

# Indoor Surveillance with Multimodal Wireless Networks

John Aa. Sørensen, Zoltan Safar, Jianjun Chen, Kåre J. Kistoffersen, and Martin Schiøtz  
Department of Innovation, IT University of Copenhagen, Copenhagen, Denmark

**Abstract**—In this paper, we propose a new family of wireless networks, the multimodal wireless networks. These networks offer multiple functionalities realized on the same infrastructure. We describe a wireless network that has two modes of operation: the communication mode, when the network is used as a traditional wireless communication network, and the surveillance mode, when the network is used as a distributed sensor network that can detect illegal intrusion. The surveillance functionality is realized by analyzing the properties of the received signals, and the change of the propagation environment caused by the intruder serves as the basis for intrusion detection. We also develop a general single-receiver model for detecting changes in a signal parameter of interest and derive a parameter change detector. The experimental results demonstrate that low-cost, off-the-shelf IEEE 802.11b WLAN hardware can be used as building blocks for multimodal networks.

**Index Terms**—WLANs, sensor networks, multimodal networks, surveillance

## I. INTRODUCTION

There has been an abundance of research activities in the area of wireless networks for short to medium-range wireless communication [1]. Results of these efforts so far are the widely utilized IEEE 802.11 a, b, and g Wireless Local Area Network (WLAN) standard, the Bluetooth and the IEEE 802.15 Wireless Personal Area Network (WPAN) standard. These systems and standards were designed to maximize the efficiency of the communication between two different physical locations, while mitigating the effect of the physical propagation environment (i.e. multipath fading) on the communication [2]. These networks are one of the key prerequisites for the design of pervasive computing systems [3]. Simultaneously with the development of wireless communication networks, there is an intense research activity within wireless sensor networks, aiming to cover a physical area with sensing and communicating nodes. Each node contains one or more sensors for acquisition and analysis of the physical properties of the environment [4], [5], [6]. Examples of properties measured and analyzed are temperature, acceleration, sound, image, or chemical properties.

In paper, we propose the idea of multimodal wireless networks: networks that can offer multiple functionalities realized on the same infrastructure. We present the description of a wireless network that has two modes of operation: the communication mode, when the network is used as a traditional WLAN or WPAN, and the surveillance mode, when the communication network is used as a distributed sensor network that can detect illegal intrusion. In surveillance mode, the nodes constantly monitor the environment by analyzing the properties of the received signal, such as time of arrival or signal strength. When entering a site covered by such a network, the intruder will disturb the physical propagation environment, causing change in the characteristics of the received signals, and this change

can be used for intrusion detection. We also develop a general single-receiver model for detecting changes in the received signal parameter of interest and derive a parameter change detector based on the generalized likelihood ratio test (GLRT). The model and the detector take explicitly into account the quantized nature of the signal parameter. By performing a set of experiments using the detector, we show that it is possible to use currently available WLAN components as building blocks for multimodal networks.

So far, the problems of wireless communication and "physical" intrusion detection (i.e. detecting a person or persons entering private/corporate premises illegally) have been considered as two separate issues, and two different infrastructures have been deployed: one for communication and one for surveillance/security. However, if the communication infrastructure could also be used for security purposes, the deployment of the additional infrastructure could be avoided, resulting in a considerably more cost-effective solution. Possible applications include ad-hoc networks deployed for both communication and surveillance purposes, and indoor surveillance of corporate buildings and private houses using the existing WLAN systems.

Previous experiments investigating the impact of moving objects/humans on the propagation environment [7], [8] have shown that significant variations can be observed in the received signal strength and the rms delay spread. However, those measurements were carried out using specialized equipment, and not low-cost, off-the-shelf devices, such as a WLAN card, and the authors did not propose any signal processing architectures or algorithms for intrusion detection.

## II. THE PROPOSED SURVEILLANCE SYSTEM

The architecture of the surveillance system based on the proposed multimodal network model is shown in Figure 1. In communication mode, the wireless transceiver nodes, denoted by  $N_i$ ,  $i = 1, \dots, n$ , implement the functionality of a traditional wireless network. They can be access points or clients in a cellular network architecture, or they can be communicating nodes in an ad-hoc wireless network. In surveillance mode, the nodes transmit, for example, one by one in a round robin fashion, and the rest of the nodes receive the transmitted signal, acting as a distributed sensor network. For sufficient sensitivity and robustness, the nodes must be placed properly, and some additional low-cost nodes might be needed. First, the received signal at each node is processed by a preprocessor to extract the relevant characteristics of the propagation environment, which include time of arrival, angle of arrival, the strength of the received signal, channel impulse response, or a combination of these. The preprocessor is also responsible for reducing the undesirable effects of measurement noise and inaccuracy. The obtained set of such quantities that characterize the environment, also called as

