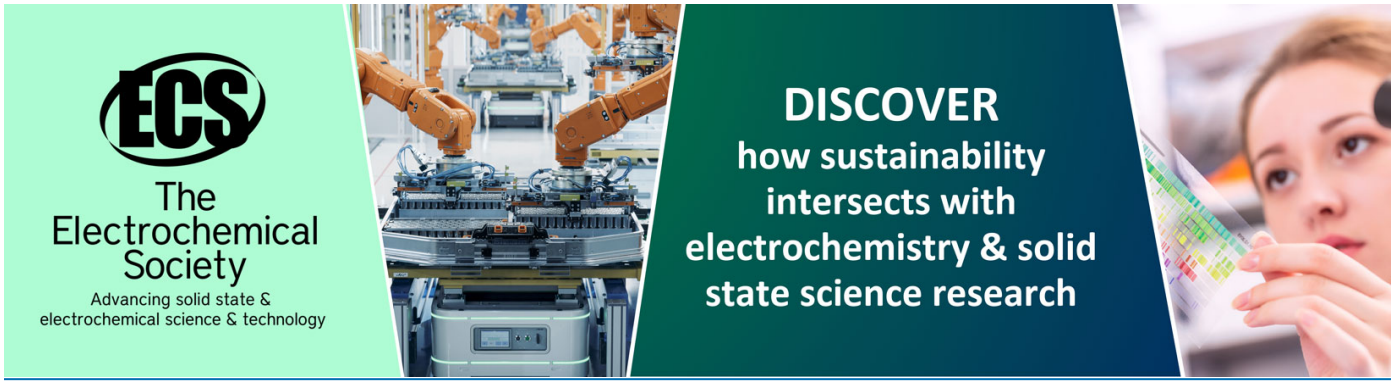
System Control Applications of Low-Power Radio Frequency Devices



IOP Conf. Series: Journal of Physics: Conf. Series **889** (2017) 012016 doi:10.1088/1742-6596/889/1/012016

System Control Applications of Low-Power Radio Frequency Devices

Roger van Rensburg

School of Physics, University of the Witwatersrand, Johannesburg 2050, South Africa

E-mail: roger.vanrensburg@wits.ac.za

March 2017

Abstract. This paper conceptualizes a low-power wireless sensor network design for application employment to reduce theft of portable computer devices used in educational institutions today. The aim of this study is to design and develop a reliable and robust wireless network that can eradicate accessibility of a device's human interface. An embedded system supplied by an energy harvesting source, installed on the portable computer device, may represent one of multiple slave nodes which request regular updates from a standalone master station. A portable computer device which is operated in an undesignated area or in a field perimeter where master to slave communication is restricted, indicating a possible theft scenario, will initiate a shutdown of its operating system and render the device unusable. Consequently, an algorithm in the device firmware may ensure the necessary steps are executed to track the device, irrespective whether the device is enabled. Design outcomes thus far indicate that a wireless network using low-power embedded hardware, is feasible for anti-theft applications. By incorporating one of the latest Bluetooth low-energy, ANT+, ZigBee or Thread wireless technologies, an anti-theft system may be implemented that has the potential to reduce major portable computer device theft in institutions of digitized learning.

Keywords: micro-controller unit (MCU), portable computer device (PCD), Bluetooth low-energy (BLE), radio frequency (RF), system-on-chip (SoC)

1. Introduction

In 2015 the South African (SA) government spent billions of rands in modernizing learning institutions by providing tablets to schools. The government stated that their goal for educational learning in SA is to digitize schools by the year 2020. Unfortunately, it was reported that more than 3000 out of 88000 tablets provided, were lost due to theft [1]. The large project undertaking was in jeopardy and under a substantial amount of stress because of the significant financial loss incurred. Consequently, more than 88000 tablets were recalled and fitted with anti-theft technology. The upgrade of the devices enabled the government to involve investigative authorities in the tracking of stolen tablets [2]. However, the tracking systems appeared only operational with the device powered on to communicate with Global Positioning Satellites (GPS) in outdoor environments.

With deficits present currently in the protection of tablets, there is need to augment the security of such devices by taking advantage of the wireless technologies today. For this reason, this research proposes a low-power wireless network design to protect PCD against theft. With such a system in place, theft may not be eliminated overnight but will make a stolen device difficult to use and less appealing to thieves. When the device functionality is removed that render the hardware of the user interfaces useless outside the working perimeter of the wireless network, a tracking system may be initiated to aid investigating authorities in the retrieval of the device.

