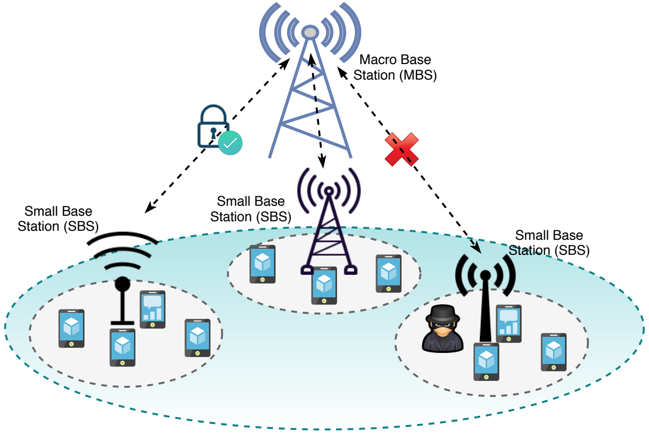
Lightweight Authentication Protocol for Inter Base Station Communication in Heterogeneous Networks

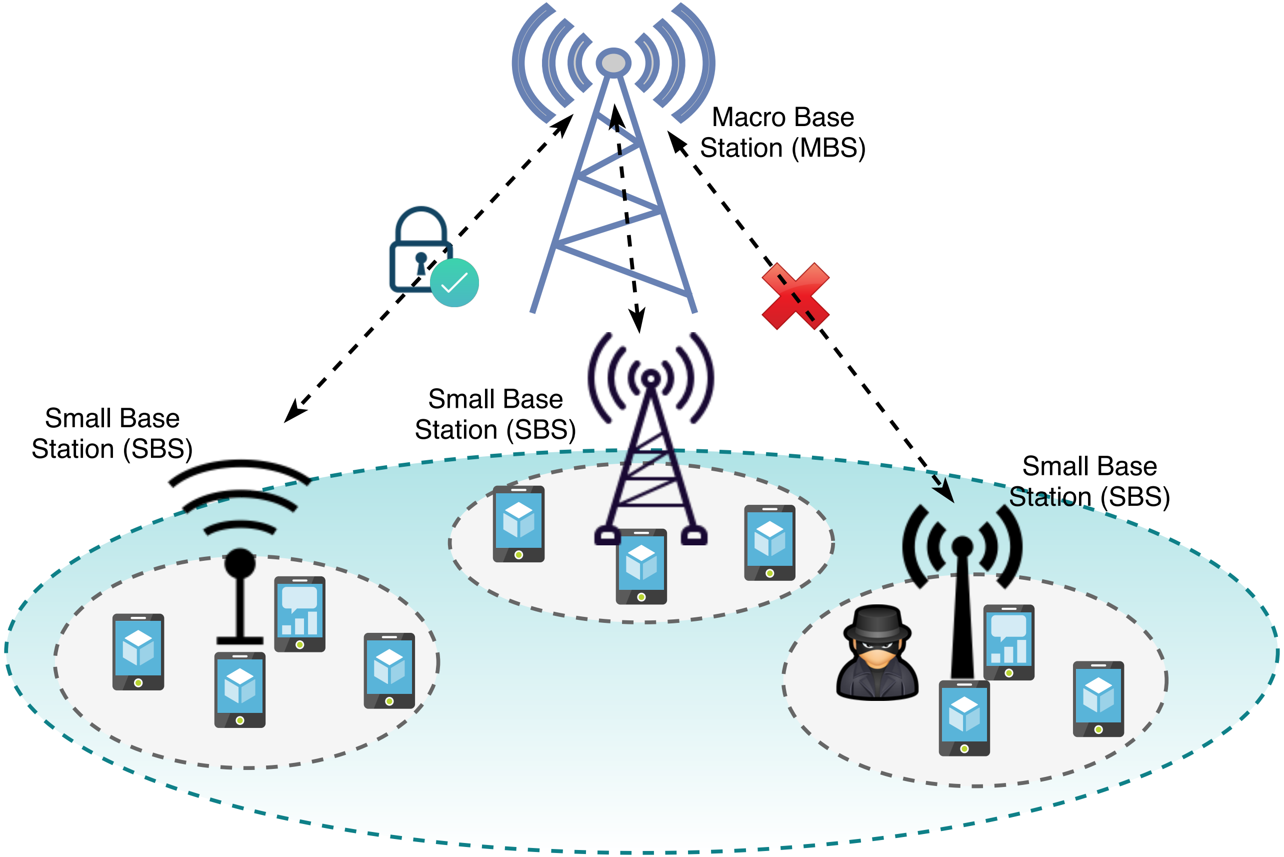
Authors: Gaurang Bansal*, Vinay Chamola**

