Ubiquitous and Secure Networks and Services

Redes y Servicios Ubicuos y Seguros

Unit 5: Ubiquitous Systems Security

Lourdes López Santidrián
llopez@diatel.upm.es, lourdes.lopez@upm.es

UNIT 5: Ubiquitous Systems Security

VULNERABILITIES OF UBIQUITOUS NETWORKS AND SERVICES

Why WSN are vulnerable against attacks?

- The sensor nodes are constrained by:
  - Battery life.
  - Computational capabilities.
  - Memory.
  - Communication band.
- Is easy to physically access to nodes:
  - Human or machine can reprogram them.
  - Human or machine can destroy them.
- The communication channel is public.
- It is difficult to monitor and control the distributed elements.

Security Threats

- **Common Attacks:**
  - Eavesdropping (passive).
  - Data injection (active).
  - Message modification (active).
  - Message replay (active).
- **Denial of Service Attacks (DoS):**
  - Jamming: target the communication channel.
  - Power exhaustion: target the nodes.
- **Node Compromise:**
  - An attacker can read or modify the internal memory of a node.

Security Threats

- **Side-channel Attacks:**
  - Monitoring of the nodes' physical properties.
  - Acquisition of security credentials (secret keys).
- **Impersonation Attacks:**
  - Sybil attack (creation of fake identities).
  - Replication attack (creation of duplicate identities).
- **Protocol-specific Attacks:**
  - Routing protocols.
    - Spoofed Routing Information.
    - HELLO Flood Attack.
  - Aggregation protocols: falsifying information.
  - Time synchronization protocols.

Security Services

- **Confidentiality**
  - Only the desired recipients can understand the message.
  - May be not mandatory.
- **Integrity**
  - If the data produced and sent over the network are altered, the receiver will have a proof.
  - In most cases it is a mandatory feature.

Security Services

- **Authentication**
  - A receiver can verify that the data is really sent by the claimed sender.
  - It is mandatory if the network needs a barrier between external and internal members.
- **Authorization**
  - It states that only authorized entities can be able to perform certain operations.
- **Availability**
  - The users of a WSN must be capable of accessing its services whenever they need them.

Security Services

- **Freshness**
  - The data produced by the WSN must be recent
- **Forward and Backward Secrecy**
  - Forward secrecy: where a node should not be able to read any future messages after it leaves the network
  - Backward secrecy: where a node is not able to read a previously transmitted message.
- **Self-organization**
  - Nodes must be independent and flexible in order to react against problems.

