Autonomous intrusion detection information system

O.Sonbul, M. Byamukama, S.Alzebda, A.N.Kalashnikov, SM IEEE
Department of Electrical and Electronic Engineering
The University of Nottingham
Nottingham, NG7 2RD, UK
eexos1@nottingham.ac.uk, Alexander.Kalashnikov@nottingham.ac.uk

Abstract – Implementation of security arrangements for insecure premises, for example, for temporary exhibitions or infrequent public events, usually results in substantial security personnel costs which can be potentially reduced by employing an easily installable ad hoc intrusion detection information system. In the paper we described the architecture, design and experimental results for a fully prototyped information system that utilizes ultrasonic sensors operating in the pulse echo mode for the perimeter control and ZigBee transceivers for wireless networking. The system consists of inexpensive autonomous sensor nodes with the component cost of less than £25 and a control terminal with a graphical user interface controlled by a touch screen. The nodes are programmed wirelessly to detect intrusion within any user set distance up to the operating distance of the node, and can operate unattended for days.

Keywords: intrusion detection; ultrasonic sensors; wireless sensor networks; ad hoc security systems

I. INTRODUCTION: LOW COST *AD HOC* INTRUSION DETECTION INFORMATION SYSTEMS FOR SECURITY APPLICATIONS

Electronic security systems frequently include surveillance, access control and intrusion detection devices that are permanently installed at the protected premises. They usually require substantial capital outlay for their design, components and commissioning which nevertheless enable later savings in security personnel costs.

This high capital outlay is not justifiable for some premises that, for example, temporarily house exhibitions or high value cargo, and infrequent public events. In these cases the cost of *ad hoc* security arrangements could be reduced by using easily installable and programmable low cost autonomous proximity sensors. These sensors could be set on guard for specific times only, discreetly cordoning off particular perimeters without obstructing the view of the exhibits or causing inconvenience during work hours. If an intrusion was detected, the sensor would report it wirelessly to the security personnel reducing the number of security staff required otherwise. Each proximity sensor in such a system should be of low cost and low power consumption, capable of broadcasting secure messages across.

In this paper we present a low cost ad hoc security information system that utilizes ultrasonic transducers operating in the pulse echo mode for intrusion detection, can be easily installed, can operate unattended for days and reports an intrusion wirelessly.

II. COMPARISON OF PROXMITY SENSORS SUITABLE FOR SECURITY APPLICATIONS

Various active and passive sensor technologies can be used for proximity sensing in security applications. Passive sensors (e.g., acoustic, seismic or thermal infrared sensors) use the energy received from the environment to detect the presence of the intruder [1]. For example, widely used passive infrared (PIR) sensors detect changes in infrared radiation caused by movements of the

intruder which has different temperature compared to the surroundings [2]. However, these sensors have shown a high miss rate when the intruder moves at a slow speed or use heat insulating closes.

Active sensors include infrared (IR), inductive, capacitive, and ultrasonic sensors [3-7]. The active IR sensors sense either the intensity or phase shift of the IR light back-scattered by the intruder. The IR intensity sensors frequently give inaccurate ranging results because of their non-linear sensitivity and dependence on the reflectance of surrounding objects. The phase shift option can offer medium resolution at long ranges, but at high cost [4].

Inductive and capacitive sensors are not convenient for proximity sensing in security applications for several reasons. First, they require a ratio between the maximum operating distance and the sensor diameter of about 0.5; therefore, they have very small operating range for portable sensors. Second, their sensitivity is highly dependent on the physical nature of the intruding object. Third, inductive devices operate only in the presence of a magnetic field so that a magnetic target or some permanent magnet has to be used in the system[8].