The conceptual phase of this project will mainly consist of four stages. The first stage may deal with the design and development of a proposed wireless *master-slave* network topology followed by the electronics development of the embedded hardware. The second phase may consist of researching energy harvesting methods to power each of the *slave* nodes operating independently of the *device* power supply. The third phase may consist of developing firmware to render the *device* inoperable. Optionally, a final phase may be included, which requires a gateway in the wireless network that sends notifications to the learning institution when the *device* is rendered inoperable.

2. Methodology

2.1. Introduction

Embedded hardware that integrate wireless technologies and processing capabilities on a miniature SoC will be fully utilized in the design to realize a low-powered network topology. The problem statement requires that for such a network to be practical, network independence from an Internet Service Provider (ISP) to render the *device* unusable is needed. With network independence from carriers, the anti-theft system may be used in any geographic location. The wireless technology must also provide security that prevents unauthorized connections to the ad hoc network and offer reliable communications links over long distances, even when surrounded with other Industrial, Scientific and Medical (ISM) band frequencies. In the following section, the network topologies containing low-power RF technologies are proposed.

2.1.1. Star network topology: BLE wireless technology, also known as Bluetooth Smart, is a connection orientated communications standard. BLE has proven to be more power efficient that provide higher data throughput compared to other wireless technologies [3]. High cyclic redundancy checks are guaranteed which offers very robust and secure communications. Compared to ANT+ and ZigBee, BLE is fast becoming more progressively available in smart devices today.

A star network topology is firstly proposed which consist of a *master* station and multiple PCD. Each PCD, consist of two slave nodes which integrate a low-power BLE radio and an ARM Cortex M4 processor on a single chip [4]. As depicted by Fig. 1, the PCD in Fig. 1C must request regular data updates to the *master* in Fig. 1F. Similarly all other PCD in the network are setup identically. BLE only allows a single *slave* to be connected to one *master* at a time. For this reason, each PCD incorporates two *slave* nodes shown by Fig. 1D and denoted by MS_1 and DS_1, for connections to the *master* and *device*. The *master*, which can connect and communicate up to 20 *slaves*, will be located in a secure room and does not rely on low-power consumption requirements. This proposed BLE topology, however, will only be able to operate in a space over a limited distance where there is no physical obstructions of the wireless network.

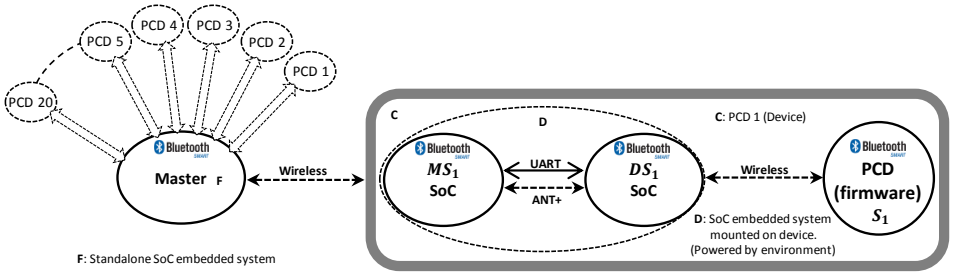


Figure 1: Proposed BLE star wireless network (concept design).

Each node (*master*, MS_1, DS_1 and PCD, incorporates a control algorithm to realise the communication system from PCD to *master* at the application layer of the network. The control algorithms, illustrated as flow-charts, in Fig. 2 are summarized as follows: The DS_1 node will advertise a connection to S_1, and similarly, the MS_1 node will advertise a connection to the *master*. Since BLE is a connection orientated wireless technology, only the *master* and PCD may initiate a connection to their respective slave node. The PCD must however run the BLE stack on its firmware while also acting as a *master* in the network. After DS_1 advertised a connection, the PCD will connect and bond with DS_1. Similarly, after MS_1 advertise a connection, the *master* will connect and establish a bond with the MS_1. Bonding of the *slaves* will ensure that whenever a connection is lost with the *master* or PCD, a secure connection with unique *slave* identification will be established to reconnect with DS_1 or MS_1 [5]. The PCD will start requesting regular data updates from DS_1 via BLE while DS_1 will request regular data updates from MS_1 via the Universal Asynchronous Receiver Transmitted (UART) or wireless ANT+ connection. Similarly, the *master* will update MS_1. If an acknowledgement error by the PCD is detected by a request not received by DS_1, after a certain number of attempts have been exceeded as illustrated by the control chart in Fig. 2B and 2C, the PCD will initiate its shut-down as illustrated by the control chart in Fig. 2A. Consequently, the *slaves* DS_1 or MS_1 will reset their MCU by their respective watchdog timers. Ideally, the initiation of the PCD shutdown may be accomplished by software development of the