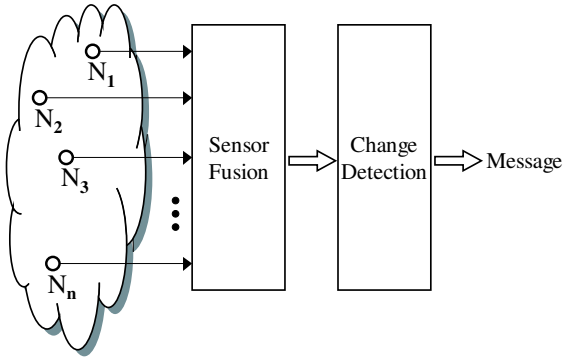


Fig. 1. The proposed surveillance system architecture.

the "signature" of the environment, is then combined by a data fusion function, which produces a single output that describes the similarity of the current signature of the environment to a stored one or a previously computed one. If significant difference is detected, it is assumed that the disturbance in the propagation environment was caused by an intruder, and the system generates an alarm signal and an estimate of the intruder's location.

In what follows, we develop a single-receiver (or single-sensor) model for the received signal parameter of interest (e.g. time of arrival or signal strength) and derive a detector for detecting change in the parameter. This parameter will serve as the "signature" of the environment, and the detection of change in the parameter value can be used as an indicator of probable intrusion.

### III. SIGNAL MODEL AND PROBLEM SETUP

The received signal model can be observed in Figure 2. The true value of the received signal parameter,  $l_0$ , is shifted by an unknown bias,  $B$ , resulting in the biased parameter,  $l$ , which is assumed to take on values between  $l_{min}$  and  $l_{max}$ . The bias represents measurement inaccuracy due to signal measurement values that are not standardized and/or not calibrated, such as the 802.11 RSSI values. The true signal parameter is further disturbed with zero-mean, white Gaussian noise  $z_n$  with variance  $\sigma^2$  at discrete time  $n$ . The observed signal is usually only available in quantized form (for example, 802.11 RSSI values), so the observations are  $\{y_n\}$ , the quantizer indices corresponding to the noisy and biased signal parameter values  $\{x_n\}$ . The quantizer is assumed to have  $N_q = 2^b$  levels, where  $b$  is the number of bits representing the signal parameter. The decision regions are denoted by  $a_0 < a_1 < \dots < a_{N_q}$ , with  $a_0 = -\infty$  and  $a_{N_q} = +\infty$ , and the quantizer maps the input value  $x_n$  to the quantizer index  $y_n \in \{0, 1, \dots, N_q - 1\}$  if  $a_{y_n} < x_n \leq a_{y_n+1}$ .

Our objective is to detect a change  $\Delta l$  with respect to the true signal parameter  $l_0$  based on a set of  $N$  observations,  $\mathbf{y} = [y_0, y_1, \dots, y_{N-1}]^T$ , so the two detection hypotheses can be formulated as follows:  $\mathcal{H}_0 : l_0$  (no intruder present), and  $\mathcal{H}_1 : l_0 + \Delta l, \Delta l \neq 0$  (intruder present). Since the detection of change is not affected by the bias  $B$ , we have the equivalent hypotheses:  $\mathcal{H}_0 : l$ , and  $\mathcal{H}_1 : l + \Delta l, \Delta l \neq 0$ . This means that the true value of the signal parameter,  $l_0$ , is not needed for our purposes.

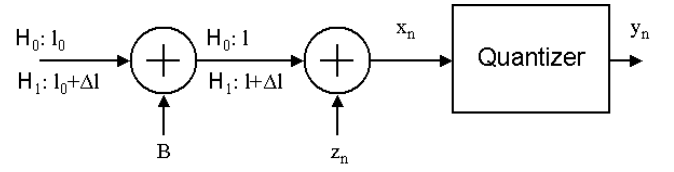


Fig. 2. The received signal model

The detection procedure will consist of the following two phases. During the first phase, the training phase, the steady state of the propagation environment is estimated. The signal (and noise) parameters  $l$  and  $\sigma$  are not known, so they must be estimated when it is ensured that  $\mathcal{H}_0$  is true (i.e. no intruder). The quantities  $l$  and  $\sigma$  are estimated by developing an approximate and an iterative maximum likelihood (ML) estimator using a larger number (1000) of training samples. This can be done during a couple of seconds when the surveillance system is armed. Note that this step is necessary since the propagation environment may change significantly during an inactive period of the surveillance system. For example, workers at a company may move furniture or open/close doors during daytime.

