Authentication for RFID and Sensor Networks

SeongHan Shin

Research Center for Information Security (RCIS), AIST, JAPAN

Contents

- Part I
  - Authentication
  - Authentication for ad-hoc networks
- Part II
  - RFID and sensor networks
  - Security requirements

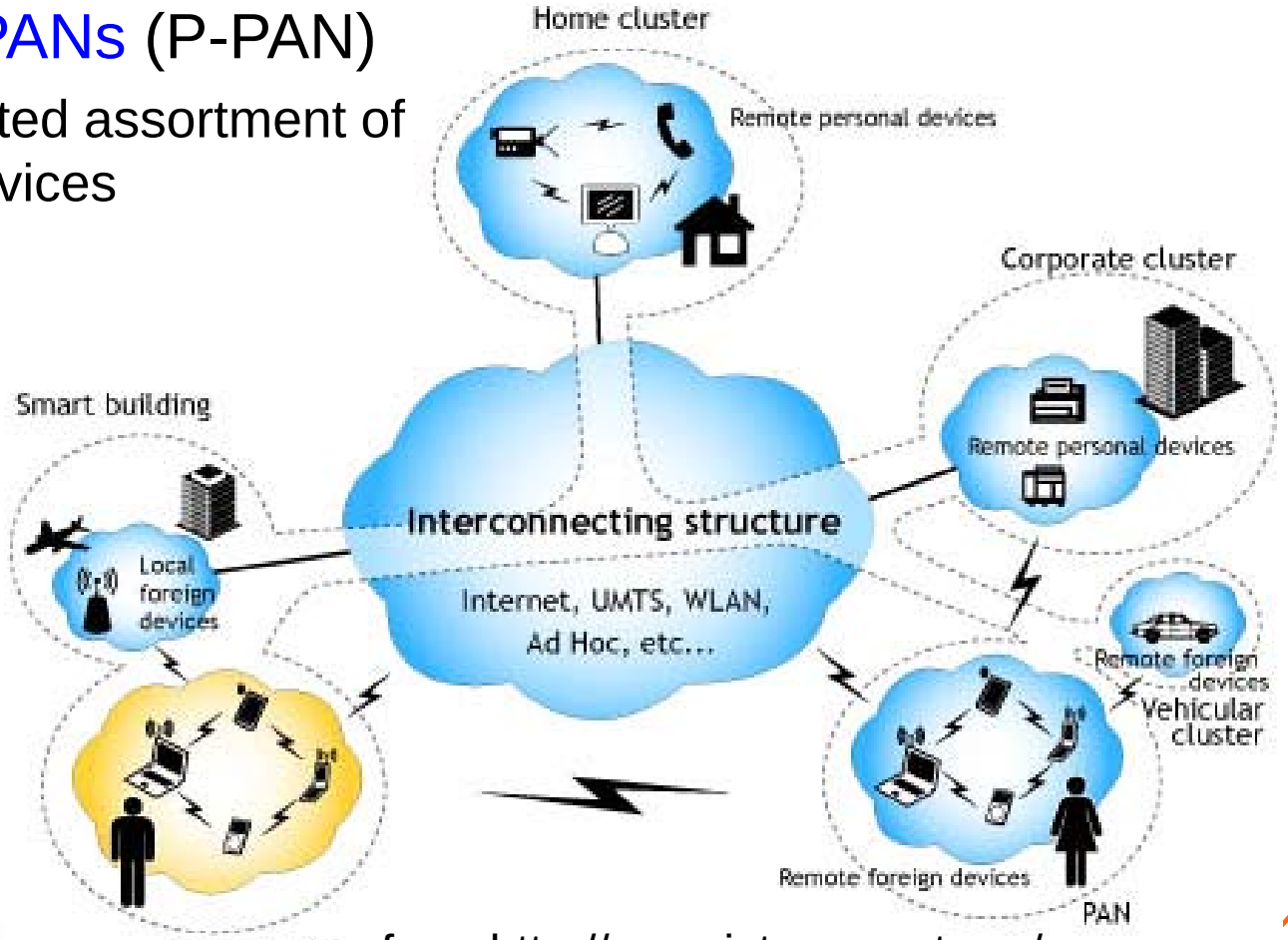
Authentication

- A means to check someone who is claimed to be
  - What you have
  - What you remember
  - Who you are

- Authentication
  - PKI-based
  - Long shared-key based
  - Short shared-key based
  - Multi-factor based