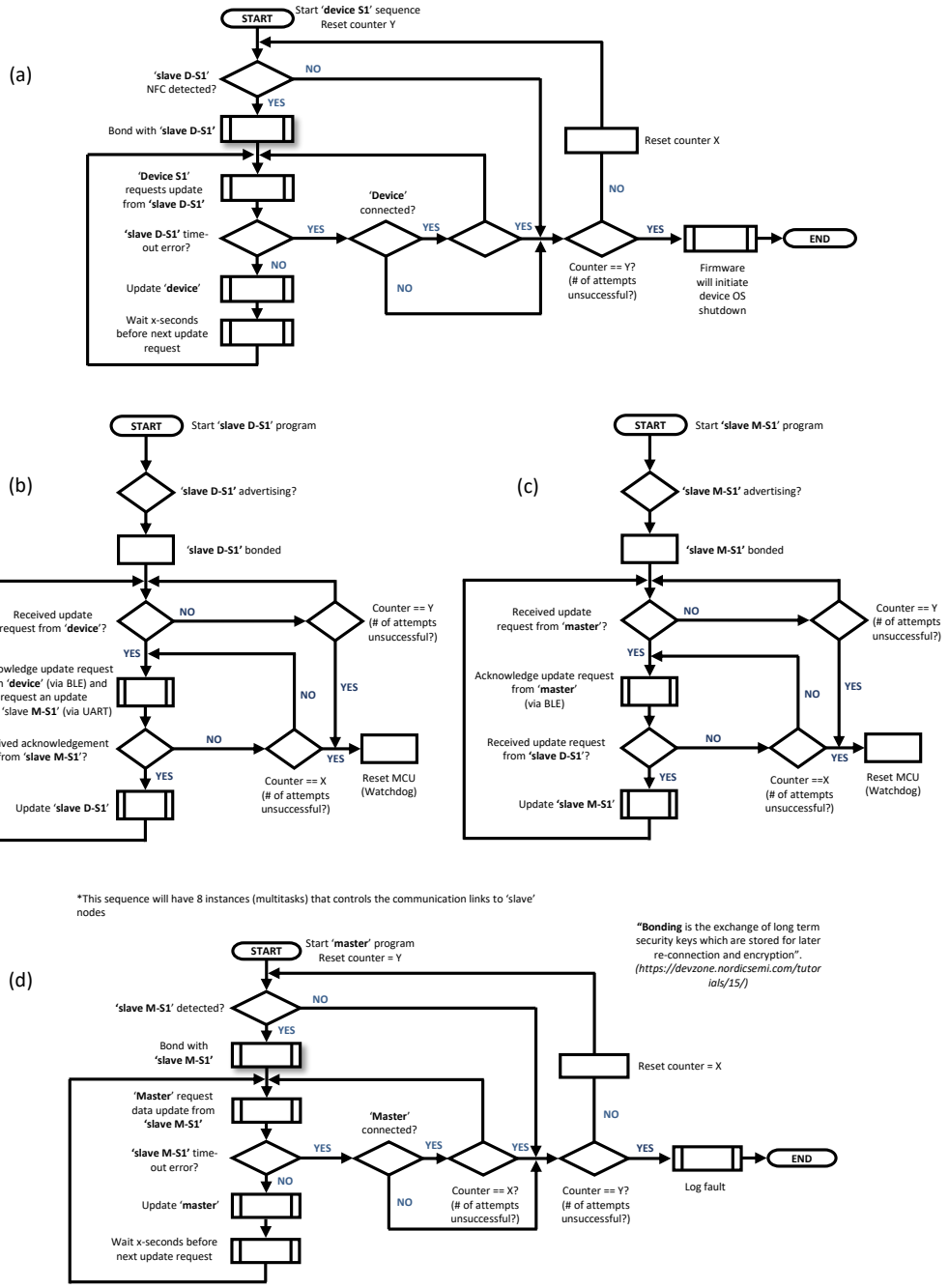


Figure 2: Proposed BLE network topology algorithms (concept design).

firmware. Potentially, after the PCD is rendered inoperable, the theft detecting mechanism may enable a tracking system. If the PCD is operated in an undesignated area or tampering is detected, the firmware must ensure that the device is rendered unusable. Subsequently, when the PCD detects a GPS, tracking must be enabled. If the connection to the GPS is lost, the state will continuously try to reconnect to enable the tracking system. For tracking, it is important that sufficient battery power is stored, before an OS shutdown, to execute the algorithm successfully.

