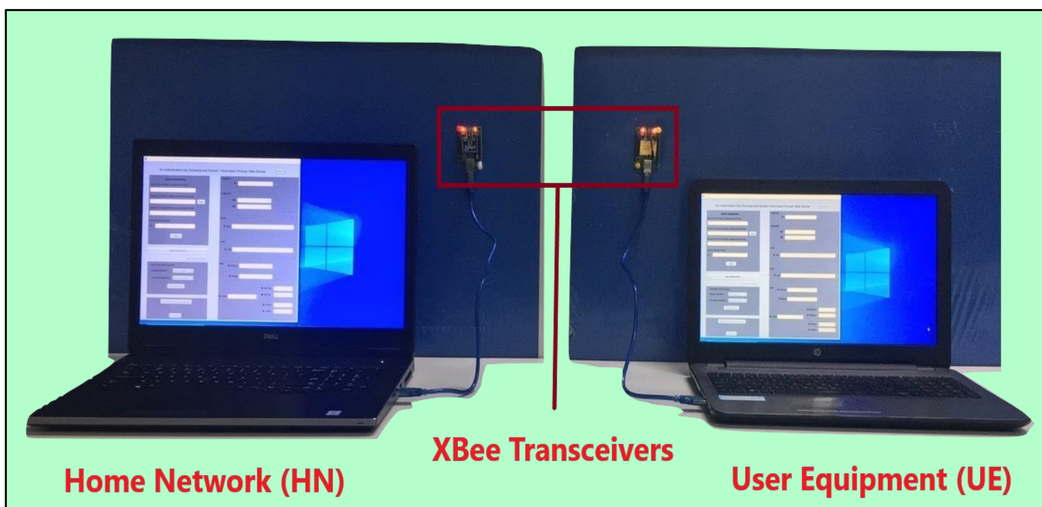
Implementation of 5G Authentication and Key Agreement Protocol on XBee Networks

