UNIVERSIDAD DE MÁLAGA

Applicability of Public Key Infrastructures in Wireless Sensor Networks

Rodrigo Roman, ***Cristina Alcaraz***

Computer Science Department

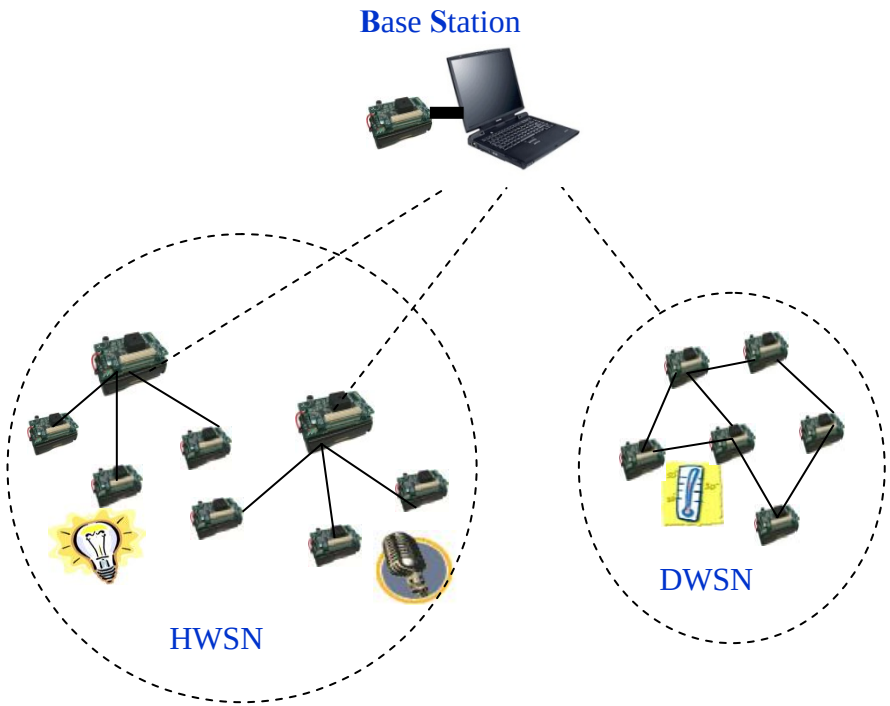
University of Malaga, Spain

June 29th, 2007

Outline

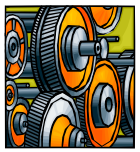
- Wireless Sensor Networks (WSN)
- Public Key Cryptography (PKC) for WSN
- Public Key Infrastructure (PKI) in WSN
- Conclusions

Wireless Sensor Networks



- Monitor: continuously check the status of the environment
- Alert: a problematic situation is happening / going to happen
- Query: provide information "On-Demand"
- Report: transmit small report of the environment
- Others: autonomous, self-configurable, computing distributed, decentralized, easily deployable, inexpensive, …





