Towards Adaptable Security for Energy Efficiency in Wireless Sensor Networks

28th Meeting of WWRF, Athens, Greece

Nikos Fotiou, Giannis F. Marias, George C. Polyzos, Pawel Szalachowski, Zbigniew Kotulski, Michael Niedermeier, Xiaobing He and Hermann de Meer

POLITECHNIKA WARSZAWSKA

UNIVERSITÄT PASSAU

euronf NETWORK OF EXCELLENCE

A WSN Use Case: Patient monitoring

- Sensors deployed on patients' body monitor vital signs
  - Medical records are created
  - Doctors are notified in case of emergency
- Patients freely move around the hospital
- Minimum power level is used to prolong battery life and to limit interferences
  - Patients form small clusters coordinated by low emission wireless access points

➡ Significant security and energy constraints

Towards adaptable security

- Step 1: For each security mechanism identify how its parameters affect its performance
- Step 2: For each operation of the WSN create an energy consumption model
- Step 3: Identify security requirements, threats and the energy required in order to fight them

Parameters tuning of security mechanisms

- For each mechanism define:
  - *L*: the protection level as function of
    - *P*: the probability of an incident occurrence,
    - ω: the impact of a successful attack
- Using as input:
  - #assets gained during successful attack
  - the knowledge required for an attack
  - cost of an attack
  - communication overhead of an attack
  - implementation complexity

An example: TESLA

- TESLA is a light-weight hash chains-based data integrity and authenticity solution
- It requires a MAC and a digital signature function

Digital Signature	MAC scheme	Security Level
RSA-1024 , ECDSA-160	HMAC-MD5	0.394
RSA-1024 , ECDSA-160	HMAC-SHA1	0.440
RSA-2048, ECDSA-192	HMAC-MD5	0.523
RSA-2048, ECDSA-192	HMAC-SHA1	0.566
RSA-3072, ECDSA-224	HMAC-MD5	0.641
RSA-3072, ECDSA-224	HMAC-SHA1	0.716

An example: TESLA (cont'd)

	Sign	Verify
ECDSA (160)	918ms	918ms
RSA (1024)	10990ms	430ms
RSA (2048)	83260ms	1940ms
ECDSA (192)	1240ms	-
RSA (3072)	-	-
ECDSA (224)	2190ms	-
HMAC (MD5)	3.7ms	3.7ms
HMAC (SHA1)	4.8ms	4.8ms

An energy consumption model

- Estimate the energy consumption of a sensor node using the following parameters:
  - P_{ia} = Power consumption of a component in its awake mode
  - P_{is} = Power consumption of a component in its sleep mode
  - t =Time of one communication round
  - t_{at} =Time spent in awake mode during communication round
  - t_{st} = Time spent in sleep mode during communication round
  - j = A task performed in addition to the base load (encryption, decryption, sending / receiving messages, ...)
  - $\#j_t$ = Number of times task is executed during communication round
  - t_j = Time needed for one execution of task
  - P_j = Power consumption of a single execution of task
  - k = Number of overall tasks that are relevant to the dynamic energy consumption
  - i = Number of components on the sensor node (sensors, GPS, RAM, CPU, ...)

$encryption_t$

Example

- high-security WSN using encryption and authentication for all messages
- j= {*send_message, receive_message, encryption, decryption, authentication, verification*}
  - #send_message$_t$= 6
  - #receive_message$_t$= 12
  - #encryption$_t$= 6
  - #decryption$_t$= 12
  - #authentication$_t$= 6
  - #verification$_t$= 12
- Calculate total energy by setting values to all parameters

Security analysis of the system

- Identify security requirements, threats, solutions and assign costs to each solution
  - Data should be confidential ->Encryption
  - Data integrity should be protected ->D.S
  - Privacy perversion -> Pseudonyms
  - Fault Data Injection -> D.S
  - Replay attacks -> Nonce
  - Data analysis -> Encryption
  - Traffic analysis -> Noise
- Each node knows the energy required in order to perform an action securely
  - Define for each action what should be done if there is not enough energy

Thank you

fotiou@aueb.gr