Developing Physical-Layer Security Schemes for Internet of Things Networks

physec

Newsletter #2
April 2021

What is PHYSEC?

Internet of Things (IoT) networks have a wide range of **applications** including **military and security** applications.

Distributed nodes in IoT networks are usually constrained by limited energy and processing capabilities. As such, employing conventional complex data security mechanisms represents a challenge to IoT nodes due to the induced complexity and high energy consumption.

The PHYSEC project will **propose lightweight security mechanisms tailored for IoT networks** considering the **physical-layer security** approaches.

Image source: Credencys GoDigital

Technical work

The first technical task of the project (T2.1) involves a detailed literature review of malicious node detection in IoT Networks. In this task, the current algorithms/protocols in the literature for detecting attackers in IoT networks will be surveyed and analysed.

The focus of this task is threefold:

- Studying all the considered attack models in the literature,
- Analysing all the proposed algorithms/schemes/protocols for detecting the malicious nodes in the literature, and
- Evaluating the performance of these works in terms of the detection efficiency, the complexity, the resource consumption, and development ability.

The outcome of T2.1 will be deliverable D2.1 - State of the art for insider attacker detection in IoT networks.

PHYSEC Publications

Journal Papers:

- A. Abushattal, S. Althunibat, M. Qaraqe, H. Arslan, *"A Secure Downlink NOMA scheme Against Unknown Internal Eavesdroppers"*, IEEE Wireless Communication Letters, Accepted, Feb 2021.

- A. Alhasanat, S. Althunibat, M. Alhasanat, M. Alsafasfeh, *"An Efficient Index-Modulation Based Data Gathering Scheme for Wireless Sensor Networks,"* IEEE Communications Letters, Dec 2020, doi: 10.1109/LCOMM.2020.3047350.

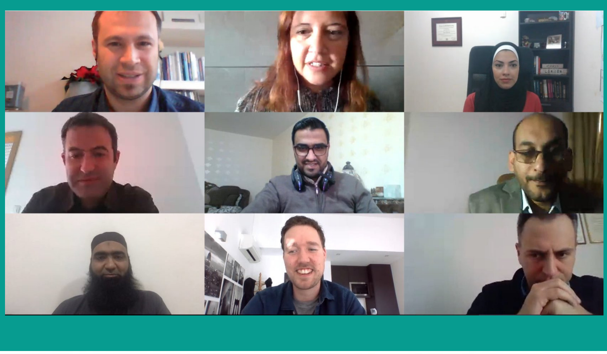
Conference Papers:

- S. C. Tokgoz, S. Althunibat, S. Yarkan, K. A. Qaraqe, *"Physical Layer Security of Hybrid FSO-mmWave Communications in Presence of Correlated Wiretap Channels"*, IEEE International Conference on Communications (IEEE ICC 2021), May 2021.

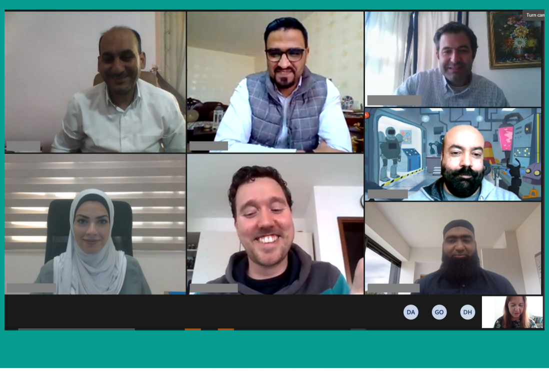
- M. Usman, S. Raponi, M. Qaraqe, and G. Oligeri, *"KaFHCa: Key-establishment via Frequency Hopping Collisions,"* IEEE International Conference on Communications (IEEE ICC 2021)

Project Meetings

1st plenary meeting - PHYSEC kicked-off on 20th November 2020, as online meeting due to the COVID-19 pandemic.



2nd plenary meeting - PHYSEC held its second meeting on 9th April 2021, in an online format.



NATO OTAN

This project is supported by: The NATO Science for Peace and Security Programme

instituto de telecomunicações

, May 2021

HAMAD BIN KHALIFA UNIVERSITY
جامعة حمد بن خليفة
عضو في مؤسسة قطر
Member of Qatar Foundation

جامعة الحسين بن طلال
AL HUSSEIN BIN TALAL UNIVERSITY

www.nato-physec.eu

Newsletter editor: Cláudia Barbosa [IT]