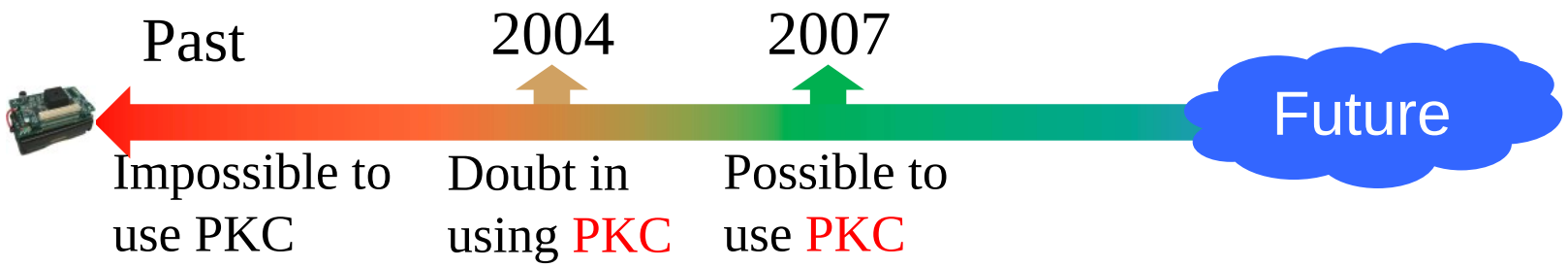

…

Wireless Sensor Networks - Problems

- Constrained hardware and software:
  - Typical sensor node specs:
    - 8 Mhz, 4kB RAM and 128kB ROM
    - Low battery capacity: 2 Months – 1 Year
    - Low-power transceiver (e.g. IEEE 802.15.4)
- And the most important:
  - Specific context of WSN → Increasing number of attacks!!
    - Physical:
      - Easy access to the network enviroment (nodes)
    - Logical:
      - Wireless communication: Confidentiality, Authenticity, Integrity

How to protect them?

- Symmetric Key Criptography
  - Low computational cost: “simple” operations
  - Key size
- Public Key Criptography
  - It provides more security than SKC… but it requires a non-trivial amount of processing power and memory



Why did that doubt arise in 2004?

PKC Primitives

- Rabin Signature Algorithm
  - ✓ Fast in encryption and signature verification: simple squaring operation
  - ✗ Signature size: 512 bits
- Elliptic Curve Cryptography (ECC)
  - ✓ Fast in computation: scalar point multiplication
  - ✓ Key size: 160 bits
- NTRUEncrypt and NtruSign
  - ✓ Fast in encryption and verification operations: simple polynomial multiplications
  - ✗ Signature size: 1169 bits
- MQ-schemes
  - ✓ Fast in signature operations: simple polynomial multiplications
  - ✗ Storage cost: 879 bytes (private key) and 8680 bytes (public key)

Result: Hardware Implementations

- Main goal:
  - to design additional extensions as part of the microcontrollers, or external chips that can balance the computational load

	ECC				NTRU	Rabin	$\mathcal{MQ}$
	Wolkerstorfer	Kumar & Paar	Gaubatz	Batina	Gaubatz	Gaubatz	Yang
Gates	23000	12000	18720	12000	3000	17000	17000
Frequency	68.5MHz	13.5Mhz	500khz	500kHz	500kHz	500kHz	100kHz
Point Mult.	9.98ms	18ms	$\sim$ 400ms	115ms	—	—	—
Encryption	—	—	—	—	58ms	2.88ms	—
Decryption	—	—	—	—	117ms	1.089s	—
Signing	—	—	—	—	234ms	1.089s	44ms
Verifying	—	—	—	—	58ms	2.88ms	—

Result: Software Implementations

- In 2004, Malan implemented the first PKC library for WSN (EccM 2.0 over field F_{2^p})
  - It was optimized by Gura: working over field F_p, using projective coordinates
- Later, Liu and Ning implemented TinyECC and Wang and Li implemented WMECC, both working over Micaz  and Telosb 
- In 2007, **we** generated a new and improved version TinyWMECC
  - Substituting the optimized SHA-1 function component from TinyECC in WMECC
  - Besides, the library WMECC has been updated by their authors for including such optimization