* Department of Computer Science, BITS Pilani, India
** Department of Electrical and Electronics Engineering, BITS Pilani, India

- **HetNet** involves a mix of radio technologies and cell types working together seamlessly.
- Deploys short-range, low-power, and low-cost base stations operating in conjunction with the main macro-cellular network infrastructure.
- **Low power nodes (LPNs)** are deployed to eliminate coverage holes in outdoor and indoor environments. Also increases the capacity/area of the network.
- **LPNs** include micro, pico, Remote Radio Heads (RRH), relay and femto nodes.



System Model



Existing Problems:

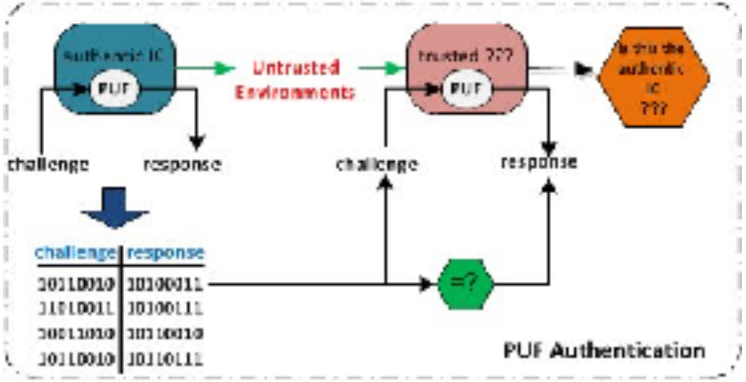
- Ensuring privacy and security in communications
- Cannot be under 24x7 human supervision
- Device tampering attacks

Possible Attacks

- Adversary may tap any communication
- Change, manipulate and withhold data
- Packet Injection
- Impersonate Base Stations
- Try to initiate sessions
- Physical Attack / Device Capture Attack

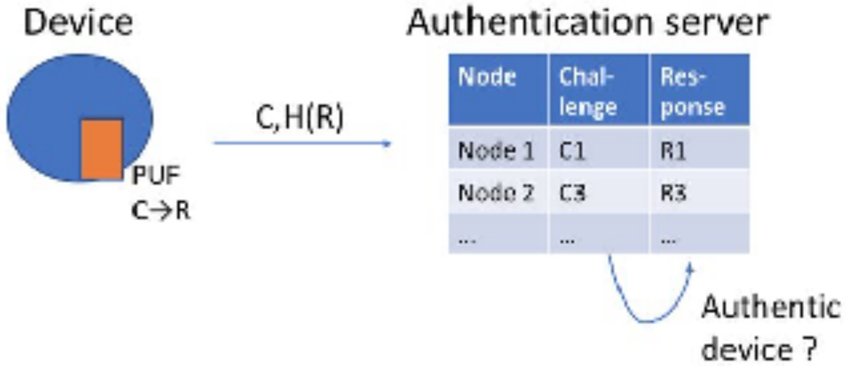
Solution ?

Physical Unclonable Function (PUF) Based Mutual Authentication



challenge	response
10110010	10100011
11010011	10100111
10011010	10110010
10110010	10110111

SRC: https://www.researchgate.net/publication/319004864_Design_and_Architecture_of_Hardware-based_Random_Function_Security_Primitives/figures?lo=1



Node	Chal-lenge	Res-ponse
Node 1	C1	R1
Node 2	C3	R3
...	...	...

SRC: https://www.researchgate.net/publication/327131986_PUF_based_authentication_protocol_for_IoT/figures?lo=1&utm_source=google&utm_medium=organic

Physical unclonable Function (PUF)

- ***A physical unclonable function (sometimes also called physically unclonable function), or PUF, is a physically-defined "digital fingerprint" that serves as a unique identifier for a semiconductor device such as a microprocessor*** - Wiki

- Similar to and as unique as the biometrics of a human.
- Uniqueness comes from physical microstructure variations during fabrication.
- Every single BS can have its own unique “fingerprint”.
- Cannot be cloned or reproduced.

