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

5G- Security Group

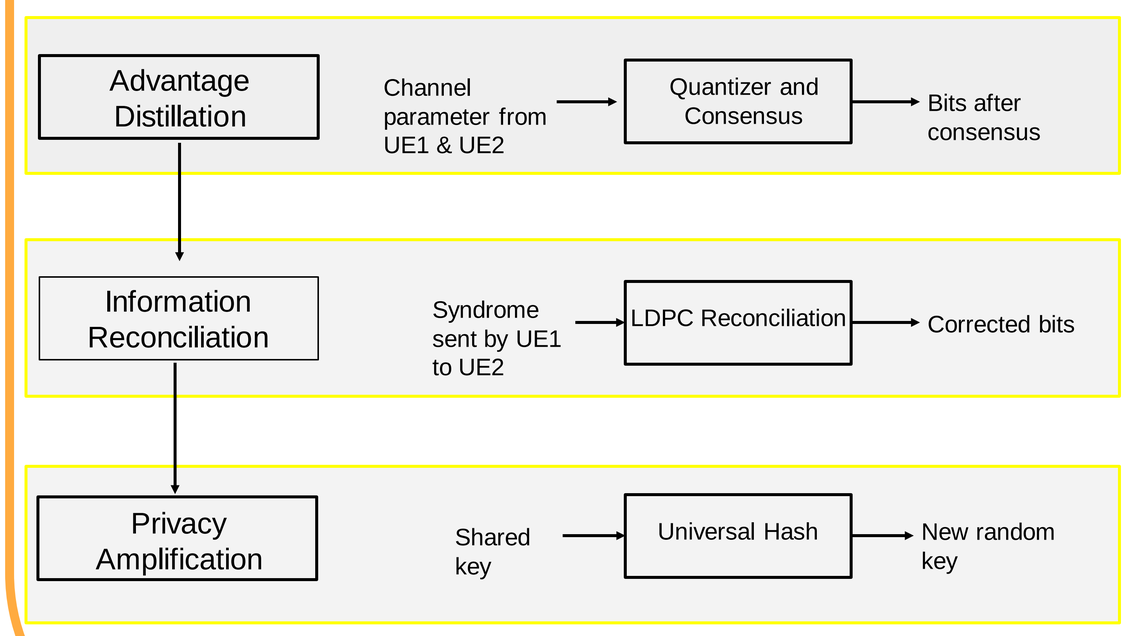
Dynamic Key Generation for D2D communication

Abstract

In this demonstration, we showcase a physical-layer key generation mechanism between two 5G-compliant User Equipment (UE) devices that operate in a D2D fashion. To present our ideas, we use a network of three XBee devices, wherein one of them acts as a base-station and the other two play the role of UEs. In order to ensure end-to-end privacy, the two UEs first authenticate with the base-station by using the standard 5G AKA protocol, and subsequently request the base-station to facilitate the design of a quantization algorithm, which in turn will be used by them to implement a physical-layer key generation mechanism for securing communication in the D2D mode. Our demonstration shows that key-exchange algorithms using physical-layer methods are feasible for implementation on 5G-compliant devices, and such methods should be considered to ensure end-to-end privacy for D2D communication in the 5G architecture.