The second phase is the detection phase, when the surveillance system detects the unknown parameter change  $\Delta l$  based on a small number (50) of observations. Since the probability of detection must be maximized for a given probability of false alarm, the detection is carried out by GLRT. Again, the value of  $\Delta l$  for the  $\mathcal{H}_1$  case is estimated by an approximate and an iterative ML estimator.

### IV. TRAINING PHASE

Given an observation vector  $\mathbf{y}$  of length  $N$  (now  $N$  represents the training data record length), we would like to estimate  $l$  and  $\sigma$ . The log-likelihood function is given by

$$\ln P(\mathbf{y} = \mathbf{i}; l, \sigma) = \sum_{n=0}^{N-1} \ln G(l, \sigma, a_{i_n}, a_{i_n+1}), \quad (1)$$

where  $\mathbf{i} = [i_0, i_1, \dots, i_{N-1}]^T$  is an observed realization of  $\mathbf{y}$ , and the function  $G(\cdot)$  is defined as

$$G(l, \sigma, a, b) = \frac{1}{\sqrt{2\pi}\sigma} \int_a^b e^{-\frac{(z-l)^2}{2\sigma^2}} dz = Q\left(\frac{a-l}{\sigma}\right) - Q\left(\frac{b-l}{\sigma}\right)$$

for notational convenience. The ML estimate of the parameters can be obtained by finding the values of  $l$  and  $\sigma$  such that  $\frac{\partial}{\partial l} \ln P(\mathbf{y} = \mathbf{i}; l, \sigma) = 0$  and  $\frac{\partial}{\partial \sigma} \ln P(\mathbf{y} = \mathbf{i}; l, \sigma) = 0$ , yielding the conditions

$$f_1(l, \sigma) = \sum_{n=0}^{N-1} \frac{X(l, \sigma, a_{i_n}) - X(l, \sigma, a_{i_n+1})}{G(l, \sigma, a_{i_n}, a_{i_n+1})} = 0 \quad \text{and}$$

$$f_2(l, \sigma) = \sum_{n=0}^{N-1} \frac{(a_{i_n} - l)X(l, \sigma, a_{i_n}) - (a_{i_n+1} - l)X(l, \sigma, a_{i_n+1})}{G(l, \sigma, a_{i_n}, a_{i_n+1})} = 0,$$

where  $X(l, \sigma, a) = \exp(-(a-l)^2/2\sigma^2)$ . The solution cannot be obtained in closed form, so we derive an approximate ML estimator and an iterative ML estimator.

The approximate ML estimator is obtained by approximating integrals as  $\int_a^b f(x)dx \approx f(\frac{a+b}{2})(b-a)$ . As a result, the

approximate log-likelihood function becomes

$$\ln P(\mathbf{y} = \mathbf{i}; l, \sigma) \approx \sum_{n=0}^{N-1} -\ln(\sqrt{2\pi}\sigma) + \frac{1}{2\sigma^2} \left( \frac{a_{i_n} + a_{i_{n+1}}}{2} - l \right)^2 + \ln(a_{i_{n+1}} - a_{i_n}).$$

By taking its partial derivative with respect to  $l$ , setting it equal to zero and solving for  $l$  yields the estimator

$$\hat{l}_{ap} = \frac{1}{N} \sum_{n=0}^{N-1} \frac{a_{i_n} + a_{i_{n+1}}}{2}, \quad (2)$$

which is the sample mean of the observed reconstruction levels for uniform quantizers. Similar, taking the partial derivative with respect to  $\sigma^2$ , setting it to zero, solving for  $\sigma^2$  and using  $\hat{l}_{ap}$  for the value of  $l$  gives the estimator

$$\hat{\sigma}_{ap}^2 = \frac{1}{N} \sum_{n=0}^{N-1} \left( \frac{a_{i_n} + a_{i_{n+1}}}{2} - \hat{l}_{ap} \right)^2. \quad (3)$$

In (2) and (3), the values of  $a_0$  and  $a_{N_q}$  need to be replaced with appropriate finite values.

