Why Do Stars Twinkle but Planets Do Not?

On the Difference of Security in Traditional vs. Multihop Wireless Networks

Prof. Dr.-Ing. Matthias Hollick
Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED
Mornwegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

P. Dr.-Ing. Matthias Hollick
jointly with André König (KOM, TU Darmstadt)
matthias.hollick@seemoo.tu-darmstadt.de

Why Do Stars Twinkle ...
... but Planets Do Not?

Outline

Traditional Networks

Multihop Wireless Networks
Traditional Security: Central Control, Well-defined Procedures/Solutions

What “Bad Guys” Do ...

Active attacks
- Changing messages of others (manipulation but also replaying)
  - E.g. manipulating the content of business e-mails
  - E.g. replaying previous messages
- Pretending to be someone else (impersonation)
  - E.g. buying something for someone’s account without permission
- Denying a communication (repudiation)
  - E.g. lying about received prompt notes/signed contracts
- Disrupting someone else’s services (denial of service)
  - E.g. bringing down websites
  - E.g. disconnecting others from networks
... Attacking Servers and Network Infrastructure

Denial of Service (DoS):
- Diminishes usability of network host, network, or network infrastructure

Vulnerability attack:
- Attacker sends well-crafted messages to a vulnerable app or OS, crashing service or host

Bandwidth flooding (resource-consumption attack):
- Attacker sends a deluge of packets to the targeted host
- Target’s access link becomes clogged

Connection flooding (resource-consumption attack):
- The attacker establishes large number of half- or fully-open TCP connections at the target host
- Target becomes incapable of accepting legitimate connections

Security in Traditional Networks

Security goals
- Authenticity, confidentiality, integrity, non-repudiation, availability

In “traditional” networks
- Well-defined boundaries, administrative domains, centrally managed, reasonably well understood threats against network infrastructure
- Multilevel security solutions in place
  - Intrusion prevention, detection, response
  - Plethora of security protocols

<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 5 - APP</td>
<td>SHTTP, S/MIME, PGP, X.400, X.500, DNS Security, Key Mgmt., etc.</td>
</tr>
<tr>
<td>Layer 4 - TRANS</td>
<td>SSL, TLS, SSH, TLSP</td>
</tr>
<tr>
<td>Layer 3 - NET</td>
<td>IPSec (AH, ESP), NLSP</td>
</tr>
<tr>
<td>Layer 2 - LINK</td>
<td>PPTP, L2TP, WEP, WPA, WPAv2</td>
</tr>
<tr>
<td>Layer 1 - PHY</td>
<td>Synchronous Link</td>
</tr>
</tbody>
</table>
Outline

Traditional Networks

Multihop Wireless Networks

Exploring Multihop Wireless Network
Heterogeneity of scenarios, network characteristics, threats, and security goals

Industrial Wireless Sensor Networks
- Harsh environmental conditions, yet some physical protection vs. intruders
- Data integrity to be protected, availability to be protected
- QoS provisioning and robust operation are crucial

Mobile or Vehicular Ad hoc Networks/Wireless Mesh Networks
- VANET: integrity of warning msgs., exclusion of errant devices, location privacy
- MANET: availability of service, infrastructureless → cooperation of nodes req'd.,
- Provider WMN: closed network (nodes authenticated), QoS and availability
- Community WMN: open network, distributed mechanisms, cooperation req'd.

All of the above networks are wireless and distributed …
Threats in Multihop Wireless Networks

Security goals
- Authenticity, confidentiality, integrity, non-repudiation, availability

Attacks take place on all layers (examples)
- Jamming on PHY layer, physical security of small devices typically weak
- Selfishness on MAC layer
- Malicious behavior during routing and/or forwarding on NET layer
- TRANSPORT layer of the Internet has not been designed for multihop wireless networks, is weak even without attack
- Attacks are scenario/application dependent
  - Wireless simplifies attacks such as eavesdropping
  - Multihop simplifies attacks such as physical access, man-in-the-middle


Why Do Stars Twinkle but Planets Do Not? | ITG FA-5.2 | Stuttgart, Germany
Scenario

