System control applications of low-power radio frequency devices

R M van Rensburg[1], **B Mellado, C J Sandrock**

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

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

Abstract. This paper realizes a wireless network development for application deployment to reduce theft of portable computer devices utilized in educational institutions. The study aims to develop a low-cost, low-power and reliable wireless network that can eradicate the accessibility of a device human interface. A portable computer device which is operated in a field perimeter where device communication in the network is restricted, indicating a possible theft scenario, will initiate a shutdown of its operating system that renders the device unusable. Design outcomes thus far indicate that a robust wireless network, using low-power embedded hardware, is feasible for anti-theft applications. Preliminary results indicate the reliable performance of data communications between interconnecting nodes in a harsh indoor building environment using the Thread networking protocol.

1. Introduction

In 2015 the South African government spent billions of rands in modernizing learning institutions with the goal of fully digitizing schools by the year 2020. It was reported that a substantial amount of tablets were lost due to theft that consequently jeopardized the project because of the significant financial loss incurred by the government [1]. This led to more than 88000 tablets being recalled and fitted with an anti-theft technology in order to protect the investment. The upgrade of the devices enabled the government to involve investigative authorities in the tracking of stolen tablets [2]. The tracking systems, however, appeared only operational with the device powered-on to communicate with global positioning satellites in outdoor environments.

With deficits currently present in the protection of such devices, there is a need to improve the security of these devices by taking advantage of the wireless technologies today. This paper presents a preliminary performance analysis of a low-power wireless network for application deployment to protect a Portable Computer Device (PCD) such as a tablet against theft in indoor building environments. A PCD operated in a perimeter outside the wireless network may initiate a shutdown of its operating system by using a polling algorithm to communicate to the wireless network located at a educational institution.

2. Methodology

An embedded system with a multiprotocol radio and advance processor capabilities was fully utilized during the inception phase of the development of the network. An ad-hoc wireless

[1] Present address: School of Physics, University of the Witwatersrand, Johannesburg 2050, South Africa.

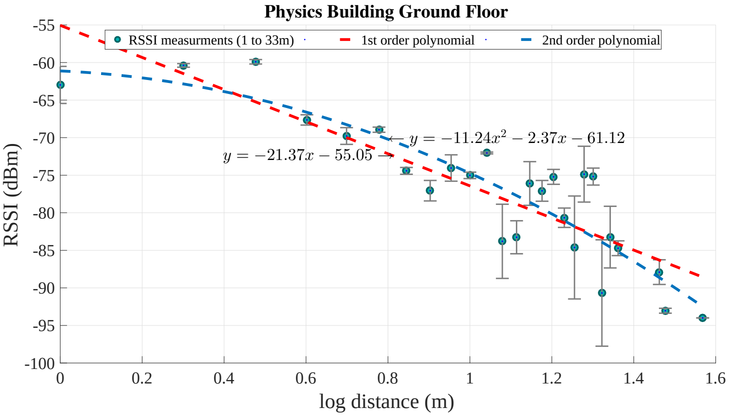


Figure 1: $RSSI$ versus $log_{10}(d)$ at Tx = 0 dBm.

network consisting of ten nodes was developed in an indoor building environment. Field measurements of each node's quality of service from a remote indoor location were recorded.

3. Experimental Study

The Physics building at the University of the Witwatersrand was used as an indoor testing environment where radios were distributed at specific areas located on the ground floor. The building consists of many obstacles or what is termed as shadow regions that may inadvertently affect radio transmissions between nodes in the network. In this section, an experiment is set up which determined the Radio Frequency (RF) path loss at a specific area of the building. Finally, the network performance and reliability is analyzed and results concluded.

3.1. Received Signal Strength (RSS) versus Distance Estimation

Path losses are signal attenuations of electromagnetic wave propagations due to reflection, diffraction and scattering in indoor environments which may be modelled to determine the RF range [3]. In the Physics building ground floor hall area, signal strength measurements between two nRF52840 transceivers were taken at various distances to determine the RF coverage area. The nRF52840 from Nordic Semiconductor integrates a miniature radio and Micro-Controller Unit (MCU) for use in ultra-low power applications. Multiple 2.4 GHz protocol stacks can be run on the System-on-Chip (SoC) concurrently. The nRF52840 (hereafter referred to the SoC) is a 7 mm x 7 mm chip that houses a 32-bit 64 MHz ARM Cortex-M4F MCU with 1 MB flash and 256 kB of RAM. Utilizing two tranceivers, the RF path loss is determined from the Log Distance Path Loss Model [3]:

$$RSSI = 10n\log_{10}(d) + E \tag{1}$$

where $RSSI$ is the received signal strength indicator in dBm, n is the path loss exponent, E is an environmental constant and d is the distance of the $RSSI$ measurement from transceivers in meters. Parameter n is determined using polynomial least-squares regression of the logarithmic distances and averaged RSS measurements. With reference to Eq.1 and depicted in Fig.1, the path loss exponent n is estimated at 2.137 ($m = 10n$) and the environmental constant E at 55.05. In free space, $n = 2$ and where obstacles are present, $n > 2$. [3].