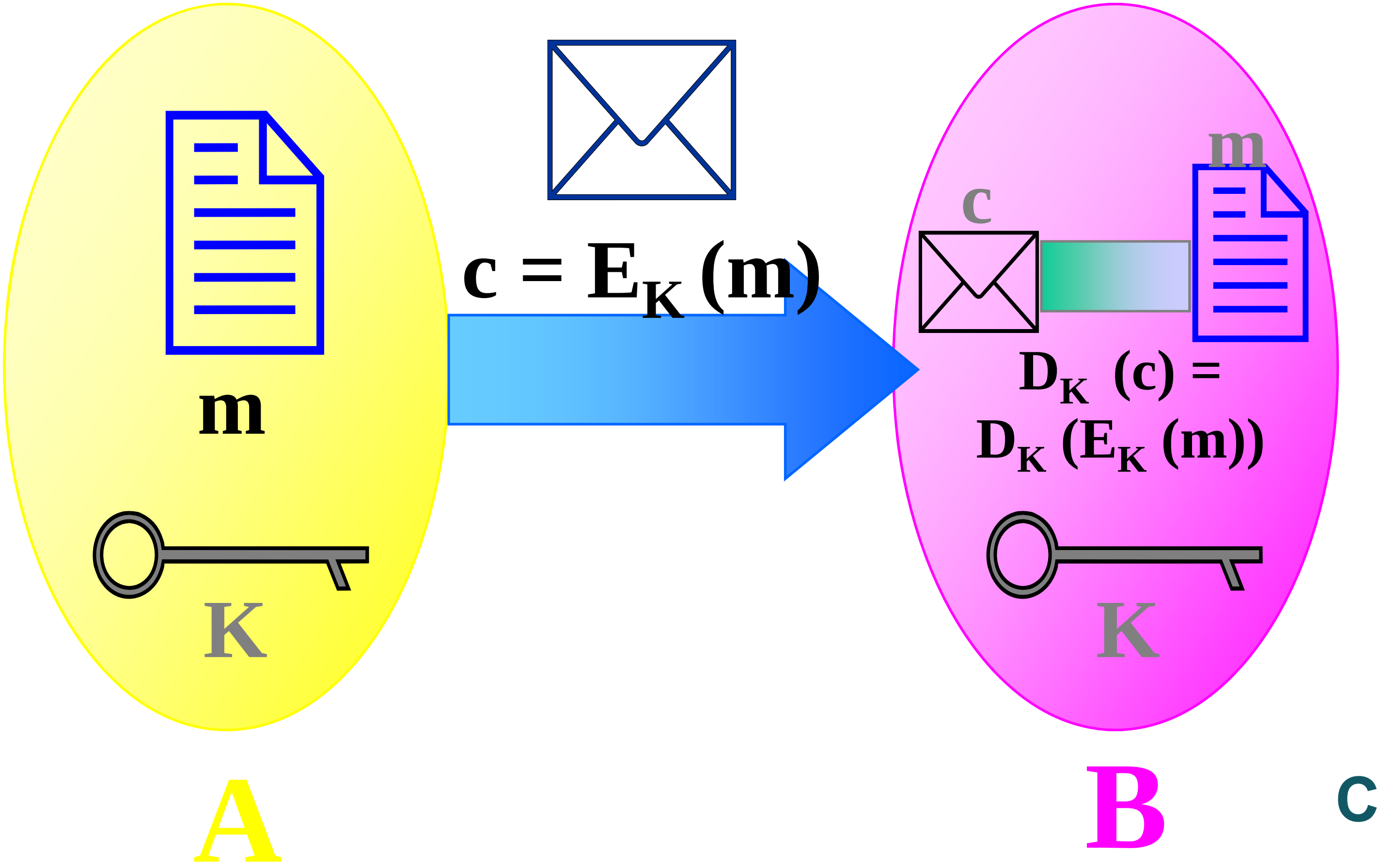
Security Services

- **Auditing**
  - The elements of a WSN must be able to store any events that occur inside the network.
- **Non-repudiation**
  - A node cannot deny sending a message, or a recipient cannot deny the reception of a message.
  - Evidence that the message was sent is necessary.
- **Privacy and Anonymity**
  - The identity of the nodes should be hidden or protected.