Active ultrasonic sensors seem preferable for this application for the following reasons. First, they can operate in various open space environmental conditions, in the presence of fog, dust, dirt, lighting or strong electromagnetic interference (EMI). Second, ultrasonic sensors can be used for relatively accurate distance measurements by estimating the time-of-flight (TOF) of the emitted ultrasonic wave. Comparing to laser or microwave emissions propagating at the speed of light, ultrasonic sensors require much simpler and cheaper electronics because of low speed of sound in air (around 340 m/s at 20^{o}C). Third, ultrasonic sensors can be fabricated at a low cost using electrostatic or piezoelectric principles [9].

The above considerations are summarized in table I that illustrates suitability of active ultrasonic sensors for low cost intrusion detection security networks.

TABLE I
COMPARISON AMONG DIFFERENT PROXIMITY SENSOR TECHNOLOGIES

Sensor technology	**Advantages**	**Disadvantages**
Passive infrared	▪ Low cost ▪ Short response time	▪ High miss rate
Inductive Capacitive	Low cost	▪ Short range ▪ Poor sensitivity
Active Infrared, Microwave, Laser	▪ Short response time ▪ Long range	▪ High cost
Ultrasonic	▪ Low cost ▪ Wide angle of operation	▪ Long response time ▪ Medium range

III. CONSIDERATION OF WIRELESS NETWORKING OPTIONS

Recent advances in micro-electromechanical systems, embedded computing, and low power radio communication technology resulted in wide deployment of wireless sensor networks (WSNs). The WSNs consist of a large number of small, low cost, and low power sensor nodes, which gather and broadcast data. WSN applications include surveillance systems, habitat monitoring, fire rescue, dynamic field measurement [10-13]. Additionally WSNs can significantly decrease the risk to and the need of manpower for highly dangerous tasks [14]. Although infrared wireless communication

can be used for WSNs in principle, it usually requires relatively high power, direct line of sight among nodes, is subject to daylight and lighting interference and multipath propagation [15]. Figure 1 compares the principal radio frequency (RF) WSN technologies in terms of two key performance characteristics - wireless radio range and data transmission rate.

Bluetooth is a technology for short-range wireless data and real time two-way voice transfer supporting data rates up to 3 Mb/s. It operates at 2.4 GHz frequency in the unlicensed ISM-band (Industrial, Scientific, and Medical) using frequency-hopping spread spectrum (FHSS) modulation technique. The operating range of Bluetooth communication varies from 10 to 100 meters indoors [16]. However, it introduces significant complexity in establishing a connected topology thus Bluetooth usage is often limited to ad hoc networks with a very limited number of nodes [17].

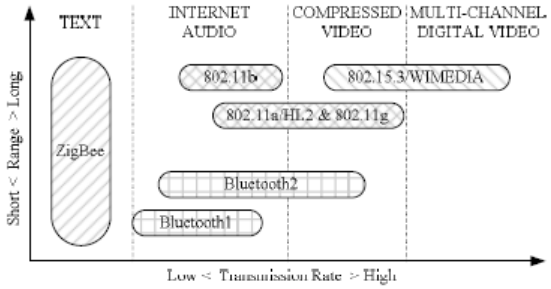


Figure 1 Comparison among wireless RF networking technologies [18].

Wi-Fi networks operates in the GHz range and offers a very high data rates (54 Mbps and above) for a substantial number of devices operating simultaneously. However, Wi-Fi is not suitable for battery operated wireless nodes because of the inherent high power consumption and high cost of the transceivers [19].

ZigBee is a name for a low rate wireless network defined by the ZigBee Alliance and IEEE 802.15.4 standard for low-cost, low power systems consisting of unsupervised groups of nodes. The IEEE standard defines only the Physical (PHY) and Medium Access Control (MAC) layers as shown in Figure 2. Members of ZigBee alliance developed further specifications covering the network/link, security and application profile layers so that the commercial potential of the standard could be realized [18].