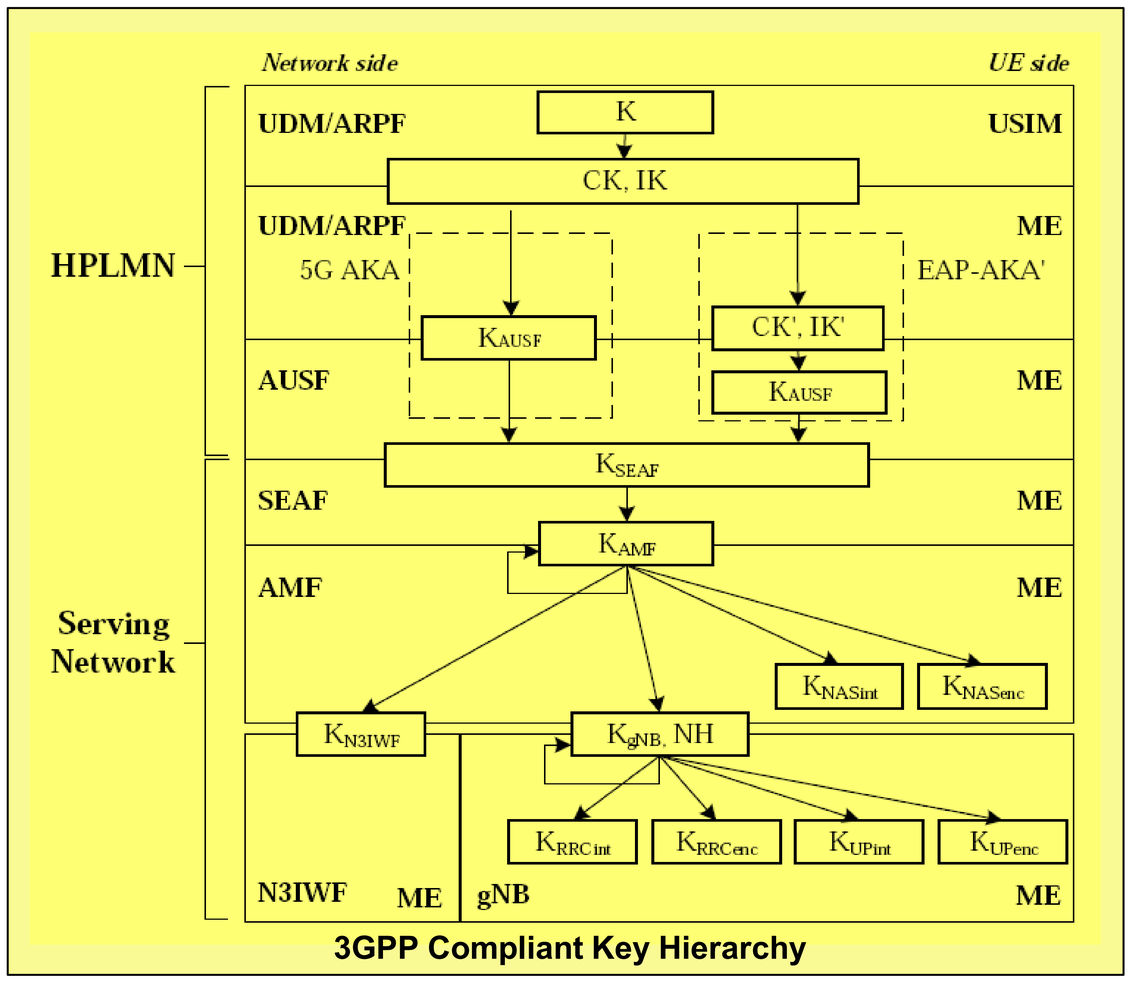
5G- Security Group

ABSTRACT

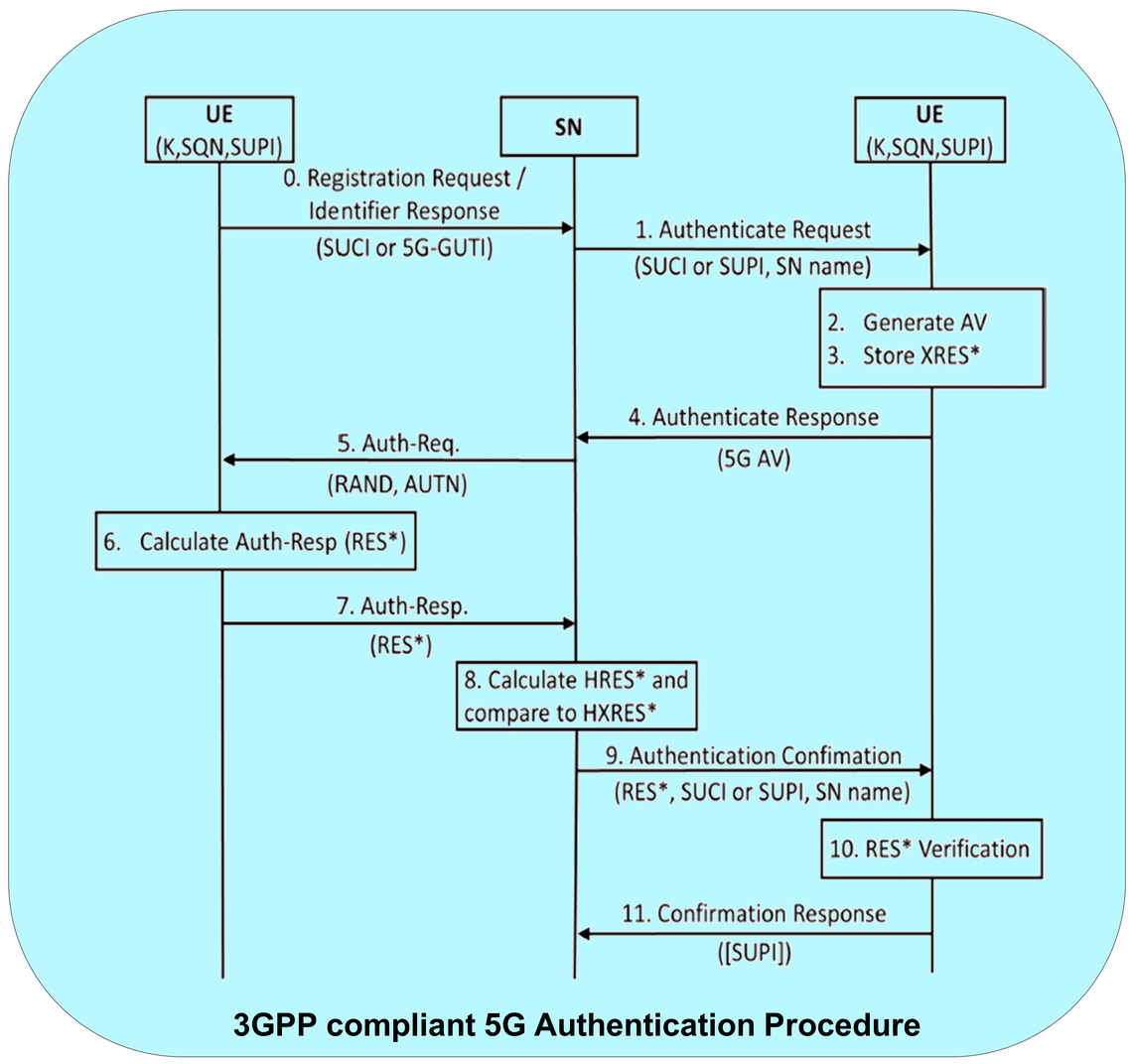
This demonstration provides first hand collation and description of state-of-the-art details on 5G security architecture in a simple and unified manner. We implement the 3GPP compliant 5G-AKA protocol on a network of XBee S2C devices wherein the protocol involves a sequence of modules involving secure authentication, key exchange and payload transmission. To implement the security protocol, we extract the precise recommendations of 3GPP and also use open-source algorithms wherever the implementation. is left open as proprietary solution.