Effects of Node Misbehavior in Multihop Wireless Networks

Simulation Study: Selected Results

<table>
<thead>
<tr>
<th>Factor</th>
<th>Misbehavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraction of misbehaving nodes</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4% 8% 12% 16%</td>
</tr>
<tr>
<td>8.8% 1.6% 2.4% 3.2% 4.0%</td>
<td></td>
</tr>
<tr>
<td>Average end-to-end delay in ms</td>
<td></td>
</tr>
<tr>
<td>76.60 71.68 69.48 65.34 61.79</td>
<td></td>
</tr>
<tr>
<td>58.56 45.43 33.99 31.75 34.25</td>
<td></td>
</tr>
<tr>
<td>Average loss</td>
<td></td>
</tr>
<tr>
<td>4.8% 15.1% 24.8% 33.6% 42.1%</td>
<td></td>
</tr>
<tr>
<td>49.0% 61.5% 68.0% 74.1% 77.6%</td>
<td></td>
</tr>
<tr>
<td>Avg. path length</td>
<td></td>
</tr>
<tr>
<td>7.19 7.53 7.65 7.72 7.87</td>
<td></td>
</tr>
<tr>
<td>5.38 4.72 4.29 3.94 3.71</td>
<td></td>
</tr>
<tr>
<td>Control Msg. per Data Msg.</td>
<td></td>
</tr>
<tr>
<td>5.61 7.78 10.40 13.59 17.21</td>
<td></td>
</tr>
<tr>
<td>3.33 2.77 2.47 2.29 2.13</td>
<td></td>
</tr>
<tr>
<td>RREQ/Ctrl.Msg.</td>
<td></td>
</tr>
<tr>
<td>95.1% 94.8% 94.6% 94.5% 94.4%</td>
<td></td>
</tr>
<tr>
<td>90.2% 87.2% 84.9% 82.6% 80.0%</td>
<td></td>
</tr>
<tr>
<td>RREP/Ctrl.Msg.</td>
<td></td>
</tr>
<tr>
<td>3.3% 3.4% 3.4% 3.4% 3.4%</td>
<td></td>
</tr>
<tr>
<td>7.5% 10.2% 12.3% 14.3% 16.3%</td>
<td></td>
</tr>
<tr>
<td>RERR/Ctrl.Msg.</td>
<td></td>
</tr>
<tr>
<td>1.6% 1.8% 2.0% 2.1% 2.2%</td>
<td></td>
</tr>
<tr>
<td>2.3% 2.6% 2.8% 3.2% 3.6%</td>
<td></td>
</tr>
</tbody>
</table>

Setup

- 250 nodes, low node mobility (1-2m/s)
- AODV with expanding ring search
Observations for Ad hoc Networks and Black Holes

Results
- Successful communication is possible only in close proximity
- Packet loss is extremely high, even for few black holes
- Packet loss further increases with node mobility

Multihop Wireless Networks: Beyond Traditional Security
Exploiting Geo-Location

GeoSec – exclude misbehaving nodes based on location
  - Setting up ‘quarantine zones’ void of communication
  - Results in cross-layer and attack-independent defense
Performance Evaluation
GeoSec vs. Address-based IRS

Metric
- Packet drop rates
- Attacker vs. IRS

Setup
- Low node mobility, AODV with expanding ring search, 1000 nodes

Exploiting Delay Tolerance

“Bad guy”

... or even much later
... then a bit later
If not now ...
Exploiting Delay Tolerance

Approach: buffer packets during attack and retransmit later
- Transparent operation, i.e. sender is informed about IRS event
- Non-transparent operation, i.e. “silent” or “localized” operation of IRS

- Early (continuous) buffering vs. late (as soon as IDS is triggered) buffering

Summary of Results

Avg. Delivery Ratio

<table>
<thead>
<tr>
<th></th>
<th>Transparent, Late Buffering</th>
<th>Non-transparent, Late Buffering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. Delivery Ratio</td>
<td>In studied scenario up to ~80%</td>
<td>Performance independent of number of retransmissions</td>
</tr>
<tr>
<td></td>
<td>In studied scenario up to ~75%</td>
<td>Performance dependent of number of retransmissions</td>
</tr>
<tr>
<td></td>
<td>In studied scenario up to ~95%</td>
<td>Performance independent of number and scheduling of retransmissions (but congestion observed)</td>
</tr>
<tr>
<td></td>
<td>In studied scenario up to ~90%</td>
<td>Performance independent of number of retransmissions (but congestion observed)</td>
</tr>
</tbody>
</table>

In studied scenario up to ~80% delivery ratio
Performance independent of number of retransmissions

In studied scenario up to ~75% delivery ratio
Performance dependent of number of retransmissions

In studied scenario up to ~95% delivery ratio
Performance independent of number and scheduling of retransmissions

In studied scenario up to ~90% delivery ratio
Performance independent of number of retransmissions (but congestion observed)
Summary & Conclusion

“Traditional” Networks
- Well-defined boundaries, administrative domains, centrally managed, reasonably well understood
- Multilevel security solutions in place
  - Intrusion prevention, detection, response
  - Such as PGP, TLS, IPsec, firewalls, filters network & host-based IDS, etc.

Multihop Wireless Networks
- No strict boundaries due to wireless nature
- Localized behavior results in emergent properties
- Operation without infrastructure requires cooperation
- Security solutions need to ACK the above properties
- Security solutions can exploit the above properties
Why Do Stars Twinkle ...

... but Planets Do Not?