Paper Review: A Physical Layer Endogenous Security Architecturewith Dynamic Slicing Encryption for IoT

isomo

February 10, 2025

NOTE: Here is the second review of the paper. The first review process involved two reviewers; the first decided it only needed minor fixes. The two reviewers talked about the paper's extension for future work, noting not many issues regarding the scheme proposed by the paper.

1 Quick Look at the Paper

1.1 Abstract

We propose a novel physical layer endogenous security (PHY-ES) architecture with a dynamic slicing encryption (DSE) scheme for the physical layer of Internet of Things (IoT) systems.

We present the algorithm for the scheme, and give its performance evaluation method with parameters of data life cycle (DLC), average cost (AC) and deciphering probability.

Compared with other schemes, the SEK-based DSE scheme can reduce the DLC and AC by about 42% and 35% on average, respectively.

1.2 Introduction

However, the above schemes or protocols based on the traditional architecture lack an independent security function layout and corresponding transmission control channels, and the current physical layer of IoT cannot secure the sensing data traffic of the uplink channels. Therefore, it is necessary to re-plan and re-construct the physical layer architecture of the IoT.

To the best of the authors' knowledge, there exist no reports of a solution that combines suitable physical layer architectures and security functions without using external key source systems for IoT sensing data in the physical layer. Therefore, we propose a novel physical layer endogenous security (PHY-ES) architecture with sensing endogenous keys (SEKs) based dynamic slicing encryption (DSE) scheme for IoT. not only supports basic physical layer functions, but also provides both endogenous encryption and decryption functions for sensing data.

2 Issues

- The figure not clear enough, need to be svg format.

- The Performance Comparison of the DES item is not only the KGNet and BCFL key generation schemes compared with the DES, should compared the work similar the SEK, which encryption on the physical layer.

- The Security Analysis should add like the chosen-text attack, etc. (Not sure the Chosen-text attack is can run this scheme, but have other attack can run this scheme.)

- if above the physical layer of the sensing data is security, the security of the physical layer of the IoT system can be guaranteed. Not need the encryption on the physical layer. (Have similar work, so have some significant.)