Authentication Of the Internet of Things Devices Over ZigBee Networks
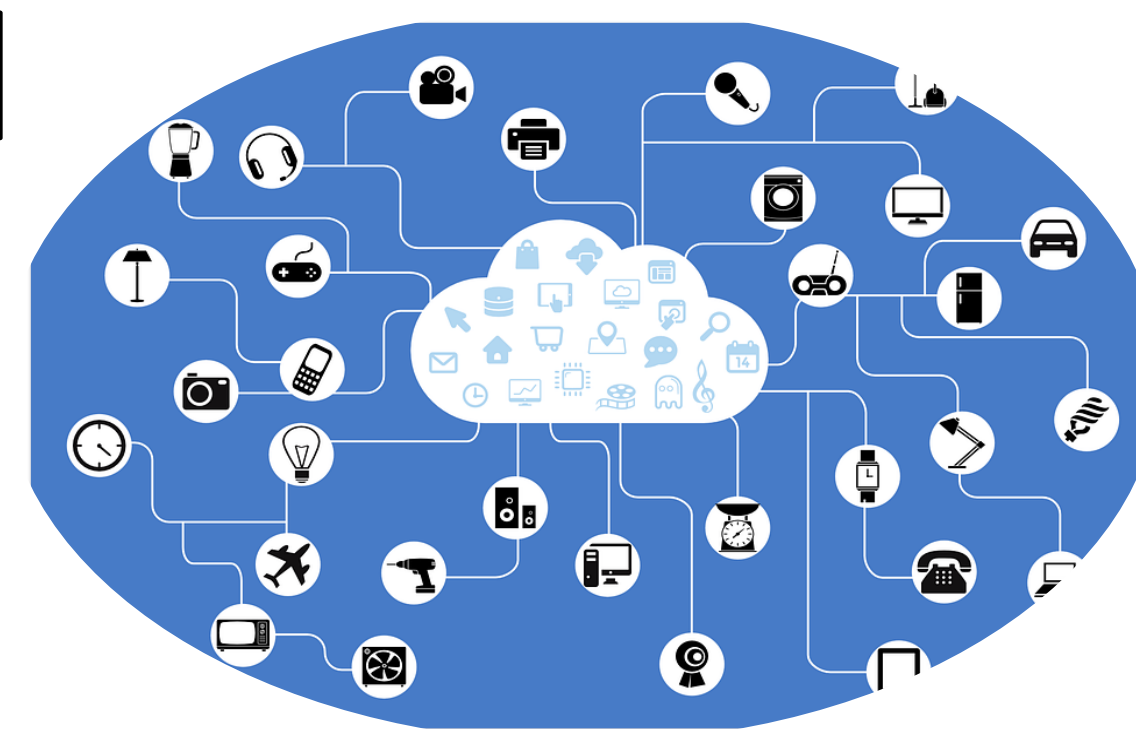