Ad-hoc Networks

- User-centric clusters of personal area networks (PAN) and private PANs (P-PAN)
  - Interconnected assortment of personal devices



from http://www.ist-magnet.org/

MAGNET Architecture

- **M**y personal **A**daptive **G**lobal **NET**
- PN, PAN and P-PAN are in compliance with the MAGNET architecture
  - All devices are under absolute control of its user/owner
  - No device is supposed to be shared between two different users
  - Each PN/PAN/P-PAN has an associated PNI (Personal Network Identifier)
  - Communications between two devices are carried out in an ad-hoc way, involving no assistance from infrastructure networks
  - Each device is in range but they are most unlikely to be in direct Light of Sight (LOS)
  - Communications among devices will proceed only after clear approval from each of the communicating devices

Motivation

- Recent advances in wireless communications and mobile computing devices made PN, PAN and P-PAN deployment a feasible reality
  - Intensive investigation on the concepts and issues have been conducted and are still on the move

- The use of LTKs seems to provide an appropriate level of security. However…
  - Devices' loss or theft (or, leakage of the stored secrets)
    - It results in the total break-down of security in personal networks
  - No forward secrecy of messages
    - A compromise of any device (e.g., by virus) allows an attacker to get all the previously-transmitted messages

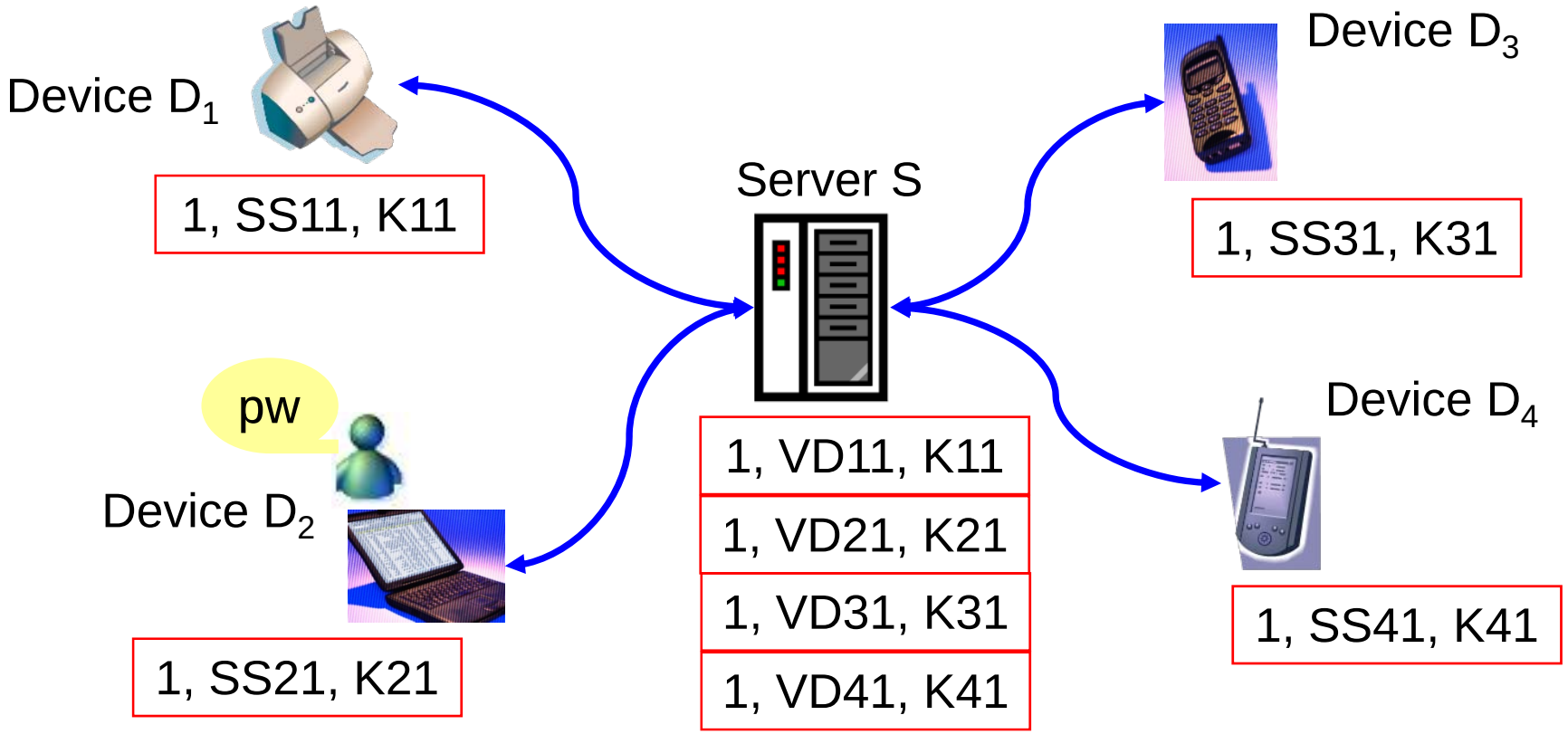
Our Contributions

- **Protecting personal devices *perfectly* is not possible**
  - One can not provide perfect security against all possible leakages of stored secrets
  - Our approach: *minimize the damage caused by the leakages*

