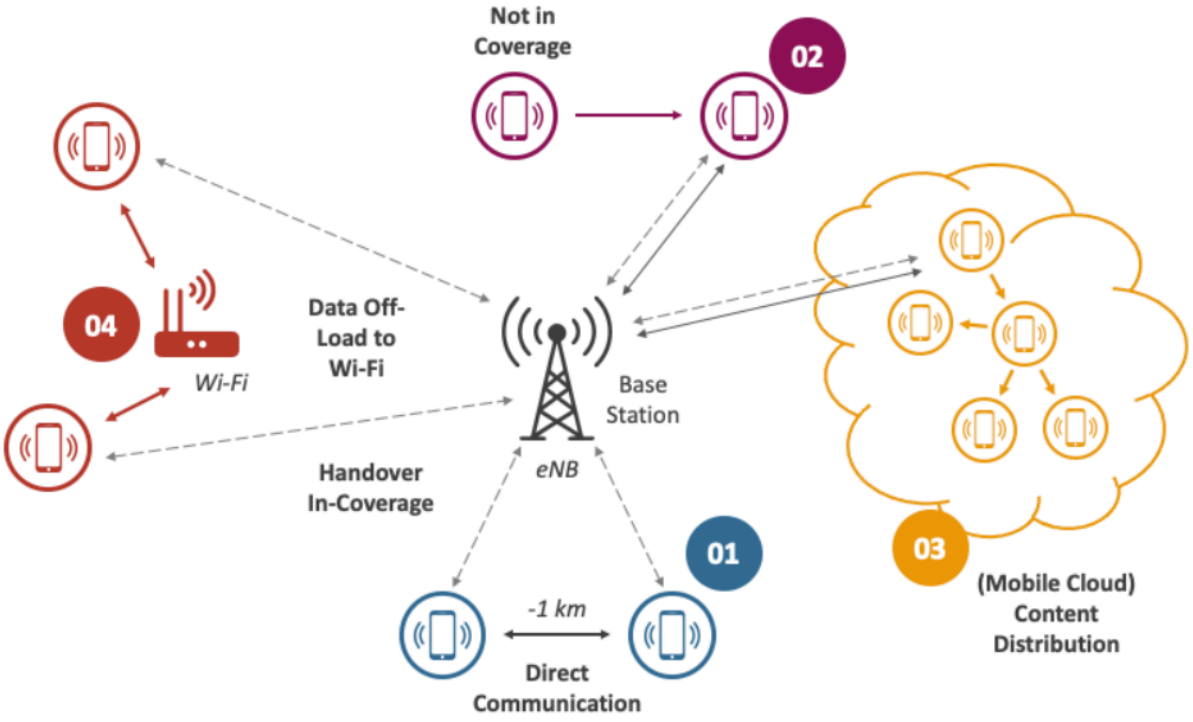
Secure Data Transmission in Device-to-Device (D2D) Communication via HMAC :

Project topic adaptable for Oberseminar Informationstechnik 2025/2026



Reference : www.collidu.com

Objective of Work

Network coding has emerged as a promising technique for optimizing network communication, particularly over lossy links. It is especially effective in wireless networks, where intermediate nodes can perform *recoding* to enhance reliability and throughput. A widely adopted approach is Random Linear Network Coding (RLNC). In RLNC, packets are typically equipped with CRC checksums to detect errors caused by intentional *pollution attacks* or unintentional *channel noise*. However, once a packet is corrupted, new CRC checksums cannot be calculated for the recoded packets since access to the original packet is lost. A potential solution is to replace CRC checksums with Homomorphic Message Authentication Code (HMAC) tags, enabling the combination of polluted packets without the need for checksum re-calculation, thus allowing these packets to participate in the recoding process. This study aims to evaluate the performance of HMAC tags in detecting both intentional and unintentional packet modifications and to analyze the trade-offs involved in using tags instead of CRC checksums.

In the thesis, the following tasks should be addressed:

- Conduct literature research on Random Linear Network Coding (RLNC), CRC checksum and Homomorphic Message Authentication Codes (HMAC)
- Understand the trade-off between CRC checksums and HMAC tags in terms of security, computational complexity and communication overhead.
- Develop a simulation framework to investigate the impact of payload size and keypool size on the performance in terms of computational complexity, security and communication overhead.
- Present the results in a scientific way.

Material for Further Reading

- An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks | International Journal of Information Security
- Padding for orthogonality: Efficient subspace authentication for network coding | IEEE Conference Publication | IEEE Xplore

Keywords

random linear network coding, HMAC, CRC, security, computational complexity, overhead,

Contact Details

- Supervisor: Mehmet Akif Kurt (mehmet_akif.kurt@tu-dresden.de)
  Hosein Kangavar Nazari (hosein.kangavar_nazari@tu-dresden.de)
- Language: English