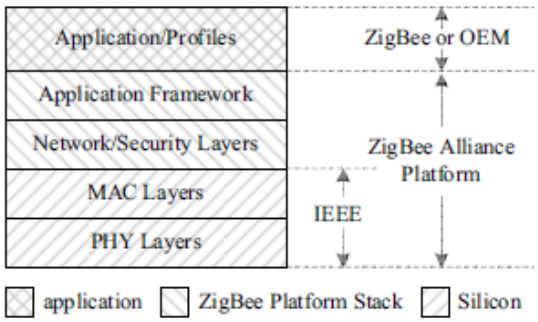


Figure 2 Components of ZigBee [18].

Table II summarizes the most notable parameters of the considered WSN technologies in terms of the communication medium, the range, the size of the network, the maximum data rate, the power consumption, the cost, the interference and security. We selected ZigBee technology for the security system because it matches the requirements for secure, reliable, low cost, long battery life and simple networking.

TABLE II
COMPARISON AMONG NETWORKING TECHNOLOGIES

Property	Infrared	Bluetooth	ZigBee	Wi-Fi
Communication medium	Infrared light	RF waves	RF waves	RF waves
Typical range	0 – 2 m	10 - 100 m	10 - 80 m	90 - 150 m
Size of the network	Two devices	2 - 8 devices	Dozens of devices	Dozens of devices
Maximum data rate	16 Mbps	3 Mbps	20 to 250 kbps	54 Mbps
Power consumption	High	Low	Low	High
Component cost	Very low ($1)	Low ($4)	Low ($3)	High ($15)
Tolerance to third-party interference	Excellent	Good	Good	Bad
Authentication, Authorization and encryption	No	Yes	Yes	Yes

IV. SYSTEM ARCHITECTURE AND OPERATION

The developed intrusion detection system integrates several autonomous battery operated nodes and the control terminal as shown in fig.3. Every node consists of an ultrasonic proximity sensor, a network adapter and a microcontroller. The microcontroller wirelessly receives the operating parameters and reports intrusion when it is detected. Fully autonomous low cost nodes can be installed using quick fasteners (magnets or screws), and require no extra wiring. The nodes can go to sleep if not in use or between the consecutive transmissions consuming only 20nA.

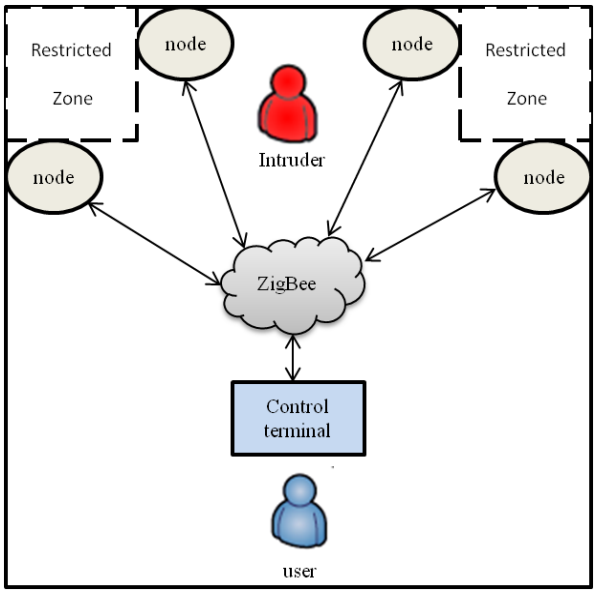


Figure 3 The architecture of the system.

The range of object detection is 2.7m with the accuracy of 1cm in the pulse-echo mode of operation. This feature allows reducing the number of nodes comparing to conventional proximity sensors because there is no need for separate transmitter and receiver (Figure 4).

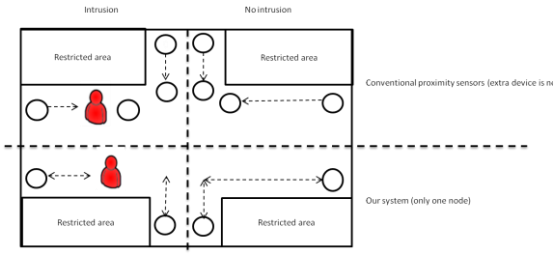


Figure 4 Number of nodes required for different proximity sensors.

