Evaluation of WiFi Beacon transmissions for wireless based passive radar

H. Guo, K. Woodbridge, and C. J. Baker
Department of Electronic and Electrical Engineering, University College London
Torrington Place, WC1E 7JE, London, UK
phone: + (44) 2076793255, fax: + (44) 2073889325, email: h.guo@ee.ucl.ac.uk
web: www.ee.ucl.ac.uk

***Abstract*—Wireless transmissions are a potentially powerful and widely available source of transmissions for passive radar detection. In this work we have carried out a detailed study on the use of IEEE 802.11 (WiFi) transmissions in a passive radar system. The WiFi transmission sequence has been found to be complex and dependent on the user environment but is dominated by Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) signals. An ambiguity function analysis of the DSSS based WiFi beacon signal has been carried out followed by field measurements using a wireless based passive radar system. Range and Doppler characterization of this system is reported and compared with the theoretical predictions. Detection of moving human targets has been achieved for the first time using 802.11 transmissions. This work shows that this technique has considerable promise for a low cost and widely deployable detection and tracking system.**

***Keywords*—Passive Radar, Ambiguity function, Wireless networks.**

I. INTRODUCTION

A large number of wireless local area network (WLAN) are being developed based on the IEEE 802.11 standards. The three most commonly being deployed are 802.11a, 802.11b and 802.11g. These protocols operate in either the 2.4 GHz or 5 GHz spectrum bands and have different modulations and coding schemes which change with data rate and user range. These transmissions are becoming widely available and are therefore a reliable and regular transmission of opportunity for wireless based passive radar. Development of a surveillance capability from such a ubiquitous and accessible source will have major implications for improving security in all types of buildings and in the identification and tracking of goods and people. This type of passive sensing could be used in public areas such as railway and airport terminal or private commercial premises such as office buildings or warehouses. Some preliminary waveform analysis and simple detection experiments have been reported in a previous paper [1]. In this work we examine in more detail the radar detection properties of an 802.11b beacon signal. 802.11 access points emit management frames to establish and maintain communications. The Beacon signal is one such frame and is a periodically emitted signal frame to inform potential users of the presence and properties of the access point host network. The frame format of the beacon signal is defined in the 802.11 standards [2] and is routinely available regardless of user activity. A theoretical ambiguity analysis has been carried out initially to determine the basic range and Doppler capabilities of this transmission. This has been followed by experiment in an outdoor environment to verify the performance of the experimental data. We compare theory and experimental results and analyse the performance and potential of a wireless based passive radar system. It should be noted that in a real transmission environment many data signals would also be present in addition to the beacon signal. This study is therefore not applicable to all operational situations but nevertheless gives a good understanding of some of the fundamental characteristics of a passive radar system using this type of waveform. We have recently carried out a detailed study on the properties of real data signals and a full study is expected to be published in the near future [3].

II. DSSS BEACON SIGNAL CHARACTERISATION

The emitted beacon signal consists of two parts both using DSSS modulation. One part uses Differential Binary Phase Shift Keying (DBPSK) coding and a data rate of 1 Mbps while the second part of the signal uses Differential Quadrature Phase Shift Keying (DQPSK) and a 2 Mbps data rate. An 11 element Barker code is used to realize the spectrum spreading which has the following format:

$$[+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1]$$

The DSSS signal can be basically expressed as

$$s(t) = e^{j2\pi f_0 t} \cdot \sum_{n=1}^{N} e^{j\varphi_i} p(t) \qquad (1)$$

where n is the number of bits and $p(t)$ is the pulse shape function. However, for the ambiguity analysis, the effect of

the Barker code applied to each bit must be highlighted in the signal expression. The expression for the 1 Mbps DSSS&DBPSK signal therefore becomes:

$$s(t) = e^{j2\pi f_0 t} \cdot \sum_{n=0}^{N-1} \sum_{m=0}^{10} e^{j\cdot\varphi_{n,m}} \cdot P(t - mT - 11nT) \qquad (2)$$

where T is the chip duration and m is the length of the Barker code.