The fit demonstrated a 87.58 % of the total variation in the data about the average. By running similar experiments, nodes may be optimally distributed to cover a wide range of areas in the building. RF attenuation due to obstacles may be determined experimentally through similar field measurements. To aid in indoor propagation modelling, researchers have accumulated huge

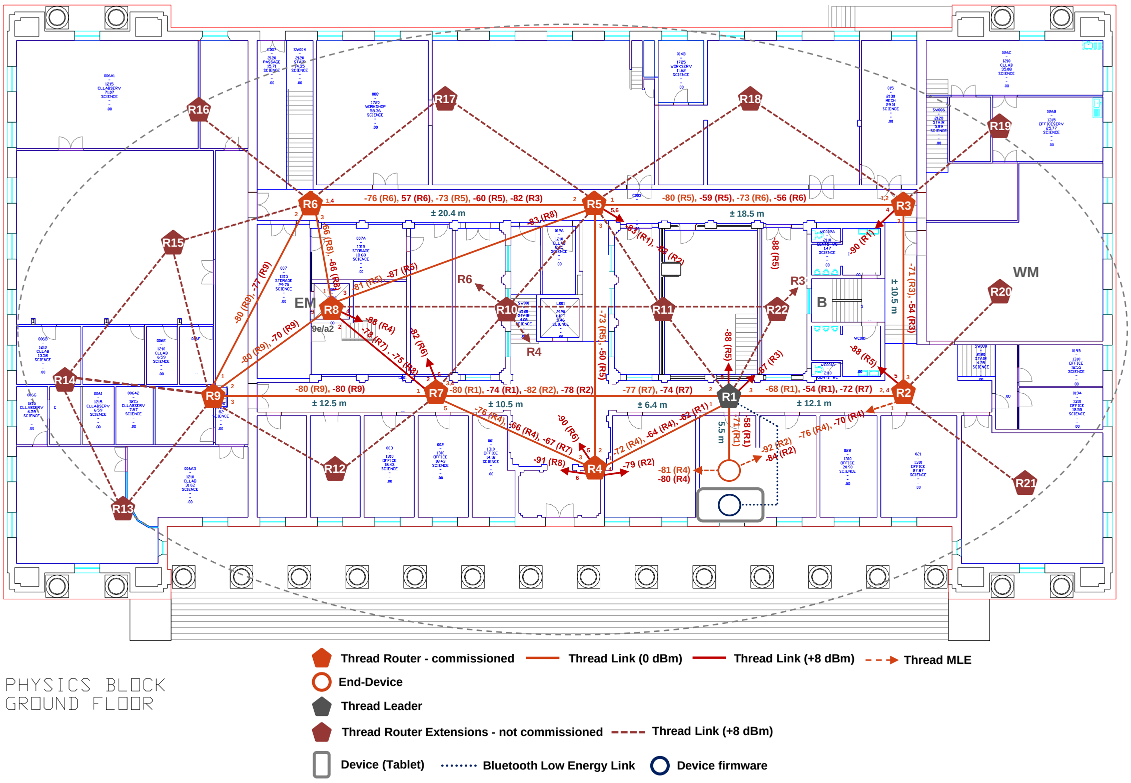


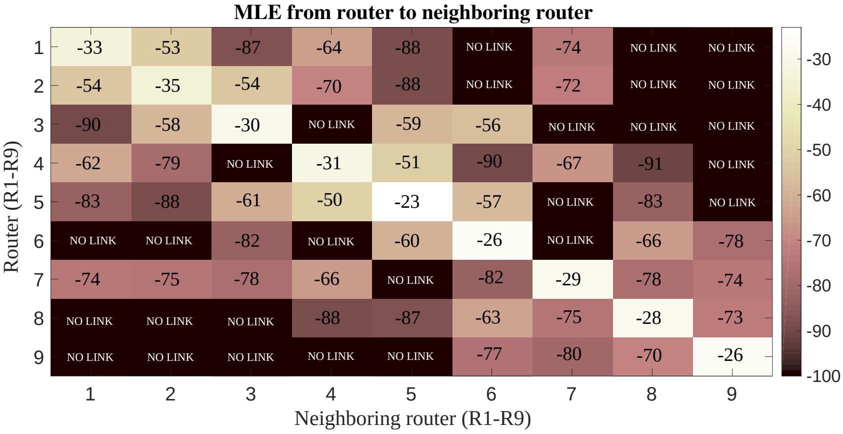
Figure 2: Experimental development of Thread network.