Another advantage of ultrasonic proximity sensors relates to their wider beam (60° typical) comparing to, for example, optical transmitter-receiver pair. It enables using smaller number of sensors/nodes for the same area as shown in fig.5.

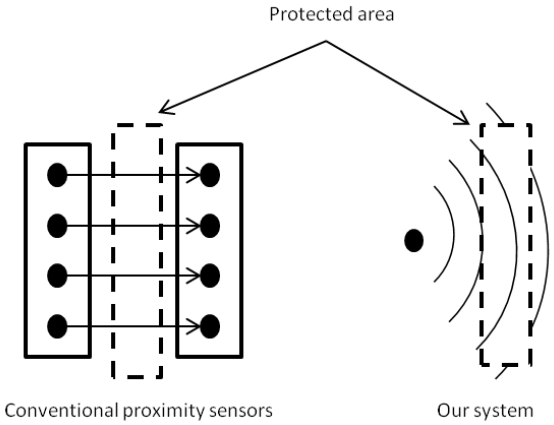


Figure 5 Protection area formed by different proximity sensors.

The control terminal consists of a touch screen, a network adapter, a secure digital (SD) card and a microcontroller. The user programs the nodes using a graphical user interface, and may store and retrieve the operating parameters from the non-volatile SD card. Security systems require setting their operating parameters in order to balance the probability of the false alarm with the probability of the hit. In the considering case the user needs to set the threshold level for detection above the noise level, and the time instant for the ultrasonic receiver before which the intrusion must be detected. This is aided by displaying the output waveforms received from the particular node. The user is then able to select the position in the time domain and the threshold level on the graph. After programming the nodes the terminal waits for the alarm signal from nodes and displays the reference to the node that detected an intrusion.

V. DESIGN OF THE ULTRASONIC NODES AND THE CONTROL TERMINAL

A. Ultrasonic nodes

A system node consists of a PIC18F46J50 microcontroller, analog circuitry, communication module, DC/DC converter and semiconductor switches assembled on a custom designed PCB (fig.6).

