A Remotely Programmable Modular Testbed for Backscatter Sensor Network Research

Eleftherios Kampianakis, John Kimionis, Konstantinos Tountas, and Aggelos Bletsas

ECE Department, Technical University of Crete, Greece
{ekabianakis, ikimionis, ktountas}@isc.tuc.gr, aggelos@telecom.tuc.gr

Abstract. The necessity of backscatter sensor networks (BSNs) has recently emerged due to the need for large–scale, ultra low–cost, ultra low–power, wireless sensing. Development of such networks requires tools for rapid prototyping and evaluation of key-enabling BSN technologies. Although tools for testing wireless sensor networks (WSNs) have been widely developed over the last few years in the form of *testbeds*, almost no significant testbed examples exist for BSNs. Throughout this work, a set of hardware, firmware and software components have been designed and implemented, creating a BSN research testbed. The latter employs a modular architecture and enables rapid prototyping of critical components for low–cost, large–scale BSNs. Testbed components enable microwave, detection, coding and multiple access research, tailored for backscatter radio and networking. The testbed offers dynamic reconfiguration through implementation of remote, over the air programming (OTAP), that reduced programming time per node by two orders of magnitude. An overview of the testbed is given, and its modular tools are described in terms of functionality and importance for BSN research.

1 Introduction

Technologies such as wireless sensor networks (WSNs) [1] and backscatter sensor networks (BSNs) [2, 3] lead towards large-scale, low-cost, wireless connectivity. Development tools for WSNs are widely developed, with typical examples being demonstrated in [4]. Testbed architecture includes wireless nodes under test, connected to interface boards acting as *monitors*. A gateway using a high level network interface (e.g Ethernet, 802.11) communicates with the interface boards.

On the other hand, limited research tools exist for BSN research and development. One example towards that direction is the work in [5], where a set of custom microwave devices for monitoring performance of radio frequency identification (RFID) antennas is presented. However, the setup is confined in measuring only microwave and antenna parameters.

This paper describes the hardware and software components for the development of a BSN testbed. A prototype node with a single microcontroller unit (MCU) is developed that accommodates both a backscatter and a high level radio interface. The backscatter radio interface is implemented with a single RF

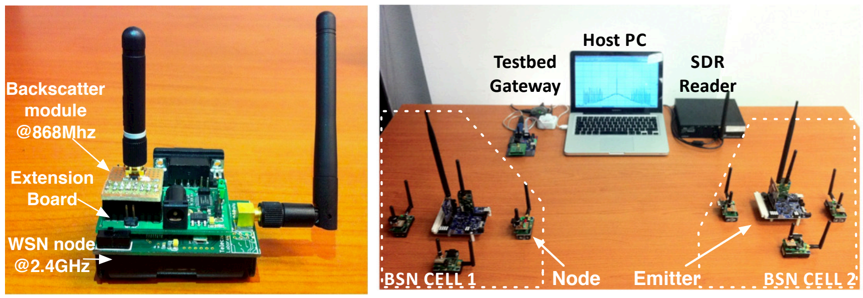

Fig. 1. Left: Hybrid testbed node. Right: Experimentation testbed.

transistor controlled by the MCU. The transistor acts as an antenna load switch, thus achieving backscatter modulation when an incident wave is reflected by the antenna [6]. For the high level control link, a 2.4Ghz radio module is utilized.

The hybrid node developed (Fig. 1-left) acts both as the DUT, which is a semipassive backscatter *tag* similar to the one presented in [7], and as the unit for remote programming, control and debugging functions. The DUT and monitor functions are constructed in software such that they are completely independent to one another.

The constructed testbed is shown in Fig. 1-right and its architecture is shown in Fig. 2. Remotely controlled Carrier emitters at the UHF band (868MHz) illuminate the hybrid testbed nodes; the latter scatter back modulated information using a single transistor front-end. A software defined radio (SDR), tuned at the UHF band, acts as the tag receiver (reader). The SDR is connected to a host PC, where all signal processing takes place in software. The PC also hosts the testbed gateway, which transmits control packets and executable code to the hybrid nodes and the carrier emitters, over a reliable 2.4GHz link. It also receives debugging messages and feedback from the monitoring nodes. Instead of monostatic architecture, commonly used in RFID systems, bistatic backscatter radio is utilized (i.e emitter dislocated from receiver). Bistatic architecture allows extended communication ranges thus rendering broad area BSNs [8] viable.