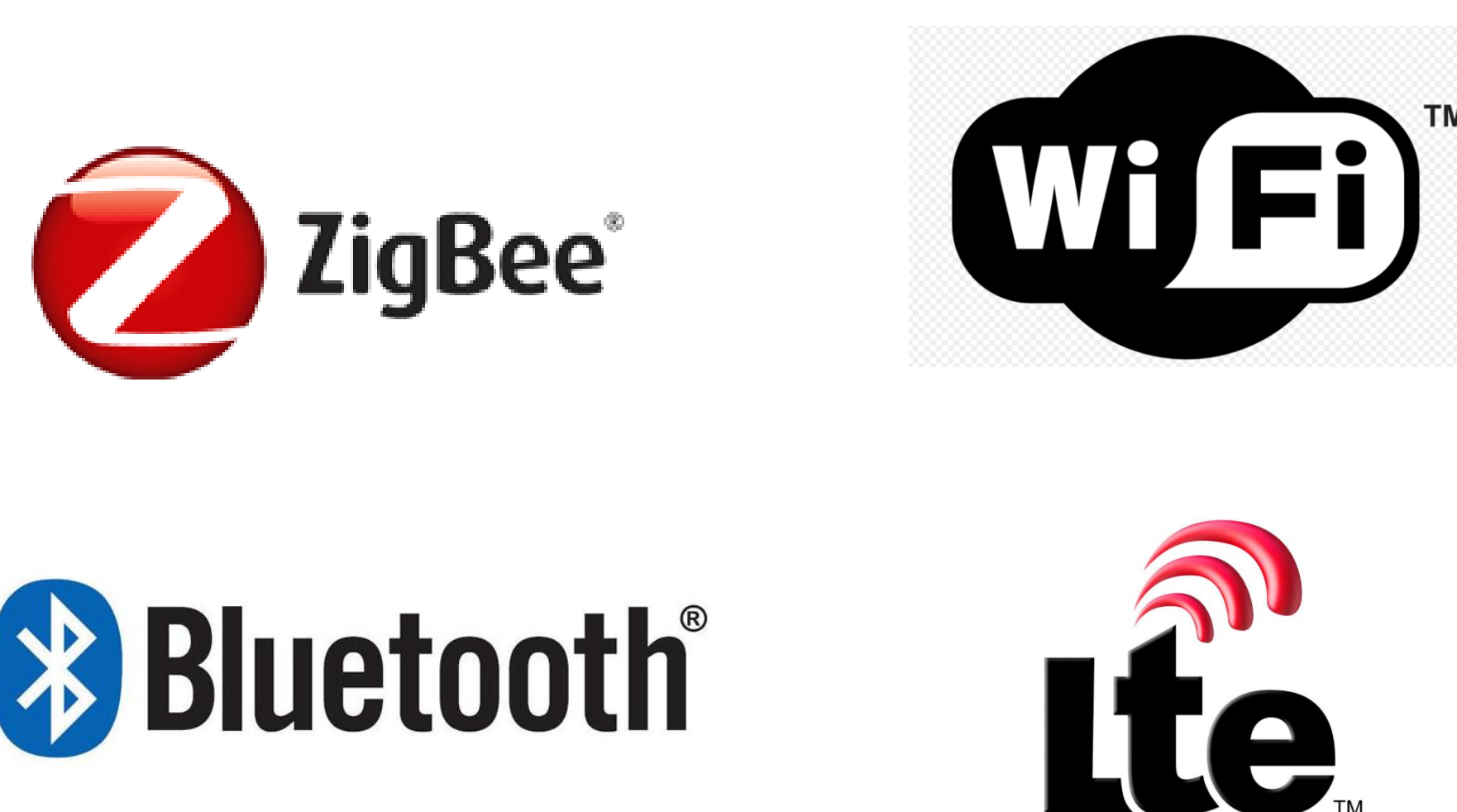
James Althoff, Advisor: Feng Ye,Ph.D.,Department of ECE ,University of Dayton

