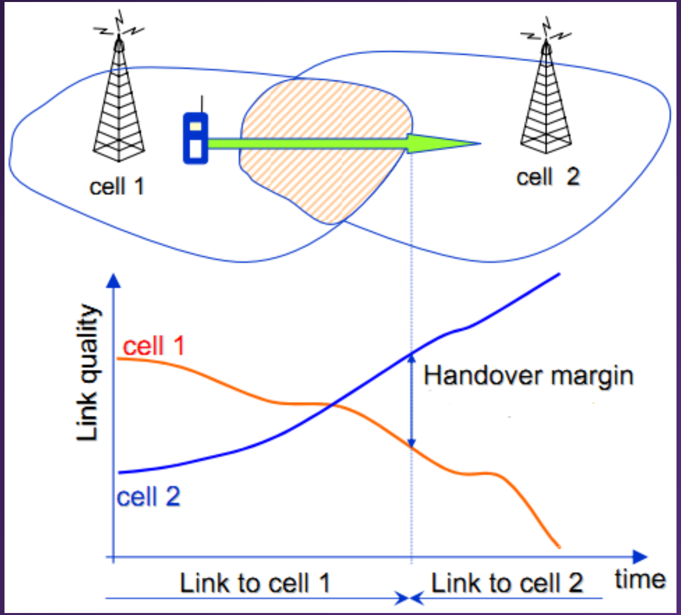
Security and privacy aware handover authentication for next generation mobile networks

Project Presentation By
18JE0746 Satyavart
Scholar : Prasanta Kumar Roy
Guide : Prof. Ansuman Battacharya

What is Handover?

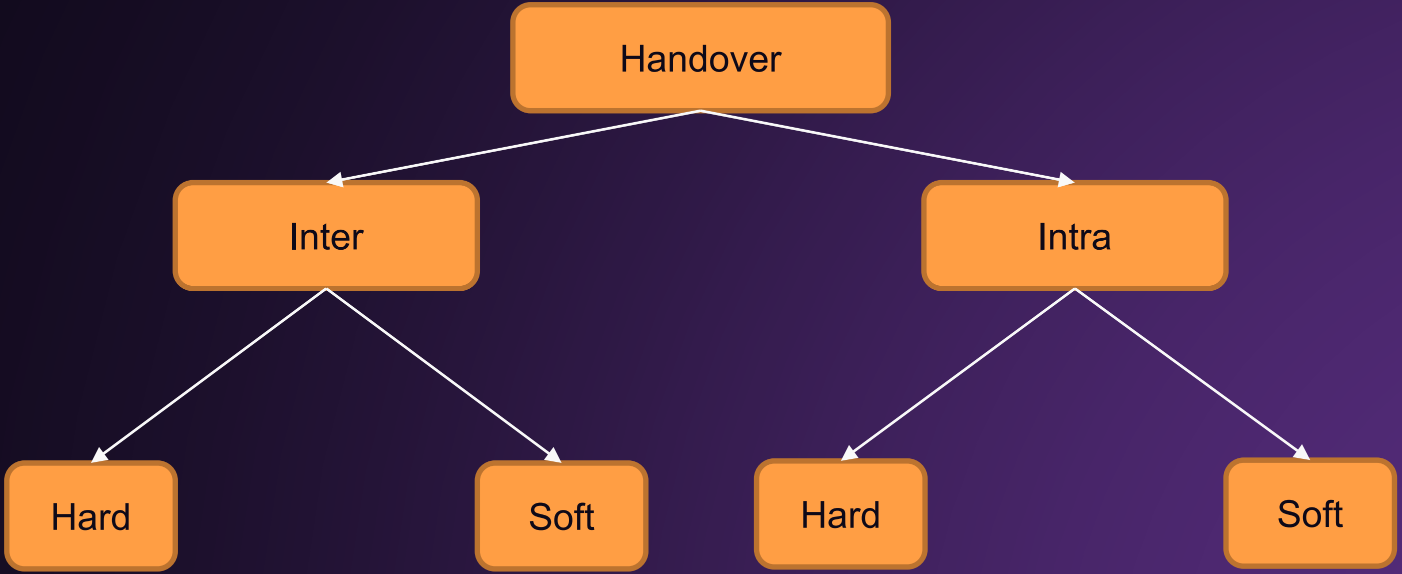
A handover is a process in telecommunications and mobile communications in which a connected cellular call or a data session is transferred from one cell site (base station) to another without disconnecting the session.

Cellular services are based on mobility and handover, allowing the user to be moved from one cell site range to another or to be switched to the nearest cell site for better performance.



