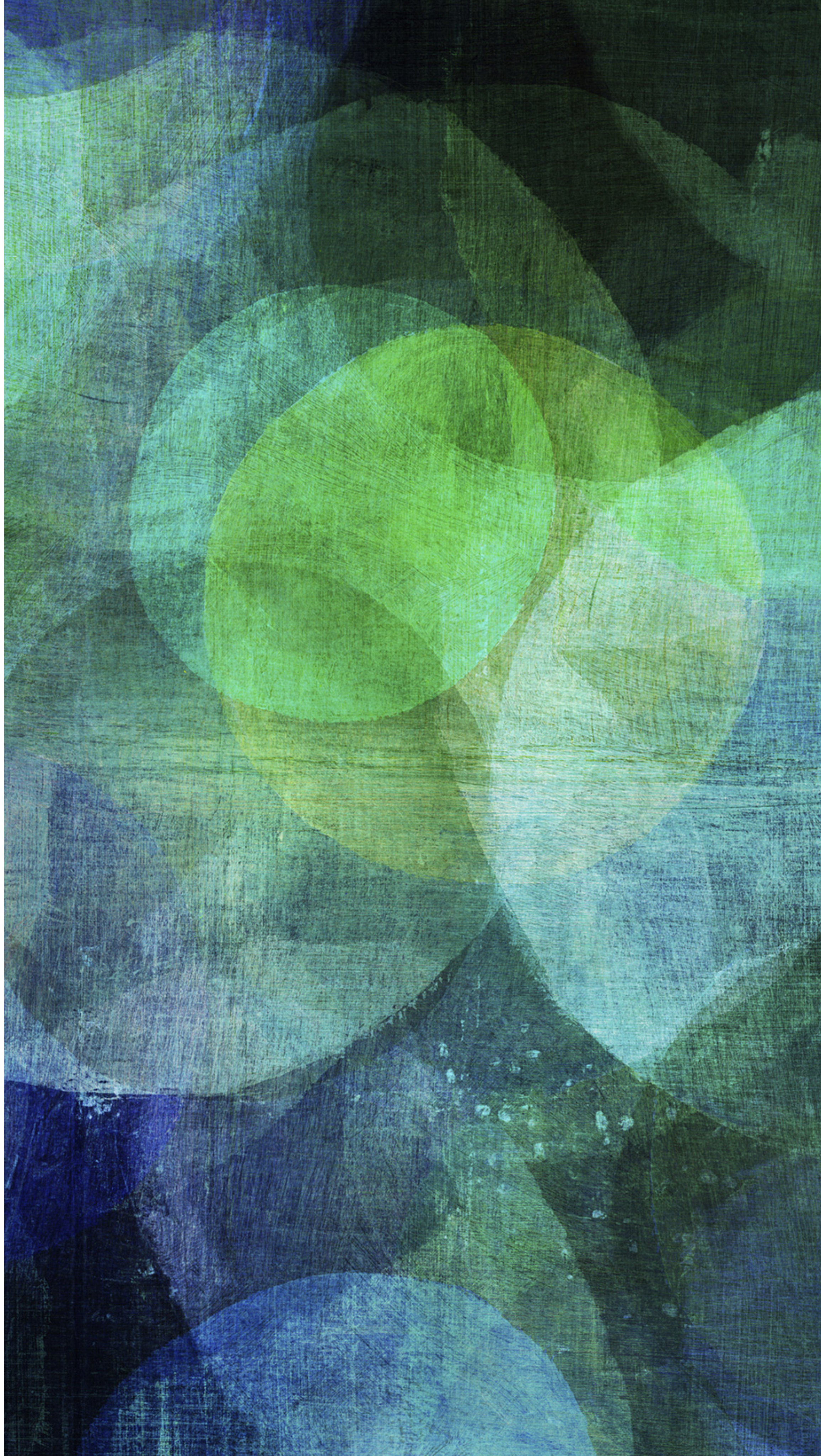
Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions

Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos

Emre Özdil - 150120138
Güneş Yurdakul - 150140141
Gamze Akyol - 150140142



IOT

- composed of physical objects embedded with:
  - Electronics
  - Software
  - Sensors
- sensed and controlled remotely across network
- now everywhere
- required:
  - Huge Volumes of Data Storage
  - Processing Power

ABOUT PAPER

- Due to the resource constraints of IoT devices - > resorts to the cloud for outsourced storage and computation
  - security
  - privacy threats

- In this article:
  - architecture
  - security and privacy requirements

for the next generation mobile technologies on cloud-based IoT

MOTIVATION

- Cloud-based IoT can be categorized
    - Static
    - Mobile - more challenging in protocol design

- 5G

- Secure Packet Forwarding to avoid security gaps during routing
    - layer removing/adding attack

MOTIVATION

- periodically collecting and broadcasting certain kinds of passing service
- high computational complexity
- privacy-preserving lightweight authentication
  - avoid duplicate packet transmission
  - reduce both the computational and communication cost

NETWORK ARCHITECTURE OF CLOUD BASED IOT

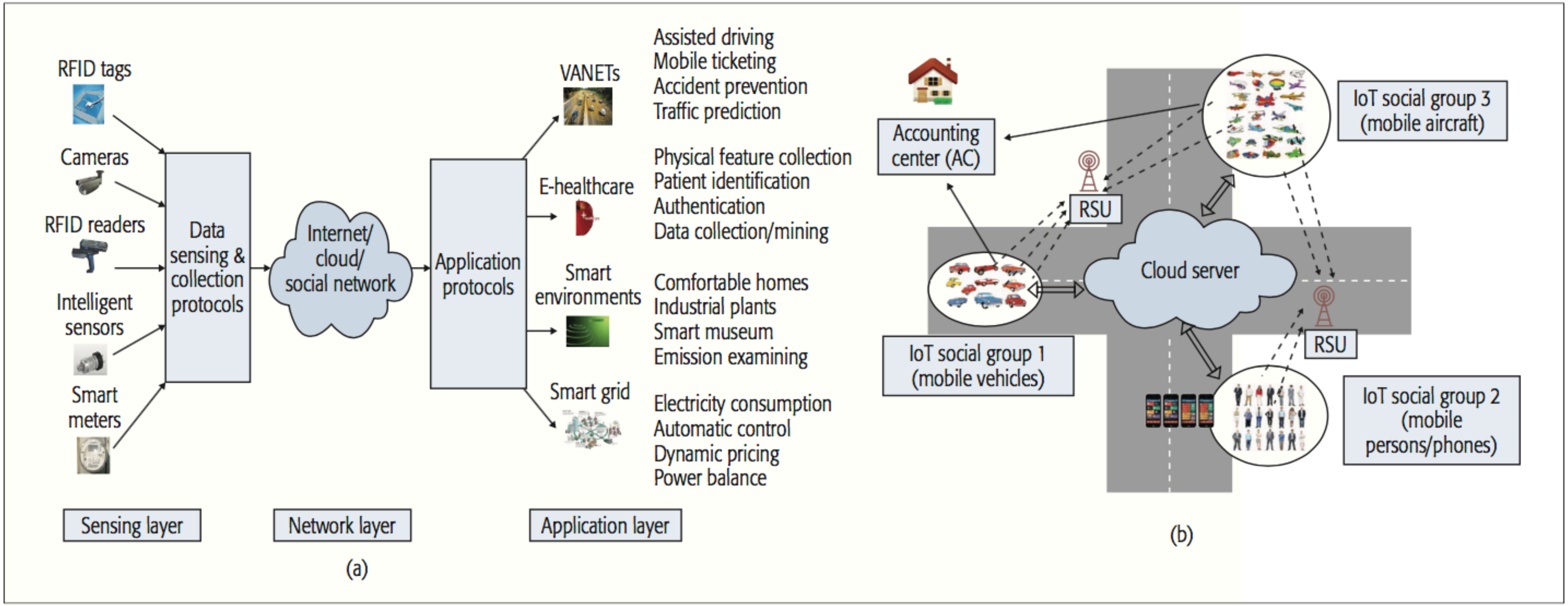
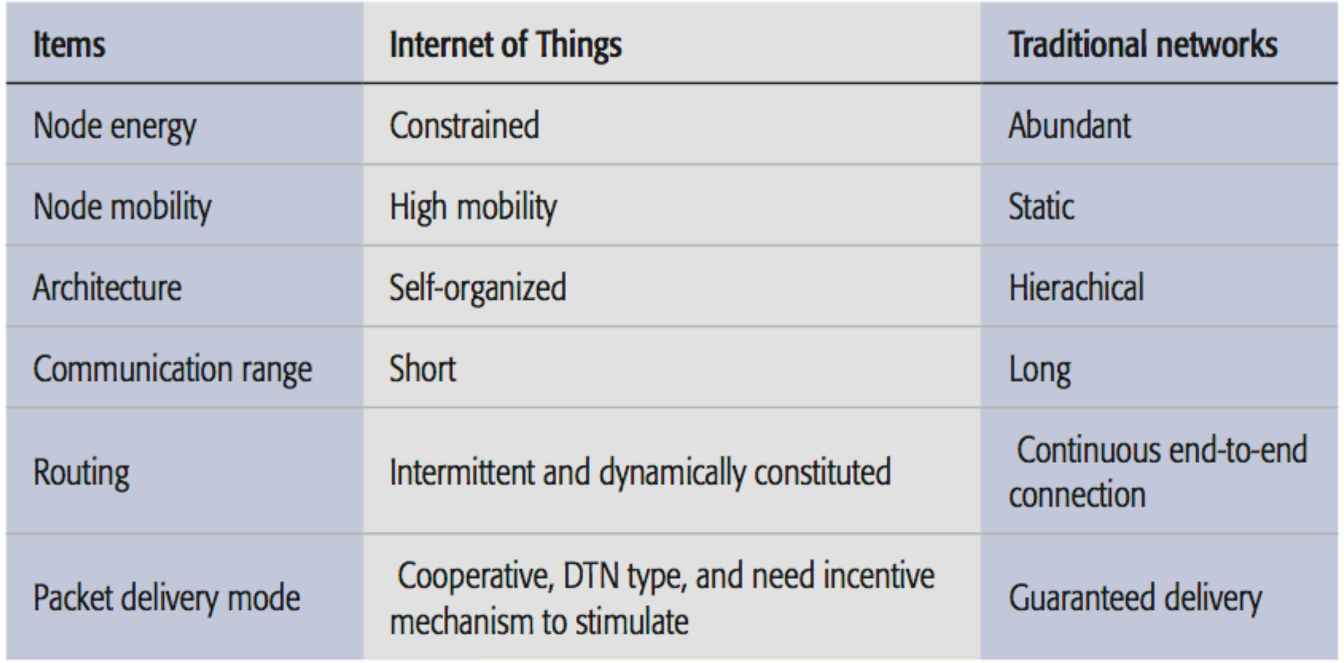