We assume a rectangular pulse such that:

$$P(t) = \begin{cases} 1, 0 \le t \le T \\ 0, otherwise \end{cases} \qquad (3)$$

Similarly, the 2 Mbps DSSS&DQPSK signal can be represented by:

$$s(t) = e^{j2\pi f_0 t} \cdot \sum_{n=0}^{(N-1)/2} \sum_{m=0}^{22} e^{j\cdot\varphi_{n,m}} \cdot P(t - mT - 22nT) \qquad (4)$$

In this case two 11-Barker codes are used in order to modulate two bits per cycle rather than one.

III. AMBIGUITY ANALYSIS

Preliminary work on the ambiguity properties of this passive system was used to judge the potential system performance. Although the passive system is inherently bistatic we used a self ambiguity analysis which is geometry independent [4]. Ambiguity diagrams were generated in Matlab for both of the above beacon types. In the simulations the 802.11b signal bandwidth of 11MHz and a rectangular effective pulse shape were used. For the comparison between two modulated signals, an effective integration time of 192 bits was assumed which represents the header and the preamble of a long Physical Layer Convergence Protocol (PLCP) in a PCLP Service Data Unit PSDU format [5]. Using this assumption means the integration time used for the DBPSK modulation is 192 µs, and for the DQPSK modulation is (192/2 = 96) µs.

1. *DSSS/DBPSK modulated signal*

The ambiguity function of a signal *u(t)* is defined as

$$\left|\chi(\tau, f_d)\right| = \left|\int_{-\infty}^{\infty} u(t) \cdot u^*(t-\tau) \cdot \exp(j2\pi f_d t) dt\right| \qquad (5)$$

Substituting Eqn. (2) into Eqn. (5), the following expanded ambiguity expression for the DSSS coded signal is obtained.

$$\left|\chi(\tau, f_d)\right| = \left| \int_{-\infty}^{\infty} \sum_{n_1=0}^{N-1} \sum_{m_1=0}^{10} \exp(-j\cdot\varphi_{n_1,m_1}) \cdot P(t - m_1 T - 11 n_1 T) \cdot \sum_{n_2=0}^{N-1} \sum_{m_2=0}^{10} \exp(j\cdot\varphi_{n_2,m_2}) \cdot P(t - \tau - m_2 T - 11 n_2 T) \cdot \exp(j2\pi \cdot f_d \cdot t) \cdot dt \right| \qquad (6)$$

Using a similar procedure to Franken [6], we arrive at the expected value of this ambiguity function:

$$\left|E\{\chi(\tau, f_d)\}\right| = \left|\sin c(\pi \cdot f_d \cdot 11TN)\right| \cdot \left|(A_{X1,2} + A_{X3,4})/2\right| \qquad (7)$$

Where $A_{X1,2}$ and $A_{X3,4}$ are the ambiguity functions of the two sequences after spreading spectrum using 11 Barker code and DBPSK modulation. The two sequences are shown as the following.

$X_{1,2}$= [-1 -1 1 -1 -1 1 -1 1 1 1], when the un-coded bit is 0 ,
$X_{3,4}$= [1 -1 -1 -1 1 1 1 1 -1 1 -1], when the un-coded bit is 1.

In this expression, the Doppler information is represented by the sinc function in equation (7) while the range information is obtained from the combined ambiguity of the two sequences, which can be seen in the second part of the equation.

The ambiguity diagram and zero range and Doppler cuts of the DSSS/DBPSK signal generated by using (6) are shown in Figure 1.

