УДК 621.396.9

THEORETICAL RESEARCH AND PRACTICAL DESIGN OF IOT TESTBED SOLUTION BASED ON ESP8266 SOC AND BLYNK COMPONENTS

Chekunov M., Osypchuk I., Kyrashchuk V., Osypchuk S.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: osypchuk_ivan@i.ua

Теоретичне дослідження та практична імплементація тестового IoT-рішення на базі плати ESP8266 та сервера Blynk

Робота відображає результати попереднього теоретичного й послідовного практичного проектування експериментального IoT-девайсу, зконструйованого на базі модуля ESP8266, що підтримує стандарт IEEE 801.11, та серверної технології Blynk. Отримані дані дозволяють зробити висновки стосовно можливості використання наявного експериментального макету при роботі як одного IoT-датчика, так і декількох різних датчиків одночасно.

The Internet of Things, also known as IoT, refers to billions of physical devices around the world that are now connected somehow (to the Internet, for example), collecting and sharing data. IoT adds a decent level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without us, people, being involved, and merging the digital and physical worlds this way [1].

The IoT is more than some kind of convenience for consumers. It offers new sources of data and different business operating models that can boost productivity in a variety of industries: health care, manufacturing, retail, telecommunications, transportation, utilities and others. The proposed IoT architecture used in current work, is presented on Fig. 1.

Internet of Things applications have diverse connectivity requirements in terms of range, data throughput, energy efficiency and device cost. WiFi is often an obvious choice because in-building WiFi coverage is almost ubiquitous, but this is not always the appropriate choice due to high energy consumption and high data rate what is not necessary in most cases of IoT applications. Anyway, WiFi was selected as a wireless technology for IoT testbed as it met the financial and goal purposes [2].

A number of standards based and proprietary last mile connectivity options have evolved to service IoT, and each has advantages and limitations. A reference table of telecom technologies available for IoT connectivity is shown in Table 1. WiFi, or 802.11, is a wireless protocol that was built with the intent of replacing Ethernet using wireless communication over unlicensed bands. Its goal was to provide off-the-shelf, easy to implement, easy to use short-range wireless connectivity with cross-vendor interoperability. WiFi, while being the obvious choice for IoT, has big limitations in both range and energy efficiency [3].