Figure 1. Network architecture of cloud-based IoT.

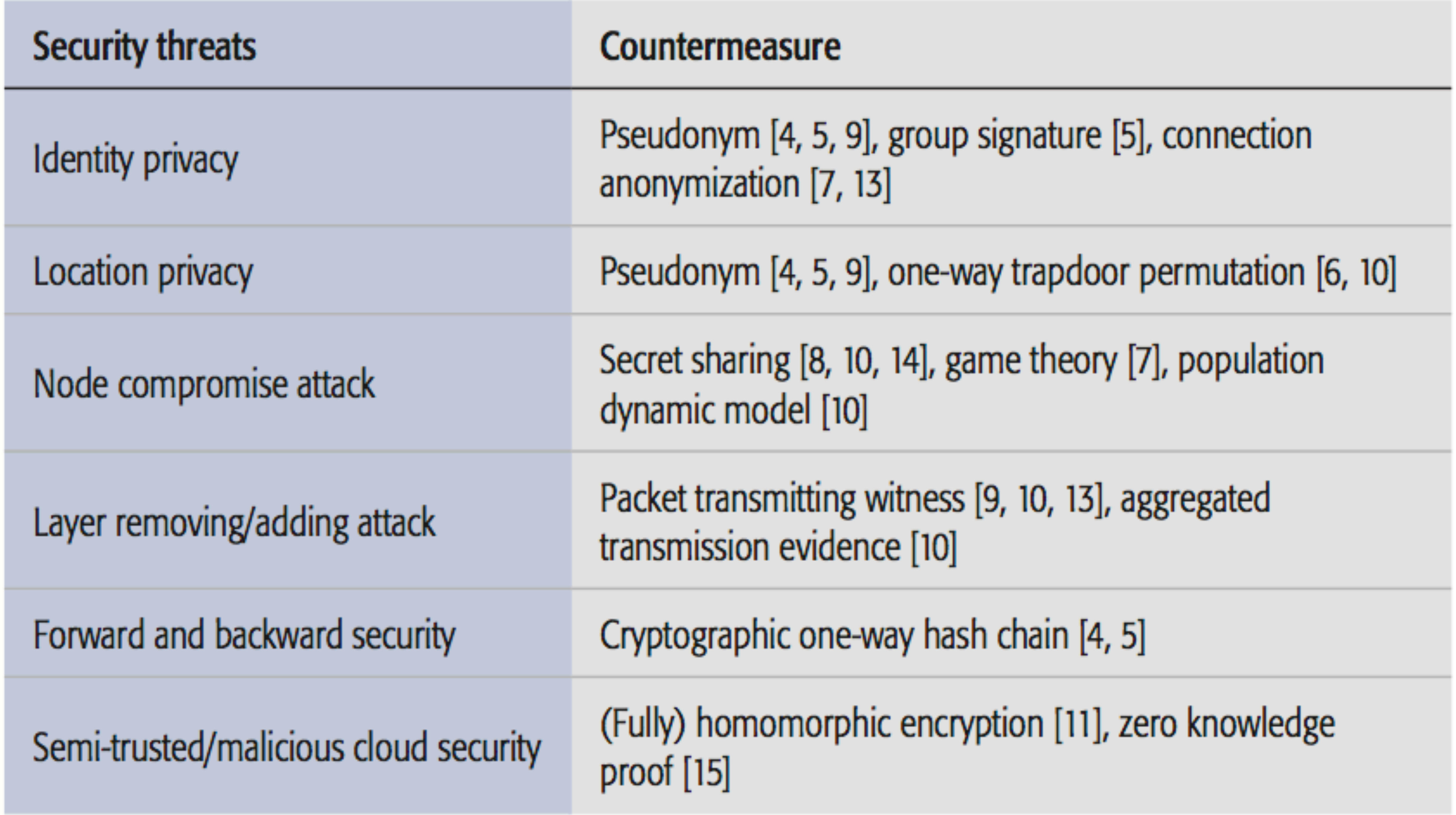
NETWORK ARCHITECTURE OF CLOUD BASED IOT

- Resource Constraints
- Mobility
- Self Organization
- Short-Range Communication



Items	Internet of Things	Traditional networks
Node energy	Constrained	Abundant
Node mobility	High mobility	Static
Architecture	Self-organized	Hierachical
Communication range	Short	Long
Routing	Intermittent and dynamically constituted	Continuous end-to-end connection
Packet delivery mode	Cooperative, DTN type, and need incentive mechanism to stimulate	Guaranteed delivery

Table 1. Characteristic comparison between cloud-based IoT and traditional networks.



Security threats	Countermeasure
Identity privacy	Pseudonym [4, 5, 9], group signature [5], connection anonymization [7, 13]
Location privacy	Pseudonym [4, 5, 9], one-way trapdoor permutation [6, 10]
Node compromise attack	Secret sharing [8, 10, 14], game theory [7], population dynamic model [10]
Layer removing/adding attack	Packet transmitting witness [9, 10, 13], aggregated transmission evidence [10]
Forward and backward security	Cryptographic one-way hash chain [4, 5]
Semi-trusted/malicious cloud security	(Fully) homomorphic encryption [11], zero knowledge proof [15]

Table 2. A taxonomy of main security threats in cloud-based IoT.

SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED IOT

- Identity Privacy
- Location Privacy
- Node Compromise Attack

SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED IOT

- Layer Removing/Adding Attack
- Forward and Backward Security
- Semi Trusted and/or Malicious Cloud Security

SECURE PACKET FORWARDING IN CLOUD-BASED IOT

The mechanisms which prevent packet forwarding from attacks:

SMART

- Secure credit-based incentive scheme
- **Pi** does not consider the outsider threats.
- Layer adding collision cannot be solved in both SMART and Pi.

TCBI

- Threshold credit-based incentive mechanism
- Node compromise attacks are blocked effectively
- Equality between IoT users is provided
- Optimize IoT users' utility

COMPARISON OF SMART AND TCBI

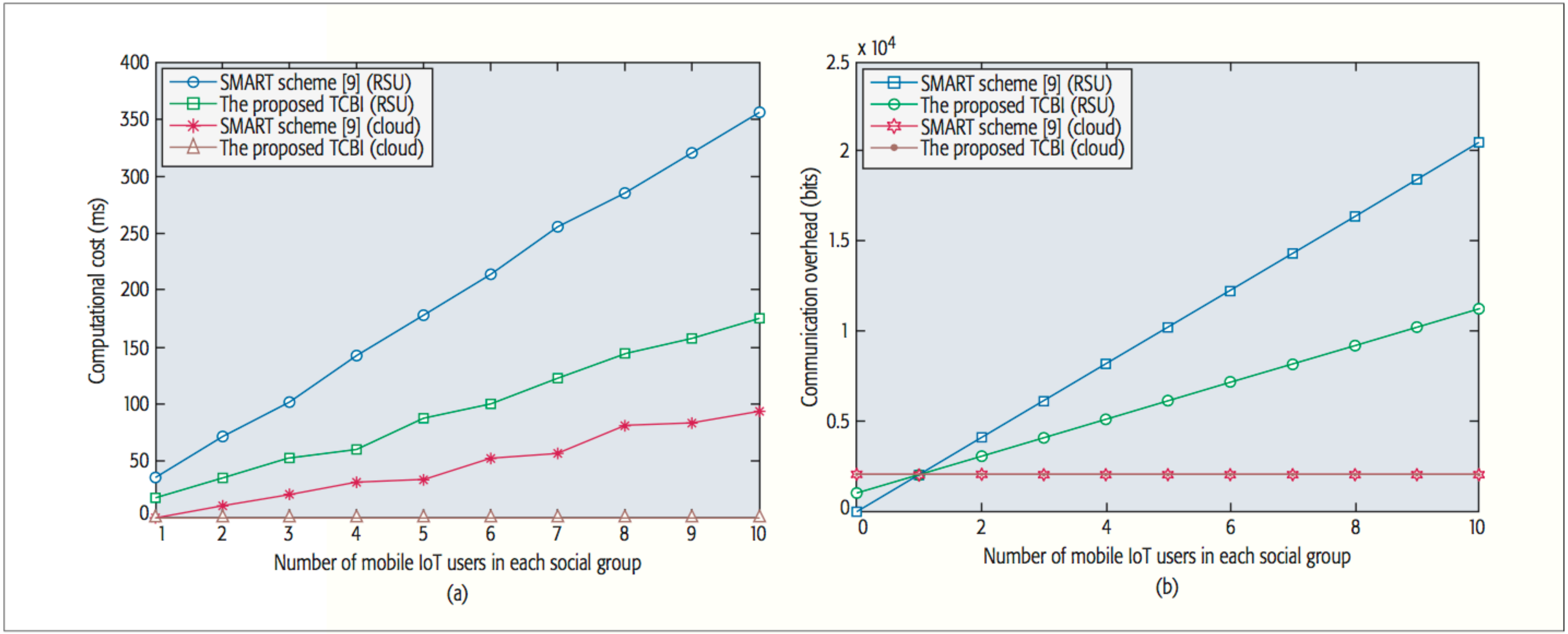


Figure 2. Efficiency comparison between SMART [9] and TCBI: a) computational cost; b) communication cost.