- Contributions
  - Authentication and key exchange
  - Key management for users
  - Portable devices' loss or theft
  - Interception and modification of messages or MIM attacks
  - No availability of trusted and reliable third parties
  - Forward secrecy of messages

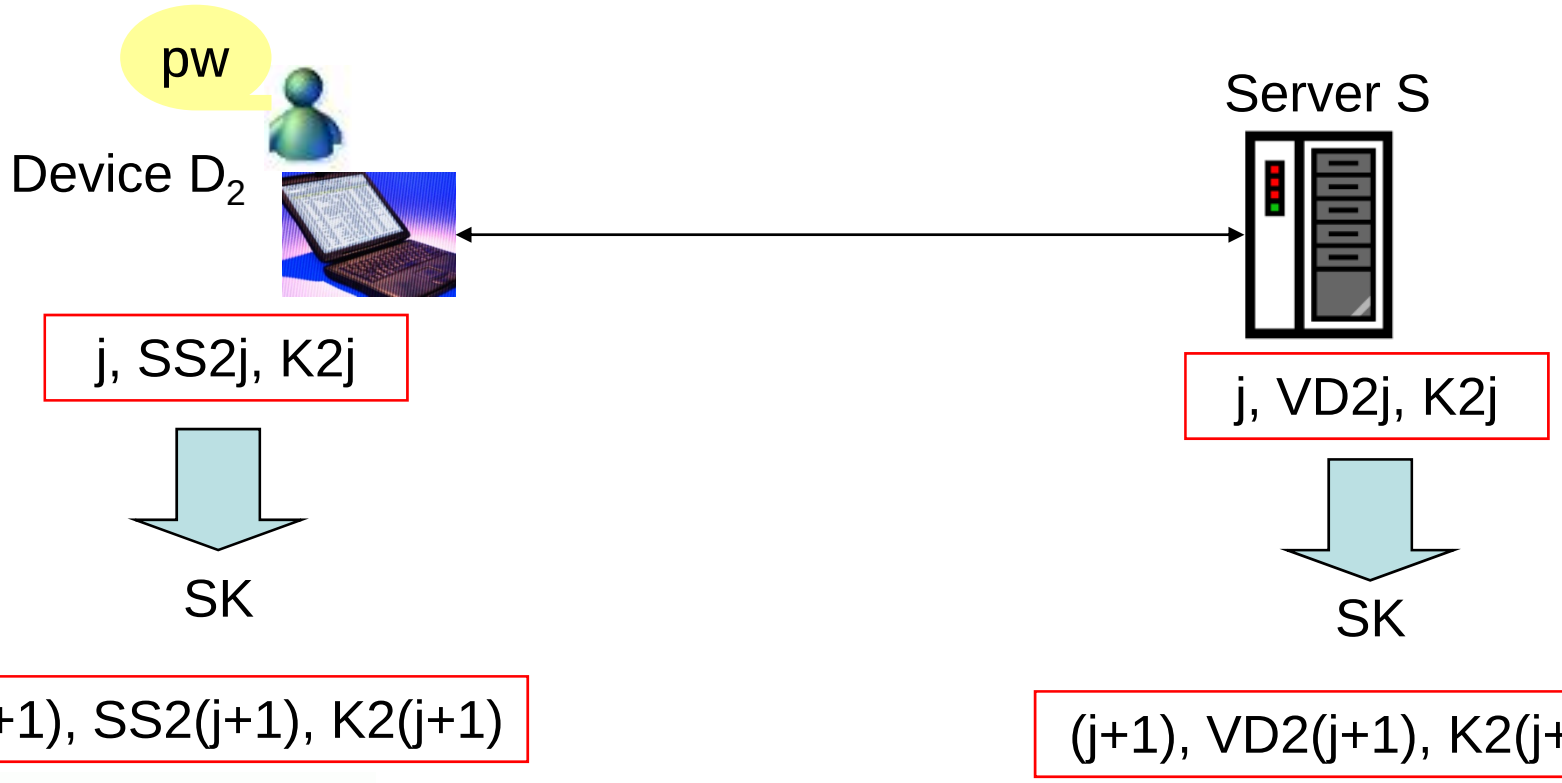
The Imprinting Procedure

- The imprinting procedure using private PAC