The iterative ML estimator performs a series of Newton-Raphson iterations using the estimates from the approximate ML estimator as initial values:

$$\begin{bmatrix} \hat{l}_{k+1} \\ \hat{\sigma}_{k+1} \end{bmatrix} = \begin{bmatrix} \hat{l}_k \\ \hat{\sigma}_k \end{bmatrix} - \begin{bmatrix} f_{1,1}(\hat{l}_k, \hat{\sigma}_k) & f_{1,2}(\hat{l}_k, \hat{\sigma}_k) \\ f_{2,1}(\hat{l}_k, \hat{\sigma}_k) & f_{2,2}(\hat{l}_k, \hat{\sigma}_k) \end{bmatrix}^{-1} \begin{bmatrix} f_1(\hat{l}_k, \hat{\sigma}_k) \\ f_2(\hat{l}_k, \hat{\sigma}_k) \end{bmatrix},$$

where  $k$  is the iteration index, and  $f_{i,j}(l, \sigma)$ 's are the appropriate partial derivatives of  $f_1(l, \sigma)$  and  $f_2(l, \sigma)$  with respect to  $l$  and  $\sigma$ . These derivatives can be obtained after some tedious, but straightforward calculations, and they are omitted here for brevity. The iterations stop if two consecutive solution vectors are closer to each other than a predefined threshold value  $\delta$ .

## V. DETECTION PHASE

In the detection phase, the detector observes a quantizer index vector  $\mathbf{i}$  of length  $N$  (now  $N$  is considerably smaller than that for the training phase), and decides whether there is a significant change in the signal parameter  $l$  ( $\mathcal{H}_1$ ) or not ( $\mathcal{H}_0$ ). The detection algorithm is based on the GLRT: decide  $\mathcal{H}_1$  if

$$\frac{P(\mathbf{y} = \mathbf{i}; \mathcal{H}_1)}{P(\mathbf{y} = \mathbf{i}; \mathcal{H}_0)} > \gamma, \quad (4)$$

and  $\gamma$  is the decision threshold. For both hypotheses, the previously estimated  $l$  and  $\sigma$  values are used. In addition, for the hypothesis  $\mathcal{H}_1$ , the value of  $\Delta l$  also has to be estimated, while for  $\mathcal{H}_0$ ,  $\Delta l = 0$  is assumed.

The value of  $\Delta l$  under  $\mathcal{H}_1$  can be estimated similarly to the method described in Section IV, but now we are interested only in the level change  $\Delta l$  ( $l$  and  $\sigma$  are assumed to be constant). In this case, the log-likelihood function becomes

$$\ln P(\mathbf{y} = \mathbf{i}; \Delta l) = \sum_{n=0}^{N-1} \ln G(\Delta l, \hat{\sigma}, a_{i_n} - \hat{l}, a_{i_{n+1}} - \hat{l}), \quad (5)$$

and the ML estimator can be obtained by setting  $\frac{\partial}{\partial \Delta l} \ln P(\mathbf{y} = \mathbf{i}; \Delta l)$  equal to zero, and the resulting condition is

$$f_1(\Delta l) = \sum_{n=0}^{N-1} \frac{X(\Delta l, \hat{\sigma}, a_{i_n} - \hat{l}) - X(\Delta l, \hat{\sigma}, a_{i_{n+1}} - \hat{l})}{G(\Delta l, \hat{\sigma}, a_{i_n} - \hat{l}, a_{i_{n+1}} - \hat{l})} = 0.$$

The approximate ML estimator for  $\Delta l$  is found to be

$$\hat{\Delta l}_{ap} = \frac{1}{N} \sum_{n=0}^{N-1} \frac{a_{i_n} + a_{i_{n+1}}}{2} - \hat{l}, \quad (6)$$

and the iterative ML estimator calculates

$$\hat{\Delta l}_{k+1} = \hat{\Delta l}_k - \frac{f_1(\hat{\Delta l}_k)}{f_{1,1}(\hat{\Delta l}_k)},$$

where  $f_{1,1}(\Delta l)$  is the partial derivative of  $f_1(\Delta l)$  with respect to  $\Delta l$ . Again, the approximate ML estimator provides the initial value for the iterative ML estimator.