- Handovers are a core element in planning and deploying cellular networks

Classification of Handover



Handover

Inter

Intra

Hard

Soft

Hard

Soft

Efficieny Requirement (LTE, LTE-A, 5G, Next Gen network)

- Increase system capacity
- Increase seamless mobility
- Higher resource utilization
- Improve coverage area

Note: Heterogenous Network Connectivity

Possible Solution

- Increasing small cell deployment density under macro cell coverage (cell spitting and cell sectoring).

- Logically centralized and physically distributed control over heterogenous network (EPC, SDM like approach).

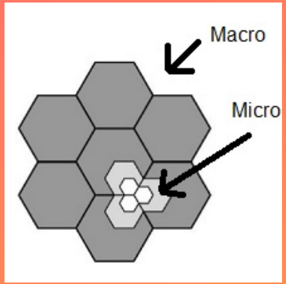
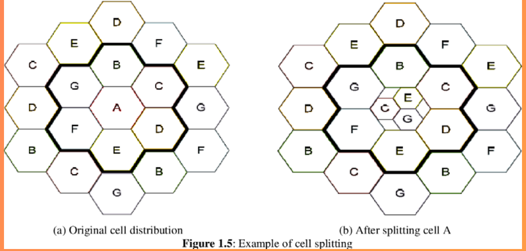


Fig.2 Cell splitting



(a) Original cell distribution

(b) After splitting cell A

Figure 1.5: Example of cell splitting

Fig.3 Cell Sectoring

Security Requirement

- Confidentiality
- Integrity
  - Entity Authentication
  - Data Authentication
- Availability
  - DoS
  - Desynchronization
- Resistant to active and passive attacks

- Session Key Secrecy
  - Forward/Backward Secrecy
  - Key Escrow
  - Ephemeral Secret Leakage
- Privacy
  - Conditional Privacy
  - Anonymity
  - Unlinkability

Possible Solution

- Mutual Authentication and Key Requirement
- Proper Key agreement
- Dynamic Key
- Desynchronization Resistant
- Dynamic Pseudonym
- Include short term and long term secrets