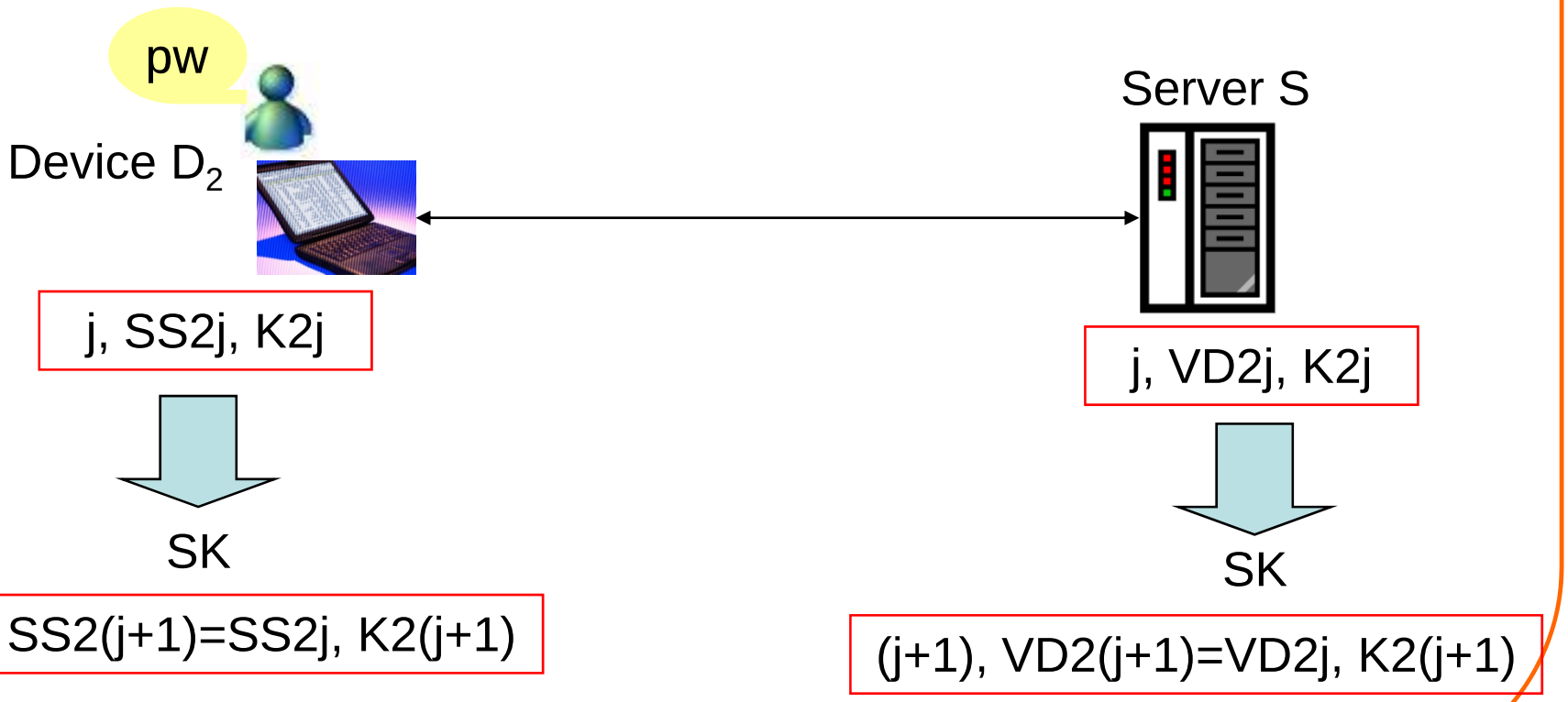
The LRFS-AKE1 Protocol

- The LRFS-AKE1 protocol
  - When the assistance of a user is possible
  - j-th protocol execution using insecure communication channels



The LRFS-AKE2 Protocol

- The LRFS-AKE2 protocol
  - When a user is not present
  - j-th protocol execution using insecure communication channels