This is the first effort towards the construction of a complete BSN testbed that is flexible, remotely programmable, and BSN research-oriented. Research topics such as detection schemes, resource allocation techniques, networking algorithms, as well as RF hardware (e.g switching transistors) and antennas where examined end evaluated with the utilization of this work.

The paper is organized as follows: Section 2 describes the benefits of utilizing the BSN testbed. Section 3 gives the description of the hardware and software components required for the testbed implementation. Section 4 provides a set of research-oriented experimentation scenarios for testbed evaluation. Finally, Section 5 offers the conclusion of this work.

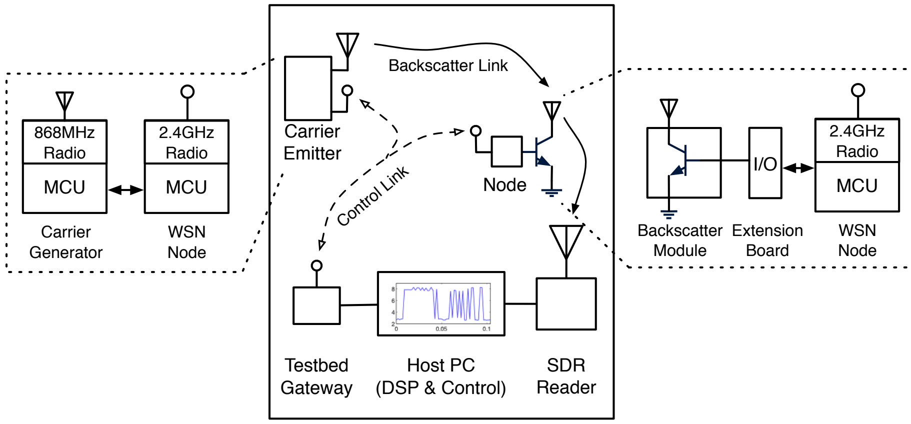

Fig. 2. Center: Testbed overview. Left: Carrier emitter. Right: hybrid node architectures.

2 Benefits/Features of a BSN Testbed

The utilization of a BSN testbed offers engineers *mobility–portability*, *long range remote programmability*, *debugging and network monitoring*, high level of software and hardware *flexibility*, *dynamic reconfigurability*, with relatively *low cost* and most importantly, *reduced experimentation time.*

Portability is a critical feature for real-life, outdoor network testbeds. Fig. 3 shows a testbed deployment outdoors, where environmental sensing applications are evaluated. Six hybrid nodes are place around a battery-operated carrier emitter and up to 17 meters away from the reader. The SDR reader the host PC and a spectrum analyzer (for debugging purposes) are placed in fixed position due to the power supply needed for the SDR. However , the latter could be modified for completely portable operation (e.g. see work in [9]).

Over the air programming (OTAP) is utilized in this work, as in many WSN testbeds. It allows wireless programming of network nodes with limited access, and accelerates the overall software development process. Particularly, with wired programming, for an outdoor, six node network such as the one in Fig. 3, a total time of 12 minutes (720 seconds including mobility) is required for programming the network. With OTAP utilization, programming time is reduced to 12 seconds (i.e two orders of magnitude reduction).

All components of the testbed are low-cost commodity solutions, or custom-built, in-house fabricated hardware. Particularly, backscatter radio hardware (i.e RF transistor, antenna) can be replaced and various sensors and actuators can be easily installed. Carrier emitters are fully configurable through software in terms of frequency and output power. Applications, from simple LED blinking to backscatter communication schemes are written in simple C language. Finally the total cost of the testbed depicted in Fig. 1-right is approximately 2300 Euros, with the PC and SDR being the most expensive, while hybrid nodes cost an order of magnitude less.

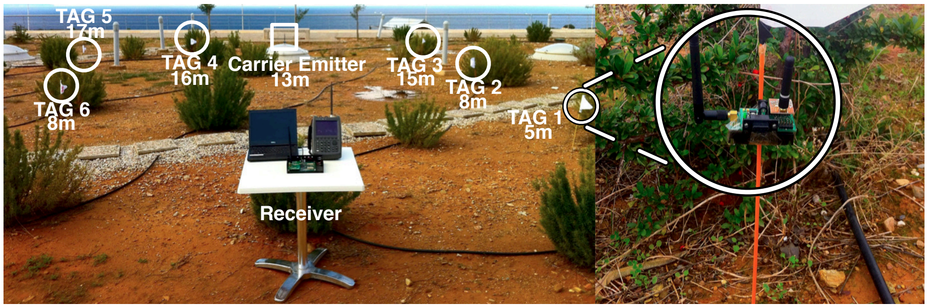

Fig. 3. Remotely programmable testbed and hybrid node, outdoor deployment.