Result: Software Implementations

- Our experiments were

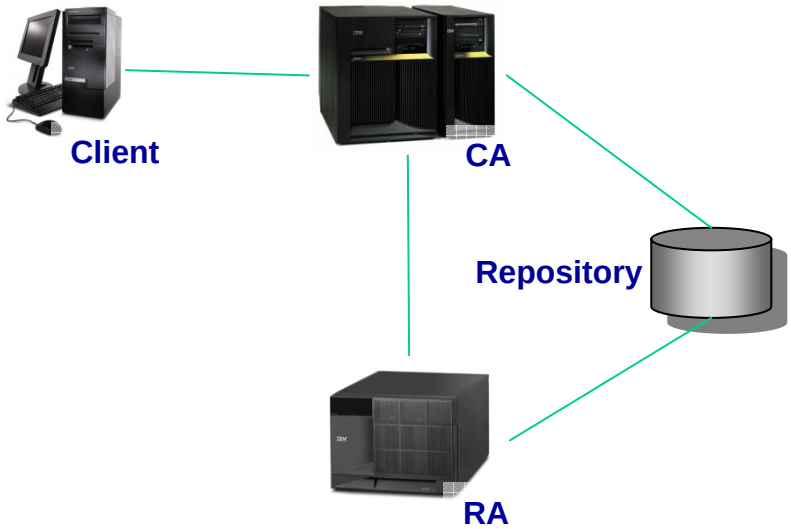
	TinyECC		WMECC		TinyWMECC	
	Micaz	Telosb	Micaz	Telosb	Micaz	Telosb
Test - ROM size	28266	26048	57982	46156	29734	25774
Test - RAM size	2306	2327	1685	1657	1643	1599
ECC init	1.837s	-	1.809s	1.744s	1.809s	1.744s
ECDSA init	3.550s	5.225s	0s	0s	0s	0s
Pub. Key Gen.	1.788s	-	1.261s	1.425s	1.261s	1.425s
Signature	1.916s	4.361s	1.348s	1.498s	1.348s	1.498s
Verification	2.431s	5.448s	2.017s	2.207	2.019s	2.209s

What is our proposal?

To integrate a PKI in a WSN …

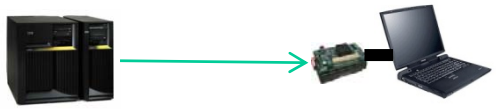
It is possible to use a PKI in WSN?

- Following the PKIX Model:
  - Clients
  - Certification Authority
  - Registration Authority
  - Certificates Repository



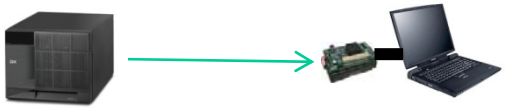
Mapping a PKI herarchy into a WSN

- Certification Authority



  - Why the BS?
    - BS configures and initializes all nodes before their deployment
    - The BS is a trustworthy entity, thus it can generate the private & public keys
  - Then, it is in charge of generating the digital certificates

- Registration Authority

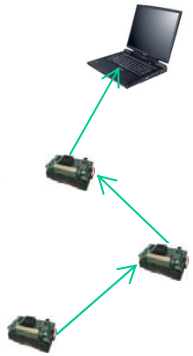


  - Why the BS?
    - BS configures and initializes all nodes and it is a trustworthy entity for generating the keys
  - Then, it is in charge of keeping the initial authentication of the nodes