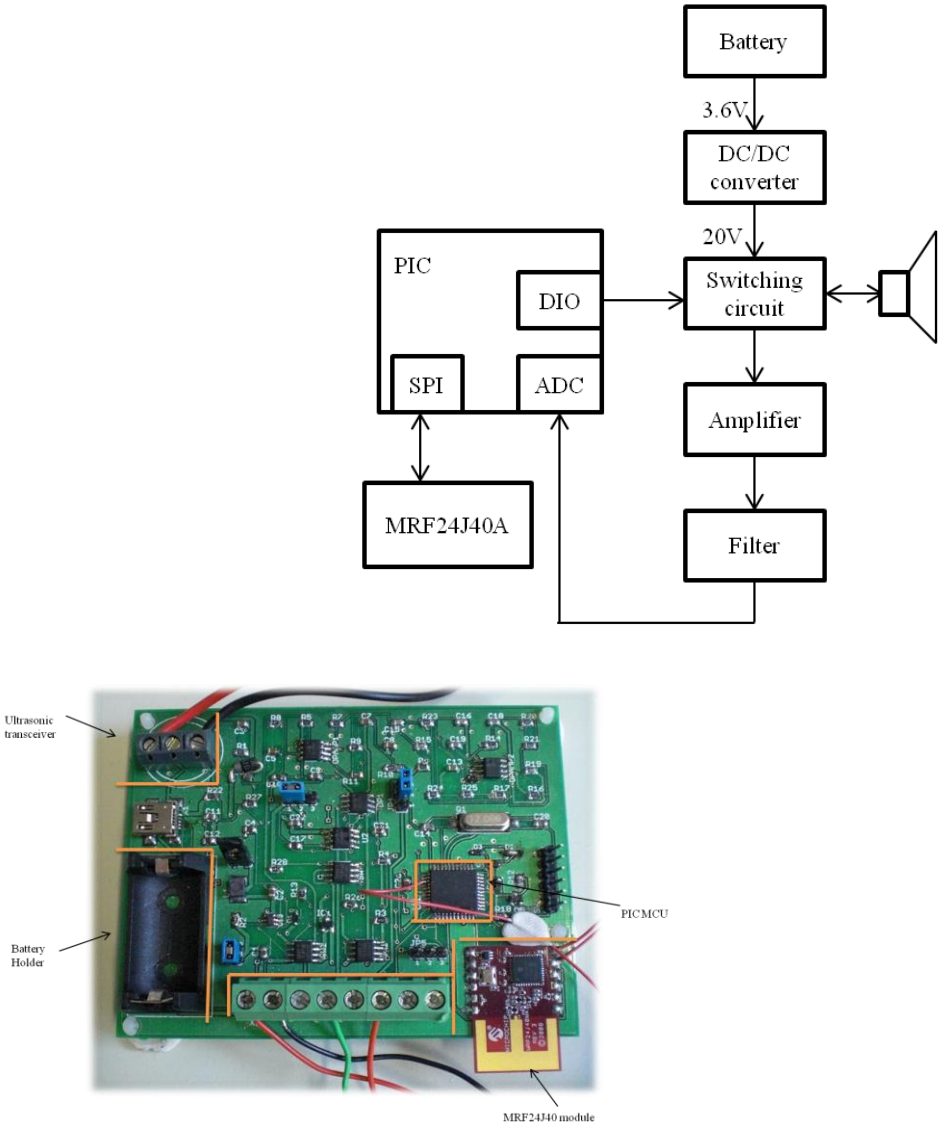


Figure 6 Block diagram and photograph of an ultrasonic node.

A typical pulse-echo ultrasonic system includes a pulser, a duplexer and a receiver acting as an analogue front end (AFE). In this design the switching circuit acts as the first two, and the receiver consists of the amplifier of the echo signal and the 40 kHz bandpass filter.

The converter increases the voltage applied to the switching circuit from 3.6 V up to 20 V.

During the ultrasound transmission the microcontroller controls the H-bridge formed by the switching circuit which doubles the voltage applied to the transducer; then connects the transducer to the amplifier.

The ADC is used to digitize the echo. The echo samples are then compared to the threshold in order to detect the intrusion.

ZigBee communication is provided by the MRF24J40A module that features on board antenna and is controlled over the SPI protocol by the microcontroller. Node design featured several energy savings features that were considered essential for the autonomous battery operation. The selected microcontroller supported the nanoWatt eXtreme Low Power (nanoWatt XLP) microcontroller's technology from Microchip. DC/DC converter and Zigbee module both had enable pins that were set to disable state from time to time in order to reduce the power consumption. The amplifier and the filter were connected to the power supply via a load switch which enabled further reduction of the consumed power when off.

The firmware for the ultrasonic node was written using Microchip's MPLAB IDE and C18 compiler. Free Microchip's wireless (MiWi) peer-to-peer (P2P) protocol stack based on IEEE 802.15.4 was adopted for the development. The MiWi P2P protocol modifies the IEEE 802.15.4 specification's Media Access Control (MAC) layer by adding commands that simplify the handshaking process. It simplifies link disconnection and channel hopping by providing supplementary MAC commands. The protocol specifies no routing mechanism; therefore the wireless communication coverage is defined by the radio range. Guaranteed Time Slot (GTS) and beacon networks are not supported; hence communicating transceivers cannot go to the sleep mode simultaneously [20].

B. The control terminal

The control terminal was based on a MicroLCD UI Development Kit from Sytech Designs [21]. It consisted of a Freescale i.MXS applications processor which had several peripherals such as a UART, SPI and Ethernet interfaces. The MRF24J40MA device was used to add the RF capability to the control terminal. This module was hardwired to the main board to be controlled over the SPI module of the processor. The SD card was present in the development kit, and was used to record the settings and waveforms (Figure. 7).

