Using Woluxi for Wi-Fi provisioning of IOT devices.

Introduction:

Whenever a consumer buys a IoT device, the first step is to configure it so that it connects to the Wi-Fi network and to the internet. There are a couple of methods that vendors use to accomplish this.

1. Using a Wi-Fi protected setup(WPS) button, if that is available on both the device and the router, but this push button method has a number of known security flaws and if it fails there is no way to debug this.
2. Another method is to have the device appear as an access point with its own SSID and a pass-phrase, this pass-phrase is supplied with the manual/quick start guide. The user disconnects from his home network and connects wirelessly to this device with the pass-phrase and configures the device.

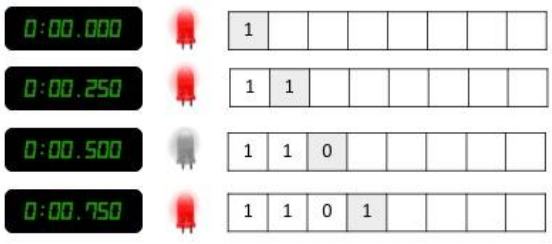
The second approach works for most of the cases but is difficult to navigate for non-technical users, it also has the following flaws.

a. It might not be the most secure approach depending on how the manufacturer handles the startup scenario e.g. by hardcoding the passphrase.
b. Some consumers may not do this initial configuration and it would remain visible and accessible to anyone nearby.
c. If you need to reconfigure the device to add to a different network, you will need to save the manuals or store the passphrase.

You can enhance the second approach using the Woluxi framework, which makes it secure and easy.

Solution

Woluxi uses the existing device LED in an innovative way, it uses the LED to transmit data, using a binary protocol similar to Morse code and interpreting the blinking using a smartphone. Due to the ubiquity of LEDs in devices and smartphones with end-consumers, this novel solution does not require any hardware changes to the device, only firmware upgrade to add required software. Obvious advantage is that the devices which are already in the field can also incorporate this technique.



It consists of 2 components

1) **"Woluxi library"** embedded in the device, which consists of 2 parts.
   a) A LED control library, which controls the blinking of LED to send out information from the device using a predefined protocol, where ON means logic-1 and OFF means logic-0 at a fixed duty cycle.
   b) A Web service, which will construct credentials and transmit them using the LED control Library. I would also configure and bring up host AP with those credentials.
2) **"Vendor App"** bundled with the Woluxi library scans the blinking status light, extracts the credentials and uses it to log into the device.

Advantages

- Consumer doesn't have to remember the pass-phrase/credentials or store it anywhere, so it would be easy to reconfigure when needed.
- The device can generate security credentials periodically. Doing so makes it more secure by avoiding Brute force attacks, even if the consumer leaves the device un-configured, it is still locked down and cannot be compromised.