ATHENS INFORMATION TECHNOLOGY

CENTER OF EXCELLENCE FOR RESEARCH AND GRADUATE EDUCATION

# Autonomic Communication Security in Sensor Networks

4 October 2005

Tassos Dimitriou, Ioannis Krontiris

International Workshop on Autonomic Communication (WAC 2005)



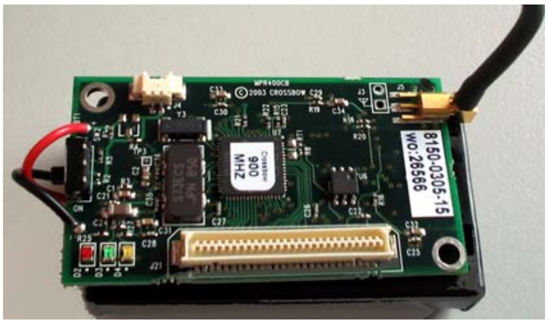


## Goal

- **Emphasize on the communication security aspects of sensor networks**
- **Present challenges and opportunities**
- **Highlight importance of an autonomic communication approach**

## Generic Sensor Node Example

Berkeley/Crossbow MICA2 Mote
• www.xbow.com



| | |
|---|---|
| Atmel ATMEGA128L | 8MHz |
| Program Flash Memory | 128K bytes |
| Measurement (Serial) Flash | 512K bytes |
| Configuration EEPROM | 4 K bytes |
| Serial Communications | UART |
| Analog to Digital Converter | 10 bit ADC |





## Deployment

- Sensors are deployed randomly (ad hoc network) to reach a desired local density
- After deployment, sensors periodically communicate to each other to establish and maintain a connected network.

## Main Objectives

- Advanced techniques for power efficiency of wireless devices and wireless networks
- Provide distributed services that enable distributed sensor software components to
  - self-organize, without central administration,
  - adapt to changing requirements,
  - react to network changes,
  - survive sensor failures
- **Provide mechanisms for remote execution of distributed application services (network programmability)**
- Implement distributed services on top of a dynamic network routing protocol (e.g. directed diffusion)





## Limitations in Sensor Networks

- **Deployed in Hostile Environment**
  - Vulnerability to physical capture
- **Random Topology**
  - No prior knowledge of post-deployment topology
- **Limited Resources**
  - Energy Restrictions
  - Limited Communication and Computational Power (10 KB RAM, 250 kbps data rate)
  - Storage Restrictions

## Key Establishment and Initial Trust Setup

- Confidentiality → guarantee the secrecy of messages. Only authorized users have access to data
- Integrity & Authentication → Detect modified, injected or replayed packets.

⬇ **Symmetric Cryptography**

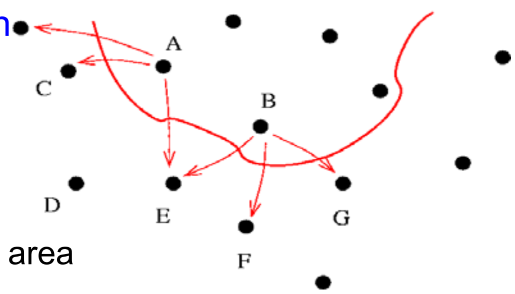
- Members leave and join the group according to some membership rules
- **Adding new nodes in the group**
- **Isolating malicious nodes**
- Self-revocation of a key when the network detects an intrusion or the lifetime of the key has expired.





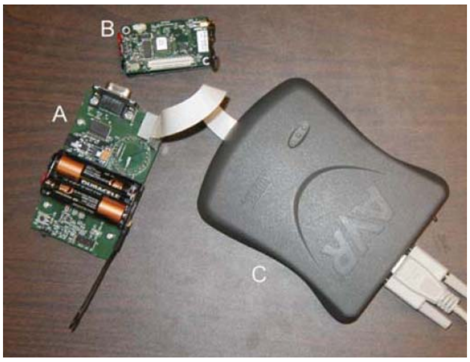
## Resilience to Denial of Service Attacks

- **DoS attack**
  - Broadcasting a high-energy signal
    - If the transmission is powerful enough, the entire system's communication could be jammed
  - Violating the 802.11 MAC protocol
    - By transmitting while a neighbor is also transmitting or by continuously requesting channel access with a RTS signal
- **Defense against jamming**
  - Spread-spectrum communication
    - Not commercially available
  - Jamming-resistant network
    - Detecting the jamming, mapping the affected region, then routing around the jammed area
  - Frequency hopping



