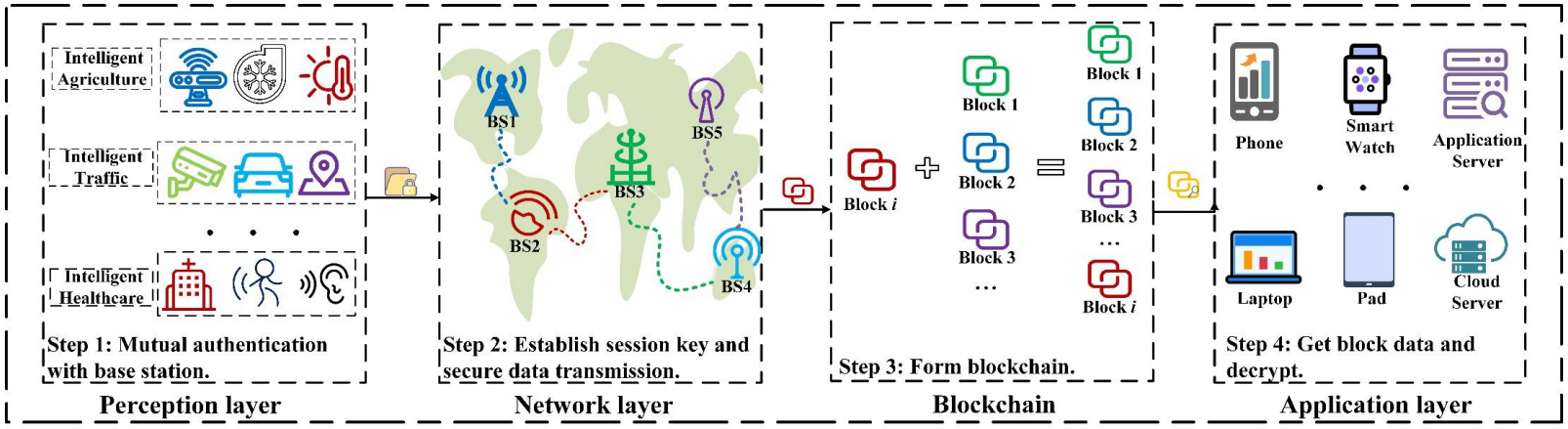
An anonymous authentication and secure data transmission scheme for the Internet of Things based on blockchain

Xingxing CHEN , Qingfeng CHENG, Weidong YANG, Xiangyang LUO

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2595-x

Problems & Ideas

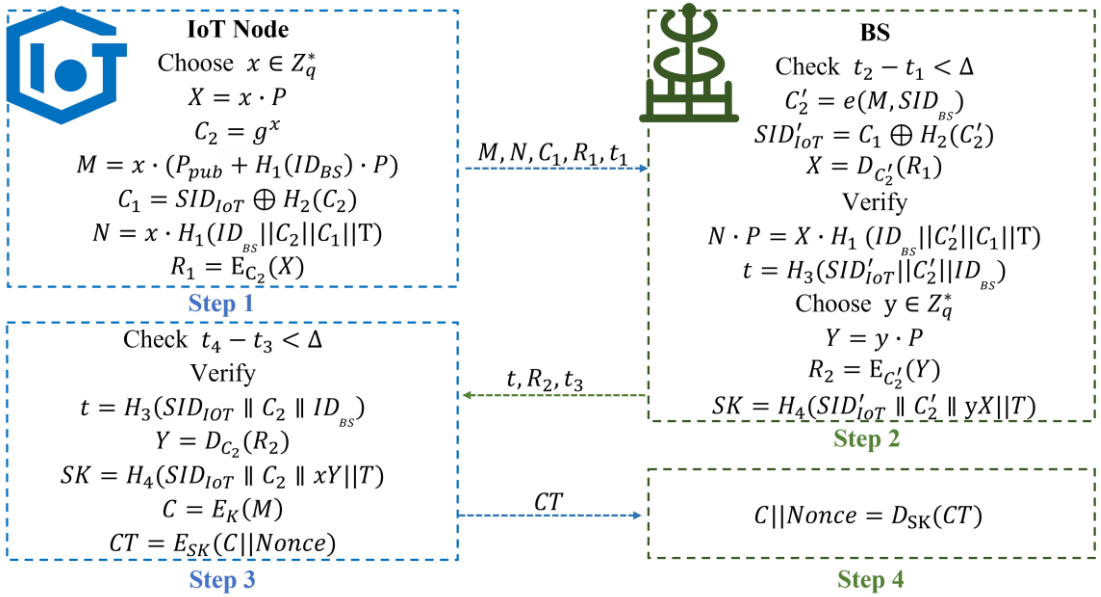
- Problems of authentication and data transmission schemes:
  - IoT devices used for data sensing are constrained by memory and processing power.
  - The scheme of fan et al. which is one of the most advanced schemes lacks consideration of ephemeral secret compromise attacks and anonymity of IoT nodes.
- Ideas: A new anonymous authentication and key agreement scheme, taking into account the processing power of IoT devices and their resistance to various security attacks.



The data sensed by the IoT nodes is transmitted to the network layer through a secure data transmission protocol. Then, the base station will form a block of the received sensing data and upload it to the blockchain, waiting for the application server to call.

Main Contributions

- Contributions:
  - Proposed a new anonymous authentication and key agreement protocol for secure blockchain-based data transmission in the IoT environment;
  - The formal security proof and detailed security attribute analysis show that the proposed scheme can resist various security attacks, and Scyther is used to verify the correctness of the proposed scheme;
  - The proposed scheme has lower computational and communication cost.



Specific details of anonymous authentication and key agreement protocol, which implements anonymous authentication of IoT nodes and base stations and agrees on a secure temporary session key.