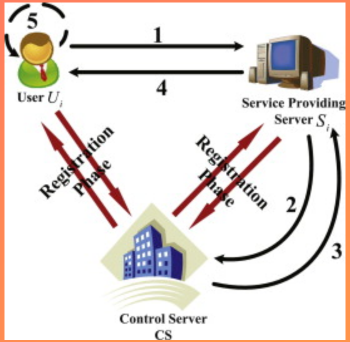


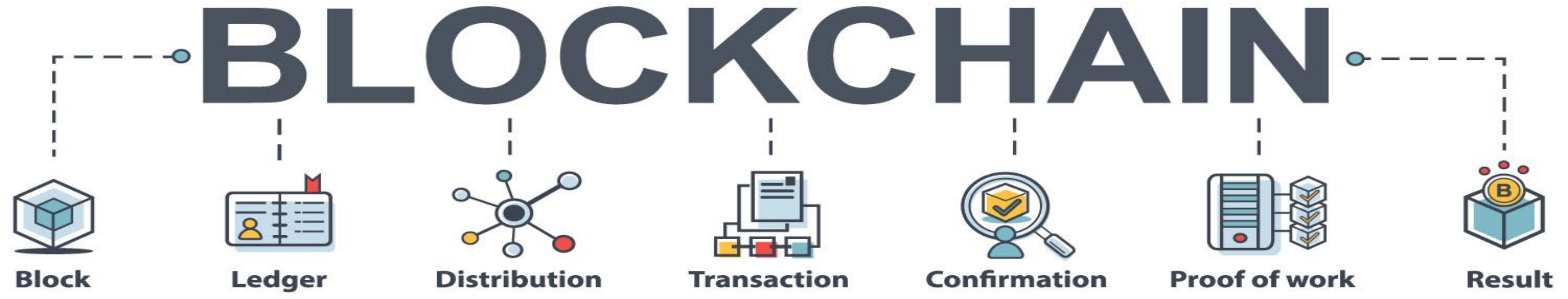
Fig.4 Dynamic Pseudonym illustration

Note: Reduced computational, communicational and storage overweight

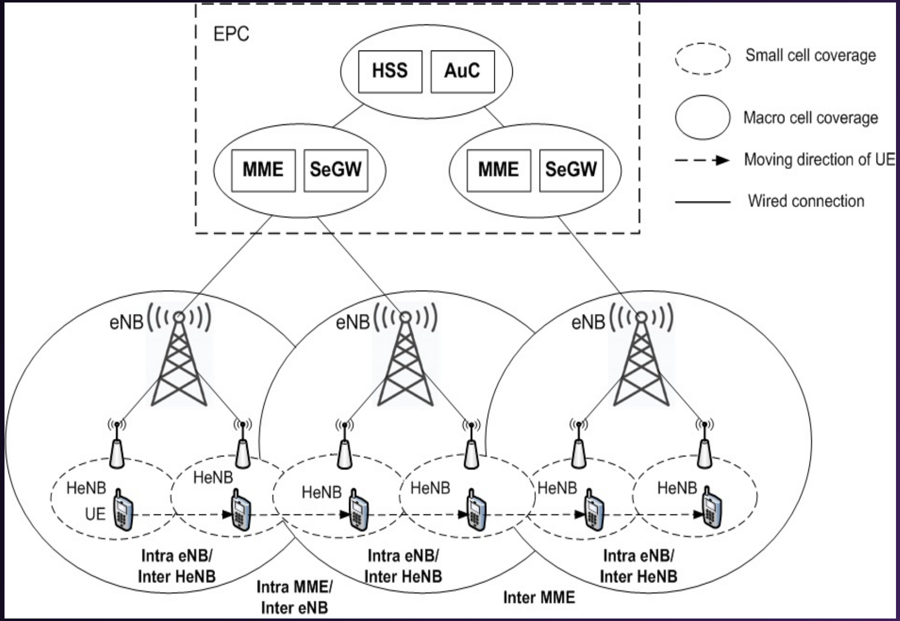
What is Blockchain?

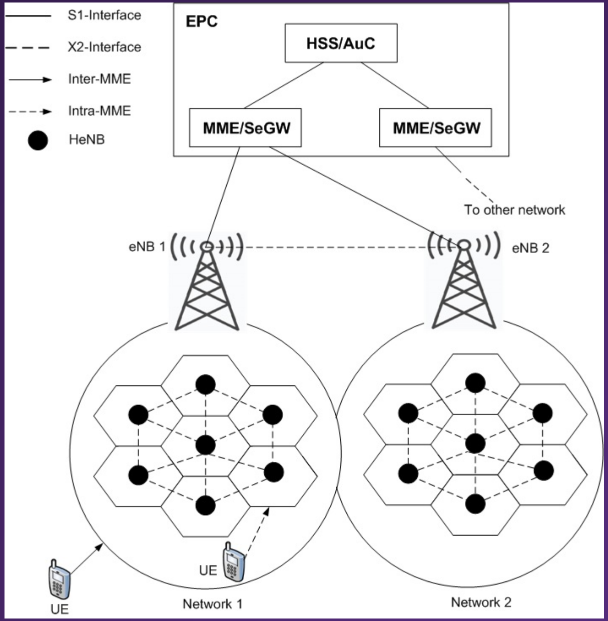
- Blockchain is **a system of recording information in a way that** makes it difficult or impossible to change, hack, or cheat the system.

- A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.



System Model





Security Model

Blockchain is proposed for implementation for secure and energy-efficient handover in distributed mobility management.

In this scheme, mutual authentication, confidentiality, integrity, FWS, nonrepudiation, user anonymity, and non-traceability can be guaranteed.

