SECURITY OF DIGITAL AGRICULTURE NETWORKS: LORAWAN CASE STUDY IN BENIN

Dr Anne-Carole Honfoga
Electromagnetism and Telecommunications Department
University of Mons, Mons, Belgium
anne-carole.honfoga@umons.ac.be

Prof Véronique Moeyaert
Electromagnetism and Telecommunications Department
University of Mons, Mons, Belgium
veronique.moeyaert@umons.ac.be

INTRODUCTION

Agriculture constitutes one of the business sectors which really participates to the Benin's economic development.

Digital Farming describes the agricultural engineering from Precision Farming to connected, knowledge-based farm production systems and is characterized by a fusion of emerging technologies such as the **Internet of Things (IoT)**, robotics, big data, artificial intelligence (AI), and blockchain technology.

This concept has been conceived with the fast development of industry (from industry 1.0 to 4.0) where the fourth industrial revolution provides the opportunity to transform industrial agriculture into the new generation, namely Agriculture 4.0 or digital agriculture (Figure 1).

The aim of this work is to study the ruggedness of LoRaWAN against malicious attacks in digital agriculture (case of Benin country). ➡ **Sustainable Development Goals 2, 5, 9 and 15 achievements of United Nations.**

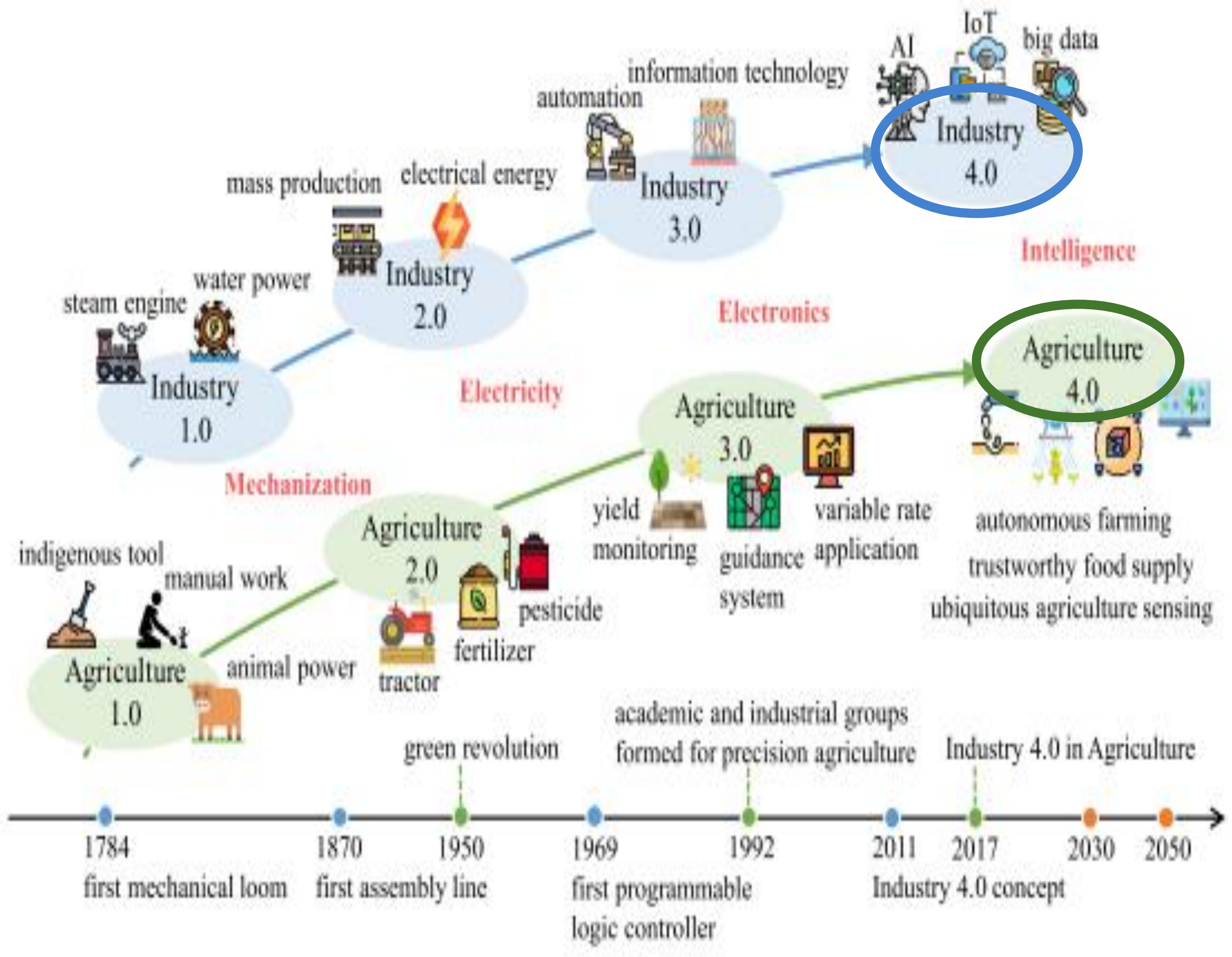


Figure 1: The Roadmaps of the agricultural revolution and industrial revolution

THEORICAL BACKGROUND

IoT represents the technology really exploited to monitor cattle, crops, forests, fish farming and water quality and level. It refers to the process of connecting physical objects to the Internet, enabling the exchange (sending and receiving) of data over wireless networks with limited human intervention.

LoRaWAN (Long Range Wireless Area Network) is the most used network as it presents a good coverage (>5km), a low battery consumption and uses an unlicensed spectrum (Figure 2). However, recent works have shown that this network presents several security vulnerabilities at each layer (physical, communication or application).

These vulnerabilities call into question network security principles such as confidentiality, authenticity, integrity and availability as each LoRa device transmits signals which can be received by any LoRa gateway remaining in its network coverage and an IP network is used to ensure communication between the gateway and the end-device (Figure 3).