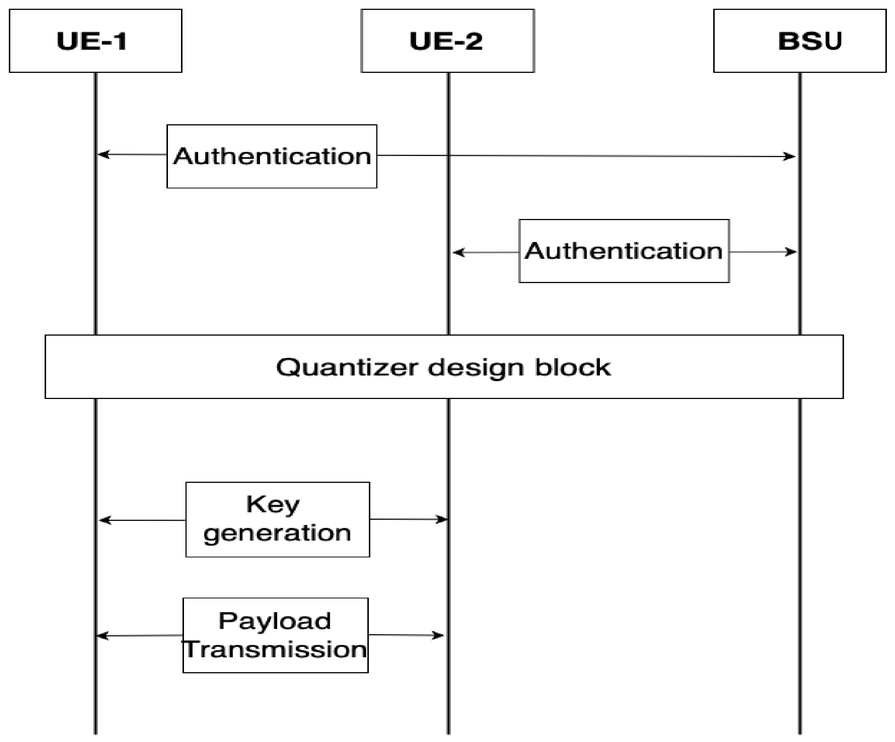
Dynamic Key Generation

- Known pilots are exchanged between the two UEs to estimate correlated random channel state sequence (RSSI in XBees)
- Base Station Unit (BSU) observes joint channel characteristics between the two UEs and designs the optimal quantizer
- Both the UEs quantize their long sequences into bits with the same quantizer and apply consensus algorithm on the sequence
- LDPC reconciliation is done so as to correct mismatches in bits
- Zero mismatch scheme corrects every disagreement in bits
- Privacy amplification compensates for public data revealed in above steps and gives random key
- Keys are then used by 3GPP compliant encryption schemes for payload transmission



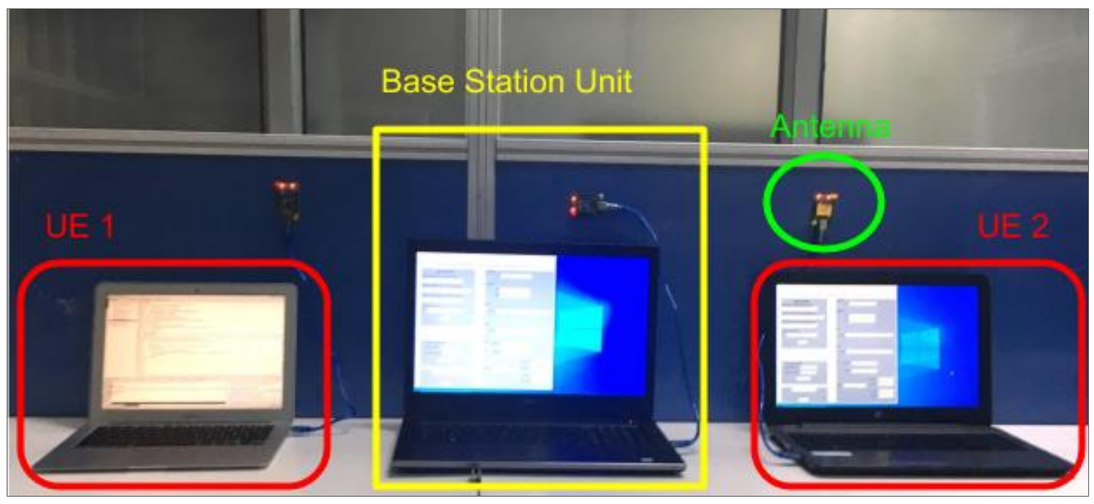
Model

- UEs' embedded secret key is used for authentication with the BSU
- A set of keys compliant with 3GPP standards is derived for the two wireless links (UE-1 to BSU and UE-2 to BSU)
- BSU facilitates UEs by designing appropriate quantizer for DKG by observing their joint channel characteristics
- DKG scheme is then initiated to achieve end-to-end privacy



Testbed Setup

- Testbed comprises of a Base Station Unit (BSU) and two UEs
- The two authenticated UEs want to communicate to each other in the available D2D fashion
- BSU facilitates them to achieve an end-to-end privacy by using DKG scheme



Acknowledgement

This work is funded by the indigenous Test Bed project from the Department of Telecommunication, Ministry of Communication, New Delhi, India.

Reference:

S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik, "Radio- telepathy: extracting a secret key from an unauthenticated wireless channel," in ACM MobiCom '08, September 14-19, 2008, pp. 128–139, 2008