USB Wireless Adapter

Wojciech Wodo[1], Lucjan Hanzlik[1], Konrad Zawada[2]
Wroclaw University of Technology
[1] Faculty of Fundamental Problems of Technology,
[2] Faculty of Electronics,
Wybrzeze Wyspianskiego 27, 50-370 Wroclaw, Poland,
e-mail: [first_name].[last_name]@.pwr.edu.pl

Abstract: In this paper we investigate the issue of wireless USB hubs. Our aim is to adapt any USB device to its wireless version. We propose a minimized mobile hardware solution in the form of an electronic device and software allowing remote usage of peripherals such as keyboards, mice, USB sticks, etc. On the U.S. market similar solutions are known, but they are based on a many-to-one communication model and their design does not encourage mobility. With these designs peripheral devices still have one common point (in this case a hub instead of a computer). Additionally, hubs need external power supplies, thus they are connected to the grid by cable. Our solution is based on a one-to-one communication model and have a few key advantages for mobility. First, there is the possibility of minimizing the device itself and shortening the wire of the corresponding peripheral. Furthermore power consumption of the transmitter is much lower, and therefore there is no need to use an external power supply.

Key words: USB, wireless, Wi-Fi, communication, hub

Introduction

Recently one could notice the increasing popularity of mobile solutions. Smartphones, tablets, and laptops replace their stationary ancestors. In fact this mobility is to a certain extent limited by peripherals (e.g. mice or keyboards) plugged to these devices. Long cables do not make it easy to move or use devices in some places. Although there are wireless versions of these peripherals, they are relatively expensive and one must buy them as new equipment. This require users to discard old peripherals.

There are some solutions available on the market of course – they are called USB hubs e.g. *Iogear GUWIP*204 [1] or *Belkin F5L009* [2], but what makes them inefficient is lack of real mobility. They need to be connected to power supply by a wire and are much more like USB concentrator not the mobile units.

We propose a solution for the stated problem by designing an electronic device allowing the adaptation of any USB wire device (compatible with *Human Interface Devices – HID* [3]) to its wireless version. We create a virtual wire connecting the existing peripheral with corresponding destination point. Our device consists of two parts: a receiver plugged into the destination point (e.g. computer) and a transmitter connected to a particular peripheral. The transmitter is relatively small (size of 2,5' external hard drive) in order to allow comfort work and simultaneously has enough power capacity to supply peripheral for a few hours. It is powered by a li-ion battery charged from any computer USB port. Moreover in the transmitter design is considered a special spot for rolling the wire of connected peripheral providing maximal mobility of device.

Conceptual Part

In this section we present data on the analysis of the stated problem and particular functional requirements. We point out some recommendations regarding materials and solutions which should be used in the device.

Analysis

We want to design a system to replace USB wire communication (in standard 1.1) with a wireless version. Our goal could be achieved by creating a transparent interface responsible for communication between two devices (a mobile peripheral and end-point workstation). Such a system has to fulfill a set of requirements to be practical:

- secure communication of transmitter and receiver,
- minimal physical size (i.e. at most 2,5' hard disk size),
- compatibility with all USB devices (according to the HID) without special drivers,
- reasonable endurance for its power supply (i.e. 6-8 hours of operation without necessity of charging) for devices such external hard drives etc.,
- charged by micro USB port.

Secure communication of transmitter and receiver

The communication stream must be secured to prevent eavesdropping (e.g. files from hard drives) or manipulating (e.g. keystrokes or mouse movements).

In our solution we propose using communication based on standard *IEEE 802.11g* [4] with encryption *Wi-Fi Protected Access II – WPA2* [5] and private Wi-Fi network (shared by transmitter).

Physical size

A critical feature for the design of the device is its mobility. Usage of standard Wi-Fi communication let us minimize the size of the device. It might be software implemented, i.e. we can simulate receiver by an application run on computer, however, we propose using an additional Wi-Fi card (not internal) devoted to this purpose. That allows connecting more devices to the workstation (each device means one Wi-Fi private network).

The size of the transmitter is determined by the size of the battery used. There is some trade-off between physical size (in fact mobility) and usability.

Power supply

It was mentioned before that the power supply for the device is crucial. In order to provide a high level of usability we propose using a battery of reasonable capacity, e.g. at the level of 4400 mAh. That value was estimated not only based on device self-power consumption but mainly based on power request of the destination peripherals, e.g. external USB hard drive. The system should provide adequate work time for devices of high power consumption (at least few hours without charging). Using li-ion battery allows multiple charging. We propose using the plug-in micro USB standard. By using this standard, device may be charged via a standard USB port in a workstation or a smartphone charger.

An essential part of the designed system is an automated cut off of power supply to the device, when it is plugged in to charge. This is to prevent the overload of the power source, e.g. a USB port or charger. Thus, we can guarantee that current drawn from the power source does not exceed assumed safe value of 480 mA.

