Physical layer authentication for automotive cyber physical systems based on modified HB protocol

Ahmer Khan JADOON, Jing LI, Licheng WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-020-0010-4

Problems & Ideas

- Problems of physical layer secret keys generation schemes are:
  - Current state-of-the-art methods uses information reconciliation schemes to correct mismatched bits by exchanging information over a public channel. This can be an immense security threat as it may let an adversary attain and recover segments of the key in known channel conditions.
  - Existing methods uses HASH function for privacy amplification due to the exchange of information over a public channel, which causes a computation workload.
- Ideas: HB protocol based Physical layer authentication:
  - The information collected from the shared channel is used as secret keys for the HB protocol and the mismatched bits are used as the induced noise for learning parity with noise (LPN) problem.
  - The HB protocol works on the LPN problem which does not require reconciliation of mismatched bits and HASH function.

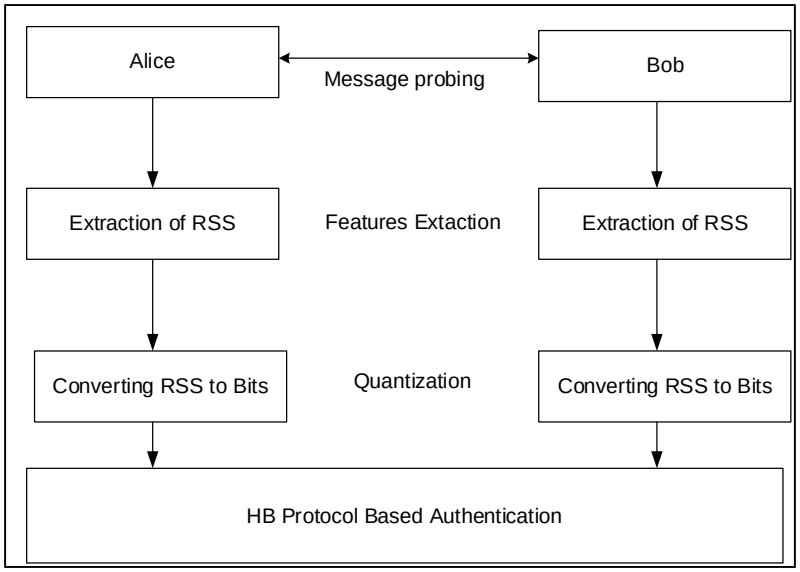

Fig. 1: Physical layer based authentication using HB protocol.

Main Contributions

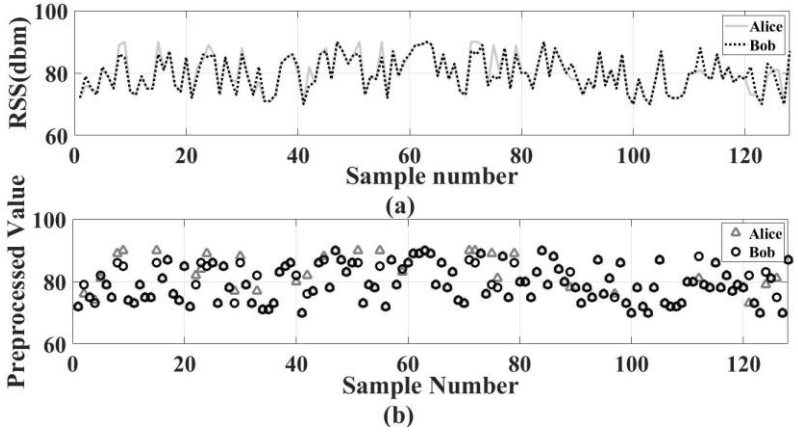

Fig. 4: (a) RSS values extracted for Alice and Bob,
(b) Pre-processed values for Alice and Bob.

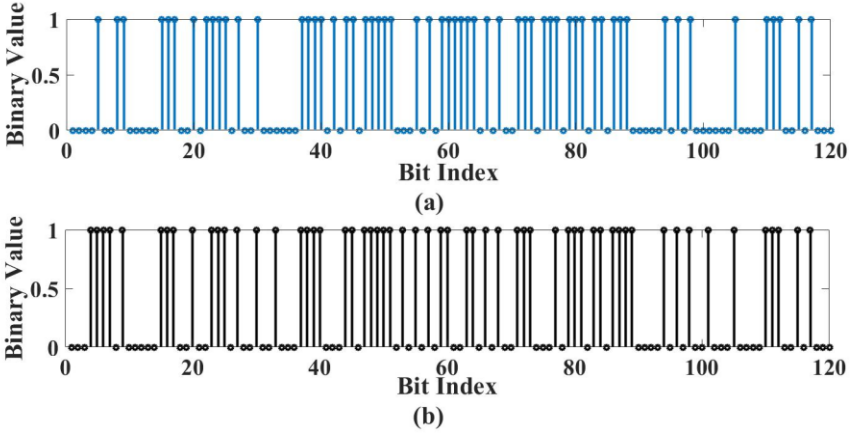

Fig. 5: (a) Secret key generated for Alice,
(b)Secret key generated for Bob.

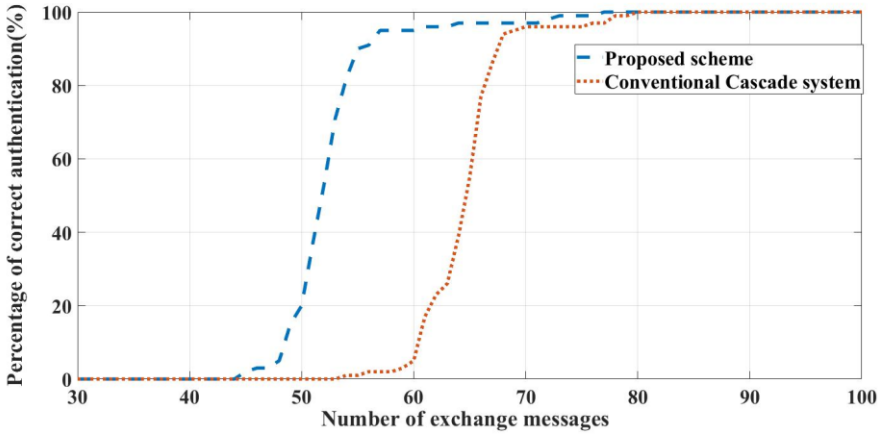

Fig. 6: Rate of Authentication VS Exchange Messages.