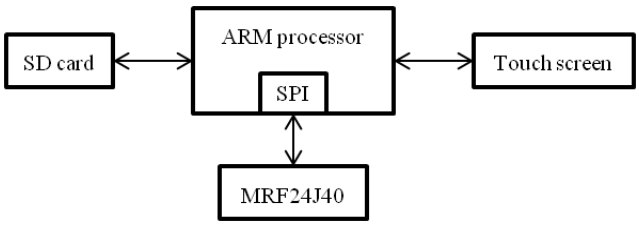


Figure. 7 The block diagram of the control terminal.

The firmware code was developed in C# using the .Net Micro Framework. The transceiver was programmed to transmit and receive data to and from another transceiver terminal. These data were then displayed on the LCD touch screen connected to the processor directly. Figure 8 shows sample waveforms that were received from the PICDEM Z board used as the node simulator and plotted using a custom developed graphics library.

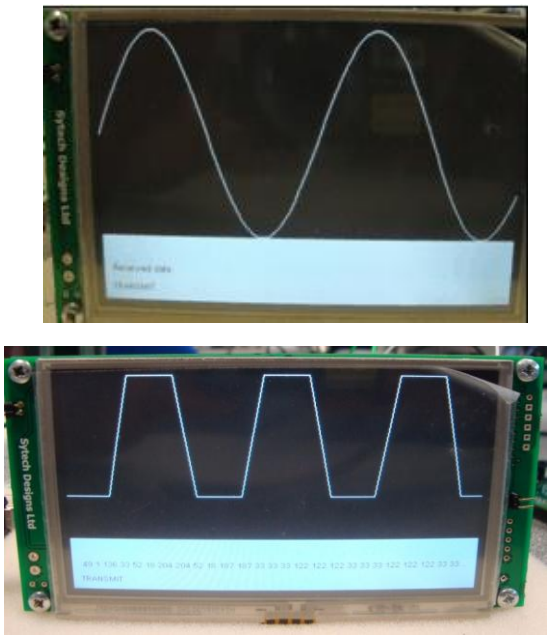


Figure 8 Sample waveforms received wirelessly from the node simulator.

VI. EXPERIMENTAL RESULTS

C. Current consumption

Insufficient power supplied to the node terminates its operation and requires battery replacement or recharging.

To achieve the longevity of node operation without replacing/recharging the batteries, parts of the node are to be switched off when not in use. Additionally, we found that the operation of DC/DC converter induced substantial noise to the amplifier. Therefore the DC/DC converter was set off most of the time. Its operation for a few milliseconds was enough to accumulate a charge at the output storage capacitor that enabled generation of several hundred pulses without significant reduction of their amplitude.

ZigBee module does not increase the power consumption to inacceptable levels because it listens most of the time.

Because the system behaves differently at different times, the consumed current shows substantial variations (table III).

TABLE III
CURRENT CONSUMPTION FOR DIFFERENT MODES OF THE NODE OPERATION.

Modules powered	**Current consumption**
PIC alone	9 mA
PIC + AFE	44mA
PIC+ AFE + ZigBee module	47mA
PIC + AFE + ZigBee + DC/DC converter	60mA

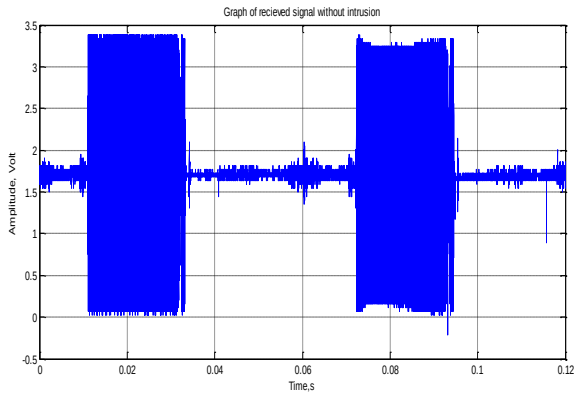
If a node is programmed for the range of, say, 3m, the receiver needs to be switched on for less than 20 ms for every transmission. Transmission once in a second therefore would require the average current of

(980ms*9mA+44mA*20ms) /1000ms < 10mA.