Experimental Part

In this section we present our solution in the form of a hardware device that meets stated requirements. There are also remarks on the prepared prototype of the system, see Fig. 1.

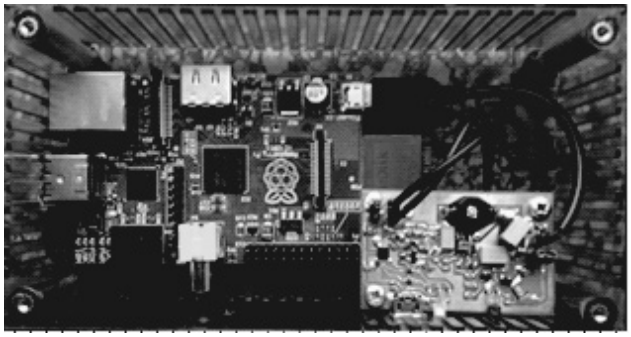

Figure 1. Prototype – Raspberry PI and power supply unit with converter

Framework

The prototype framework is split into two parts: the transmitter and the receiver. The former consists of:

- microcomputer *Raspberry PI* [6],
- external Wi-Fi USB card,
- electronic power supply unit and charger unit,
- li-ion battery of 4400 mAh capacity.

In case of the latter we use only an external Wi-Fi USB card, analogical to transmitter.

Integration and software

The battery powered Raspberry PI microcomputer creates a private Wi-Fi network using an unique password in WPA2 encryption mode. To achieve this, we used the following software*: hostapd* and *isc-dhcp-server*. The user via Wi-Fi card connects to the networks shared by transmitter. One uses the default network name and generated password assigned to each device by the manufacturer.

Next, the software installed on the workstation searches for a transmitter in the new connected network. After a successful search, the USB peripheral plugged into the transmitter device is automatically connected. The device works in such a way that it would be plug directly into the workstation (locally connected). The software installed on the workstation can work as a daemon service and start automatically when the OS reboots. For transferring USB messages via Wi-Fi channel we use library *VirtualHere* [7].

First launching

After installing the appropriate version of *VirtualHere* (i.e. 32 or 64 bits) the software user must enable option *Auto-Find Hubs* from *USB Hubs* menu (see Fig. 4). It needs to install the *Bonjour* plug-in.

The next step is connecting to networks shared by transmitter (we use the default network name and password

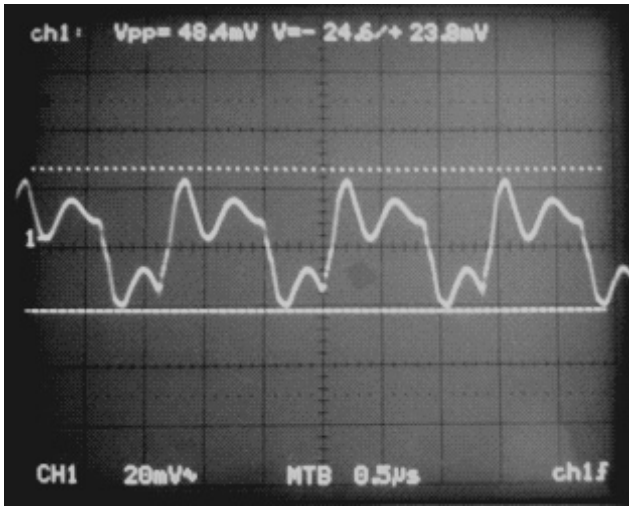

Figure 2. Converter output distortions

generated by manufacturer). After successfully connecting, the user selects a device name and enables the option *Auto-Use Port* in the submenu *USB Wireless.* Such configured software could be added to the auto start of the OS, it is possible to work as a daemon as well.

We performed dozen tests involving different sort of devices (i.e. pendrives, keyboards, hard disk drives and internet cameras) transmitting data in a wireless manner at a distance of 6-8 meters inside the building (even through two walls). In the cases of mass storage data we measured transfer rate, average speed was at the level of 400 Kbytes/s and maximal was 966 Kbytes/s.

Charging unit and converter unit

During process of designing the converter we tried to implement the best practices taken from the newest literature [8], [9]. The converter unit is based on Linear Technology LT1308B chip, which is equipped with an embedded comparator with an internal voltage reference level of 200 mV for detection of discharge of the battery. Hysteresis for detecting battery discharge is set on 0.5 V to eliminate dropping of the voltage level caused by battery internal resistance, tracks resistance and converter distortions. If voltage drop on the input of the comparator is lower than 3.0 V, it causes cut off output of the converter via output key constructed on a MOSFET transistor (see Fig. 3).

