exhaustion
  – Repeated collisions and retransmissions
  – Interrogation attack
    • Repeatedly seek resources forcing nodes to talk

• Defense
  – Rate limiting admission control
  – Limit responses that require radio transmissions

• Unfairness
  – Use smaller frames
  – Cheating ??

Network and Routing Layer

• Neglect and Greed
  – Drop packets
  – Give undue priority to one’s own packets

• Defense
  – Multiple routing paths
  – Redundant messages

• Homing
  – Encryption

• Misdirection
  – Divert traffic towards a victim

• Black Holes
Defense

- Authorization
  - Only authorized nodes exchange routing information
  - Scalability: every node is a potential router
  - Centralized certification authority is a single point of failure
  - What if it is subverted
- Monitoring
- Probing
- Redundancy

Transport layer

- Flooding
  - Client puzzles
  - Connectionless protocols
- Desynchronization
  - Forge sequence numbers and control flags

Protocols analyzed

- Adaptive rate Control
  - Gives preference to route-through traffic over originating traffic
- RAP
  - Velocity monotonic scheduling
  - Global clock

Securing Ad Hoc Networks

Zhou and Haas
Secure Routing

- DOS attacks
- Detection of compromised nodes is difficult
  - Topology changes
- Redundancy
  - Outdated information
- Diversity coding

Cryptography to the rescue

- Only authorized nodes allowed to exchange routing information
- Certification authority binds public keys to nodes
- These must be refreshed periodically
  - Node may loose certification
  - Key may be cracked
- In an asynchronous network trust can be distributed

What is Certification

- CA issues certificates signed by its Private key
  - certificate=(identity, E_p( identity ))
  - Routers verify certificate using CA’s Public Key
    - identity=D_p(E_p( identity ))

- Identity = Router ID + Router’s Public Key
- n servers
  - Store Public keys of all nodes including other servers

Threshold cryptography

- (n,t+1) threshold cryptography scheme.
- Divide private key into n shares such that at least t+1 shares are required to reconstruct it.
- Mobile adversary
  - Share refreshing
  - If K_1: (s_1^1,s_2^1,...,s_n^1) and K_2: (s_1^2,s_2^2,...,s_n^2)
    then K_1 + K_2: (s_1^1+s_1^2,s_2^1+s_2^2,...,s_n^1+s_n^2)
- So s_j=s_j + s_i s_j
LaGrange Polynomial

- \((n,m)\) scheme
- \(m-1\) dimensional polynomial with \(a_0 = \text{Message}\)
  - \(F(x) = a_{m-2}x^{m-1} + \ldots + a_0 : a_i < p\)
- Shadows
  - \(F(x) \mod p\)
- If \(s\) is largest possible message
  - Choose \(p > n\) and \((s-1)(m-1)/e + m\)
  - \(e\) is probability of successful cheating

Summary

- Studied the kinds of attacks on Sensor networks
  - Necessary to factor security in original design
- Studied an implementation of threshold cryptography for authentication
  - Effective technique
  - Overhead may not be tolerable in sensor networks
  - Works only for asynchronous networks

Threshold algorithms

- Message defined as a point in \(m\) dimensional space and shadows are equations on \(m-1\) dimensional hyperplane passing through the point.
- Karnin-Greene-Hellman
  - \(V_0 \ldots V_n\) : \(m\)-D vectors, rank\((V_i^T V_j) = m\)
  - \(U\) : \(m\)-D row vector
  - Message = \(U V_0\)
  - Shadows \(U V_i, 0 < i < n+1\)
Spread Spectrum Communication

- Communicator Power = S
- Jammer Power = J
- Data rate = Rb, Bandwidth used = W
- q = W/Rb
- Jammer spreads signal over fraction \( \frac{q}{W} \) of whole bandwidth
- \( P_e = \max_{0 \leq \phi \leq \frac{W}{Rb}} \left( \phi / 2 \exp(-S \phi / 2J) \right) \)

Public Key Cryptography

- C = \( E_k(P) \) encrypt message using private key.
- P = \( D_k(C) \) decrypt using public key.
- E.g RSA
  - Public key
    - n = pq where both p and q are primes.
    - e is relatively prime to \( (p-1)(q-1) \).
  - Private key
    - \( d = e^{-1} \mod ((p-1)(q-1)) \)
    - Encryption: \( c = m^e \mod n \)
    - Decryption: \( m = c^d \mod n \)