amounts of signal loss measurement data of building material in indoor environments [3]. With reference to Fig.1, further analysis indicates reliable data transmissions should be expected between transceivers not exceeding $\log_{10}(20)$ line-of-sight distances or $RSS \geq -80\ dBm$ in both directions for the SoC radio transmitter outputting power at Tx = 0 dBm. With the radio transmitting at Tx = +8 dBm, more than double the RF distances may be covered for reliable data transmissions but with an increase in SoC power consumption.

3.2. Development of the network

OpenThread, which is a relatively new wireless technology developed by Nest, is an open-source implementation of the Thread networking protocol. Nordic Semiconductor and several hardware platforms from other manufacturers are contributing members to the development of Thread. OpenThread (hereafter referred as Thread) is a Thread certified component which adheres to all the features defined in the Thread 1.1.1 specification [4].

The Thread network contains *border-routers*, *routers* and *end-devices*. *Border-routers* are *routers* that connect the IEEE 802.15.4 Thread network to WiFi or Ethernet networks for remote monitoring and control. *Routers* are nodes in the network that provide communications services between nodes. The Thread networking protocol provides autonomous mesh connectivity between all *routers* in the network by continuously checking the reliability of links between nodes in both directions using the Distance Vector Routing (DVR) protocol and Trickle algorithm [9]. An *end-device*, also known as a *sleepy child*, is a low-power device which operates under small duty cycles. The child device may only communicate directly with its *router* parent to other *routers* in the network. The Thread networking layer also ensures automatic reallocation of an *end-device* to a parent *router*. When the *end-device* is moved to a different area and coverage to the existing parent route is lost or a parent *router* fails, a new parent *router* will be allocated



	1	2	3	4	5	6	7	8	9
1	-33	-53	-87	-64	-88	NO LINK	-74	NO LINK	NO LINK
2	-54	-35	-54	-70	-88	NO LINK	-72	NO LINK	NO LINK
3	-90	-58	-30	NO LINK	-59	-56	NO LINK	NO LINK	NO LINK
4	-62	-79	NO LINK	-31	-51	-90	-67	-91	NO LINK
5	-83	-88	-61	-50	-23	-57	NO LINK	-83	NO LINK
6	NO LINK	NO LINK	-82	NO LINK	-60	-26	NO LINK	-66	-78
7	-74	-75	-78	-66	NO LINK	-82	-29	-78	-74
8	NO LINK	NO LINK	NO LINK	-88	-87	-63	-75	-28	-73
9	NO LINK	NO LINK	NO LINK	NO LINK	NO LINK	-77	-80	-70	-26

Figure 3: Mesh Link Establishment (MLE) by RSS at Tx = +8 dBm .

to the *end-device* based on the quality of alternative links in the network. One of the *routers* is always selected as a leader and is responsible for joining other *routers* in the network. All *routers* in the network share persistent data of the leader. If the leader fails, another *router* node will be selected as leader, therefore ensuring no single point of failure [5].

Nordic Semiconductor's Thread Application Programming Interface (API) consists of programming functions to interface with the Thread stack. The Thread stack is flashed as binary files to the MCU using the GCC compiler and SEGGER-link programmer tools. The API was used to configure a Thread network by programmatically setting node roles and testing the performance of the network.