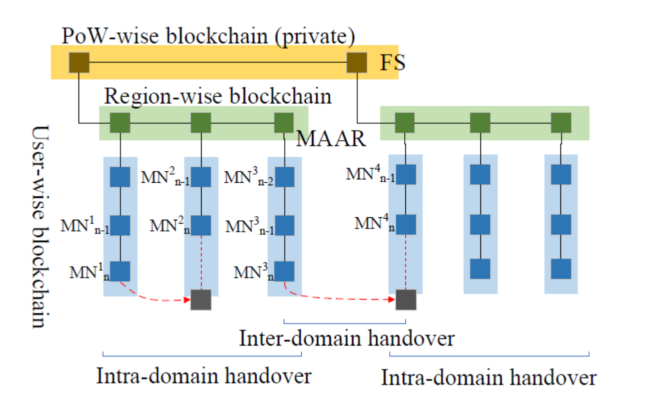
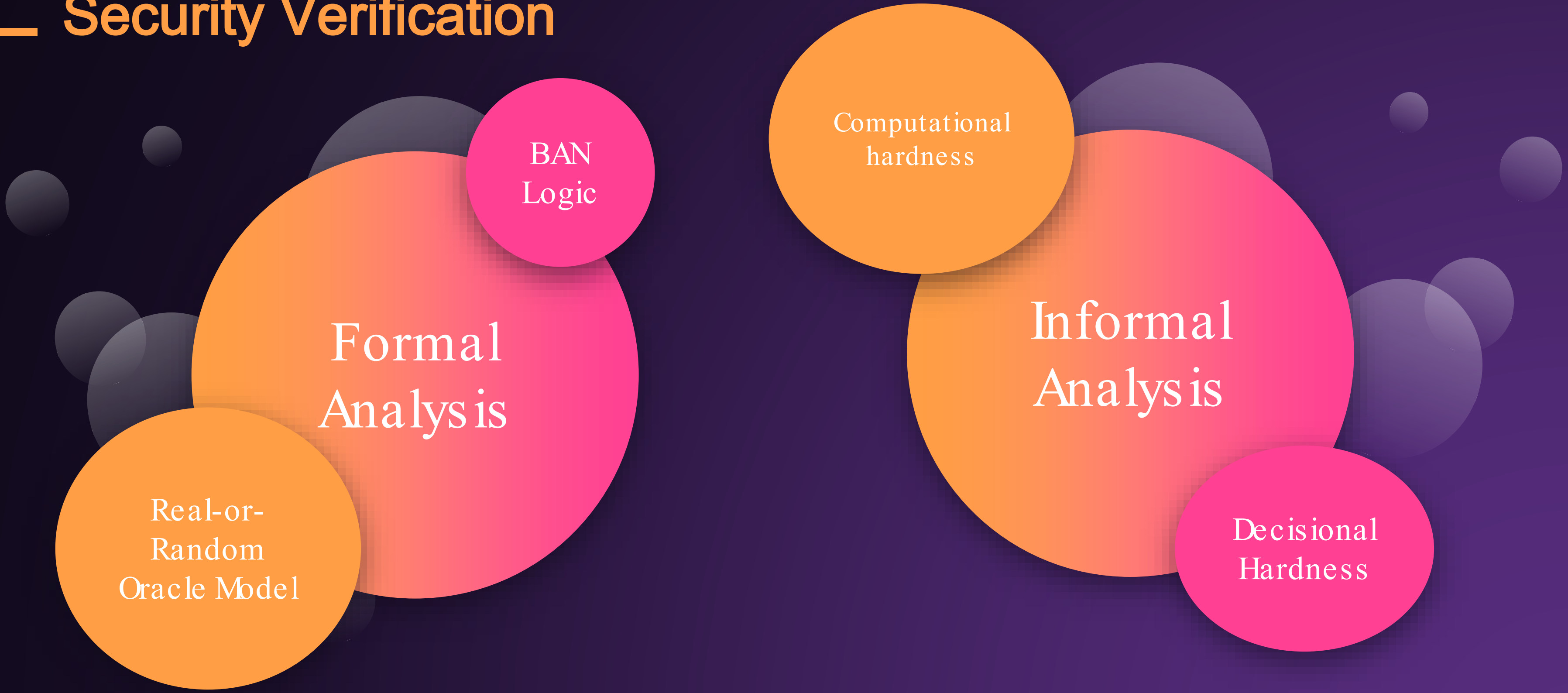


Fig. Structure of blockchain-based DMM

Security Verification



Formal Analysis

BAN Logic

Real-or-Random Oracle Model

Informal Analysis

Computational hardness

Decisional Hardness

Simulation Platform

- Security – AVISPA
- Computational Complexity – Python(pycryptodome, pycrypto, etc.)
- Blockchain – Python
- System Model – Discrete event network simulator (ns3, Oment++, Mininet, Mininet-WiFi)

References

- A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, “Authenticated key agreement scheme with user anonymity and untraceability for 5genabled softwarized industrial cyber-physical systems,” IEEE Transactions on Intelligent Transportation Systems, 2021
- R. Canetti and H. Krawczyk, “Universally composable notions of key exchange and secure channels,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2002, pp. 337–351
- C.-C. Chang and H.-D. Le, “A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” IEEE Transactions on wireless communications, vol. 15, no. 1, pp. 357–366, 2015
- Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426(1871), 233-271 (1989).
- “Desynchronization resistant privacy preserving user authentication protocol for location based services”, PK Roy, A Bhattacharya, Peer-to-Peer Networking and Applications 14 (6), 3619-3633
- “A group key-based lightweight Mutual Authentication and Key Agreement (MAKA) protocol for multi-server environment” ,PK Roy, A Bhattacharya, The Journal of Supercomputing, 1-28
- “Secure and efficient authentication protocol with user untraceability for global roaming services “, PK Roy, A Bhattacharya, Wireless Networks, 1-18
- “Is 5G Handover Secure and Private? A Survey” Dongsheng Zhao, Zheng Yan, Senior Member, IEEE, Mingjun Wang, Peng Zhang, and Bin Song, Senior Member, IEEE

THANKS!