## Resilience to Node Capture

- **Node capture attack**
  - Capture sensor nodes, extract cryptographic secrets, modify their programming
  - Replace them with malicious nodes under the control of the attacker
- **Sensor nodes are likely to be placed in locations readily accessible to attackers**
- **Challenge**
  - Build resilient network
    - Operate correctly even when several nodes have been compromised





```
00000170  94 56 6d 98 9b 76 97 fc  b2 c2 b0 fe db 20 e1 eb  |.Vm..v....... ..|
00000180  d6 e4 dd 47 4a 1d 42 ed  9e 6e 49 3c cd 43 27 d2  |...GJ.B..nI<.C'.|
00000190  07 d4 de c7 67 18 89 cb  30 1f 8d c6 8f aa c8 74  |....g...0......t|
000001a0  dc c9 5d 5c 31 a4 70 88  61 2c 9f 0d 2b 87 50 82  |..]\1.p.a,..+.P.|
000001b0  54 64 26 7d 03 40 34 4b  1c 73 d1 c4 fd 3b cc fb  |Td&).@4K.s...;..|
000001c0  7f ab e6 3e 5b a5 ad 04  23 9c 14 51 22 f0 29 79  |...>[...#..Q".)y|
000001d0  71 7e ff 8c 0e e2 0c ef  bc 72 75 6f 37 a1 ec d3  |q~.......ruo7...|
000001e0  8e 62 8b 86 10 e8 08 77  11 be 92 4f 24 c5 32 36  |.b.....w...O$.26|
000001f0  9d cf f3 a6 bb ac 5e 6c  a9 13 57 25 b5 e3 bd a8  |......^l..W%....|
00000200  3a 01 05 59 2a 46 1b 6f  bd 4b 85 9a bb 6d cd 15  |:..Y*F.o.K...m..|
00000210  4b 93 f6 eb 71 30 00 00  00 00 00 00 00 00 00 00  |K...q0..........|
00000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000280  1b 6f bd 4b 85 9a bb 6d  00 00 1b 6f bd 4b 85 9a  |.o.K...m...o.K..|
00000290  bb 6d 00 00 1b 6f bd 4b  85 9a bb 6d 00 00 1b 6f  |.m...o.K...m...o|
000002a0  bd 4b 85 9a bb 6d 00 00  1b 6f bd 4b 00 00 00 00  |.K...m...o.K....|
000002b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```






## Resilience to Node Capture

- **Direction for resilient networks**
  - Detect inconsistencies
    - Replicate state across the network and use majority voting
    - E.g., sending packets along multiple, independent paths and checking at the destination for consistency
  - Crosscheck multiple, redundant views of the environment
    - Extreme outliers may indicate malicious spoofed data

  Defenses based on redundancy are good for sensor networks

## Routing Security

- **Security goals**
  - Integrity, authenticity, and availability of messages
- **Many sensor routing protocols are quite simple, and for this reason are even more susceptible to attacks.**
- **Attacks for routing**
  - DoS attack
  - Injection attack