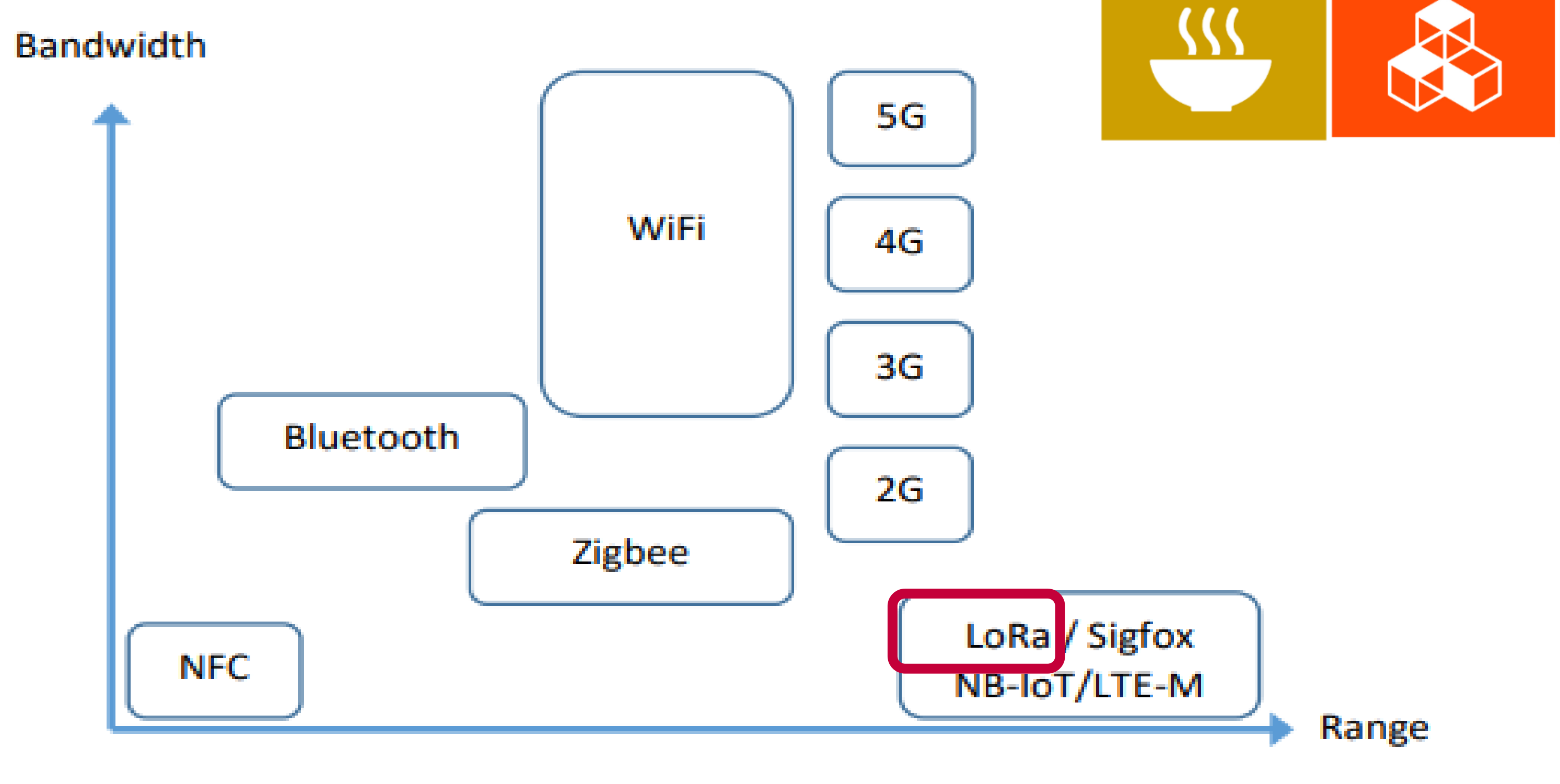
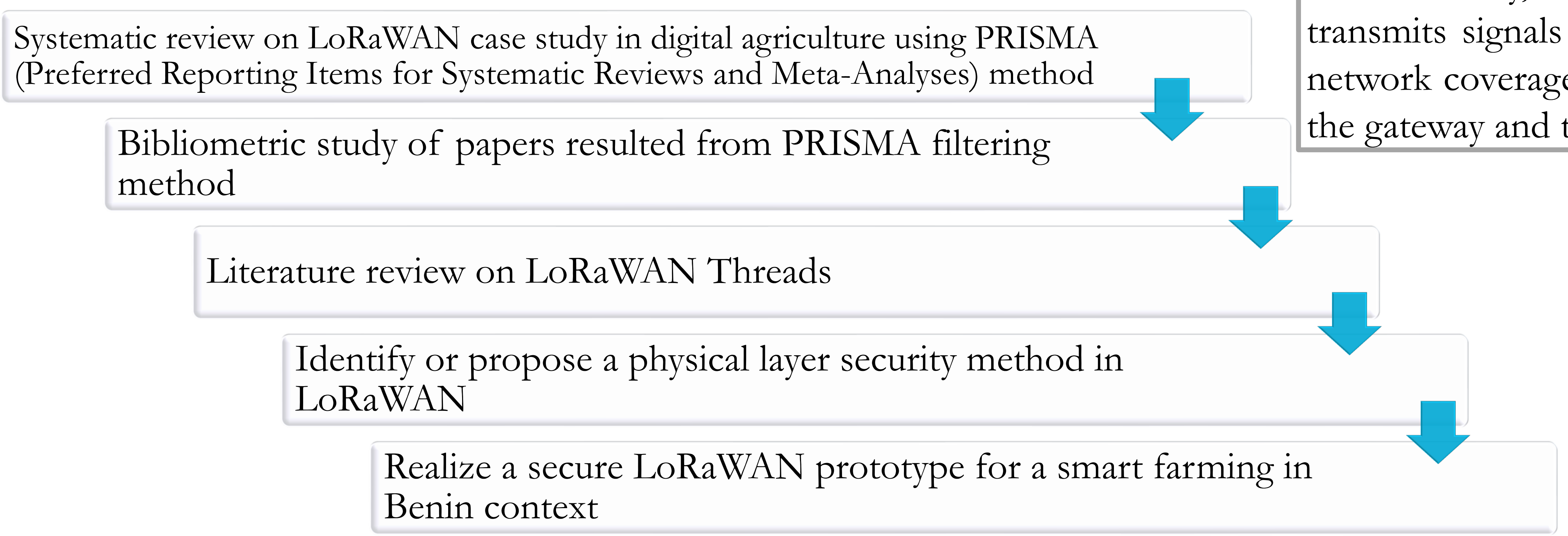


Figure 2: Wireless technologies: power consumption or bandwidth versus communication range

METHODOLOGY



Systematic review on LoRaWAN case study in digital agriculture using PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method

