George Mason University

Implementing OTA Updates for an IoT Security Device

Authors:
Gerson Dalton Cardozo
M. Sohail Iqbal
Aneesh Malhotra
Mohamed Nur
Ryan Thomas

Supervisor:
Dr. Jens-Peter Kaps

March 25, 2018

1 Executive Summary

This project will build upon a previous ECE 492 project *FPGA Enhanced Wireless Sensor Node for IoT Applications*. The project sought to create a more secure wireless sensor node network by using an FGPA. In addition to enhancing security, they had the goal of maintaining low power consumption throughout the operation of the network. In the event that this system is compromised, however, we would like to be able to re-secure this device by updating the already existent firmware over-the-air. This will allow for mass distribution of potential updates in the event of a security breech.

2 Problem Statement

(Insert Problem Statement Here)

3 Approach

(Insert approach here)

4 System Design

4.1 Application

4.1.1 Camera Module

- The camera being used is the ArduCAM v5 5MP camera with night-vision capability ($21).
- The camera module will be controlled by the MSP430 through I^2C for instructions, and SPI for the images.

4.1.2 Android Development

- The Android app is used to receive photos via the Dropbox cloud from the gateway.
- The app will allow the user to manually request a snapshot.
- The app will setup a private connection via ECC, and allow the user to update the private key of the user.
- The app will be updated to deliver OTA updates via the dropbox cloud.

4.2 Dropbox Cloud

- Used to store updates and photos, as per the user's request.

4.3 Gateway

- Uses a BeagleBone Black to connect the node to the Dropbox cloud.
- Communicates to the network via Ethernet, which is secured by transport layer security.
- Communicates with the node via the ZigBee protocol, which is secured through AES.

4.4 Node

4.4.1 FPGA

- The Actel Igloo Nano will be used for securing the user's phone to the node.
- The FPGA will use elliptic curve cryptography, which uses smaller private keys than alternatives, allowing for more efficient use of memory.

4.4.2 MSP432

- Used as a controller for the FPGA, XBee, ArduCAM, and PIR Motion Sensor.
- The MSP432 will be initialized by the motion sensor or user input, and send a signal to the ArduCAM to take a snapshot.
- The MSP432 will receive the snapshot in JPEG format via SPI, and transmit the image to the XBee via the UART protocol.
- The MSP432 will use the key generated by the FPGA to secure this communication with the user.

Schematic

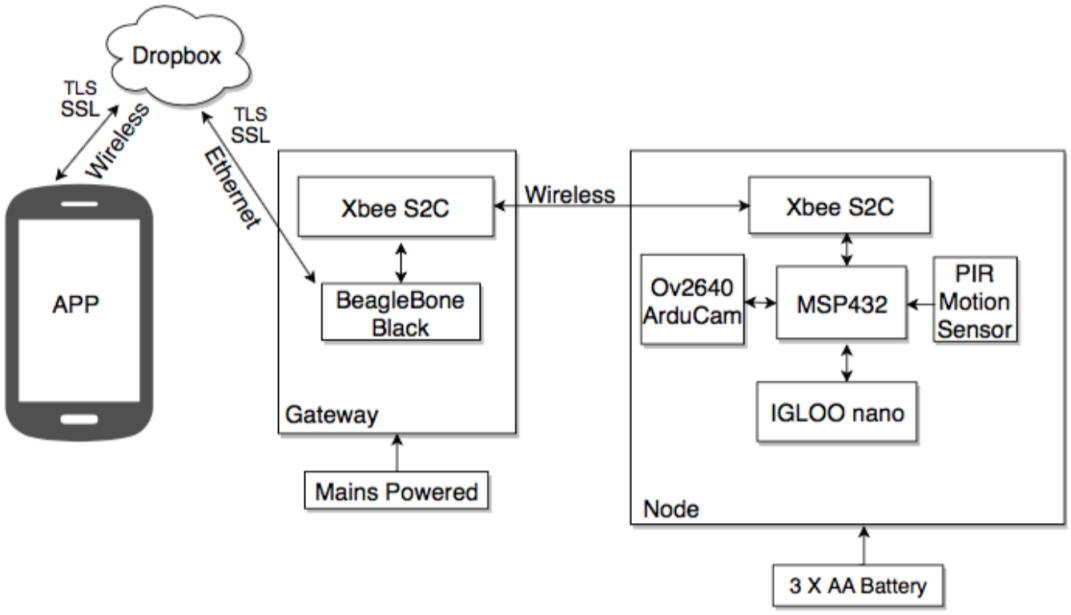

Figure 1: Top Level Schematic

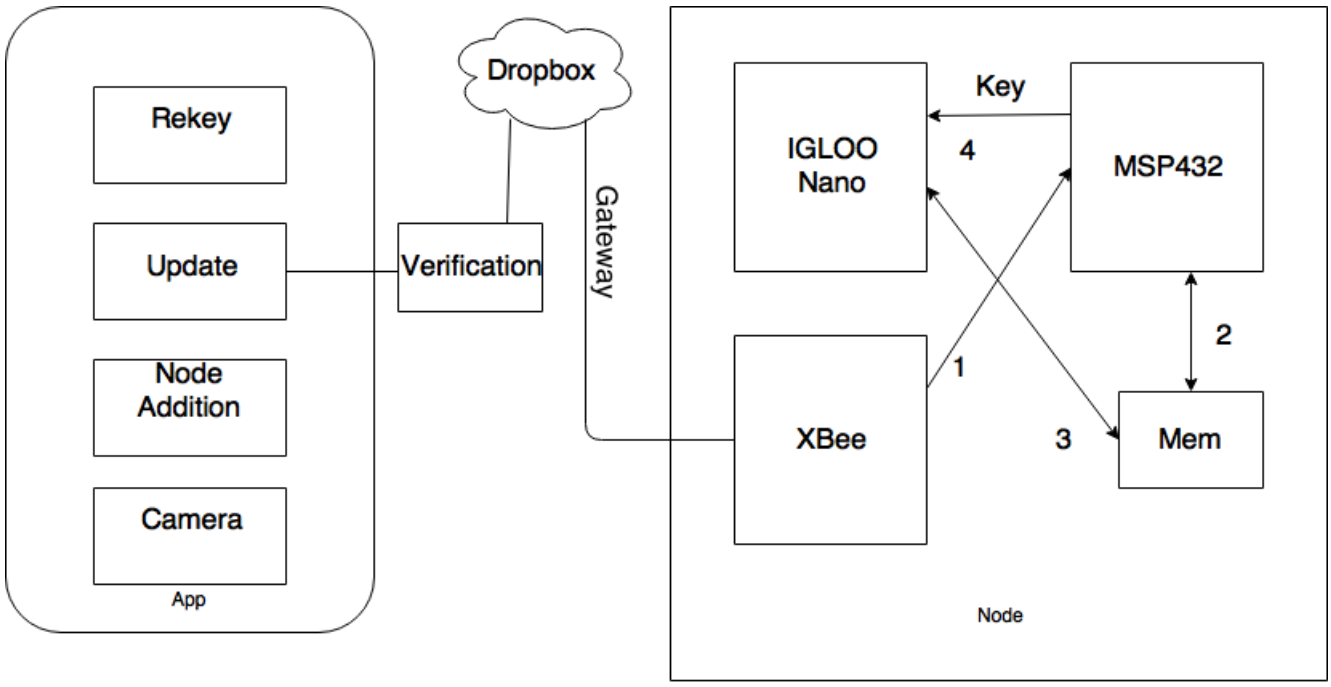

Figure 2: Top Level Diagram