As depicted in Fig.2, the development of the Thread network consisted of nine *routers* (R_1 to R_9) distributed on the ground floor. Routers R_8 and R_9 were mounted at a mezzanine area where walls obstructed the propagation of RF waves but sufficient links were established with neighboring routers. An *end-device* was used to send Internet Control Message Protocol (ICMP) packets to individual *routers* from a remote location to test the performance of the network. In Fig.2, R_{10} to R_{22} illustrate potential *router* installations in the building ground area which may add additional redundancy in links connectivity between nodes in the mesh network. Thread allows up to a maximum of 32 *routers* and 511 *end-devices* per parent *router* to be connected to a single network provided ample MCU processing and memory are allocated to run the Thread stack. MLE periodically sends multicast messages defined by the DVR protocol to estimate the quality of the links from neighboring *routers* in the network [4]. Advertisements or messages are sent periodically by the Trickle algorithm to determine the rate of change of network traffic in order to update routers [9]. The quality of the *router* links of the network is presented in Fig.3 where the link information was used to determine the mesh topology in Fig.2. The diagonal elements from left to right represent the *end-device* link quality placed within one meter to a *router* followed by the link quality of the *router* with neighboring routers displayed in the rows. As an example, depicted in Fig.2 and displayed in Fig.3, R_1 established five potential links with neighboring routers R_2, R_3, R_4, R_5 and R_7 at Tx = +8 dBm. The DVR protocol will ensure that a link is established with a neighboring *router* in both directions with the best link quality, in this example R2 at -53 dBm (R_1, R_2) and -54 dBm (R_2, R_1). If for some reason R_2 fails, the next best available link is $R4$ for data transmissions at -64 dBm (R_1, R_4) and -62 dBm (R_4, R_1). As expected, results indicate more links with neighboring *routers* are established at Tx = +8 dBm which may provide better reliability of data transmissions over longer multi-hopping distances. For more information on Thread and MLE, a comprehensive specification is available on the Thread Group website at [4]. The OpenThread software stack can be found at [8].

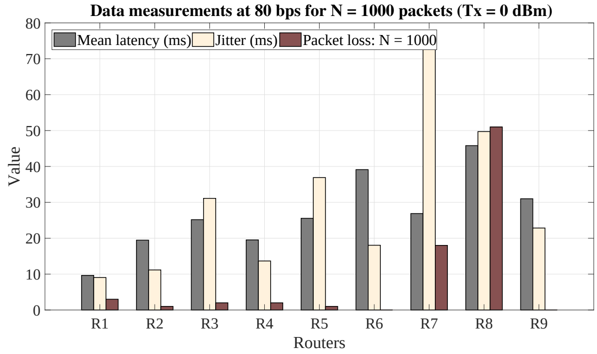


Figure 4a: Performance at Tx = 0 dBm.

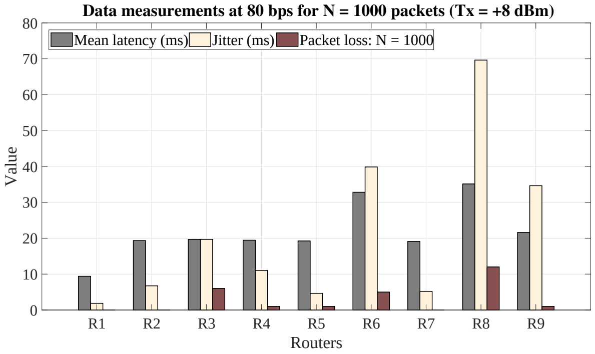


Figure 4b: Performance at Tx = +8 dBm.

3.3. Data Collection and Analysis

In this section, the reliability and performance of the network are evaluated. A loop containing 1000 samples of data packets was sent at a throughput of 80 bps from the *end-device* to a *router* and echoed back to the *end-device* where the latency measurements were recorded. A statistical approach was followed whereby the distributions and probabilities of the latency measurements were computed. The following figures are analyzed:

- In Fig.4a and Fig.4b, the test results concerning the network reliability and performance are presented from *end-device* to each *router* in the network for each node programmed at Tx = 0 dBm and Tx = +8 respectively.
- In Fig.5, latency measurements concerning the network performance from the *end-device* to R_1 through to R_9 are combined in a single data vector. The latency distribution and probability plot are shown at Tx = 0 dBm and Tx = +8 dBm respectively.

Assuming a constant packet loss, the reliability of the network is computed by the packet delivery ratio $PDR = packets\ recieved\ \times (total\ number\ of\ packets\ send)^{-1}$ which indicate reliable packet transmissions for both Tx = 0 dBm and Tx = +8 dBm field measurements. However, there does exist a variation of latency delay known as jitter which may be caused by obstacles in the RF propagation region, especially routers R_7 and R_8 because of their location in a mezzanine area. At a throughput of 80 bps, the latency data in Fig.5 lies approximately on the straight lines and therefore the data is approximately lognormal distributed. The lognormal distributions provides a reasonable model for analyzing the the performance of the network:

- Fig.5a reveal a 99 % confidence interval of $\mu = 26.80 \pm 0.31$ and $\sigma = 11.49 \pm 0.22$. There exist a 1 % probability that latency delay are $\geq$ 60 ms.
- Fig.5b reveal a 99 % confidence interval of $\mu = 21.72 \pm 0.2357$ and $\sigma = 8.66 \pm 0.17$. There exist a 1 % probability that latency delays are $\geq$ 50 ms.