Bibliometric study of papers resulted from PRISMA filtering method

Literature review on LoRaWAN Threads

Identify or propose a physical layer security method in LoRaWAN

Realize a secure LoRaWAN prototype for a smart farming in Benin context

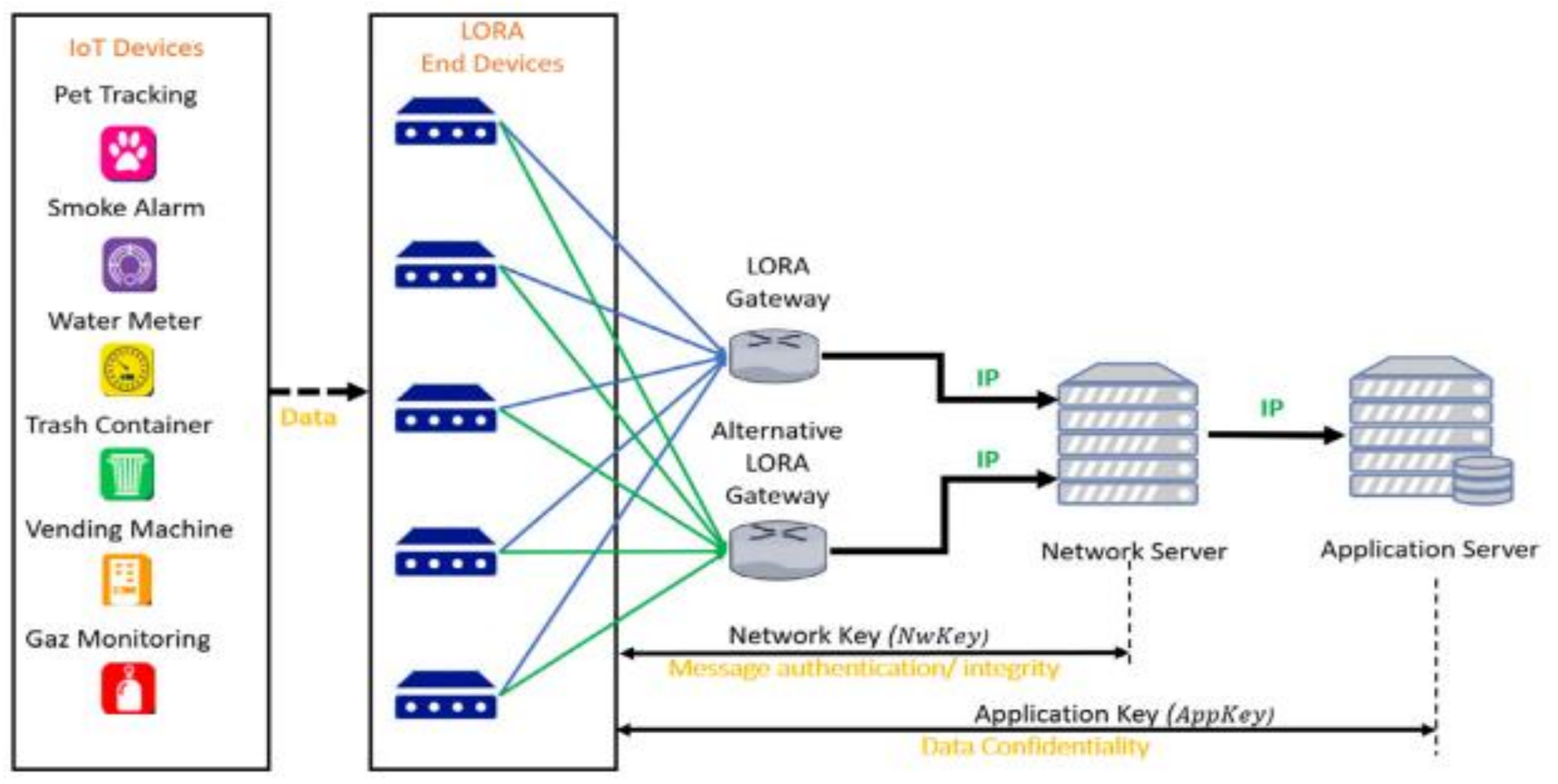


Figure 3: LoRaWAN Topology

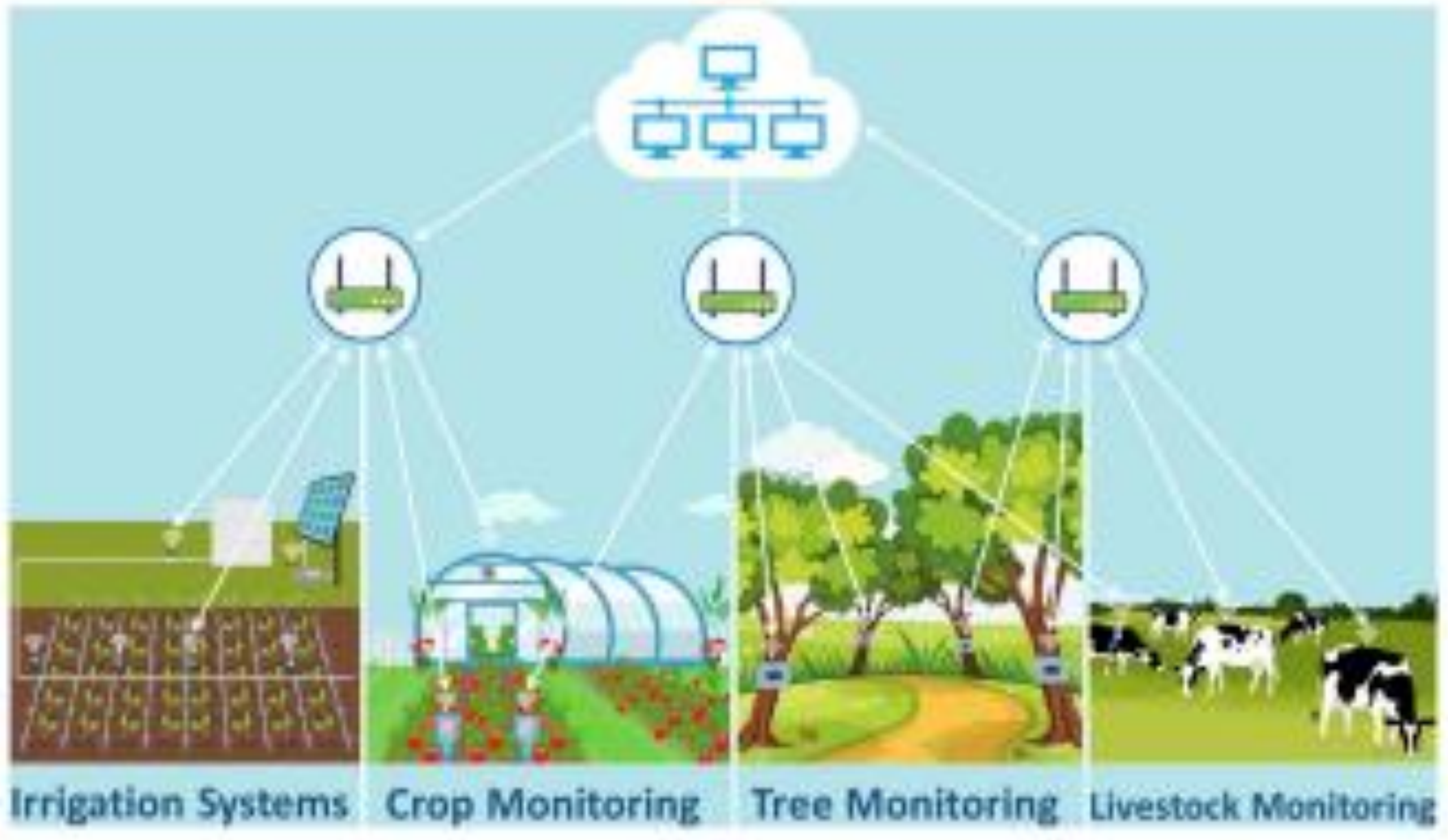


Figure 4: Four reference applications of LoRaWAN in smart agriculture

Expected results

Report summarizing applications of LoRaWAN in smart agriculture, the related countries of implementation, the relevant authors and their affiliation	Report giving an overview of LoRaWAN threads studied in the literature and their migitation measures proposed at the lower layers of the network	LoRaWAN network prototype design with jaming attack, replay attack… testing and a proposed mitigation measure

REFERENCES

[1] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges", IEEE Transaction on Industrial Informatique, Vol. 17, No. 6, June 2021.

[2] H. Noura, T. Hatoum, O. Salman, J-P. Yaacoub, A. Chehab, "LoRaWAN security survey: Issues, threats, and possible mitigation techniques. Internet of Things", vol. 12, p. 100303, 2020.

[3] M. Sylvain, "A Low Power, Long Range, wireless technology", Book, Semtech, Savoie Mont Blanc University, 2021.