What is IoT?

- IoT (Internet of Things): *Inter-networking* of smart devices and embedded systems.

Networking in IoT

ZigBee is the technology we apply to the project.
Note: Both ZigBee and Bluetooth are based on the **IEEE 802.15** family.

Security in IoT Networking

- **Authentication (our focus on the project)**
  Prove the identity to the system, and/or vice versa.
- Confidentiality
- Data integrity
- Non-repudiation
- Etc.

Authentication for a Smart Lock

A user must first be identified by the lock before access is given
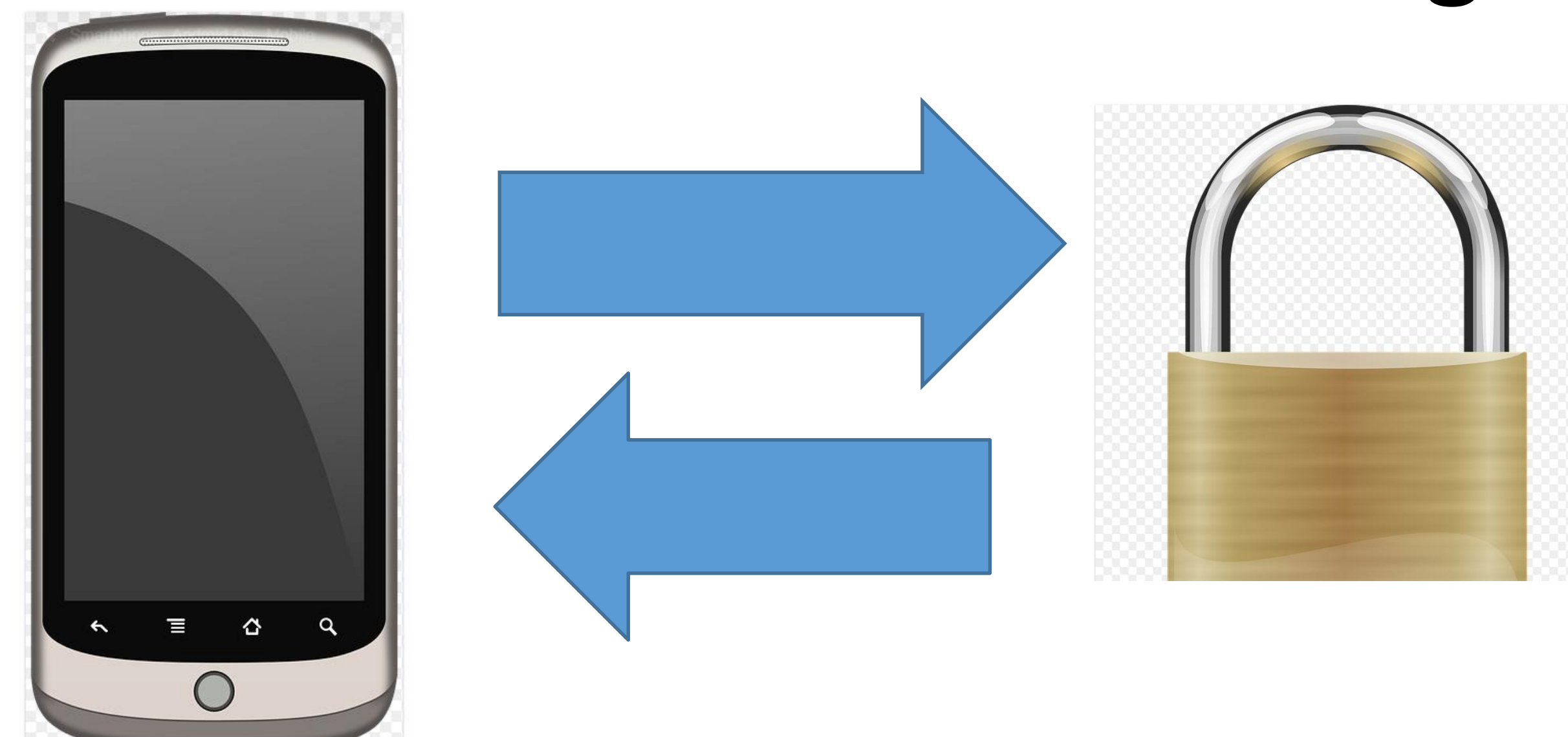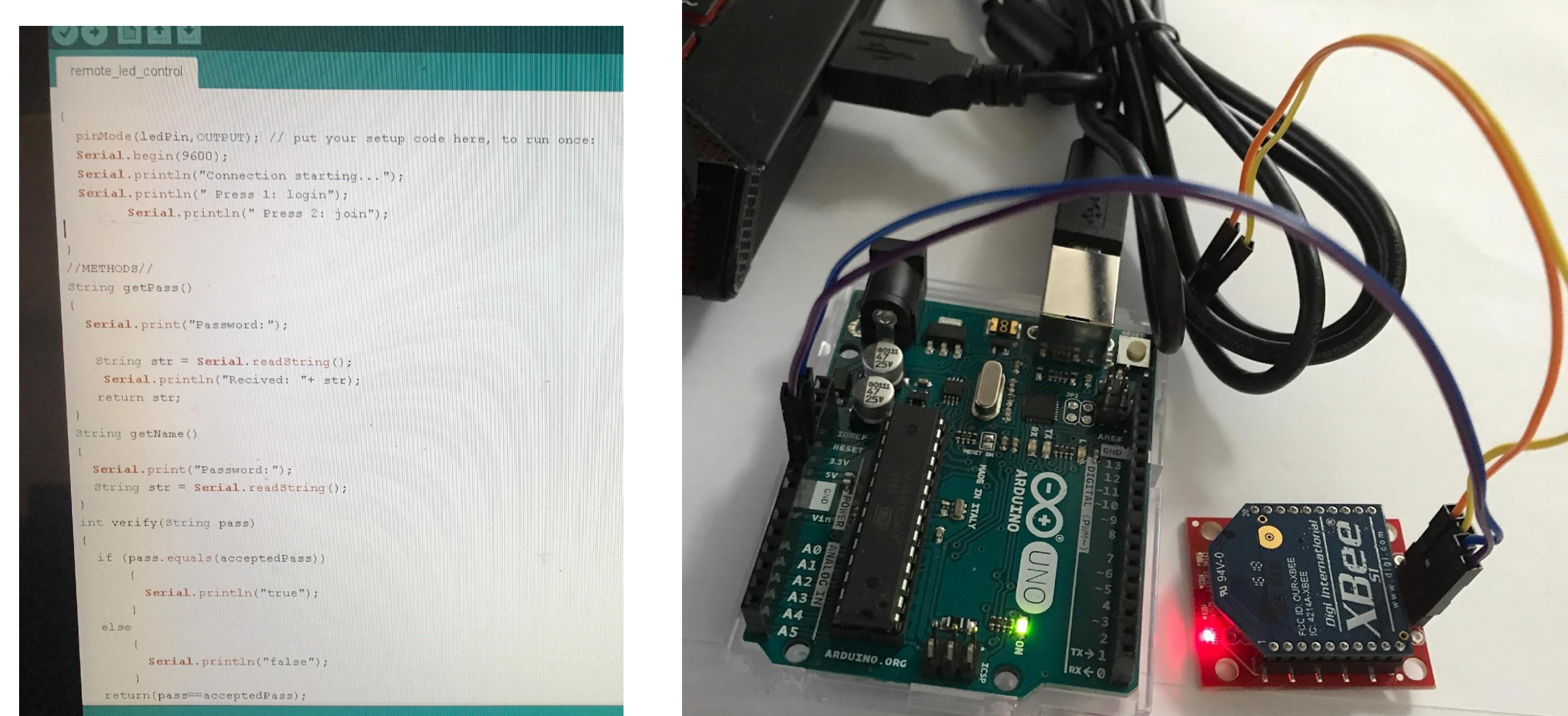
IoT Node Setup