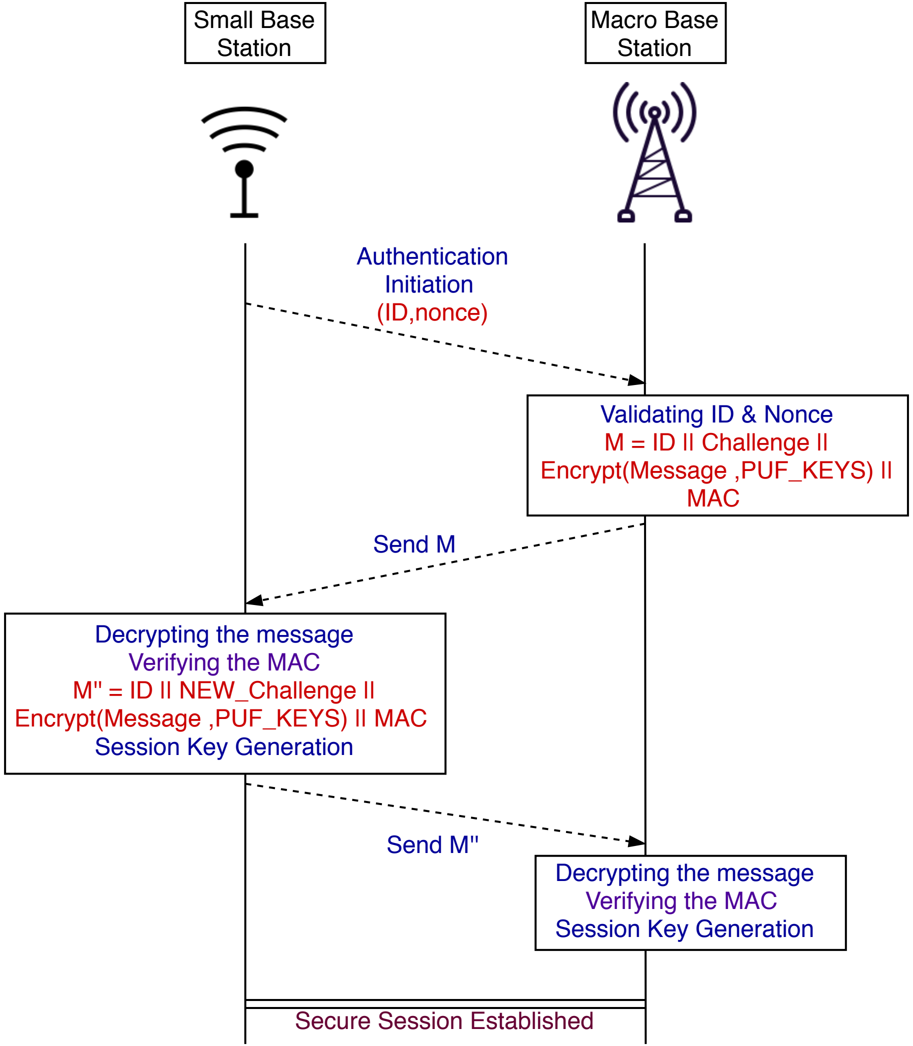
K = PUF(C) { C: Challenge, K: Response }

PUF Properties

1. If an input C is given to the same PUF many times, it produces the same response K.
2. If the same input C is given to different PUFs, the responses obtained from each PUF differ greatly from each other.

Assumptions

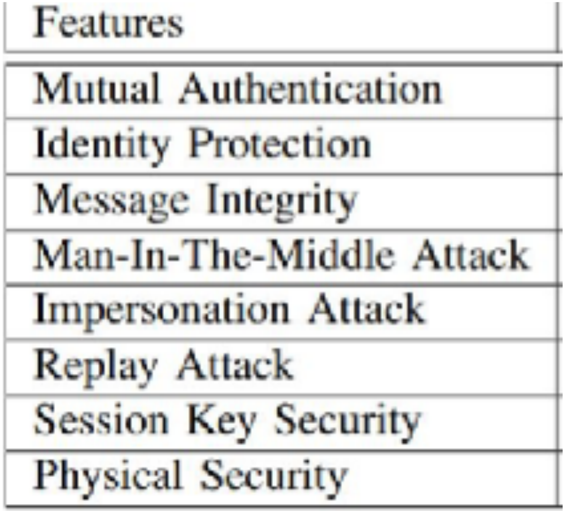
1. PUF is a small hardware component that is present with each participating device and is unique.
2. The communication between a device and its PUF is secure and tamper-proof.


