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

isomo

February 11, 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.

- PHY-ES Architecture Providing both Endogenous Encryption and Decryption Functions
- SEK-based DSE Scheme: A SEK-based DSE scheme is proposed, where the SEKs are generated by quantifying the randomness of the sensing data, without the need for any external key sources to encrypt the sensing data in the physical layer directly.
- Novel SEK-based DSE Algorithm and its Experimental Platform

1.3 Algorithm of SEK-based DSE Scheme

According to the SEK-based DSE scheme, we give the corresponding algorithm as follows

$$Y = E(X) = \prod_{v=1,2,3} E_v(X) = E_1\{E_2[E_3(X)]\} \tag{1}$$

Algorithm 1 Algorithm E_1

Require: Input: $X_1 = X$; Require: Y_1

for $j = 1:1:L$ **do**
  $E_1(j) = 0$
  for $i \leftarrow 1$ **to** S **do**
    $E_1(j) = \text{Calculate}[E_1(j), X_1(i,j)]$
  end for
  $Y_1(j) = E_1(j)$
end for
output $[Y_1(1), \ldots, Y_1(L)]$

Algorithm 2 Algorithm E_2

Require: Input: $X_2 = Y_1$; Require: $K = Y_2$

1: initial $B = \lfloor L/S \rfloor$
2: **for** $i = 1 : 1 : S$ **do**
3: $\quad Y_2(i) = X_2 \cdot E_2(i) = Y_1 \cdot (O_1, \ldots, I_i, \ldots, O_S)'$
4: **end for**
5: **output** $K = Y_2 = \begin{bmatrix} Y_2(1) \\ \vdots \\ Y_2(S) \end{bmatrix}$

Algorithm 3 Algorithm E_3

Require: Input: $X_3 = X$ and K; Require: $Y = Y_3$

1: initial $T = (T_1, \ldots, T_S)$
2: **for** $i = 1 : 1 : S$ **do**
3: $\quad Y_3(i) = E_3[X_3, i, T_i]$
4: **end for**
5: **output** $Y = Y_3 = \begin{bmatrix} Y_3(1) \\ \vdots \\ Y_3(S) \end{bmatrix}$

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 Algorithm of E1-E3 and D, not use the algorithm name symbol on the algorithm, it confusion with the recursive function.
- The Algorithm E3 the i-th row K how to inserted to i-th row X please more detail.
- The Security Analysis should add like the chosen-text attack, etc. example, if the chosen-text all the one bit, then the Initial SEKs K is all zero when the S is odd. then the disarranging is be easy distinguish. So the security of the SEK-based DSE scheme is not good.
- 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.)

3 Review Comments

The paper proposes a novel PHY-ES architecture with a SEK-based DSE scheme that provides endogenous encryption and decryption for IoT sensing data. The overall concept of combining physical layer security with endogenous key generation is interesting and timely; however, the algorithm descriptions and security analysis require further clarification and logical structuring, and there is a need to distinguish the proposed algorithms from conventional recursive functions by avoiding potential notational conflicts. While the idea is promising, several issues need to be addressed to improve the clarity and strength of the work.

3.1 Detailed Comments

- **Figures:** The figures should be provided in SVG format to ensure clarity and scalability.
- **Performance Comparison:** The current performance comparison focuses on KGNet and BCFL key generation schemes against DES. It should also include a comparison with similar SEK-based works, particularly those that encrypt on the physical layer.
- **Algorithm Notation:** The algorithm naming (E1-E3 and D) currently creates confusion as it seems to imply recursive functions. It is recommended to revise the notation to clearly distinguish sequential steps.
- **Algorithm E3 Clarity:** In Algorithm E3, more details are needed on how the i-th row of the generated key K is inserted into the i-th row of X. A step-by-step explanation would be beneficial.
- **Security Analysis:** The security evaluation should incorporate discussions on potential attacks. For instance, if a chosen-text attack is applied with a constant one-bit plaintext, the initial SEKs K might become all zeros (in cases where S is odd), making the disarranging easily distinguishable. This raises concerns regarding the overall robustness of the SEK-based DSE scheme.