By taking the logarithm of (4) and using (5) with the estimate of  $\Delta l$  for  $\mathcal{H}_1$ , the GLRT becomes: decide  $\mathcal{H}_1$  if

$$\sum_{n=0}^{N-1} \ln G(\hat{\Delta l}, \hat{\sigma}, a_{i_n} - \hat{l}, a_{i_{n+1}} - \hat{l}) - \ln G(0, \hat{\sigma}, a_{i_n} - \hat{l}, a_{i_{n+1}} - \hat{l}) > \gamma' = \ln \gamma.$$

## VI. EXPERIMENTAL RESULTS

To illustrate the performance of the change detector, we performed some computer simulations and some experiments. The observations were the RSSI values provided by an 802.11b ZyAIR B-100 WLAN card, and the signal parameter  $l$  was the received signal strength. We used a uniform quantizer matched to the properties of the WLAN card: it had  $N_q = 128$  levels with  $l_{max} = 27.5$  dB and  $l_{min} = -100.5$  dB, and the decision regions were  $a_i = l_{min} + i\Delta$ ,  $i = 1, 2, \dots, N_q - 1$ , with  $\Delta = (l_{max} - l_{min})/N_q = 1$ . For the approximate ML estimators, the values  $a_0 = l_{min}$  and  $a_{N_q} = l_{max}$  were used, and for the iterative ML estimators, the convergence threshold was set to  $\delta = 0.01$ .

Figure 3 shows the simulated performance of both the approximate ML estimator and the iterative ML estimator when the true values  $l = -32.42$  dB and  $\sigma^2 = 0.5$  were to be estimated. The upper part of the figure depicts the average mean squared error (MSE) for the level  $l$  as a function of the training data record length, while the lower part depicts the average MSE for the noise parameter,  $\sigma$ . From the figures, it can be seen that in case of the signal level  $l$ , both estimators have the same performance. However, in case of the noise parameter  $\sigma$ , the iterative estimator yields better estimates at longer data record lengths: at  $N = 1000$ , its accuracy is one order of magnitude better than that of the approximate ML estimator. If the data record length is very small, the initial values provided by the approximate estimators are not accurate enough, so the iterative estimator will converge to a local optimum point, as opposed to the global optimum point, resulting in worse performance. However, if the data record length is long enough, the iterative method is able to find the global optimum point, improving its performance compared to the approximate estimator.

The performance of the detector was evaluated by performing a set of experiments using two laptops with 802.11b WLAN cards. One laptop was configured to send beacon frames in every 10 ms, and the second one captured those frames in monitor mode and recorded the received RSSI values. The laptops were placed in the opposite ends of two rooms, and a wooden door along their line of sight was opened, half-closed and closed.

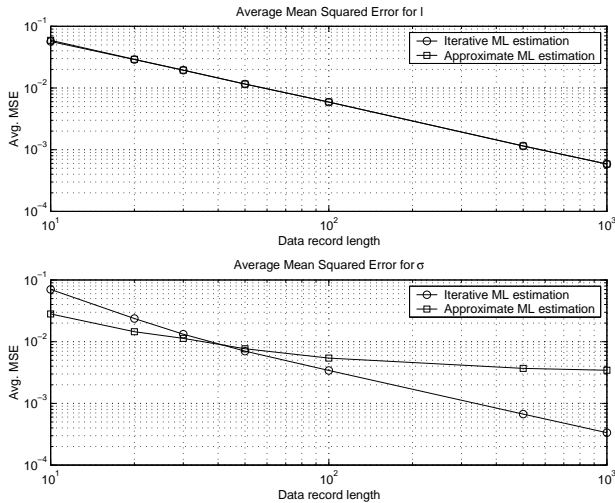


Fig. 3. The performance of the estimator

The decision hypotheses were:  $\mathcal{H}_0$ : the door is closed, and  $\mathcal{H}_1$ : the door is not closed. Figure 4 shows an example RSSI value sequence corresponding to the closed door case (bottom curve) and the half-open door case (top curve). For the training phase,  $N = 1000$  samples were used to estimate  $l$  and  $\sigma$  with the iterative ML estimator when the door was closed. Then, blocks of  $N = 50$  samples were used to detect the change in the signal level  $l$  with different threshold values  $\gamma'$ . To calculate the average probability of false alarm, 159980 blocks of RSSI values were recorded with closed door. To calculate the average probability of detection, 2000 blocks of RSSI values were recorded with both open door and half-open door. The resulting detector performance curves can be observed in Figure 5, using both the approximate and the iterative ML estimators to estimate the level change  $\Delta l$ . The top curves correspond to the open door case, while the bottom curves correspond to the half-open door case. The curves show that the change in the received signal strength due to opening the door could always be detected, even with  $10^{-5}$  probability of false alarm. In case of the half-open door, the probability of detection was slightly reduced, but we can still observe at least 0.9975 probability of detection at  $10^{-5}$  probability of false alarm. Note that the performance of the detector with the iterative ML estimator is a little worse due to the short data record length.