2.1.2. Hybrid mesh-star network topology: The nRF52 from Nordic Semiconductors provide application programming interfaces which support the BLE, ANT+ and Thread stacks while other low-powered SoC is widely available for ZigBee such as the CC2640/CC2650 from Texas

Instruments [6]. The latest nRF52 low-powered SoC solution can run BLE and the proprietary 802.15.4 stacks concurrently. A developer may also choose to utilize ZigBee on the nRF52 SoC which requires the protocol to be built on top of the hardware layer of the IEEE 802.15.4 standard. Fig. 3 proposes a hybrid mesh-star topology (ANT+, ZigBee, or Thread) that offers a distinct advantage over the proposed BLE topology in Fig. 1 by what is known as mesh multi-hopping in a network. Furthermore, the ZigBee and Thread protocol mesh topologies, allows hundreds of nodes to communicate over the network and may be adapted to the proposed network topology.

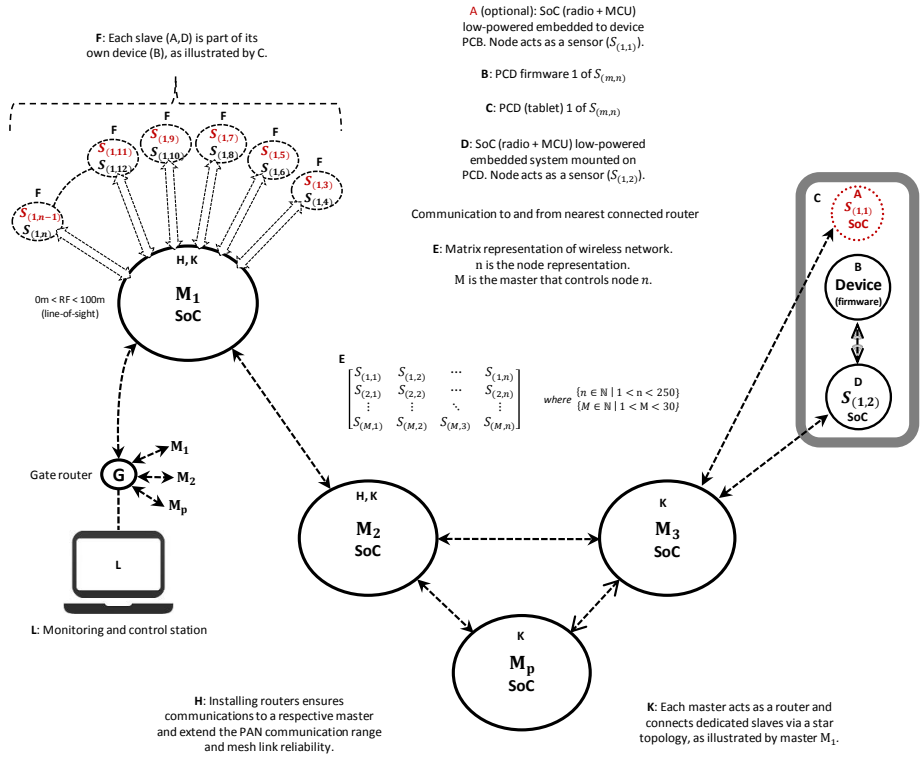


Figure 3: Proposed hybrid mesh-star wireless network (concept design).

In Fig. 3, a Wireless Sensor Network (WSN) is configured in a building on a campus (large educational institution) area. ZigBee and Thread uses Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) to ensure reliable and robust communications in the mesh network which provides highly secure AES-128 standard encryption and decryption of packets over the air [7]. A *master* acts as a router and can relay data packets from slaves or *end-devices* to other routers in the network. The router will continually run the SoC radio and processor program and does not rely on low-power consumption requirements. A PCD shown in Fig. 3C, shown as the *end-devices* $S_{(1,1)}$ and $S_{(1,2)}$, requests regular updates about connectivity from its *master* or from the nearest *router* in the network. *End-devices* consumes very little power since the SoC goes into sleep mode when not communicating with its *master*. However, the ZigBee and Thread wireless technologies, does not provide the routing of packets directly over the network by consecutive *end-devices* [8].