    - Injecting malicious routing information into the network
  - Node capture attack
    - Routing protocols are susceptible to node-capture attack
  - Wormhole attack, sybil attack, hello flood attack





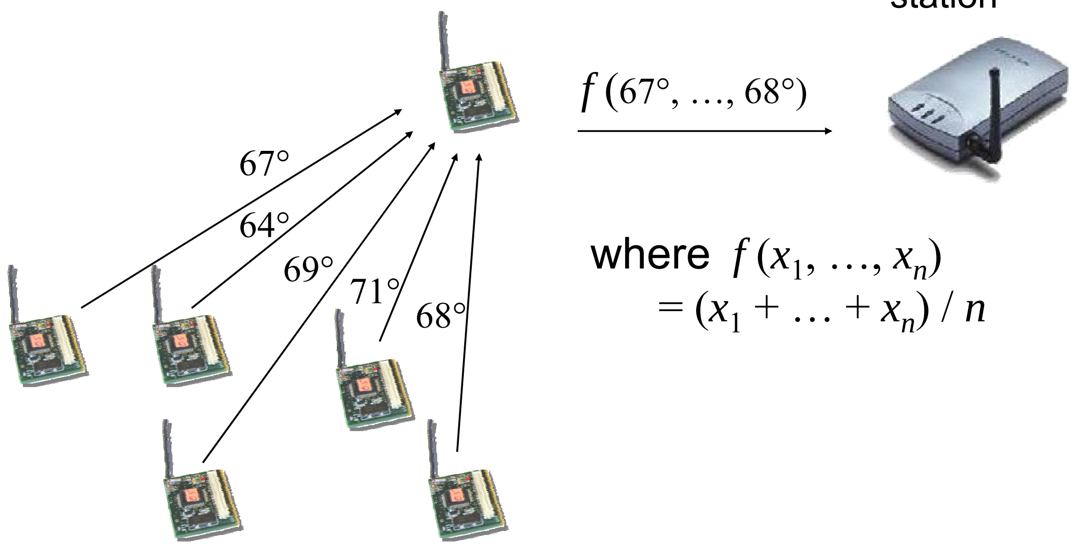
## Routing Security

- **Self-selective routing**
- Not statically pre-configured into each node → Re-configured
- Self-optimization (scalable)
- highly performance, even under “high” network traffic and frequent faults.

# Resilient Aggregation

## Computing the average temperature

base station




where $f(x_1, \ldots, x_n) = (x_1 + \ldots + x_n) / n$

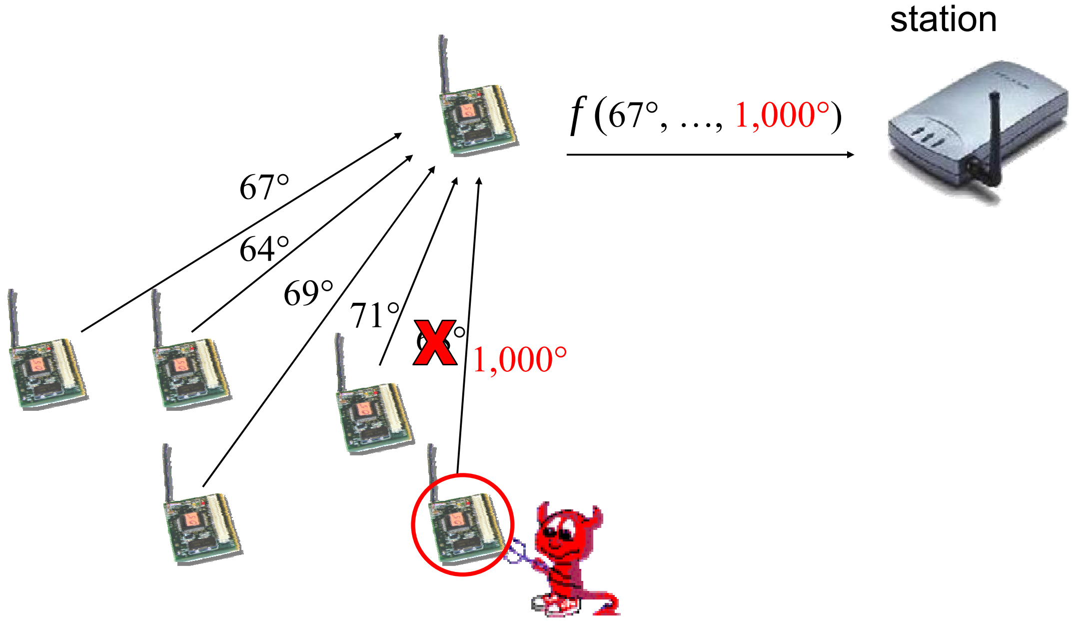




# Resilient Aggregation

## Computing the average temperature

base station



# Intrusion Detection

- Secure not individual nodes but overall network
- Detect early and isolate intrusion
- Instant and autonomous decision making.
  → Self-Diagnostic
- Group oriented
- Based on security rules

**Real-time Auditing rules**

What is safe and secure behavior?

**Danger discovery & propagation rules**

Disseminate alert to network. Collaboratively isolate and minimize damage.





# Intrusion Detection

- <u>Distributed policy-based control</u>
  - Adaptive
  - Fully distributed and inexpensive in terms of communication, energy, and memory requirements
  - Context-awareness (richer information sharing between group members that triggers each other)
  - Selfware behaviour definitions, characterize normal and malicious behavior
  - Self-healing → Cut-off the intruder, change routing paths, update cryptographic material
  - Self-optimization (be able to function under the sudden communication load of a DoS attack)

## Conclusions

- **Security in wireless sensor networks is more challenging than in the conventional networks**
  - Sever constraints and demanding deployment environments of wireless sensor networks
- **We have the opportunity to architect security solutions from the outset**
- **A vision of using context-awareness and distributed policy-based control to achieve a holistic approach that encompasses autonomic responses over a broad range of attacks**





## Contact Info


- **Prof. Tassos Dimitriou**
  - E-mail: tdim@ait.edu.gr
  - Web: http://www.ait.edu.gr/faculty/T_Dimitriou.asp
  - Phone: +30 210668-2753
- **Ioannis Krontiris**
  - E-mail: ikro@ait.edu.gr
  - Phone: +30 210668-2734