Figure: Configuring the Arduino

The Proposed IoT AUTH Protocol

(in progress, subject to change)

System Time
Challenge
Password, Time2 → PW?, valid Time?
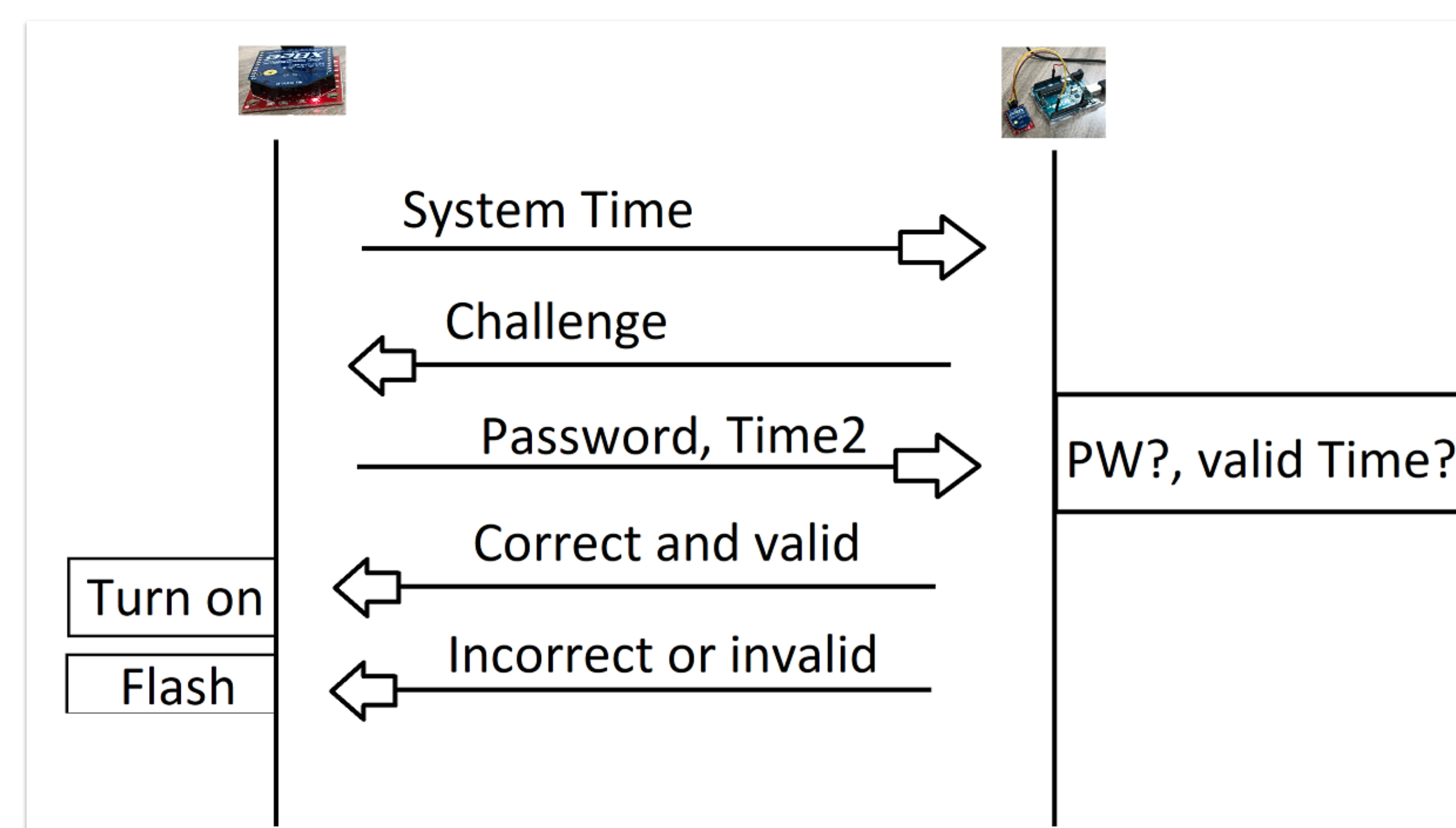Correct and valid → Turn on
Incorrect or invalid → Flash

