Resiliency of Wireless Sensor Networks: Definitions and Analyses

Orange Labs & CITI Labs INSA-Lyon

O.Erdene-Ochir, M. Minier, F. Valois, A. Kountouris
February 10, 2010, presentation to CITI seminar
Thesis context

- Research area: Sensor Networking (routing in particular)
- Focus: Security beyond cryptography (protocol resiliency)
  - Our goal: Analyze and create inherently resilient protocols against internal (insider) attacks
- CRE between
  - Orange Labs (TECH/MATIS/CITY) and
  - CITI Laboratory of INSA-Lyon (ANR VERSO ARESA2)
- Advisors (academic): M. Minier, F. Valois
- Advisor (Orange Labs): A. Kountouris
- Start date: 1/10/2009
Contents

- Context
- Motivation
- Related works
- Simulation and analysis
- Conclusion and future directions

*Worldsens*, a small sensor node developed in the CITI lab
http://worldsens.citi.insa-lyon.fr/
Context: Wireless Sensor Networks

- **Characteristics**
  - Radio communication
  - No infrastructure
  - Decentralized architecture
  - Open network architecture
  - Multi-hop routing

- **Why sensor networks?**
  - Rapid deployment
  - Cheap
  - Self organized
  - Fault-tolerant

- **Applications of WSNs:**
  - Scientific data collection
  - Military applications
  - Environmental monitoring (temperature, pollution, pressure...)
  - Home, building, industrial automation (electricity, water metering...)

- **Challenges**
  - Scalability
  - Adaptability
  - Low energy, long lifetime
  - Security
Motivations (1/2)

- **Why not use traditional cryptography-based security?**
  - limited resources (memory, energy, computation power ...)
  - an open and hostile environment (physical attacks)
  - not always a solution against multiple internal attacks stemming from node compromise

Our goal: Analyze and create inherently resilient protocols against internal (insider) attacks

Our definition: **Resiliency** is the ability of a network to continue to operate in presence of $k$ compromised nodes, i.e. the capacity of a network to endure and overcome internal (insider) attacks.
Definition of **Survivability** [ELLM1999]:

Survivability in information systems is defined as the ability of the network computing system to provide essential services in the presence of attacks and/or failures, and recover full service in a timely manner.

Definition of **Robustness** [SKHJ2002]:

Robustness is defined as the requirement to accommodate hardware and software failures, asymmetric and unidirectional links, or limited range of wireless communication.
Related works: Attacks and Defenses (1/3)

[KW2003], [WS2002]

- **Hardware** attacks (node compromise) [BBD2006]

- **Physical** layer attacks
  - Jamming [WSS2003]

- **Link** layer attacks
  - Collision
  - Exhaustion
  - Link layer jamming [LPHDHH2009]

- **Routing** layer attacks
  - Sybil [NSSP2004]
  - Node replication [PPG2005]
  - Selective forwarding
  - Blackhole
  - Sinkhole
  - Wormhole [HE2004], [HPJ2003]
Related works: Attacks and Defenses (2/3)

- **Routing layer attacks**
  - Sybil [NSSP2004]
  - Node replication [PPG2005]
  - Selective forwarding

![Diagram showing Sybil attack, Node replication, and Selective forwarding]
Related works: Attacks and Defenses (3/3)

• **Routing layer attacks**
  – Blackhole
  – Sinkhole
  – Wormhole [HE2004], [HPJ2003]
Related works: Routing layer security (1/5)

• **Goal:** find a route between source and destination

• Routing layer responsibility:
  – Naming and addressing
  – Neighborhood discovery
  – Multi-hop routing

• Specific secure protocols:
  – SRP [PH2002]
  – ARIADNE [HPJ2005]
  – ARAN [SDLSB2002]
  – SPINS (SNEP+μTESLA) [PSW2001] …

→ Use cryptography
Related works: WSN routing protocols (2/5)

- Multi-hop routing
  - different ways to find the route
  - message traverse many hops
  - intermediate nodes can be compromised

- Study of existing routing protocols
  - enumerate the various routing mechanisms
  - classification is required for efficient choice
  - analysis of some routing protocols under multiple attacks
  - determine good properties for resiliency
Related works: Classification (3/5)
Related works: Choice of routing protocols (4/5)

- Dynamic source routing [JM1996]
  - Flooding based
  - Route discovery

- Gradient based routing [MS2001]
  - Flooding based

- Greedy forwarding [KK2000]
  - Geographical
  - Location information required

- Random walk routing [SB2002]
  - Probabilistic routing
  - Random choice of neighbor
Related works: Implemented attacks (5/5)