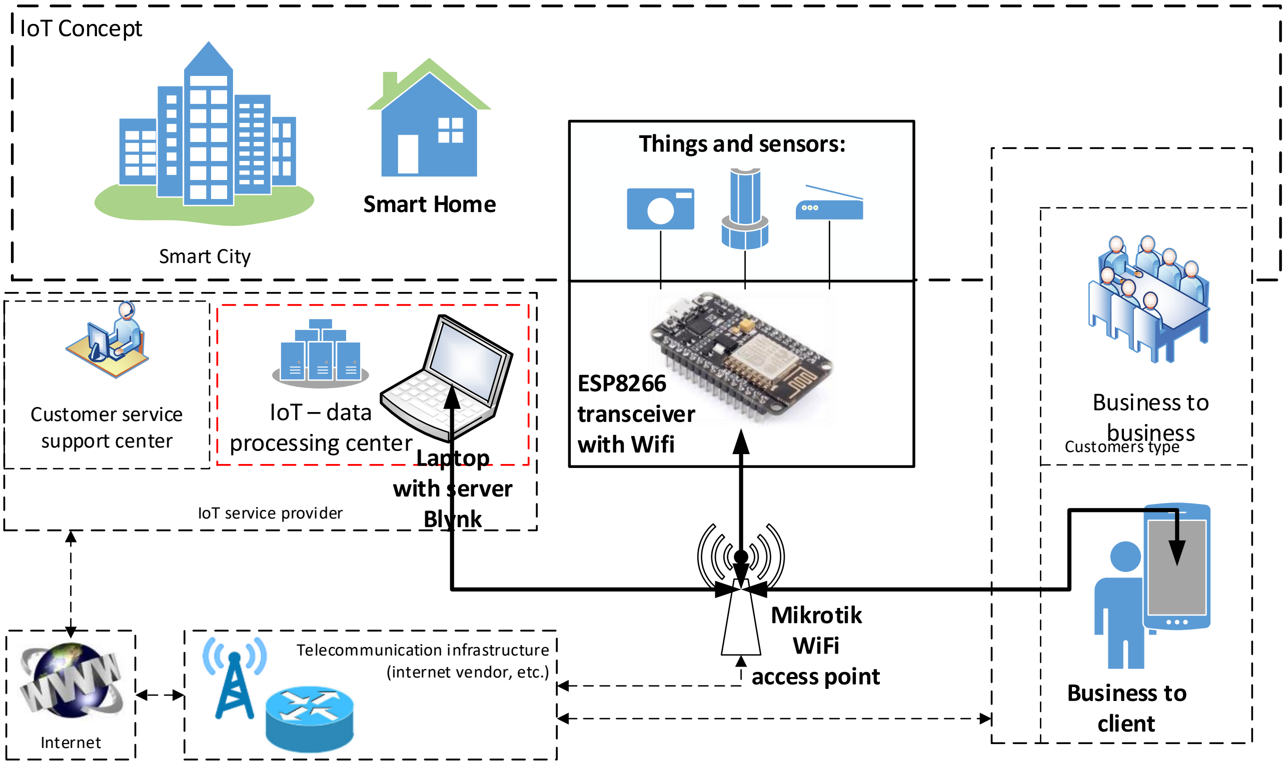
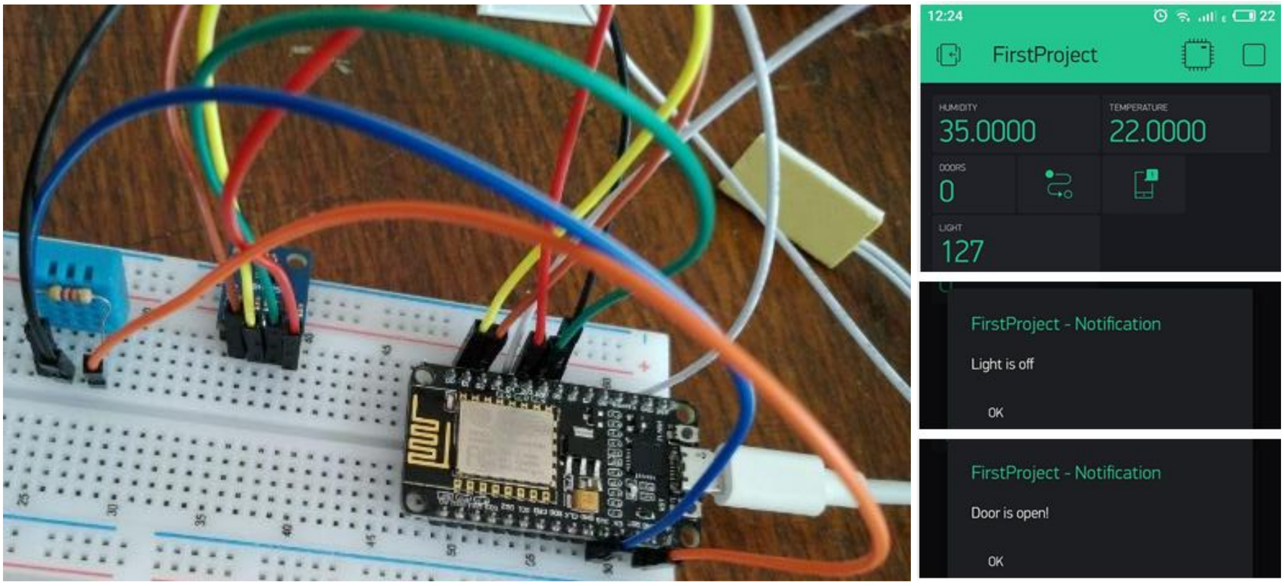

IoT Concept
Smart City
Smart Home
Things and sensors:
ESP8266 transceiver with Wifi
Business to business
Customers type
Customer service support center
IoT – data processing center
Laptop with server Blynk
IoT service provider
Mikrotik WiFi access point
Business to client
WWW
Internet
Telecommunication infrastructure (internet vendor, etc.)