3 Testbed Implementation

Hardware. The core testbed module is a hybrid node.

Having the classic WSN testbed in mind a WSN node was utilized to act as the monitoring device and as the DUT. A module equipped with a backscatter RF front-end is connected to the interface board of the WSN node [10]. The node exchanges control data with the gateway using the embedded 2.4Ghz RF module and backscatter communication is achieved with the backscatter module.

The backscatter module is equipped with a RF transistor and an SMA antenna connector. The transistor's base is driven by an MCU pin, while the other two are connected to the antenna terminals. When the MCU drives the base pin on high level or low level, the transistor acts as a short or an open circuit, respectively. This allows switching between two antenna reflection coefficients, therefore enabling backscatter modulation [6, 11]. Fig. 1-left depicts the implemented node and Fig. 2 (right) depicts node architecture.

To enable backscatter communication, low-cost, battery-operated RF carrier emitters are utilized. These devices, in the form of monolithic MCU–radio, are programmable signal generators. These modules are connected with the WSN nodes via the reliable 2.4GHz link and as result, there is full control over the whole network. Several of the devices may exist on a test field, promoting experimentation with bistatic/multistatic backscatter links. These are less-explored backscatter architectures, with emerging research interest [8, 12, 13].

For the reception of backscatter signals, a commodity software defined radio (SDR) is used, while the processing takes place on a host PC, using MATLAB. This offers the flexibility to study communication schemes in depth. Since full control over the physical layer is required, no commercial "black box" devices are utilized.

Software. The major software component of this work implements remote testbed programmability. The testbed's software system architecture is depicted in Fig. 4 and mainly consists of three parts: the bootloader, the gateway firmware, and the application. The application may be any type of code that can be executed by the node platform. Initially, the user application image file is trans-

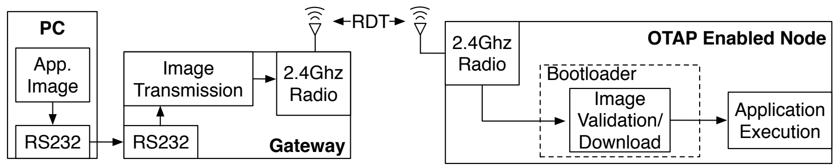

Fig. 4. Over the air programming block diagram.

ferred to the gateway from the host PC through an RS232 interface. The gateway firmware is responsible to reliably transmit the image file to all the network nodes within its range. Mechanisms for compressing image data in order to reduce the overall programming time, as well as reliable data transmission (RDT) protocols have been employed. The bootloader installed in each node 1) handles the wireless code reception via the 2.4GHz interface, 2) validates the code, and 3) begins the program execution. The fact that the bootloader is the sole responsible module for programming the nodes renders its fail-safe operation critical. Thus, functions such as checksum image file validation and watchdog timing have been developed, in order to address any undesired situation. Finally, the bootloader is invoked by the application when a new program needs to be downloaded.

The above procedure, accelerates development, since the average time for wireless programming per node is about 2 seconds. Methods and devices that require physical contact are time consuming (more than 30 seconds per node) and messy.

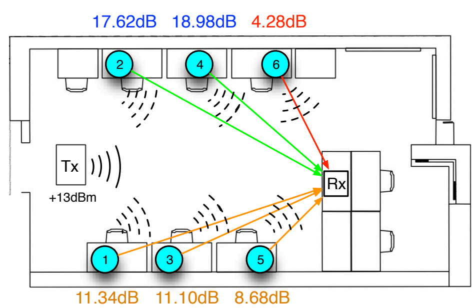

Fig. 5. Measured SNR values per backscatter node in lab deployment.

4 Research with a BSN testbed: Scenarios and Applications

High level modularity of the testbed's software and hardware components allows various experimentation possibilities. With the setup of Fig. 5, a set of research application scenarios have been implemented and evaluated on the proposed testbed. Six nodes have been used, however, the number of BSN nodes can be extended to several hundred.