Test bed comprising XBee devices emulating a UE and a home network as part of 5G



3GPP Compliant Key Hierarchy



3GPP compliant 5G Authentication Procedure

4G vs 5G

- Service based architecture – modularization of control plane
- Use of asymmetric encryption instead of symmetric
- Encryption of SUPI with public key of home operator (SUCI)
- Routing information (home network ID) in clear
- SUPI revealed to VPLMN only after authentication
- Binding of SUPI into key
- UE and HPLMN have to use the same SUPI: requested for lawful intercept purposes
- Respond to identifier request with SUCI
- No SUPI based paging

KEY TAKEAWAY FROM DEMO

- **Collation of the essential documents required for implementation of 5G security architecture.**
- **Implementation of 3GPP compliant, prescribed security architecture which involves authentication, key exchange and secure payload transmission.**
- **Implementation has been done using standard devices such as XBee S2C and terminal equipment etc.**
- **Depiction of the modular hierarchical key exchange process in home network (HN) and User equipment (UE). This is shown in the dedicated user interface developed for the demonstration.**
- **Depiction of MAC and SYNC failure in case of non matching key between UE and HN.**

ACKNOWLEDGEMENT

This work is funded by the Indigenous 5G Test Bed project from the Department of Telecommunications, Ministry of Communications, New Delhi, India.

REFERENCES

[1] ETSI TS 135 206 V16.0.0 (2019-11).
[2] ETSI TS 133 501 V16.0.0 (2019-11).
[3] ETSI TS 133 102 V16.1.0 (2019-04).
[4] D. Basin, J. Dreier, L. Hirschi, S. Radomirovi ́c, R. Sasse, and V. Stettler, "Formal analysis of 5G authentication," ArXiv e-prints, Oct. 2018.
[5] R. P. Jover and V. Marojevic, " Security and Protocol Exploit Analysis of 5G Specifications," ArXiv e-prints, Nov. 2018.