Figure: Authentication protocol with nonce implemented

DEMO Setting for Authentication

The Arduino is used for the user controller. The ZigBee module is used for transmission.
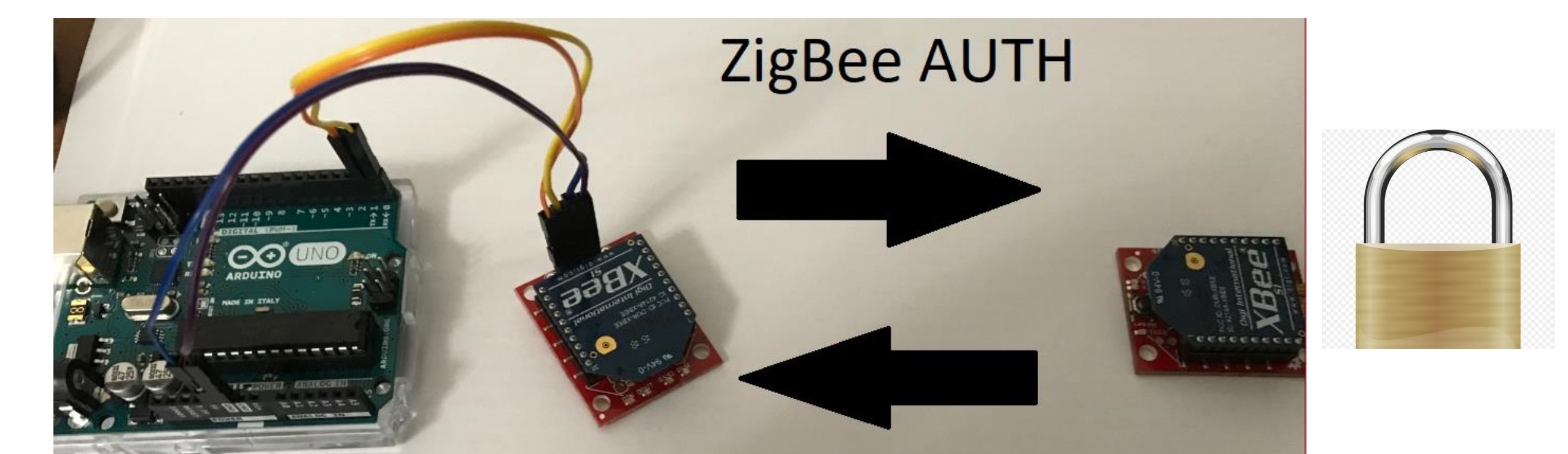
ZigBee AUTH
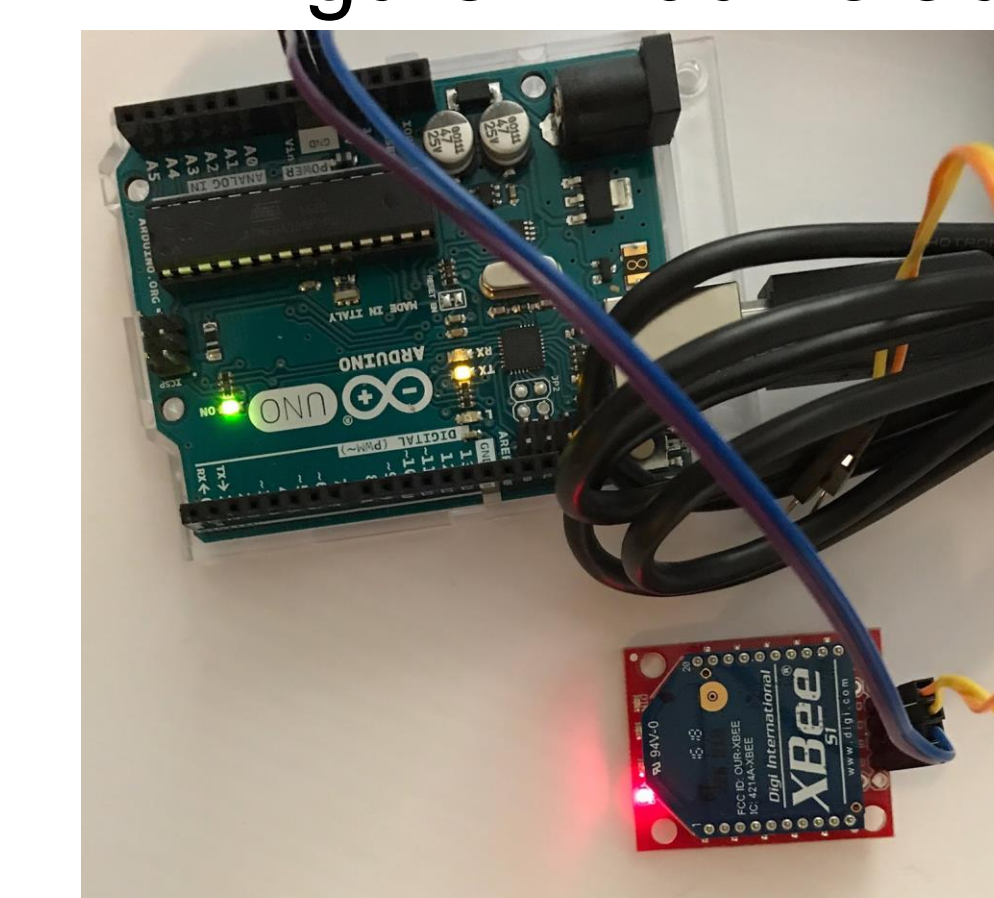
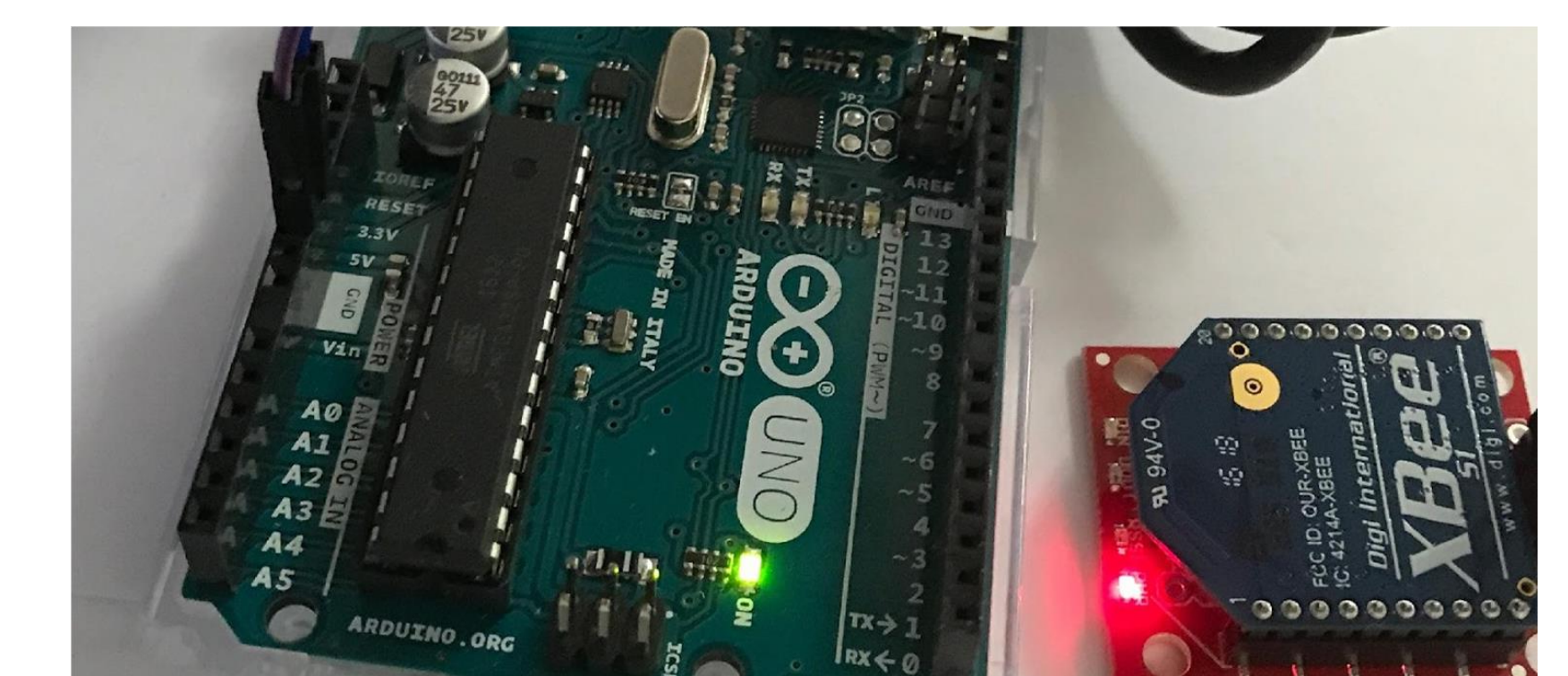Figure: Arduino authenticating itself to the XBee module