## VII. CONCLUSIONS AND FUTURE WORK

We introduced the notion of multimodal networks that can offer multiple functionalities on the same infrastructure: the communication functionality, and surveillance functionality. The surveillance functionality is implemented by using a wireless communication network as a wireless sensor network, and the effect of moving objects or humans on the characteristics of the radio signal propagation is used to detect the intruder. It was also shown that it is possible to detect indoor physical environment changes using off-the-shelf, low-cost WLAN hardware, so existing WLAN systems have the potential to provide the infrastructure for the implementation of multimodal networks.

Future work includes developing the received signal model, efficient and reliable data fusion algorithms and intrusion detection models for multiple receivers (sensors). The development

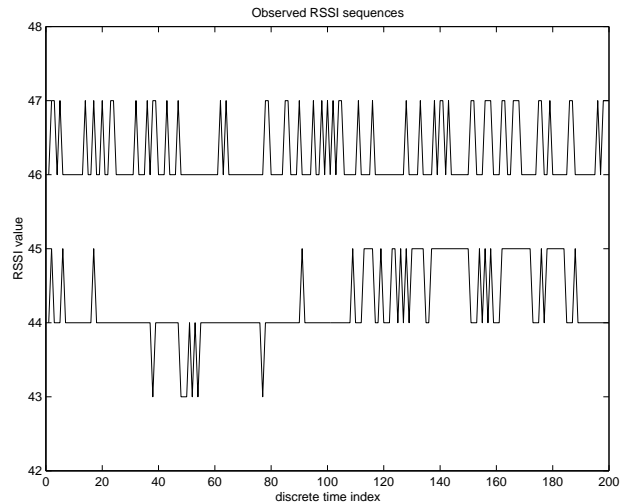


Fig. 4. Observed RSSI sequences

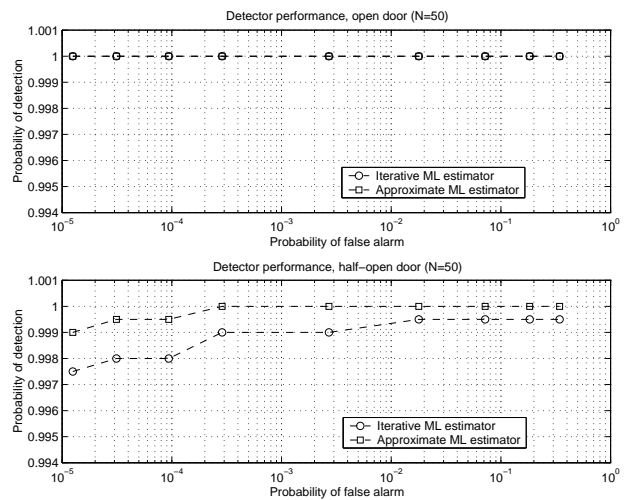


Fig. 5. The performance of the detector

of new network planning methods, simultaneously optimizing the node placement for both communication and intrusion detection is also an important problem.

## REFERENCES

- [1] T. S. Rappaport, *Wireless Communications*, Prentice Hall, 2002.
- [2] J. G. Proakis, *Digital Communications*, McGraw-Hill, 2001.
- [3] M. Weiser, "The Computer for the 21st Century", *Scientific America*, pp. 66–75, September 1991.
- [4] D. Estrin, "Connecting the Physical World with Pervasive Networks", *IEEE Pervasive Comp.*, Vol. 1, Issue 1, pp. 59-69, 2002.
- [5] I. F. Akyildiz, W. Su, Y. Sankarsubramaniam, E. Cayirci, "A Survey of Sensor Networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002.
- [6] C.-Y. Chong, S. P. Kumar, "Sensor Networks: Evolution, Opportunities and Challenges", *Proceedings of IEEE*, Vol. 91, No. 8, pp. 1247-1256, August 2003.
- [7] A. Kara, H. L. Bertoni, "Blockage/Shadowing Polarization Measurements at 2.4GHz for Interference Evaluation between Bluetooth and IEEE 802.11 WLAN", *IEEE Antennas and Propagation Society International Symposium* Vol. 3, pp. 376–379, 2001.
- [8] K. Pahlavan, *Wireless Information Networks*, Wiley & Sons, 1995.
- [9] IEEE Std. 802.11b-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band.