The Conventional Wisdom About Sensor Network Security…

David Wagner
U.C. Berkeley

The Conventional Wisdom About Sensor Network Security…

… Is Wrong

David Wagner
U.C. Berkeley

Symmetric-key cryptography

- Old CW: Symmetric-key will probably need HW support

Symmetric-key cryptography

- Old CW: Symmetric-key will probably need HW support
- New reality: Symmetric-key is trivial, even in software
  - < 10% latency, bandwidth, power [TinySec]
  - Communication costs dominate computation costs
  - Some platforms have HW support anyway [802.15.4]

Public-key cryptography

- Old CW: Forget public-key crypto; it is way too expensive for sensor nets. All you get is symmetric-key crypto.

Public-key cryptography

- Old CW: Forget public-key crypto; it is way too expensive for sensor nets. All you get is symmetric-key crypto.
- New reality: Public-key is no big deal [Sizzle]
  - And HW support may be coming (XScale2's TPM)
- Opinion: Fancy schemes (e.g., random key predistribution) are obsolete and no longer needed

[ECC-160]	Time	RAM	Code
Atmega128 (8 MHz)	0.81s	0.28KB	3.7KB
Chipcon1010 (14 MHz)	4.58s	0.27KB	2.2KB

Trust assumptions

- CW: Can't rely on trusted infrastructure.
  Need truly distributed algorithms.

Trust assumptions

- CW: Can't rely on trusted infrastructure.
  Need truly distributed algorithms.

- My opinion: Naah. Centralized solutions are fine, for many applications.
  - If you're spending $10k on 100 sensor nodes, you can afford a $1k laptop-class base station with a tamper-resistant crypto module (TPM, smartcard).

  - Exploiting hierarchy is good engineering. A trusted BS makes secure protocol design *enormously* easier.

  - Designing secure distributed protocols (with no trusted infrastructure) is still intellectually challenging — but practical relevance is uncertain.

Dealing with compromised nodes

- CW: Physical security is too hard, so if you are worried about node compromise, you'd better look for algorithms that can tolerate node compromise.

Dealing with compromised nodes

- CW: Physical security is too hard, so if you are worried about node compromise, you'd better look for algorithms that can tolerate node compromise.

- New prognosis: Well, maybe. But tamper-resistance is looking cheaper and cheaper every day.
  - Trend: Microcontrollers moving to single-chip soln. (CPU, RAM, EEPROM, radio all on one chip)
    ==> Harder to tamper with a sensor node
  - Convergence of smartcards + sensor net nodes?

Conclusions

CW: Sensor net security is one giant open problem.

My current thinking:

- There are still important and challenging research questions worth working on. But…
- For most applications, we have most of the tools needed to build reasonably secure solutions. The field has matured very rapidly.

- My vote for the most vexing open problem? Privacy.