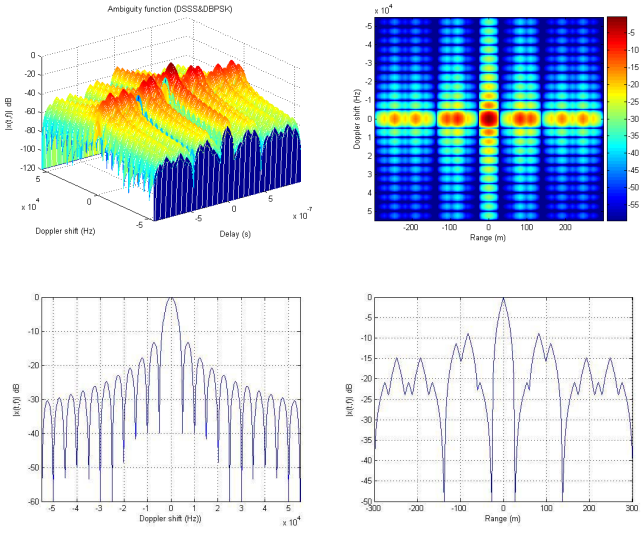

Figure 1 – Ambiguity Diagram and zero Doppler and Range cuts for DSSS/DBPSK Beacon Signal

The resolution results from the self ambiguity function are shown in Table 1 compared with (monostatic) theoretical values using the above bandwidths and integration times. The difference between the simulated and theoretical results is

thought to be due to the idealised rectangular pulse shape used in the simulation process.

Resolution	Simulation	Theory
Range	15.9m	13.6m
Doppler	4.61 kHz	5.2 kHz

Table 1 The theoretical and simulated range and Doppler resolution of the DSSS&DBPSK signal.

2. *DSSS/DQPSK modulated signal*

Using similar methodology to the previous section, the expected value of the ambiguity function for the DSSS/DQPSK signal was generated as follows:

$$\left|E\{\chi(\tau, f_d)\}\right| = \left|\sin c(\pi \cdot f_d \cdot 11TN/2)\right| \cdot \left|(A_{X1} + A_{X5} + A_{X9} + A_{X13})/4\right| \quad (8)$$

In this case, as previously mentioned, the Barker codes modulate two bits per cycle rather than one resulting in four different sequences after QPSK modulation: X1, X5, X9, X13, therefore, in the equation, A_{X1}, A_{X5}, A_{X9} and A_{X13} represent the ambiguity functions of the four sequences, shown as the following:

X1= [-j j -1 1 1 j -1 j -j -1 -1], where the initial bits are 0 0,
X5= [-j j -1 1 1 1 -j 1 1 j -j], where the initial bits are 0 1,
X9= [j j 1 1 -1 1 j 1 -1 j j], where the initial bits are 1 0,
X13= [j j 1 1 -1 j 1 j j -1 1], where the initial bits are 1 1.

The resulting ambiguity diagram and zero range and zero Doppler cuts for the DSSS/DQPSK signal are shown in Figure 2, according to the equation 8.

The resolution results from the calculated ambiguity are shown in Table 2 compared with theoretical values using the above bandwidths and integration times. In this case, when transmitting the same data, the effective integration time the DQPSK modulation need is half the previous one and thus Doppler resolution are twice the previous value.

Resolution	Simulation	Theory
Range	15.9m	13.6m
Doppler	9.21 kHz	10.4 kHz

Table 2 The theoretical and simulated range and Doppler resolution of the DSSS/DQPSK signal.

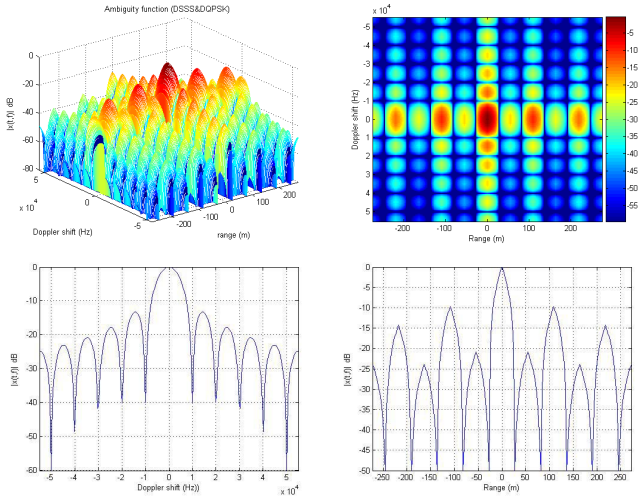

Figure 2 – Ambiguity Diagram and zero Doppler and Range cuts for DSSS/DQPSK Beacon Signal