Small Base Station
Macro Base Station
Authentication Initiation
(ID,nonce)
Validating ID & Nonce
M = ID II Challenge II
Encrypt(Message ,PUF_KEYS) II
MAC
Send M
Decrypting the message
Verifying the MAC
M'' = ID II NEW_Challenge II
Encrypt(Message ,PUF_KEYS) II MAC
Session Key Generation
Send M''
Decrypting the message
Verifying the MAC
Session Key Generation
Secure Session Established

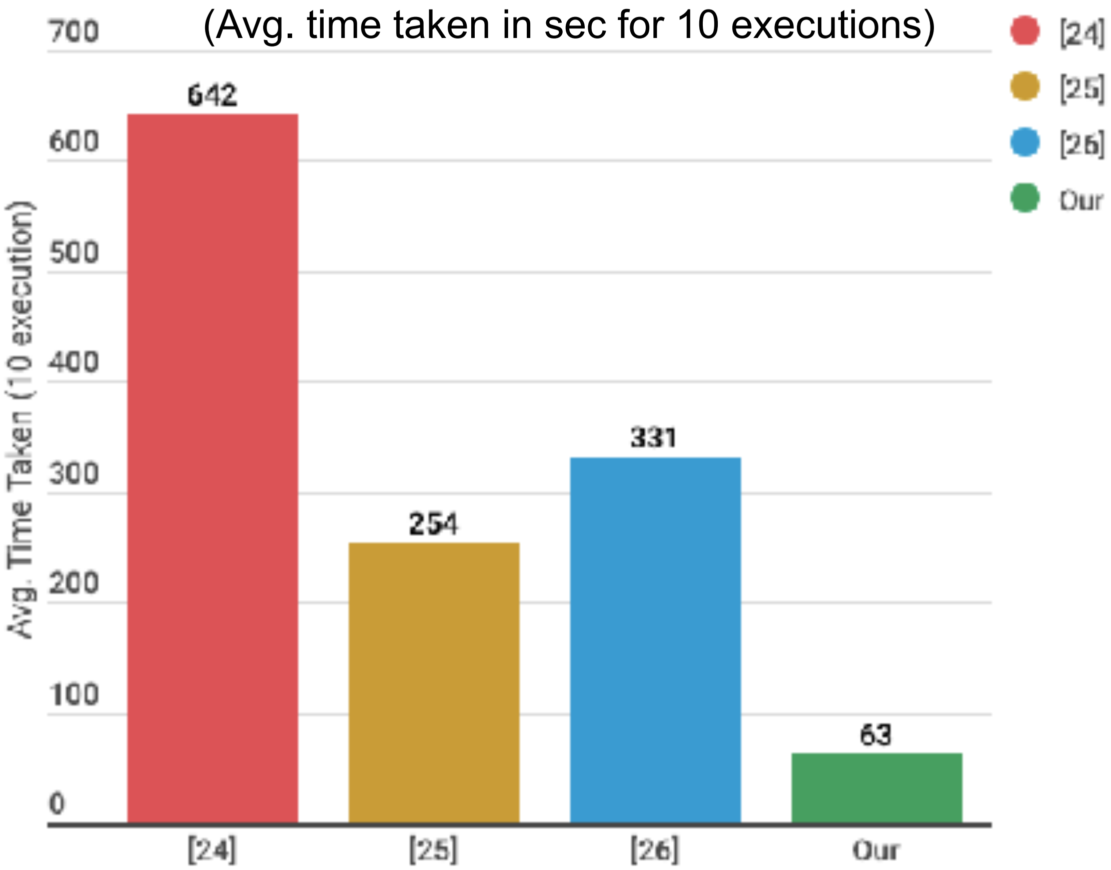
Key takeaways from protocol

- Feistel Structure Based Encryption
- Using Nonce for Freshness
- Lightweight block based encryption mechanism
- Message Authentication Code (MAC) [data integrity]
- Challenge Response Updation (each session)
- Single CRP Storage
- PUF dependent session keys in both stages
- Alias Naming (Privacy Preserved)

Performance Comparison



Features
Mutual Authentication
Identity Protection
Message Integrity
Man-In-The-Middle Attack
Impersonation Attack
Replay Attack
Session Key Security
Physical Security



(Avg. time taken in sec for 10 executions)

Thank you !