Fig. 1. The proposed and considered IoT architecture used in current work.
Bold connections show the implemented part of architecture: WiFi access point, sensors, transceiver, laptop with server application, client terminal with application

Table 1. IoT connectivity technologies

Technology	Network	Standards based or Proprietary	Range	Throughput	Energy requirement	Adoption
LoRa	LWPA	Proprietary (Semtech)	High	Low	Low	Moderate
NWave	LWPA	Proprietary (NWave)	High	Low	Low	High
RPMA	LWPA	Proprietary (OnRamp Total Reach)	High	Low	Low	High
SigFox	LWPA	Proprietary (SigFox)	High	Low	Low	Moderate
LTE-M	3GPP/LTE	Standards based (3GPP)	High	High	Low	Upcoming
NB-IoT	3GPP/LTE	Standards based (3GPP)	High	Moderate	Low	Increasing
NB-LTE	3GPP/LTE	Standards based (3GPP)	High	Moderate	Low	Upcoming
Bluetooth	Bluetooth	Standards based	Moderate	Low	Moderate	Limited Wearables
ZigBee	802.15.4	Standards based (802.15.4)	Low	High	Moderate	Limited PAN & Home
Thread	802.15.4	Standards based (802.15.4)	Low	High	Moderate	Upcoming
Z-wave	Proprietary	Proprietary (Sigma Design)	Low	Low	Moderate	Very Low
WiFi	802.11	Standards based	Moderate	High	High	Very high
HEW	802.11ax	Standards based	Moderate	High	Moderate	Upcoming

As a result, eventually we assembled the test mock-up of the IoT device. It was decided to make it based on the ESP8266 module using the IEEE 802.11 standard. In general, the experimental scheme was created according to the architecture described earlier on Fig. 1, specifically the part highlighted in bold solid line and connections. So we used several sensors: light sensor, temperature and humidity sensor, door opening/closing sensor. All these sensors are able to work simultaneously on the same module [4].



12:24 22

FirstProject

HUMIDITY 35.0000

TEMPERATURE 22.0000

DOORS 0

LIGHT 127

FirstProject - Notification

Light is off

OK

FirstProject - Notification

Door is open!

OK

Fig. 2. The developed testbed with sensors based on ESP8266 module using the IEEE 802.11 standard for data transmission, and mobile terminal screen that shows responses and notifications from sensors

The information from the sensors goes to the Blynk server through the Wi-Fi module. Blynk server deployed on the laptop. Then, using the Blynk program, we authenticated the smartphone in the experimental IoT network. So we were able to track all data from sensors in real time directly from the phone, and IoT data stored on the database of Blynk server. The photo of the ESP8266 module working at that moment of the time is shown on Fig. 2.

So, in this work the possible case of IoT solution for smart home concept was designed, configured and implemented; the working testbed is presented. Such solution might be scaled either horizontally or vertically, with other telecommunication technologies used – for specific use cases.

References

1. Chih-Yung Chang, Chin-Hwa Kuo, Jian-Cheng Chen, Tzu-Chia Wang, "Design and Implementation of an IoT Access Point for Smart Home", Applied Science.
2. Daniel Minoli, Kazem Sohraby, Jacob Kouns, "IoT security (IoTSec) considerations requirements and architectures", CCNC 2017 14th IEEE Annual.
3. M. Schwartz, Internet of Things with ESP8266, Packt Publishing Ltd.
4. M.H. Habaebi, N.I.N.B. Azizan, "Harvesting WiFi Received Signal Strength Indicator (RSSI) for Control/Automation System in SOHO Indoor Environment with ESP8266", 2016 International Conference on Computer and Communication Engineering (ICCCE).