Wireless communication Security
無線通訊安全

Lecture II-4

May 21, 2009

洪國寶

Outline

Part II:

(d) 橢圓曲線密碼技術

- 基本代數概念
- 橢圓曲線簡介
- **基本橢圓曲線密碼協定 (continued)**
- 橢圓曲線之其他性質與應用

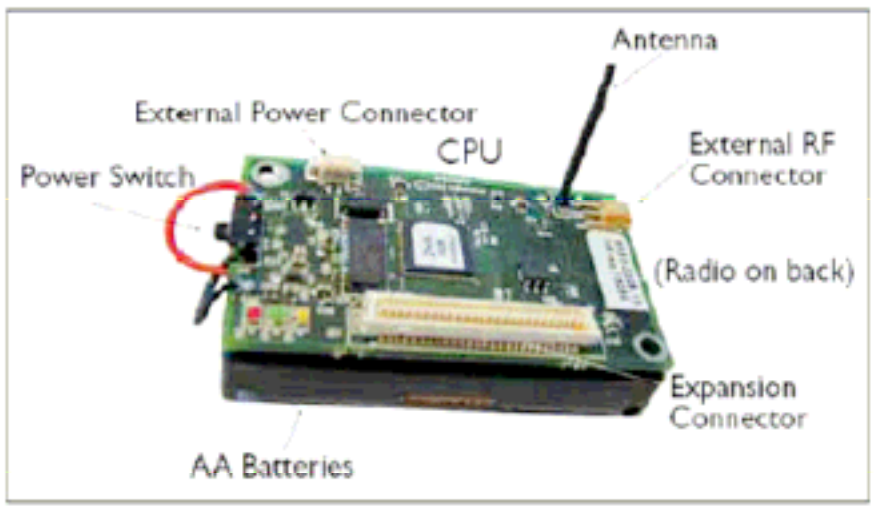
(e) 無線感測網路安全

- **無線感測網路簡介**
- 無線感測網路的安全議題
  - Key distribution/management
  - Secure routing

(f) 相關論文討論

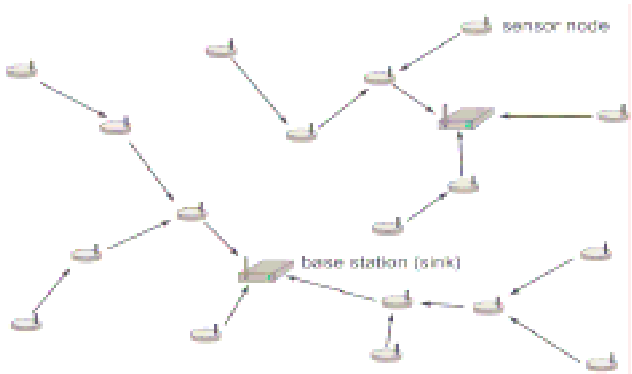
A generic sensor node

- CPU.
- On-board flash memory or external memory
- Sensors: thermometer, camera, motion, light sensor, etc.
- Wireless radio.
- Battery.



Sensor networks

- Large number of sensor nodes, a few base stations
- Sensors are usually battery powered:
  - Main design criteria: reduce the energy consumption
- Multi-hop communication reduces energy consumption:
  - Overall energy consumption can be reduced, if packets are sent in several smaller hops instead of one long hop
  - Fewer re-transmissions are needed due to collisions



Applications of sensor networks

- Ad hoc networking: easy to deploy
  - Disaster rescue.
  - Military applications.
- Real-time environment monitoring.
  - Alert system.
  - Health care.

- RFID tags
  - Warehouse management, library book management
  - Smart shopping.

Algorithmic challenges

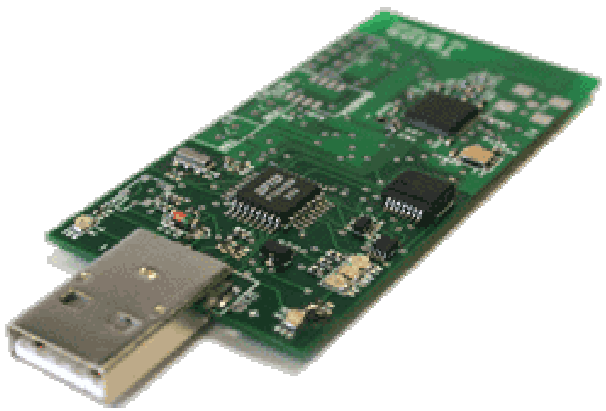
- Resource constraints:
  - Computation, communication and energy.
- Dynamic environment:
  - Network topology is dynamic.
  - Inexpensive nodes have high failure rate.
- Robust data-processing algorithms:
  - Sensor data is noisy. Sensors malfunction.
- Distributed algorithms preferred.

Sensor networks

- Security requirements:
  - Integrity
  - Confidentiality
  - Availability
- Special conditions:
  - Energy consumption
  - Computing and storage capacity of sensors is limited
  - Access to the sensors cannot be monitored

Game-changer #1: 802.15.4

- 802.15.4 radios come with link-layer crypto (AES)



Frame Counter	Key Ctr.	Encrypted Payload	MAC
4 bytes	**1 byte**	**variable**	**4 / 8 / 16 bytes**

Game-changer #2: ECC

- Sun has elliptic curve code that is *fast*

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

- Consequence: Public-key crypto is feasible for sensors

Outline

Part II:

(d) **橢圓曲線密碼技術**

- 基本代數概念
- 橢圓曲線簡介
- 基本橢圓曲線密碼協定
- 橢圓曲線之其他性質與應用

(e) 無線感測網路安全

- 無線感測網路簡介
- **無線感測網路的安全議題**
  - **Key distribution/management**
  - Secure routing

(f) **相關論文討論**

- http://secowinet.epfl.ch/slides/ch05-EstSecAssoc.ppt