Figure: Arduino lit up

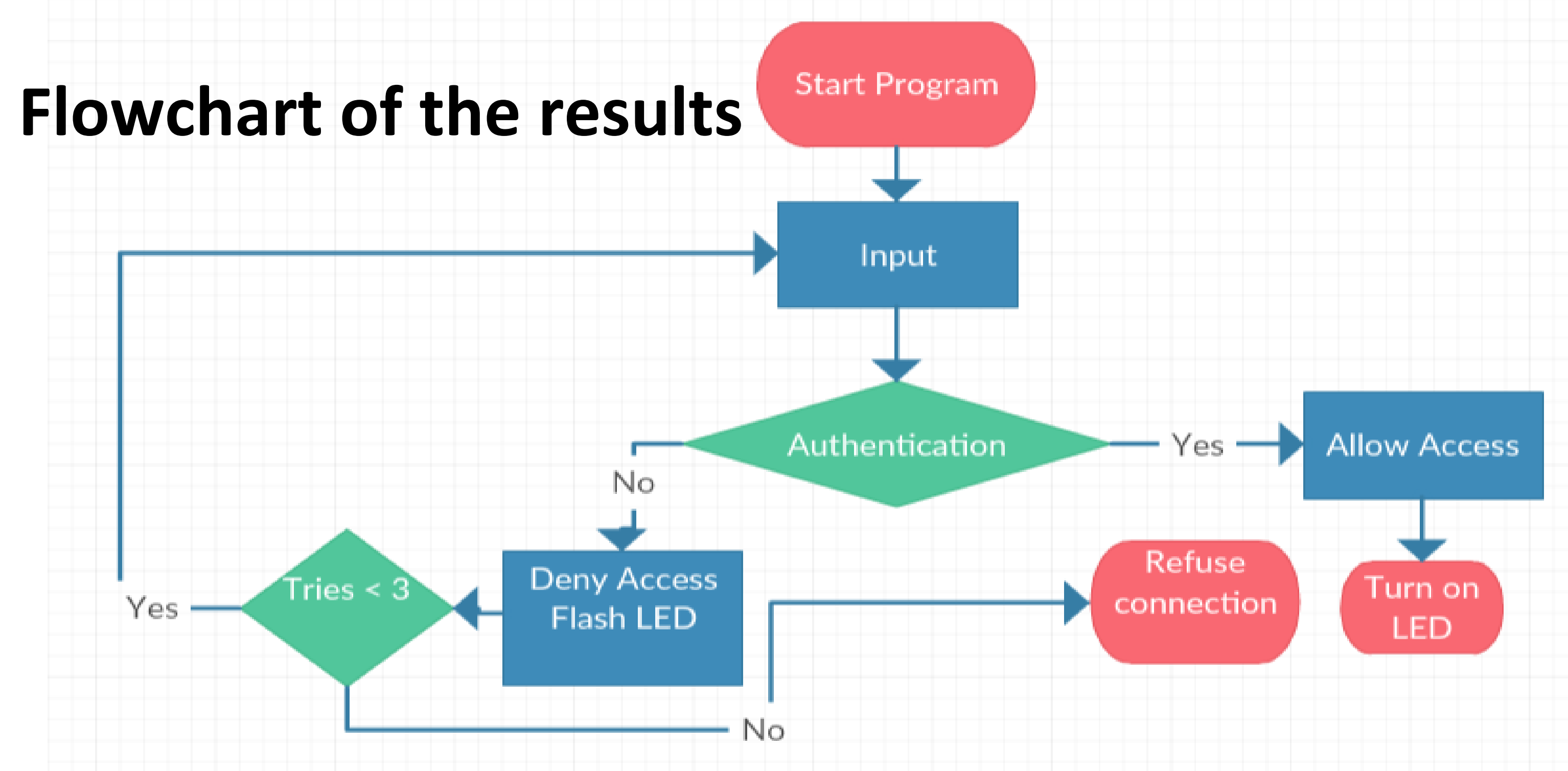Figure: Arduino not lit up

Flowchart of the results

Start Program
Input
Authentication — Yes → Allow Access
No
Tries < 3 — Yes
Deny Access Flash LED
Refuse connection
Turn on LED

- Strengthen current protocol against replay attack.
- Analyze the weakness of the current protocol
- Implement timestamp, nonce (generated by hash) in the DEMO set-up.