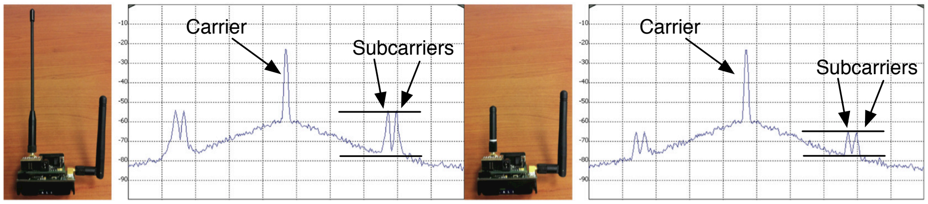

Fig. 6. Received power spectrum of a half-wavelength and a quarter-wavelength antenna with fixed tag-reader distance. The switching (i.e subcarrier) frequencies are clearly visible. The quarter-wavelength antenna backscattered signal has fairly smaller amplitude than the one backscattered from the half-wavelength antenna.

RF/Microwave Research for BSNs: Experimentation with various front-ends (i.e antennas and antenna loads) is necessary for the evaluation of tag design which greatly affects communication link performance [8]. Commodity or prototype antennas [14] can be quickly installed, and backscatter link budgets can be tested [12]. Fig. 6 depicts the received power spectrum for a half-wavelength and a quarter-wavelength antenna, respectively, with the testbed node placed at a fixed location.

Physical Layer Communication: Examination of communication schemes, receivers' performance and communication tradeoffs is feasible. On-off-keying (OOK) and frequency-shift-keying (FSK) modulations along with the corresponding receivers were developed and evaluated. Remote experimentation was conducted avoiding channel fading while full control of the testbed was maintained. Noise and received carrier power were estimated at the reader, followed by a per-tag estimation of the backscattered signals' SNR. The estimated SNR values for carrier power of +13dBm can be seen in Fig. 5, employing OOK and a nonlinear receiver. Tags were switched on and off sequentially to ensure that only one was transmitting at a time.

Finally various idiosyncrasies of bistatic backscatter links were examined such as the carrier frequency offset between carrier emitters and the reader and the "range-vs-rate" communication tradeoffs. Fig. 7 depicts the baseband received spectrum of a carrier emitter along with a tag performing FSK modulation, with 100 and 125kHz subcarriers. One can observer the increased noise floor around the carrier, which affects negatively the tags' SNR, since its subcarriers reside inside the clutter frequency region. Communication was practically impossible, with a measured BER value of 35%. Followingly the tag was reprogrammed to operate in different subcarriers (250, 300kHz), away from the clutter. The resulting BER value was 3.5%.

Cross Layer Experimentation: There are problems that require experimentation with all the layers of the testbed. Such is the study of the *capture effect*, when two nodes utilize the same communication channel simultaneously and collide. However under certain conditions, demodulation can be achieved, if the weaker signal is regarded as noise. Theoretical research on the field exists [15], but real-system study is difficult due to synchronization and control issues. Fig. 8-

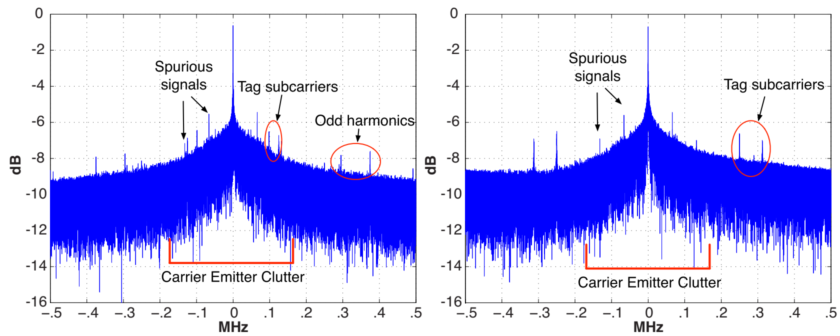

Fig. 7. Left: tag operating inside RF clutter (BER 35%). Right tag operating away from RF clutter (BER 3.5%)

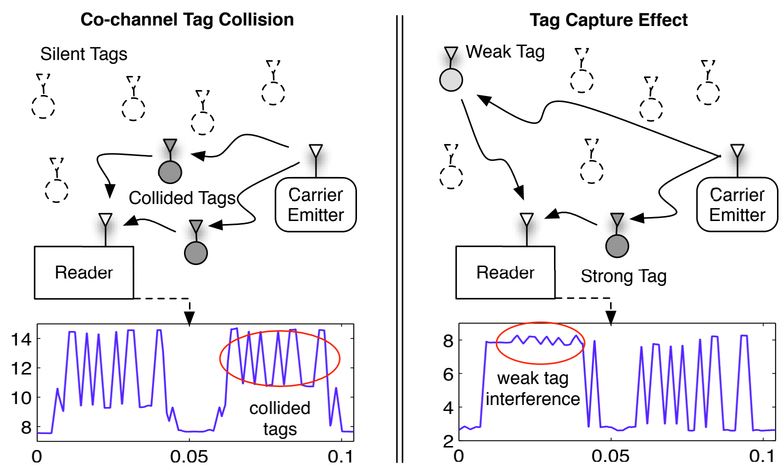

Fig. 8. Capture effect experimentation. Left: Tags collide by transmitting at the same time. Right: Tags are re-programmed to examine capture effect (strong tag is decoded successfully, even at the presence of a weak interfering tag). The figure depicts real signals captured by the SDR receiver.