Mapping a PKI herarchy into a WSN

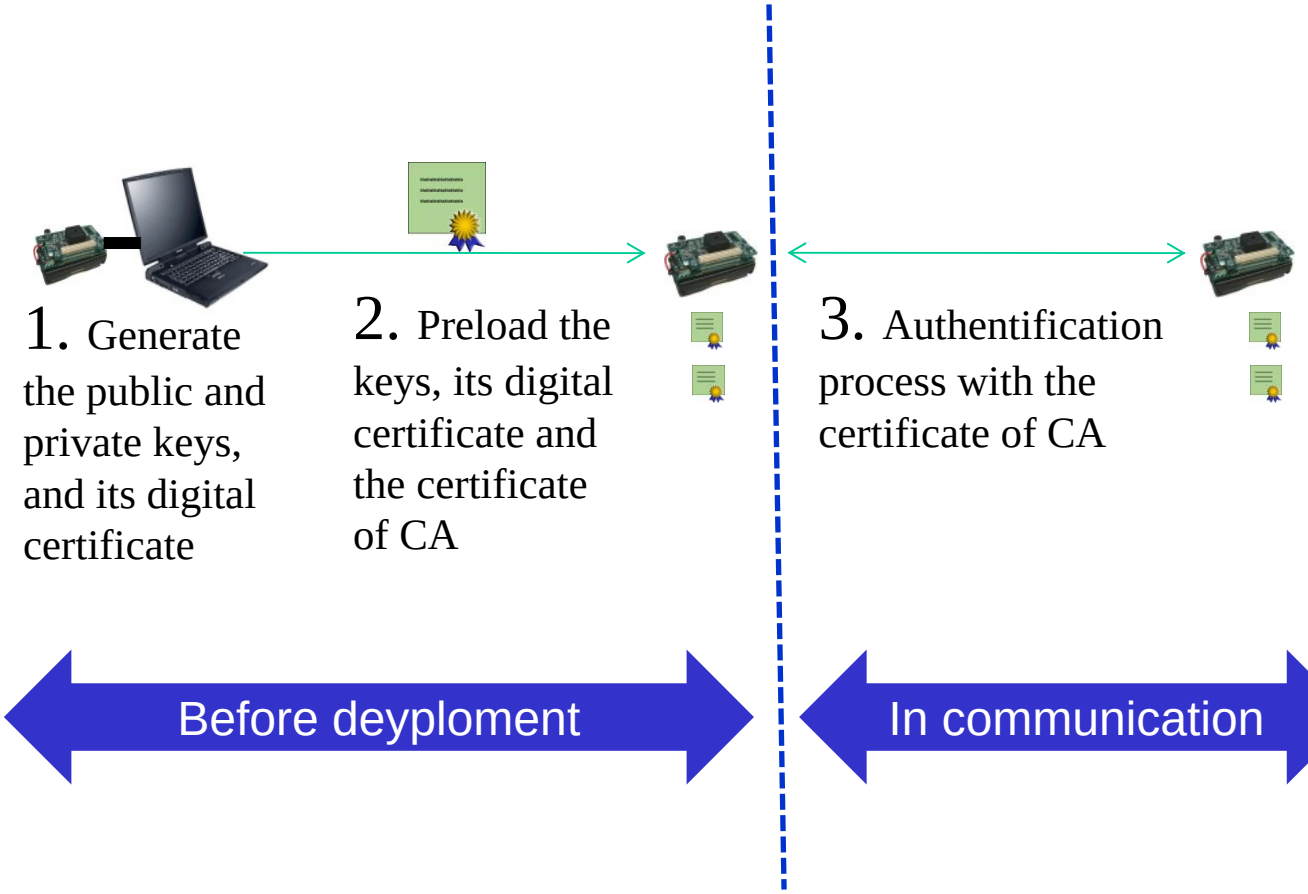
- Certificates Repository

  - Why not the BS?
    - Because it would be costly (energy and time-wise) for the nodes.
    - Why the nodes?
      - Due to network nature (decentralized), and the routing type



  - Solution:
    - Every node has its own certificate, and will provide it to any neighbour that request it
      - This exchange can be done in the first steps of the lifetime of the network

Functionality of PKI in WSN



Services of PKI in WSN

- Key Pair Recovery

  - Why the BS?
    - because it is a trustworthy entity and it could keep all the keys

- Key Update

  - When?
    - If a node is comprised and detected, the BS must revoke its certificate
  - How?
    - Easy update of certificates … it is done manually

Services of PKI in WSN

- Key Revocation 
  - To use a revocation notification mechanism
    - i.e. the BS alerts the nodes of the revocation of un certificate
  - Expiration date of a certificate: So far, it is not suitable
    - For short-lived networks:
      - The important is the “deployment” and the context of the application
    - For long-lived networks:
      - It could interrupt the services of PKI

Services of PKI in WSN

- Cross Certificate (CC) 
  - Two scenaries:
    - One BS
      - No sense on having a CC
    - Several static BS
      - CC is not necessary because all the nodes can have preloaded the certificates of every BS
  - Then, a CC is not necessary in WSN

Conclusions

- It is possible to integrate services of PKI in WSN,
  - Mapping each entity of PKI with the WSN components
  - Adapting the behaviours of the services of PKI to WSN
    - Offering mechanisms for this task
- Future lines
  - To prove the coexistence of a PKI with other public key based schemes: Homomorphic Encyption and Identity-Based Cryptography

Thanks for your Attention!

Rodrigo Roman, ***Cristina Alcaraz***

Computer Science Department

University of Malaga, Spain

June 29th, 2007