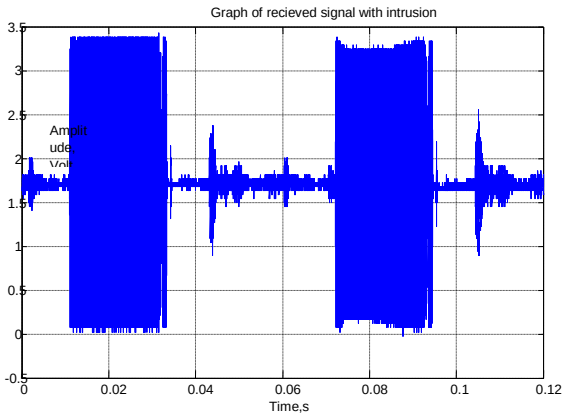
A typical rechargeable battery with the capacity of 1000 mAh would keep the node operating for more than 4 days.

D. Waveforms at the output of the receiver

The received echo is compared to the threshold that is adaptively calculated based on the ambient and electronic noise level. The threshold is set to both sides of the mean value of the output filter's voltage. The difference between the threshold and the mean value equals to the three times standard deviation of the noise. This choice allowed a reasonable compromise between the probabilities of the hit and the false alarm. Figure 9 shows an example of the recorded waveforms.



(a)



(b)

Figure 9 Received echoes without (a) and with (b) intrusion.

E. Detection range versus the excitation voltage

The operation of the node was experimentally tested for the detection of a human standing at some distance from the face of the transducer at different angles to the transducer's axis (table IV).

TABLE IV
IMPLEMENTATION RESULTS FOR DIFFERENT EXCITATION VOLTAGES

Excitation voltage	**Detection range**	**Detection angle @ 2m**
10V	2m	5º
15V	2.2m	9º

20V	2.7m	15º

These results showed that the application of the DC/DC converter extended the detection range from 2 m to 2.7 m and widened the detection angle.

VII. CONCLUSIONS

We have described the architecture, operation, design, and experimental performance of a low cost ultrasonic wireless sensor network for security information system.

All the constituents of the system were fully prototyped and successfully tested. We selected ultrasonic sensors operating in the pulse echo mode to achieve medium range detection from a single sensor node. The nodes were networked using ZigBee that enabled secure, reliable, low cost, long battery life and simple networking.

Heterogeneous processors were used in the design of the nodes and the control terminal – a simpler PIC microcontroller for the node and an ARM microcontroller for the control terminal. This enabled combination of the low cost and low power consumption for the nodes with the convenient easy-to-use graphical user interface for the terminal. A node consists of an ultrasonic transducer, a microcontroller, a DC/DC converter, a ZigBee module and semiconductor switches with the total cost of less than £25.

Experimental results showed that the node power consumption was sufficiently low to achieve unattended autonomous operation for several days. An intrusion was detected by comparing the echo with the threshold within the set range of distances. This enables setting the detection distance to any value up to the operating range of the node of 2.7 m. Further development of the system will include several security enhancements, for example, an application firmware encryption and randomization of the pulse repetition frequency around the user set average value. We believe that the considered application of ultrasonic sensors can substantially reduce the cost and increase use of intrusion detection information systems for *ad hoc* security purposes, e.g., temporary exhibitions and public events held in insecure premises.

Acknowledgment

This development was supported by a Umm Al-Qura University scholarship awarded to O.Sonbul in July 2006.

REFERENCES

[1] X. Wendong, W. Jian Kang, L. Shue, L. Yiqun, and X. Lihua, "A prototype ultrasonic sensor network for tracking of moving targets," in 1st IEEE Conference on Industrial Electronics and Applications, 2006, pp. 1-6.

