Prototyping a Generic Physical Layer Encryption Scheme for IoT Networks

Georgios Zachos
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
g.zachos@av.it.pt

José C. Ribeiro
Instituto de Telecomunicações
Aveiro, Portugal
jcarlosvgr@av.it.pt

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science,
University of South Wales
Pontypridd, UK
jonathan@av.it.pt

***Abstract*—To achieve information security objectives at the physical layer, while requiring a minimal resource footprint, Physical Layer Security (PLS) is a promising approach. In a previous work, the Grain-128PLE, a lightweight physical layer encryption (PLE) scheme derived from the Grain-128AEAD v2 stream cipher, was presented. The Grain-128PLE scheme is a generic PLE scheme that performs encryption and decryption at the physical layer, in between the channel coding and signal modulation processes. In this work, we focus on the implementation of the Grain-128PLE scheme and its performance evaluation with regards to the efficient use of resources during run-time. The evaluation results showed that the implemented PLE scheme incurs zero communication overhead and a small computational overhead that is dependent on the message length.**

Keywords— Data Confidentiality, Internet of Things, Physical Layer Encryption, Stream Cipher, Grain-128PLE

I. INTRODUCTION

Physical layer security (PLS) is an alternative and resource-efficient solution to secure communication in resource-constrained IoT networks. In a previous work in [1], the focus was on the design of a PLS-based scheme, referred to as Grain128-PLE, aiming to achieve data confidentiality as a resource-efficient solution for IoT networks. The encryption and decryption procedures of the Grain128-PLE scheme are executed in between the channel coding and signal modulation processes as shown in Fig. 1. As a result, the scheme can operate without depending on the channel conditions or the utilized communication protocol stack. In addition, the Grain-128AEAD v2, a lightweight synchronous stream cipher [2] is used for the encryption and decryption procedures of the scheme to ensure that the resources needed during run-time are minimized.

In this work, the focus is on the implementation of the Grain128-PLE scheme, running on a testbed that we built for demonstration purposes, and its performance evaluation in terms of the efficient use of resources (i.e., computational and communication overhead) during run-time. The evaluation results showed that the implemented Grain128-PLE scheme incurs zero communication overhead and a small computational overhead that is dependent on the message length.

This research work was sponsored by R-PODID supported by the Chips Joint Undertaking (GA 101112338) and its members, including the national top-up funding by Fundação para a Ciência e Tecnologia (KDT/2022/RIA/R-PODID/INSTITUTO DE TELECOMUNICAÇÕES). The authors would also like to acknowledge the NATO Science for Peace and Security Programme under grant SPS G5797.

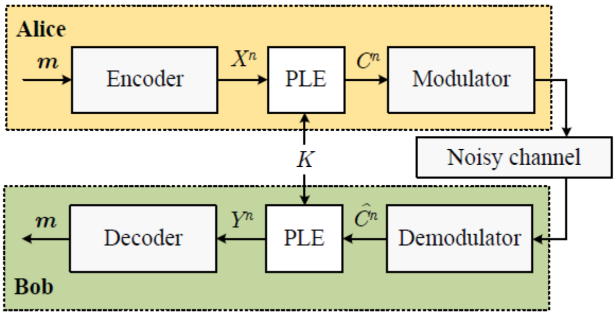

Fig. 1. The system model for generic physical layer encryption.

II. IMPLEMENTATION AND PERFORMANCE EVALUATION

In this section, we evaluate the efficiency of the Grain128-PLE scheme, proposed in [1], and analyze its communication overhead and computational overhead. For the evaluation, a testbed consisting of two laptops and two USRP (i.e., N210) devices, with each laptop controlling one USRP device, was developed as shown in Fig. 2.

Fig. 2. Testbed to evaluate the Grain-128PLE scheme.

The LabView platform (version 2011) was used, through the two laptops, to program the utilized USRP devices and develop the Grain128-PLE scheme. In particular, one USRP device acted as a transmitter, while the other USRP device acted as a receiver and vice-versa. In addition, the encryption process of the Grain128-PLE scheme was implemented on the laptop connected to the USRP transmitter as shown in Fig. 3, while the decryption of the proposed scheme was implemented on the laptop connected to the USRP receiver as shown in Fig. 4.

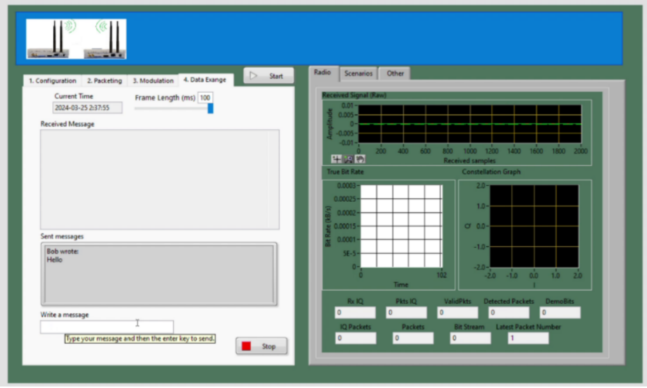

Fig. 3. User interface for transmitting a message.