UNIT 5: Ubiquitous Systems Security

CRYPTOGRAPHIC MECHANISMS AS THE BASIS OF THE SECURITY

Secret/Symmetric Key Cryptography

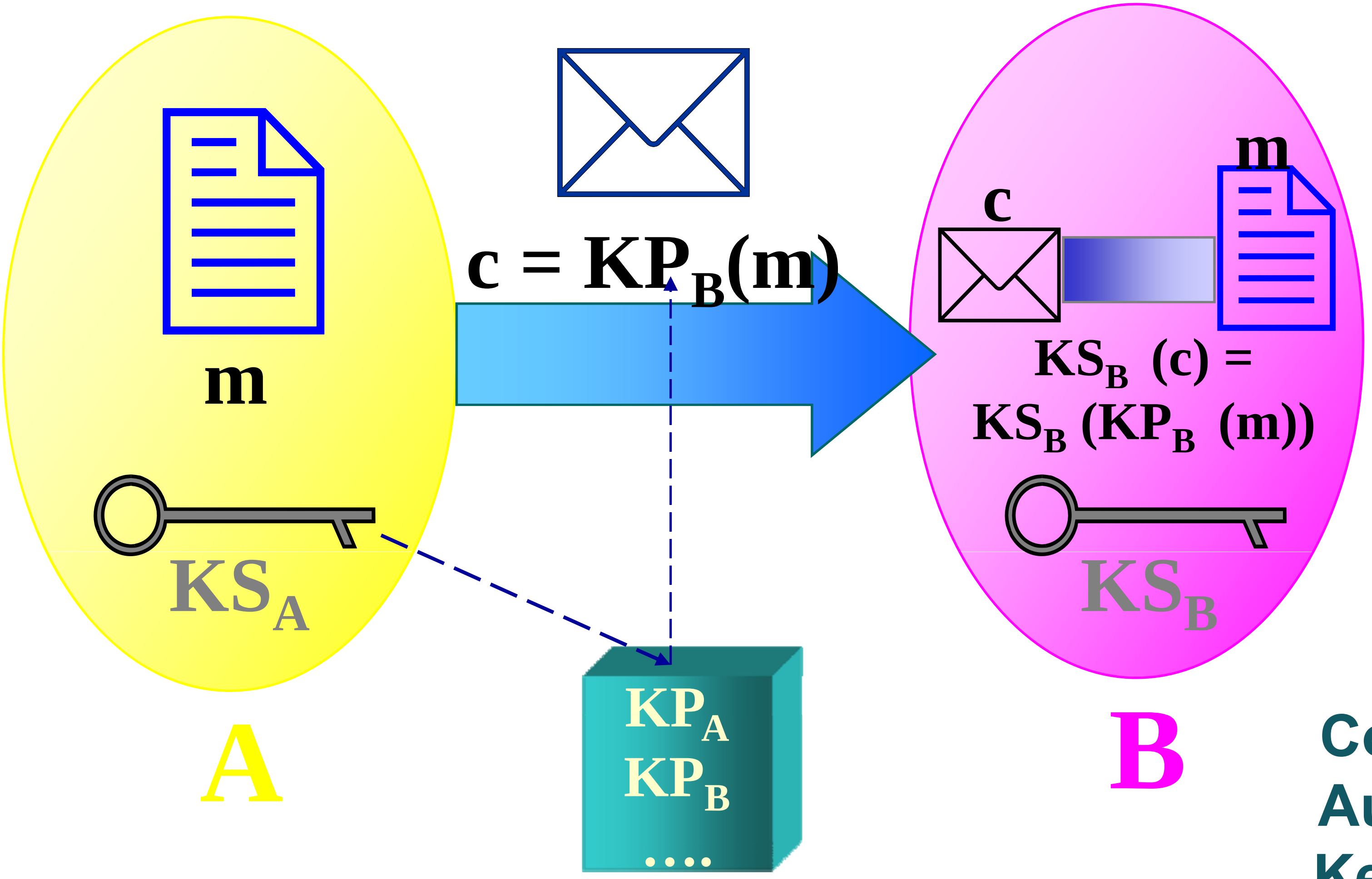


Confidentiality
Integrity

Secret/Symmetric Key Algorithms

	Time	CPU	Power	ROM
Algorithm	(ms)	Cycles	(µJ)	Memory (Kb)
SkipJack	2,16 (3)	15.925,2 (3)	51,4 (3)	19 (4)
RC5	**1,50 (2)**	**11.059,2 (1)**	**36,00 (1)**	**16 (3)**
RC6	10,78 (5)	79.478,7 (5)	258,72 (5)	16 (3)
TEA	2,56 (4)	18.874,4 (4)	61,44 (4)	15,5 (1)
XTEA	**1,45 (1)**	**12.450,2 (2)**	**40,7 (2)**	**15,5 (1)**
DES	608,00 (6)	4.482.662,4 (6)	14.592,00 (6)	31 (6)

Public/Asymmetric Key Cryptography



Confidentiality
Authentication
Key agreement

Public/Asymmetric Key Algorithm

Elliptic Curve Cryptography (ECC)

- ❑ **TinyECC**
  - ❍ ECC-based signature generation and verification (ECDSA).
  - ❍ Encryption and decryption (ECIES).
  - ❍ Key Agreement (ECDH).

Hash Functions

- One-way functions:
  - If we have *m* (any size) and *H* hash function (digital fingerprint):
    - $h = H(m)$ with fix size.
  - It is almost impossible calculate *m* from $H^{-1}(h)$

- Can be used to build:
  - Message Integrity Code (MIC).
  - Message Authentication Code (MAC).
    - Authentication.
    - Integrity.

UNIT 5: Ubiquitous Systems Security

INTRUSION DETECTION

Definition of Intrusion Detection

- **Anomaly detection:**
  - Analyze the network or system and infer what is “normal” from the analysis.
  - Application of statistical or heuristic measures.
  - If an event isn’t “normal” → generate an alert

- **Misuse detection:**
  - Know what an “attack” is.
  - Detection of “attacks”.

ID Components for WSN

- ❑ Neighbor monitoring
  - ❍ Watchdog.
- ❑ Data fusion
  - ❍ Local: neighboring nodes.
  - ❍ Global: overlapping areas.
- ❑ Topology discovery.
- ❑ Route tracing.
- ❑ History.

UNIT 5: Ubiquitous Systems Security

SECURITY MANAGEMENT

Key Management

- Key Management Systems (KMS):
  - Creation.
  - Distribution.
  - Maintenance of secret keys.
- IEEE 802.15.4 does not specify how secret keys should be exchanged.
- A key-exchange protocol is needed:
  - “Key pool” Framework.
  - Mathematical Framework.
  - Negotiation Framework.
  - Public Key Framework.

Security at WSN Standards

- **IEEE 802.15.4-2066 security:**
  - Confidentiality: HW support for AES-128.
  - Integrity: MIC or MAC.
  - Received Message Authentication: Access Control List (ACL).
- **ZigBee 2006 and 2007 security:**
  - *Standard Security.*
  - Confidentiality and Authentication at NWK and APS levels.
  - “All nodes on the network trust each other”.
- **ZigBee PRO security:**
  - *High Security.*
  - Master key for Symmetric-Key-Key-Exchange.