S. Byunghun, C. Haksoo, and L. Hyung Su, "Surveillance tracking system using passive infrared motion sensors in wireless sensor network," in International Conference on Information Networking, ICOIN, 2008, pp. 1-5.

B. Bury, "Proximity sensing for robots," in IEE Colloquium on Robot Sensors, 1991, pp. 3/1-318.

G. Benet, F. Blanes, J. Simo, and P. Perez, "Using infrared sensors for distance measurement in mobile robots," Robotics and Autonomous Systems, vol. 40, 2002.

L. Korba, S. Elgazzar, and T. Welch, "Active infrared sensors for mobile robots," IEEE Transactions on Instrumentation and Measurement, vol. 43, pp. 283-287, 1994.

C. Canali, G. De Cicco, B. Morten, M. Prudenziati, and A. Taroni, "A temperature compensated ultrasonic sensor operating in air for distance and proximity measurements," IEEE Transactions on Industrial Electronics, vol. IE-29, pp. 336-341, 1982.

W. Manthey, N. Kroemer, and V. Magori, "Ultrasonic transducers and transducer arrays for applications in air," Journal of Measurement Science and Technology, vol. 3, 1992.

J. Fraden, Handbook of modern sensors : physics, designs and applications, 4th ed. New York: Springer Science and Business Media, 2010.

L. Xi, W. Renbiao, S. Rasmi, L. Jian, L. N. Cattafesta, III, and M. Sheplak, "Acoustic proximity ranging in the presence of secondary echoes," IEEE Transactions on Instrumentation and Measurement, vol. 52, pp. 1593-1605, 2003.

A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," presented at the Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 2002.

S. Kewei, S. Weisong, and O. Watkins, "Using wireless sensor networks for fire rescue applications: requirements and challenges," in IEEE International Conference on Electro/information Technology, 2006, pp. 239-244.

S. Ping, Q. Guangping, L. Kejie, and S. Li, "High performance wireless field measurement system based on wireless sensor network," in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA '08, 2008, pp. 635-639.

B. Ying-Wen, S. Li-Sih, and L. Zong-Han, "Design and implementation of an embedded home surveillance system by use of multiple ultrasonic sensors," IEEE Transactions on Consumer Electronics, vol. 56, pp. 119-124, 2010.

W. Xun, G. Wenjun, S. Chellappan, K. Schosek, and X. Dong, "Lifetime optimization of sensor networks under physical attacks," in IEEE International Conference on Communications, ICC, 2005, pp. 3295-3301 Vol. 5.

A. Lessard and M. Gerla, "Wireless communications in the automated factory environment," IEEE Network Magazine, vol. 2, pp. 64-69, 1988.

K. Haataja, "Security in Bluetooth, WLAN, and IrDA: a comparison," University of Kuopio, Department of computer Science, Kuopio2006.

E. Vergetis, R. Guerin, S. Sarkar, and J. Rank, "Can Bluetooth succeed as a large-scale ad hoc networking technology?," IEEE Journal on Selected Areas in Communications, vol. 23, pp. 644-656, 2005.

L. Shizhuang, L. Jingyu, and F. Yanjun, "ZigBee based wireless sensor networks and its applications in industrial," in IEEE International Conference on Automation and Logistics, 2007, pp. 1979-1983.

A. B. Fadhah, A. Al-Lawati, S. Al-Maskari, A. Touzene, and A. Al-Kindi, "Experimental performance evaluation of Wireless 802.11b networks," in 1st International Conference on the Applications of Digital Information and Web Technologies, ICADIWT, 2008, pp. 151-155.

Y. Yang. Microchip MiWi P2P Wireless Protocol [Online]. Available: http://ww1.microchip.com/downloads/en/AppNotes/01204B.pdf

MicroLCD UI Development Kit data sheet [Online]. Available: http://sytechdesigns.com/MicroLCD.htm