The voltage from the battery is passed to hysteresis via low pass filter, eliminating quick changing distortions (see Fig. 2). At first we obtained high distortion level of 100 mV, to reduce them we used tantalum capacitor 470 uF and distortions dropped to 50 mV. We encountered also a problem with too quick switching off the converter by a comparator despite using low-pass filtering. We diagnosed too high voltage fluctuations between divisor of comparator's input and the reference voltage level built-in the converter chip. The potential difference in a bulk caused noise in the reference voltage level with the respect to external elements of the comparator and enhanced the distortions, which amplitude exceeded hysteresis level and activated the comparator. Applied solution based on minimizing the resistance between a bulk of voltage divisor and a bulk of reference voltage level in LT1308B chip.

To charge the battery we used a MCP73833 chip. Maximal charging current is limited to 480 mA. Charging and working of the converter is signalized by two-colors LED. The converter is turned off when the external power supply is plugged in. Device power switch cut off the converter and it is not powered during charging the battery.

During converter and charging unit designing process we performed many simulations using *SPICE* software and selected carefully elements associated with a converter chip (i.e. inductors and capacitors) in order to obtain the best efficiency (in our case 82-87% in a nominal scope of operation: 0,6 A – 1 A). We performed detailed examination of the converter using three different input voltages (see Fig. 5).