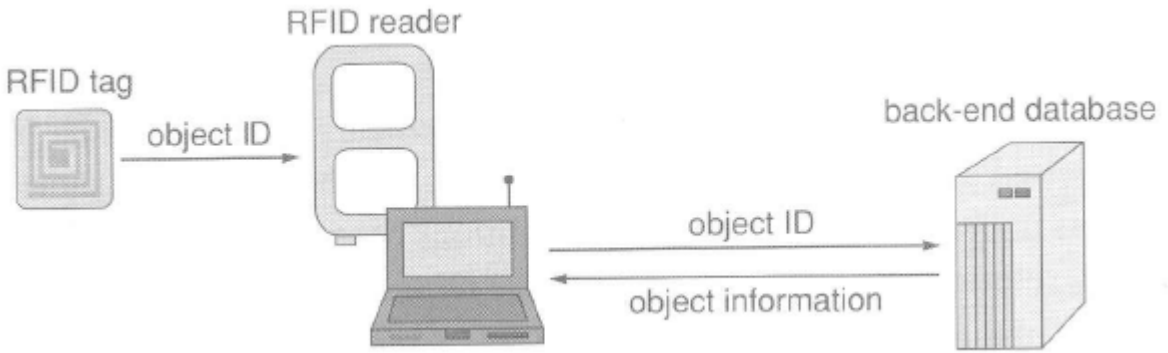
A Security Framework based on LRFS-AKE1 and LRFS-AKE2

- The framework shows how a different types of communications work securely in order to generate a session key in PN/PAN/P-PAN
  - PN wide communication
    - Two personal devices of the same user are located either a P-PAN or a PAN
  - Communication between P-PANs of two different users
    - Communication between two personal devices in different P-PANs
  - Group communication in P-PANs
    - A group session key among devices is generated

RFID (Radio Frequency Identification)

- RFID systems
  - (active/passive) RFID tags, RFID readers, back-end databases
  - Access control to buildings, toll-payment on highways, management of library books, identification of pets, …

- The reader looks up in the database the detailed object information, using the identifier obtained from the tag



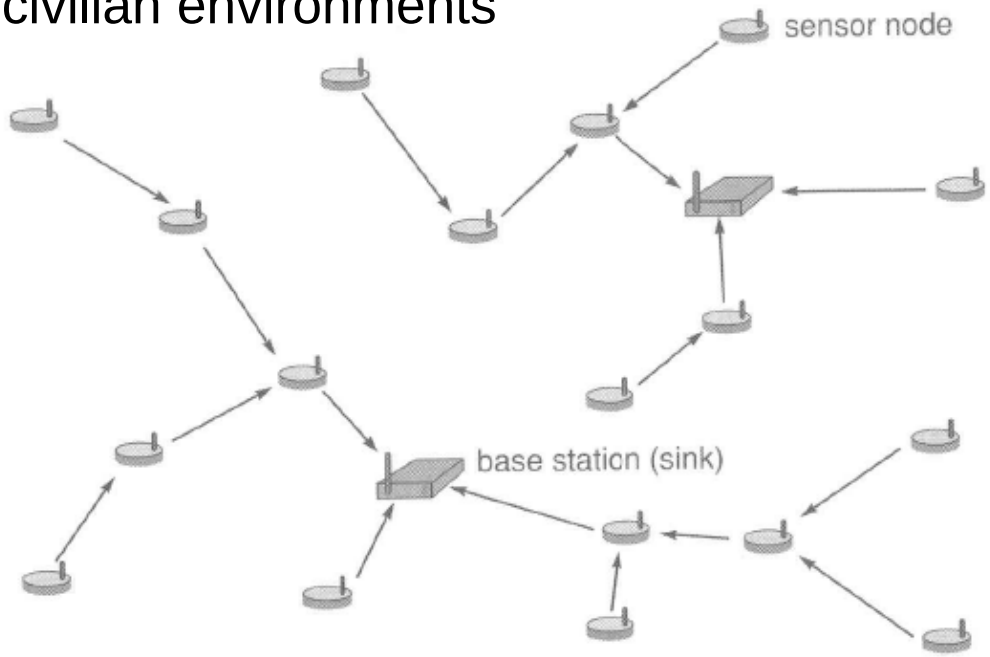
from Book entitled “Security and Cooperation in Wireless Networks”

Security Requirement for RFID

- Privacy
  - RFID technology enables automatic monitoring of the movement so that tracking people could be cheap and continuous
- Previous solutions
  - Killing and sleeping
  - Renaming
  - Blocking
  - Time-memory trade-off
  - Maintaining state
  - Using key-trees

Sensor Networks

- Sensor nodes forward packets towards the base stations on behalf of other nodes in order to mitigate the overall energy consumption and interface
  - Military/civilian environments



from Book entitled “Security and Cooperation in Wireless Networks”

Security Requirements for Sensor Networks

- Integrity(/confidentiality)
  - Data to base stations
  - Control messages to sensors
- Availability
- Energy consumption
- Computing and storage capacity
- Physical protection

Possible Directions

- “Lightweight” authentication?
  - More security
  - More efficiency

Thank you!!!