Optionally in the proposed design, if an acknowledgement is not received by $S_{(1,1)}$ from node M_3, then node $S_{(1,1)}$ will command the PCD shutdown by means of the integrated SoC hardware to the PCD. Ideally, if the PCD firmware in Fig. 1B, does not confirm from node $S_{(1,2)}$ its connectivity to the mesh network by node M_3, a shutdown of the PCD OS must be initiated. Node $S_{(1,2)}$ may be connected over the most reliable link to a router as illustrated by node M_3. If the PCD is operated in a building where it cannot directly communicate with node M_3, an alternative router have to be selected in the mesh network. Such autonomous *slave* to *master* link behavior requirements, make this application ideal for implementation for low-power Thread networks. Multi-hop hybrid mesh network topologies may be used in different building areas where PCD have to communicate over larger distances and obstacles are unavoidable. Additional routers may be installed to enable reliable communications between all masters in the network. Each node in the network will consist of the miniature nRF52 SoC shown in Fig. 4 and illustrated in Fig. 2A and 2D. As mentioned

previously, the SoC in Fig. 2A may potentially be embedded in the tablet PCB hardware to render the device inoperable. This solution will disable the PCB, but will be further explored regarding its plausibility. More realistically, a firmware-based solution however, will render the PCD inoperable when no heartbeat is sensed from $S_{(1,2)}$ to the wireless mesh network.

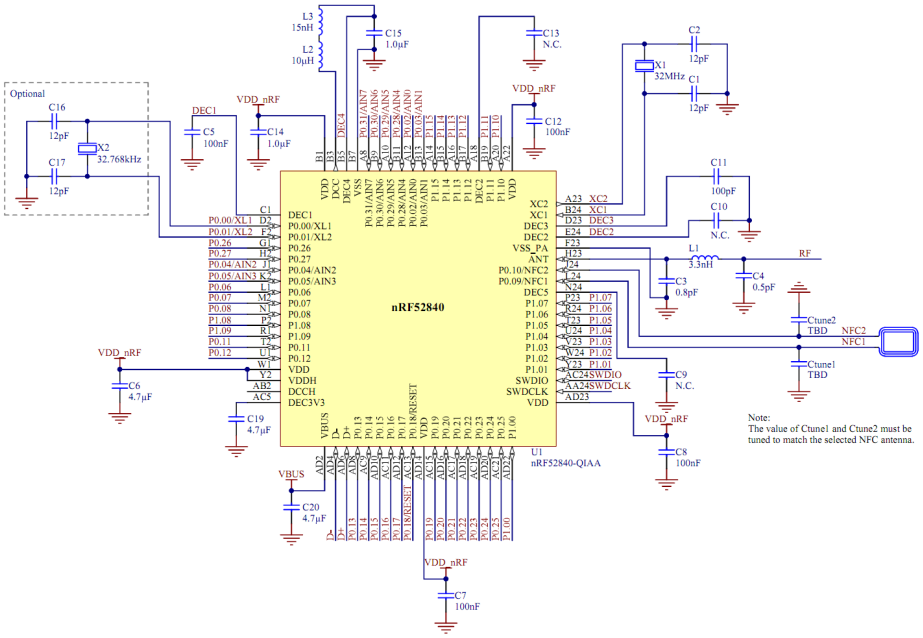


Figure 4: nRF52840 SoC IO schematic (7 mm x 7 mm 73 pin AQFN package) [6]

2.1.3. Energy harvesting: The wireless technologies described utilize low-power consumption devices that may make use of energy harvesting methods to convert energy from either or both RF and thermal sources to regulate a supply or charge a battery of a *slave* or *end-device* node. Harvesting energy from the environment requires Integrated Circuits (IC) with highly optimized DC-DC boost converters and power management circuitry capabilities. An experimental study will be conducted to determine the output power of a suitable harvesting source. Once these output levels are identified and found to be feasible, an energy harvesting solution may potentially be implemented that may integrate either the LTC3108 [9] or the MAX17710 [10] IC with the SoC. Thermal electric energy harvesters that utilize the Peltier element may offer higher source output levels compared to RF harvesting [11] because of small temperature differences that generate voltages. A PCD may naturally generate heat at its power source and central processor unit over a certain amount of working operation. A Peltier element may be installed on the PCD that absorbs the transferred heat from the junctions [12]. The electrical energy generated from the harvester can then charge a coin or thin cell battery which directly supply power to the SoC with the appropriate electronics designs in place. For this particular application, further research is necessary to determine feasibility for energy harvesting using RF or thermal sources.