- DATA packet oriented attacks
  - Selective forwarding
  - Sinkhole

- CONTROL packet oriented attacks
  - Blackhole

- HELLO packet oriented attacks
  - Sybil
Simulations and analysis  (1/8)

- Simulator: **WSNet** [HCG2008]  
  http://wsnet.gforge.inria.fr

- Assumptions:
  - Sensors can be compromised
  - A unique sink at the center of the network
  - Sensor nodes are static
  - Ideal MAC/PHY: no interferences, no collisions, (consider only impact of attacks)
  - 95% confidence interval

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>300</td>
</tr>
<tr>
<td>Area size</td>
<td>100X100m</td>
</tr>
<tr>
<td>Transmission range</td>
<td>20m</td>
</tr>
<tr>
<td>Topology tested</td>
<td>Uniformly and randomly distributed</td>
</tr>
<tr>
<td>Traffic generation</td>
<td>Poisson distribution with $\lambda = 1$ packet per sec, per node</td>
</tr>
<tr>
<td>Number of runs</td>
<td>100</td>
</tr>
<tr>
<td>Simulation time</td>
<td>100 sec</td>
</tr>
</tbody>
</table>
Simulations and analysis  (2/8)

- We tested three different evaluation metrics:
  - **Average delivery ratio:**
    - success of routing function (reliability)
    - percentage of successfully received packets
  - **Average degree of nodes:**
    - detect neighborhood abnormalities
    - average number of neighbors
  - **Average path length:**
    - number of retransmission (hops)
Simulations and analysis  (3/8)

Case 1:
- 10% compromised nodes of 300 are *uniformly* and randomly distributed across the *whole network*

Case 2:
- 10% compromised nodes of 300 are *uniformly* and randomly distributed *around the sink*
Scenario 1:
- Uniformly distributed across the whole network (case 1)
- Selective forwarding (drop all DATA packets)

Scenario 2:
- Uniformly distributed around the sink (case 2)
- Sinkhole attack (drop all DATA packets)

- Impact of attacks is more important than scenario 1
- Malicious nodes receive for retransmission more packets than other nodes

Average delivery ratio decreases when percentage of compromised node increases
RWR is worst in successful packet delivery
Simulations and analysis (5/8)

Scenario 1:
- Uniformly distributed across the whole network (case 1)
- Selective forwarding (drop all DATA packets)

- When path length is high, the number of intermediate nodes is high.
- The probability to meet malicious node increases.
- Delivery ratio is inversely proportional to the path length

Scenario 2:
- Uniformly distributed around the sink (case 2)
- Sinkhole attack (drop all DATA packets)

- Malicious nodes attract most of the traffic creating a "donut effect" around the sink
Scenario 1:

- Uniformly distributed across the **whole network** (case 1)
- **Selective forwarding** (drop all DATA packets)
- **Double sent** of each DATA packet

- RWR has better average delivery ratio with double sent
- No changes for DSR, GBR and GF
- Route should be diversified
Scenario 3:

- Uniformly distributed across the whole network (case 1)
- **Sybil attack** (false HELLO packets, multiple identities)

- Average degree increases, when the number of compromised nodes increases
- 10% of compromised node create 75 false identities
Scenario 4:

- Uniformly distributed across the **whole network** (case 1)
- **Blackhole attack** (false CONTROL packets, attract the DATA traffic)

- Impact of attacks is much more important than in previous attacks
- GBR: over 2/3 of the traffic are lost with only 10% of compromised nodes
- DSR: a single compromised node can impact 197 legitimate nodes over 299

O.Erdene-Ochir – Resiliency of WSNs: Definitions and Analysis – February 10, 2010
Conclusion and future directions

- Preliminary study for WSNs security of the routing layer.

- The more the protocol is statefull, the more it will be vulnerable to attacks targeting this information.

- Requirements for Resiliency:
  - Graph representing WSNs should be connected (reliability)
  - Degree of the nodes must be high (increases the number of candidates for next hop)
  - Route must be diversified in order to exploit the structural redundancy (randomness on their behavior)
  - Redundant sent of packets

- In the future,
  - Extending our simulations; taking into account energy consumption (tradeoff energy consuming-resiliency)
  - Quantify a measure of resiliency: which metric?
  - Improve the resiliency of existing protocols or propose a new protocol.
  - Using some entropy concept as a means to detect local attacks.
thank you
References


References


References