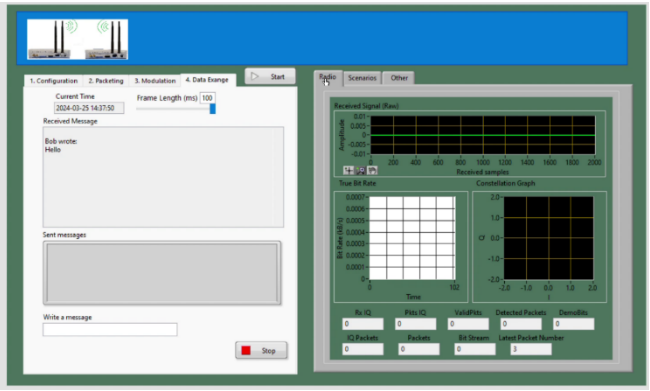

Fig. 4. User interface for receiving a message.

It is worthwhile considering the communication and computational overhead of the proposed PLE scheme. During both the encryption of a message to be transmitted and the decryption of a received message, the PLE scheme processes the message bit by bit, and does not add or remove bits from the message. Thus, the message length does not change, and the communication overhead is zero.

In addition, during run-time, the memory usage of the implemented encryption and decryption functions of the PLE scheme were measured. During message transmission, a maximum memory usage of 14.31 Kbytes was observed regarding the encryption function, while during message reception, a maximum memory usage of 12.50 Kbytes was observed regarding the decryption function. In addition, we used messages of different lengths (i.e., 100bytes, 128bytes, 1Kbyte, 10Kbytes, 100Kbytes) and measured: (i) the process time that was consumed to encrypt each message, and (ii) the process time that was consumed to decrypt each message. Using these data, the processing overhead (i.e., secs/Mbyte) was calculated as shown in Table I and Fig. 5.

TABLE I. AVERAGE ENCRYPTION/DECRYPTION TIME AND ENCRYPTION/DECRYPTION OVERHEAD.

Message Length (bytes)	Average Encryption Time (msecs)	Encryption Overhead (secs/Mbyte)	Average Decryption Time (msecs)	Decryption Overhead (secs/Mbyte)
100	0.9	9.437184	0.8	8.388608
128	1.2	9.8304	1	8.192
1024	9.9	10.1376	8.8	9.0112
10240	315.9	32.34816	258.1	26.42944
102400	25672.8	262.889472	19848	203.24352

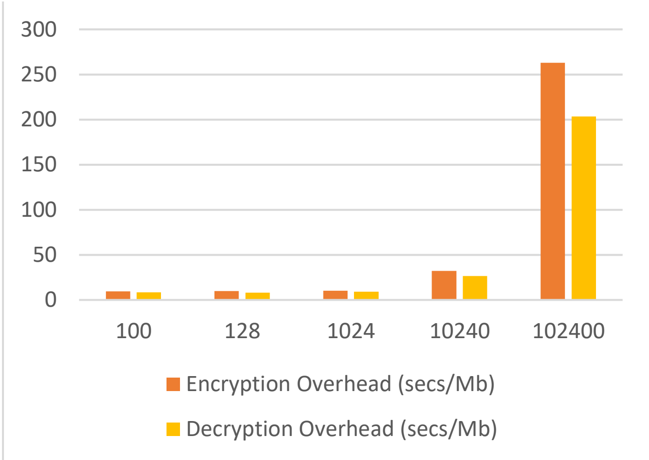

Fig. 5. Encryption/Decryption Overhead (secs/Mbyte) of the proposed PLE scheme.

From Table I and Fig. 5, it can be observed that the encryption/decryption overhead increases as the length of the message increases. In addition, it is worthwhile noticing that the Grain128-PLE scheme is more efficient when shorter messages are processed (encrypted/decrypted).

III. CONCLUSION

In this work, we focused on the implementation of the Grain128-PLE scheme, proposed in [1]. We developed a testbed for demonstration purposes and evaluated the performance of the Grain128-PLE scheme in terms of computational and communication overhead during run-time. The evaluation results showed that the implemented scheme incurs zero communication overhead and a small computational overhead that is dependent on the message length.

REFERENCES

[1] M. de Ree, G. Mantas, and J. Rodriguez, “Grain-128PLE: Generic Physical-Layer Encryption for IoT Networks,” in 2023 IEEE Globecom Workshops (GC Wkshps), 2023, pp. 1844–1849, doi: 10.1109/GCWkshps58843.2023.10464732.

[2] M. Hell, T. Johansson, A. Maximov, W. Meier, J. Sönnerup, and H. Yoshida, “Grain-128AEADv2-A lightweight AEAD stream cipher,” NIST Light. Cryptogr. Final., 2021.