3. DISCUSSION

The network topology proposed implementing BLE has shown to be more complex which may provide better network stability and security compared to other wireless technologies. At the moment, BLE has shortfalls by not allowing the mesh topology design shown in Fig. 3 and only providing a limited number of node connectivity to a *master* in the network. Mesh network topologies may be simulated in Matlab or NS-3 to test routing algorithms for implementation on embedded hardware, with a particular focus on ZigBee or Thread wireless technologies. By modeling the environment where the wireless network will be distributed, signal strength path loss exponents can be determined and routers can be placed optimally in a building area. With multi-hop formation capabilities in a network, greater RF communication distances are possible which extends routing distances for reliable data delivery from *device* to its *master*. The radio power consumption of the nRF52832, is

rated at four dBm (with wireless distances of up to 100 m line-of-sight) and estimated by the 'BLE online profiler' to only consume around 15 uW of power over two-second regulatory updates between *master* and *slave* [13]. The power consumption rating excludes the UART or ANT+ communication between DS_1 and M_1 shown in the proposed network topology of Fig. 1. The SoC will therefore consume more power than previously stated because of the utilization of the processor's UART peripheral or multi-protocol functionality of the radio with ANT+. Nonetheless, the radio power specifications indicate that a single *slave* node can run for more than four years on a coin cell battery rated at 300 mAh and efficiency of 70 %. With such low power constraints, *slave* nodes can be powered by thin cell batteries or energy harvesting sources. Similar low-power consumability of the *slave* nodes is possible in the proposed multi-hop mesh wireless topology, assuming a *slave* does not have a duty cycle (*device* active time over total time) greater than 1 % [8].

A typical solution to prevent flashing of a PCD firmware is for manufacturers to add authentication ability to their hardware [14]. Some companies provide solutions in preventing devices from factory reset and installation of new PCD firmware [15]. Such companies use patented technology whereby their firmware is built into the hardware during the PCD manufacturing process [15]. This study, however, will initially focus on an in-depth experimental study on the reliability of the proposed wireless mesh technology followed by a proprietary firmware-based solution to render the PCD unusable.

References

[1] Phaladi B 2015 http://citizen.co.za/news/news-national/382489/schools-tablet-theft-shock/
[2] Writer S 2015 https://businesstech.co.za/news/gauteng-withdraws-88000-tablets-from-schools-because-of-theft/
[3] Dementyev A, Hodges S, Taylor S and Smith J 2013 Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario *2013 IEEE International Wireless Symposium (IWS)* pp 1–4
[4] Nordic-Semiconductor 2016 https://www.nordicsemi.com/Products/nRF52-Series-SoC/
[5] Heydon R 2007 *Bluetooth Low Energy: The Developers Handbook* 1st ed (Indiana: Prentice Hall)
[6] Nordic-Semiconductor 2017 https://infocenter.nordicsemi.com/index.jsp
[7] Gislason D 2008 *ZigBee Wireless Networking* 1st ed (Burlington: Newnes)
[8] Farahani S 2008 *ZigBee Wireless Networks and Transceivers* 1st ed (Burlington: Newnes)
[9] Linear-Technology 2017 http://www.linear.com/product/LTC3108
[10] Maxim-Integrated 2017 https://www.maximintegrated.com/en/products/power/MAX17710.html
[11] Gudan K, Chemishkian S, Hull J J, Thomas S J, Ensworth J and Reynolds M S 2014 A 2.4ghz ambient rf energy harvesting system with -20dbm minimum input power and nimh battery storage *2014 IEEE RFID Technology and Applications Conference (RFID-TA)* pp 7–12
[12] Nesarajah M and Frey G 2016 Thermoelectric power generation: Peltier element versus thermoelectric generator *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society* pp 4252–4257
[13] Nordic-Semiconductor 2016 https://devzone.nordicsemi.com/power/
[14] Zetter K 2015 https://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/
[15] Absolute 2016 https://lojack.absolute.com/en/persistent/