The measurements in the above figures indicate that the latency data are multimodal and positively skewed. The skewness indicates greater latency delays in some of the multi-hopping routes and therefore causes some performance degradation in the network. The degradation may be caused by CCMA-CA operations and/or retransmissions of packets due to acknowledgements not received caused by obstructions in the environment. Outliers may be caused by CSMA-CA retransmissions, substandard link quality or packet relays/transmissions over greater multi-hopping distances.

3.4. Conclusion

In this paper, a low-power network based on the Thread networking protocol was developed. By installing an *end-device* securely onto the PCD, hundreds of *end-devices* representing tablets

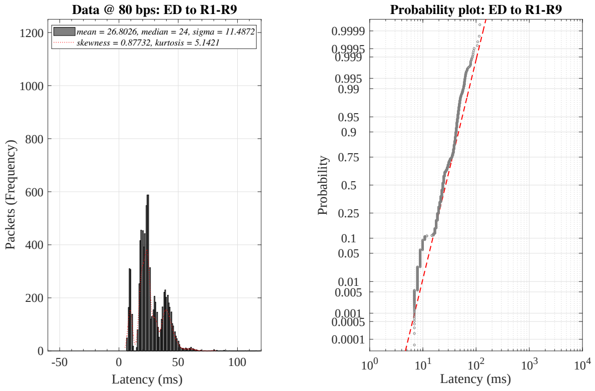


Figure 5a: Distribution at Tx = 0 dBm.

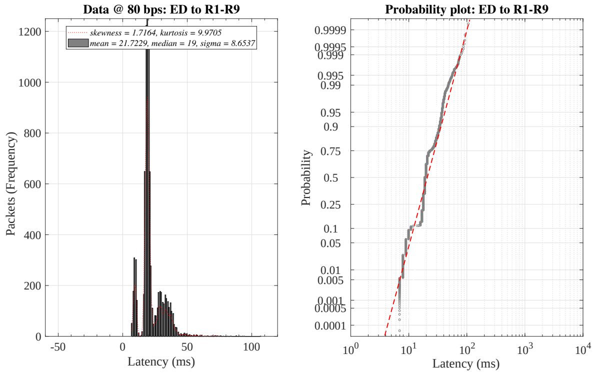


Figure 5b: Distribution at Tx = +8 dBm.

my be connected to a single router. However, by omitting the *end-device* in the network design, the PCD may communicate directly with the nearest router by using Bluetooth-Low Energy (BLE) to communicate to a router where a router runs BLE and Thread concurrently. Nordic Semiconductor provides both wireless technology solutions on their SoCs.

A simple path loss propagation model was implemented to determine the RF ranges of the SoC at Tx = 0 dBm. The estimated RF line-of-sight distance or averaged RSS value aided in the distribution of *router* nodes (R1-R9) in the building ground floor area. Additional MLE were discovered with greater RF ranges with the radio set at a higher transmitting output power. For this particular building environment, an *end-device* will mostly have at least one stable link ($RSSI > -80\ dBm$) to a parent *router* when placed at any location inside the building perimeter. However, some areas in the building do cause a high decrease in signal propagation due to obstacles and shadowing caused by concrete walls ($RSSI < -80\ dBm$). To compensate for this, the network coverage and additional MLE redundancy may be greatly improved by incorporating additional *routers* in the network development as depicted by R_{10} to R_{22}. Finally, a statistical approach was followed to represent field measurements. Results indicate acceptable latency delays and PDR between point to multipoint node communications.

3.5. Future Work

Similar latency confidence intervals are assumed if field measurements are taken for an *end-device* located at a different location inside the building perimeter, provided the *end-device* has a reliable link to its parent *router*. A comprehensive multipoint to multipoint node field measurements and analysis will be conducted. The *end-device* may be omitted from ther design by incorporating a multiprotocol wireless system using BLE of the PCD to communicate to the Thread network. A proprietary PCD firmware solution is needed from a reputable tablet manufacturer to render a device inoperable.

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/government/87334/gauteng-withdraws-88000-tablets

[3] Rappaport T 2002 *Wireless communications principles and practice* 1st ed (New York: Prentice Hall) p 69-127

[4] Thread Group 2017 http://threadgroup.org/ThreadSpec

[5] Thread Group 2017 https://threadgroup.org/ourresources

[6] IEEE Standards Association 2017 https://standards.ieee.org/findstds/standard/802.15.4-2006.html

[7] Nordic Semiconductor 2017 https://infocenter.nordicsemi.com/index.jsp

[8] OpenThread 2014 https://github.com/openthread/openthread

[9] Trickle Algorithm 2011 https://tools.ietf.org/html/rfc6206