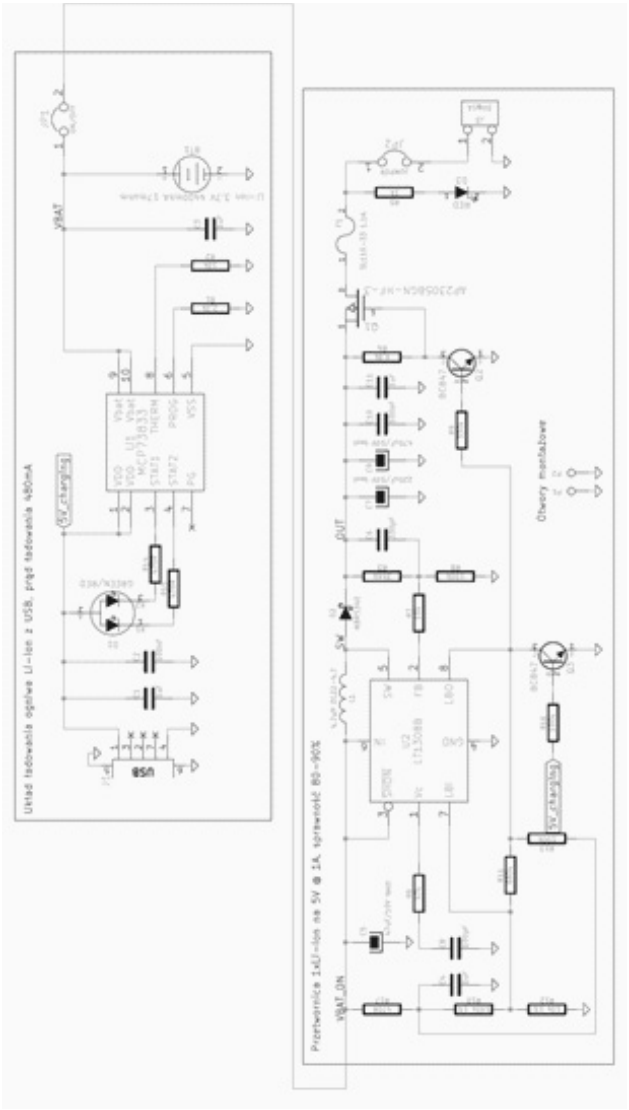

Figure 3. Scheme of charger and converter unit

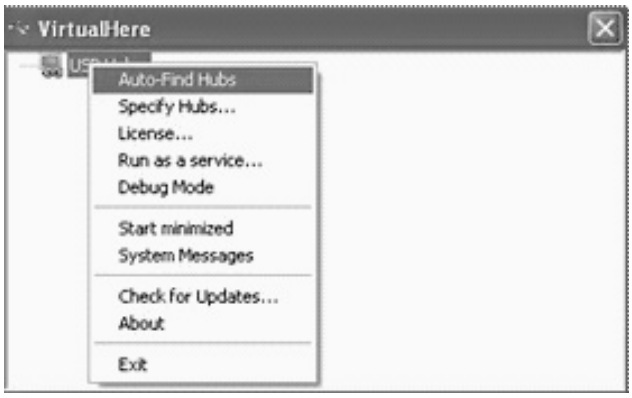

Figure 4. Application with option Auto-Find Hubs

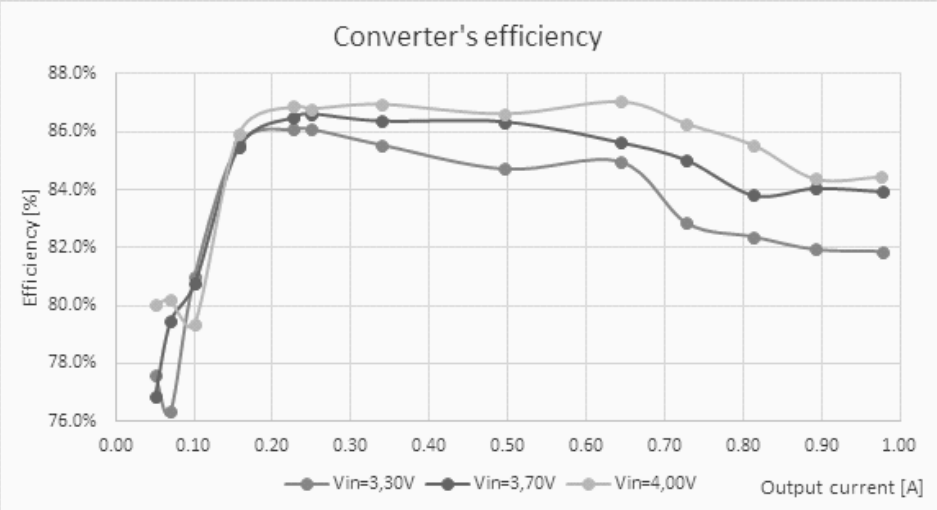

Figure 5. Examining of converter's efficiency

Conclusion

During this research we designed the concept of a system that converts a wire USB communication to its wireless version. We based our solution on the communication standard *IEEE 802.11g*, and thanks to that we did not have to construct a receiver because we could simulate it on Wi-Fi card.

The impact of research on user life is significant, there will be possible to work on data stored on external drive siting at a hammock chair on a porch or showing every nook by a camera without the necessity of carrying a laptop.

Future work on this project involves minimizing the transmitter. The first step is to replace the microcomputer Raspberry PI with a dedicated microprocessor unit. This microprocessor should be at least from the ARM family, which has hardware support for the USB protocol. Using this chip in the device and proper transferring USB messages (compatible with *VirtualHere* library) allows to replace current designed transmitter in the prototype.

Acknowledgment

This project was supported by European Union as part of the European Social Fund 8.2.1 - Dolnoslaski Bon na Innowacje.

References

[1] Iogear Guwip204 Technical Sheet, 2014, [Online] http://www.iogear.com/product/GUWIP204
[2] Belkin Belkin F5L009 Technical Sheet, 2014, [Online] http://www.belkin.com/networkusbhub
[3] Universal Serial Bus (USB), Device Class Definition for Human Interface Devices (HID), 2001, [Online]
[4] http://www.usb.org/developers/devclass_docs/HID1_11.pdf
[5] Broadcom White paper, IEEE 802.11g: The New Mainstream Wireless LAN Standard, 2003 [Online] http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf
[6] Jon Edney, William A. Arbaugh, Real 802.11 Security Wi-Fi Protected Access and 802.11i, Addison Wesley 2003
[7] Raspberry PI documentation, Raspberry Pi Foundation, 2014 [Online] http://www.raspberrypi.org/documentation/
[8] VirtualHere library documentation, 2014 [Online] http://www.virtualhere.com/client_configuration_faq
[9] Chi Kong Tse, Complex Behavior of Switching Power Converters, CRC Press, 2003
[10] Sanjaya Maniktala, Switching Power Supply Design and Optimization, Second Edition, McGraw Hill Professional, 2014

Author(s): MSc Wojciech WODO – is a PhD candidate of computer science at Wroclaw University of Technology, a graduate of special Top 500 Innovators program at UC Berkeley which focused on science management, technology transfer, commercialization and university-industry collaboration. He is a laureate of the prestigious program of Foundation for Polish Science – Impulse devoted to biometrics based on keystroking. He received a MSc degree from Wroclaw University of Technology in computer science. Mr. Wodo worked as a technology transfer specialist in Wroclaw Research Center EIT+ (2011-2012).His research fields include: cryptography, computer security, and biometrics.
MSc Lucjan Hanzlik – is a PhD candidate of computer science at Wroclaw University of Technology. He is a laureate of the prestigious program of Foundation for Polish Science – Ventures devoted to digital cryptographic signatures on smart cards. He is the author of a dozen papers about cryptography and computer security. Mr. Hanzlik received a MSc degree from Wroclaw University of Technology in computer science. His research fields include: cryptography, computer security, and smart cards.
BSc Konrad Zawada – is a MSc student of electronics at Wroclaw University of Technology. He works as on integrated circuits designer and digital signals specialist, as well as 8-bit microprocessors developer. Mr. Zawada received a BSc degree from Wroclaw University of Technology in electronics. His research fields include: integrated circuits, microprocessors, and electronics.