This initial analysis indicated that range resolution was liable to be restrictive in indoor applications. However with suitable integration times it seemed likely that useable Doppler resolution could be obtained**.** In addition, in a real system environment it would be expected that a combination of both of the above signal types would be present thus both range and Doppler properties would be in practise based on the combination of a number of signal types. In the next section of the work we have therefore investigated some of the performance bounds of wireless based passive radar in a series of real systems experiments.

IV. WIRELESS DETECTION EXPERIMENTS

1. *Description of the field experiment*

Based on the theoretical ambiguity analysis, the target detection experiment was set up in a low clutter outdoor environment (college sport field) (Figure 3). The WiFi transmitter (DWL-2000AP+) was configured to transmit in channel 6 of the Industrial, Scientific and Medical (ISM) license free frequency band, with a centre frequency of 2.437GHz. The system consisted of three nodes; the WiFi transmitter, the target echo receiver and a reference receiver to enable measurement of the direct signal (Figure 3).

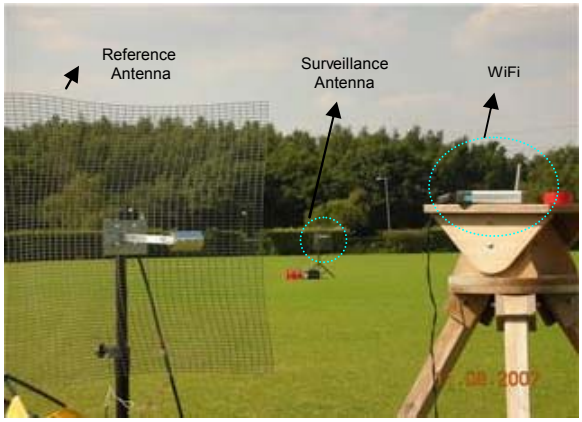

Figure 3 – Photo of the field experiment

Theoretically, the maximum EIRP of the WiFi device is 100mw (20dBm) [4], so the maximum transmitter output is 15 dbm based on the transmitter antenna gain which is 5 dbi and assuming zero loss. The receiver antenna gain is 24dbi; therefore, the maximum detection range for a 1 m^2 RCS human sized target in the monostatic configuration is approximately 120 meters. In the bistatic configuration used in this experiment this increases to 213 meters so it is clear that the detection capability is perfectly adequate for an indoor application. In order to simulate the envisioned indoor application more closely, the maximum distance between the three nodes were set to 50m (Figure 4).

The Beacon signal interval was set as 3ms, via the laptop wireless network configuration, to avoid range ambiguities**.** According to the theoretical analysis, the sidelobe appeared in the zero Doppler makes the detection of the stationary target more difficult, therefore, two moving human targets were measured which moved towards the receiver at a speed of approximately 1 m/s and a spacing of 12m or 35 m (Figure 4). This distance is much smaller (12 m) or larger (35 m) than the theoretical bistatic resolution value calculated above. This was designed to test the target resolution capabilities of the system. The targets at 12 m separation can therefore effectively be expected and considered as a single target.

Two narrow beamwidth ($8^o \times 8^o$) 24dBi gain antennas were employed to receive the direct signal and reflected signal, separately. The University College London (UCL) NetRad system was used as the two receiver nodes. This system has a data recording capacity of 512MB and is able to export the data in binary format. After recording a raw version of the digitized baseband signal, the exported data can be processed in Matlab using a software suite developed at UCL. The sampling of the baseband signal is at 100MHz. A recording time is also set to limit the amount of data recorded.