PRIVACY-PRESERVING AUTHENTICATION

- Identity/location privacy protection
- Lightweight authentication
- Pseudonym technique is proposed instead of Public Key Infrastructure (PKI).

SAVE

- An efficient privacy preserving authentication scheme
- It filters location based service contents.
- Prevents duplicate elements
- Physically dynamic tracing attack is prevented

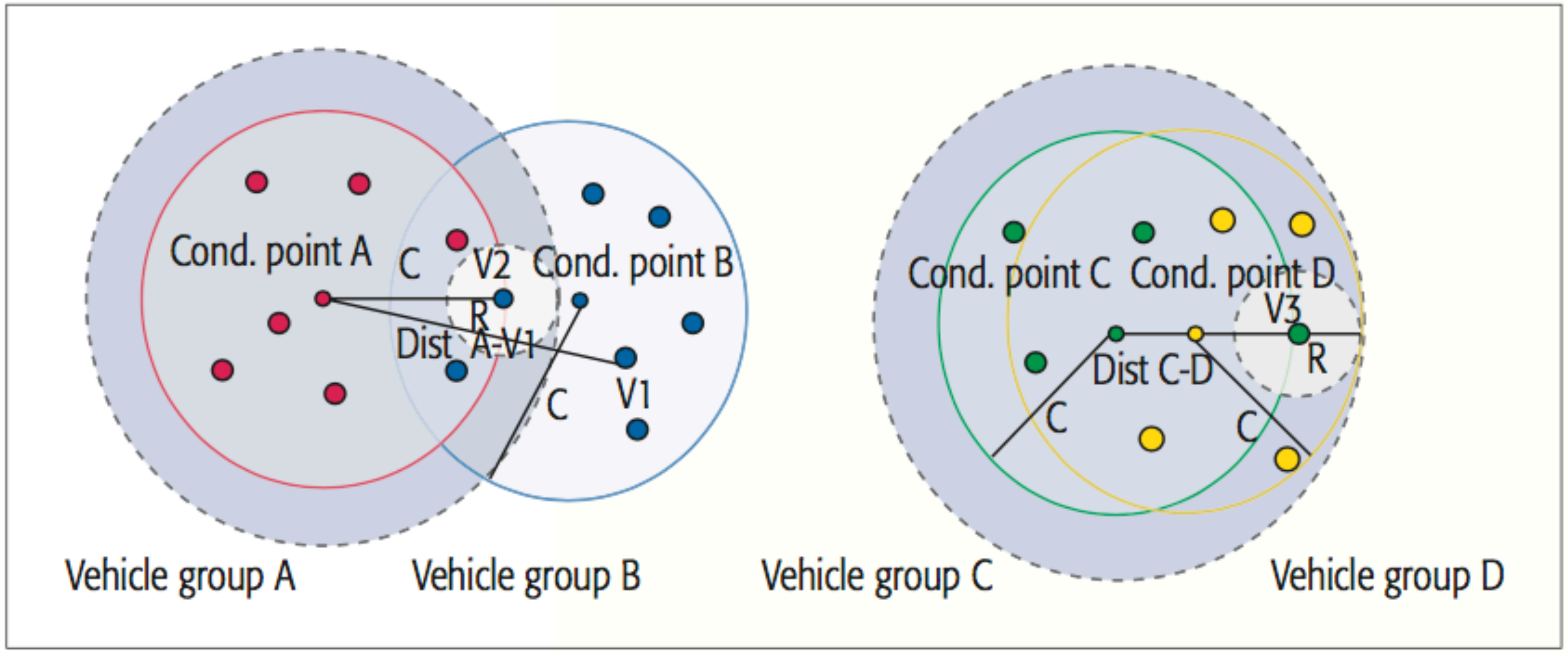


Figure 3. LBS content filtering mechanism with dynamic social group formulation in cloud-based IoT.

