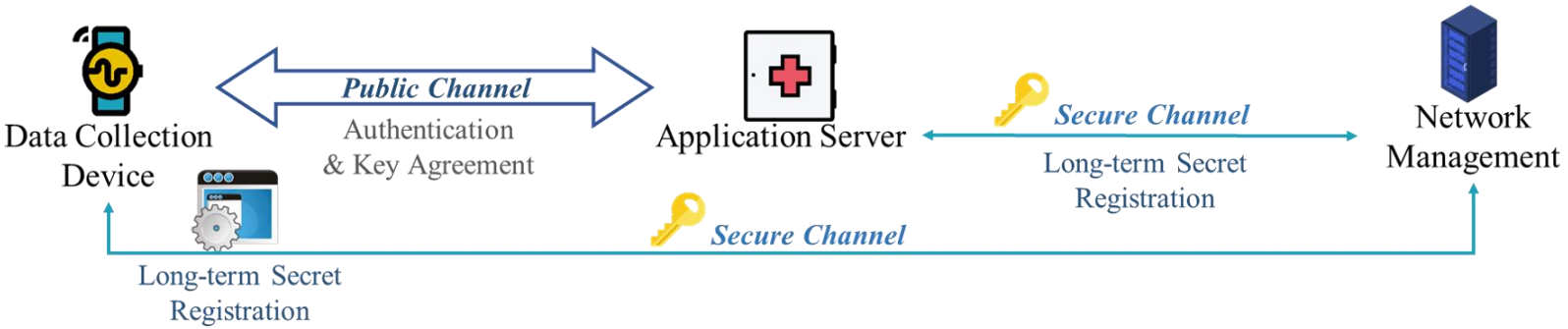
Provable secure authentication key agreement for wireless body area networks

Yuqian MA, Wenbo SHI, Xinghua LI, Qingfeng CHENG

Frontiers of Computer Science, DOI：10.1007/s11704-023-2548-4

Problems & Ideas

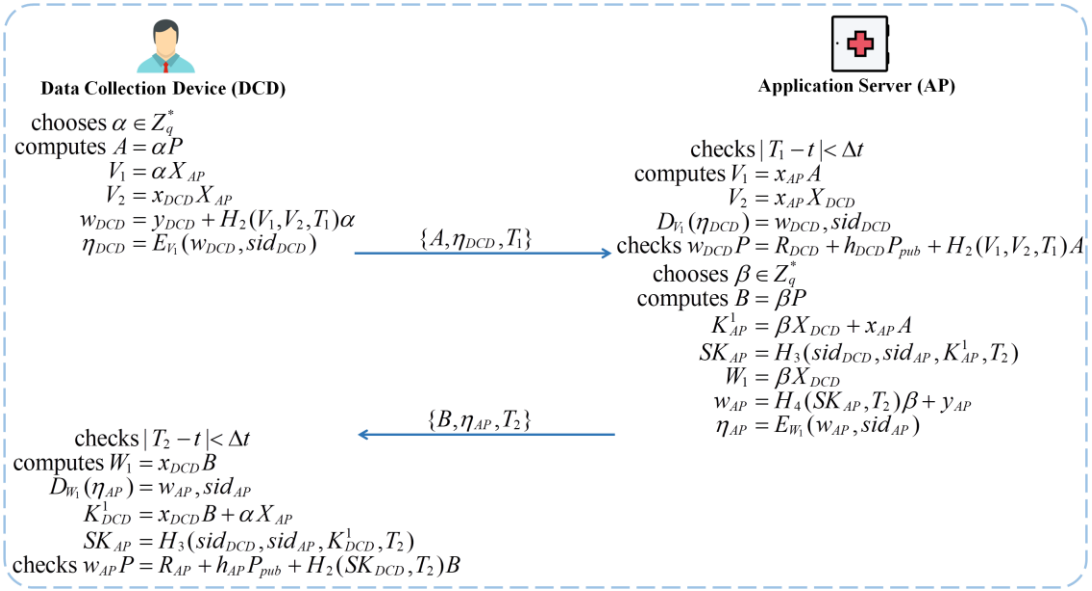
- Problems of authentication and key agreement schemes:
  - Existing security schemes can hardly meet the new requirements of anonymity and lightweight in wireless body area networks.
  - It is analyzed that Wang et al.'s novel scheme could hardly achieve the ephemeral key leakage attack resistance.
- Ideas: A secure and efficient certificateless authentication key agreement scheme, which is enhanced for the wireless body area networks, is proposed.



Data collection devices (DCD) and application servers (AP) will achieve mutual authentication and key agreement after implementing the proposed scheme. First, users, including DCDs and APs, register in network management for long-term secrets. This phase will be implemented in secure channel. Then, DCDs and Aps will agree on secure session keys by implementing the proposed anonymous and efficient authentication key agreement scheme.

Main Contributions

- Contributions:
  - Analyzed Wang et al.'s scheme and presented that their proposal could hardly resist ephemeral key leakage attacks;
  - Designed a novel secure and efficient certificateless authentication key agreement scheme considering the safeness of physiological data and private information;
  - Presented security analysis and performance evaluation claiming that the scheme can satisfy security properties and efficiency required urgently.



Specific details of anonymous certificateless authentication key agreement scheme, which is implemented between data collection device (DCD) and application server (AP) and generates a secure session key.