left shows the forced collision of two tags, making the demodulation impossible. After the OTAP (Fig. 8-right), two *distant* tags are forced to collide. The tag closer to the reader, the one with higher SNR value, is demodulated, while the second tag can be seen as noise on the top of the strong tag's waveform.

5 Conclusion

This paper describes in detail the design and implementation of a low-cost backscatter sensor network testbed that merges WSN and BSN technologies. Hardware/software flexibility and over the air testbed programmability, facilitate simple debugging and monitoring of critical backscatter communication parameters. Finally, real world, indoor or outdoor deployments demonstrated testbed mobility and portability.

Acknowledgement This work was supported by the ERC-04-BLASE project, executed in the context of the Education & Lifelong Learning Program of General Secretariat for Research $ Technology (GSRT) and funded through European Union-European Social Fund and national funds.

References

1. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks **38**(4) (2002) 393– 422
2. Vannucci, G., Bletsas, A., Leigh, D.: Implementing Backscatter Radio for Wireless Sensor Networks. In: Proc. IEEE Personal, Indoor and Mobile Radio Communications. (September 2007) 1–5
3. Vannucci, G., Bletsas, A., Leigh, D.: A software-defined radio system for backscatter sensor networks. IEEE Trans. Wireless Commun. **7**(6) (June 2008) 2170–2179
4. Werner-Allen, G., Swieskowski, P., Welsh, M.: Motelab: a wireless sensor network testbed. In: Fourth International Symposium on Information Processing in Sensor Networks (IPSN). (April 2005) 483– 488
5. Griffin, J., Durgin, G., Haldi, A., Kippelen, B.: How to construct a test bed for RFID antenna measurements. In: IEEE Antennas and Propagation Society International Symposium. (July 2006) 457–460
6. Dobkin, D.M.: The RF in RFID: Passive UHF RFID in Practice. Newnes (Elsevier) (2008)
7. Thomas, S., Reynolds, M.: QAM backscatter for passive UHF RFID tags. In: IEEE Intl. Conf on RFID. (April 2010) 210 –214
8. Kimionis, J., Bletsas, A., Sahalos, J.N.: Bistatic backscatter radio for tag read-range extension. In: IEEE Intl. Conf on RFID-Technologies and Applications (RFID-TA), Nice, France (November 2012)
9. Dickens, M., Dunn, B., Laneman, J.N.: Design and implementation of a portable software radio. IEEE Commun. Mag. **46**(8) (August 2008) 58–66
10. Bletsas, A., Vlachaki, A., Kampianakis, E., Sklivanitis, G., Kimionis, J., Tountas, K., Asteris, M., Markopoulos, P.: Building a low-cost digital garden as a telecom lab exercise. Pervasive Computing, IEEE **12**(1) (2013) 48–57
11. Bletsas, A., Dimitriou, A.G., Sahalos, J.N.: Improving backscatter radio tag efficiency. IEEE Trans. Microwave Theory Tech. **58**(6) (June 2010) 1502–1509
12. Griffin, J.D., Durgin, G.D.: Complete link budgets for backscatter-radio and rfid systems. IEEE Antennas Propagat. Mag. **51**(2) (April 2009) 11–25
13. Bletsas, A., Kimionis, J., Dimitriou, A.G., Karystinos, G.N.: Single-antenna coherent detection of collided FM0 RFID signals. IEEE Trans. Commun. **60**(3) (March 2012) 756–766
14. Kruesi, C.M., Vyas, R.J., Tentzeris, M.M.: Design and development of a novel 3D cubic antenna for wireless sensor networks (WSN) and RFID applications. IEEE Trans. Antennas Propagat. **57**(10) (October 2009) 3293–3299
15. Lai, Y.C., Hsiao, L.Y.: General binary tree protocol for coping with the capture effect in RFID tag identification. IEEE Commun. Lett. **14**(3) (March 2010) 208–210