EFFICIENCY OF LBS CONTENT FILTERING MECHANISM IN SAVE

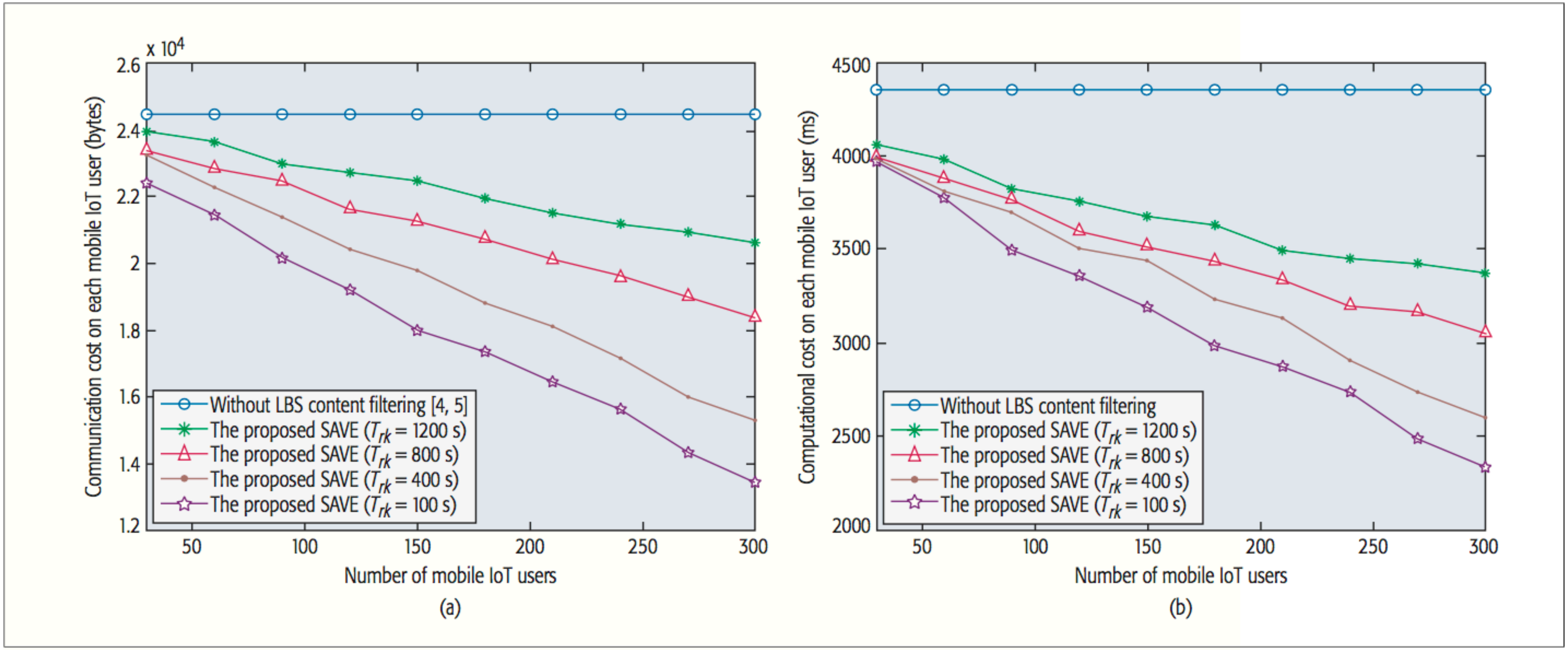


Figure 4. Efficiency of LBS content filtering mechanism in SAVE: a) communication cost; b) computational cost.

CONCLUSION AND OPEN RESEARCH ISSUES

- 5 challenging open research issues:

1. Fine-grained cipher- text access control in cloud-based IoT
   - proposed solution: designing a lightweight attribute-based encryption

2. Protection of location privacy and query privacy of cloud-based IoT users,
   - proposed solution: designing policy-hidden ABE exploiting the technique of a non-interactive proof system for bilinear groups

CONCLUSION AND OPEN RESEARCH ISSUES

3. Already proposed efficient privacy preserving technique
    - was only exploited for secure data collection from single user
      -> extend it

4. Privacy preserving outsourced data mining in cloud-based IoT

5. Extend the proposed efficient privacy preserving data aggregation method
    - without public key homomorphic encryption