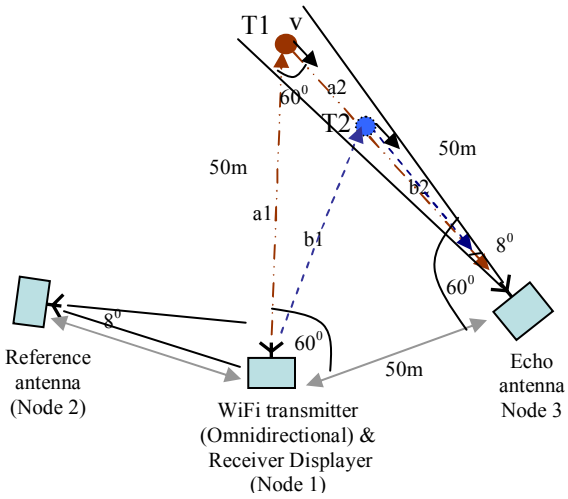

Figure 4 – Geometry configuration for WiFi based passive radar measurement. The filled and dotted circles represent the human targets moving towards the receiving antenna.

2. *DOPPLER signal processing*

To resolve the human target moving at a speed of 1m/s, an integration time of at least 62.5ms is needed. This has been calculated from the bistatic Doppler equation (9). [6]

$$\Delta f = \frac{1}{T} < f_D = \frac{|v| \cdot \cos(\beta/2) \cdot \cos\alpha}{\lambda} \qquad (9)$$

where Δf is the Doppler resolution, T is the observation time. f_D is the Doppler shift, v is the target velocity. λ is the wavelength which is 0.125. β is the bistatic angle and α is the angle between the bistatic bisector and the direction of target motion. From the figure it appears that β is 60deg and α is 30deg.

The capture time of the receiver was set to be 300 ms which encompasses several complete Beacon frame transmissions. For each Beacon pulse of the wireless transmission, the DBPSK modulation appears in the first part of the signal followed by DQPSK in the second part. As previously mentioned, the Doppler and range performance in a real system environment is thus determined by the combined signal properties in tandem with the integration time.

Following the record of the experimental data, the 100ms and the 300ms captured signal were subsequently processed for the cross ambiguity function analysis using the reference and target echo signal. In Figure 5, the cross ambiguity diagram of 100ms integration time is displayed. The presence

of the target can be detected by an asymmetry in the Doppler sidelobes. Theoretically, the target appears at about (50m, 12Hz) (black dashed circle) in Figure 5. Thus the target in the predicted region has been detected but is being masked somewhat by the sidelobes caused by direct signal breakthrough from the transmitter. Although it appears to be easier to detect a long range target, for example around 300m, this is probably not going to be generally of interest in indoor applications due to attenuation and transmitter range limitations.

To reduce the Doppler sidelobe effect, the integration time can be increased to a full 300 ms data whose analysis result is processed as in the figure 6. Compared to the above figure, the Doppler sidelobe effect is being reduced. However, the target is still not very clearly detected due to the correlation from the reference and the interference signal in reflected signal.

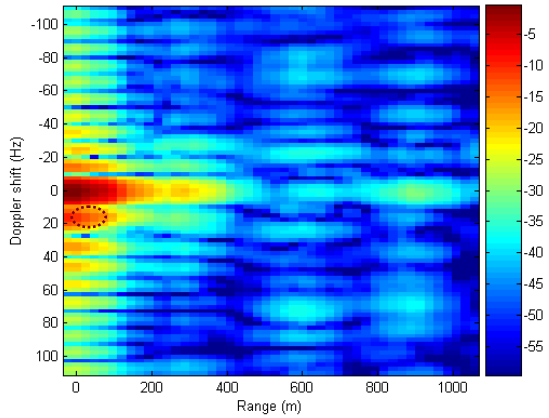

Figure 5 – Cross Ambiguity diagram for 100 ms integration time when the target is moving towards the receiver

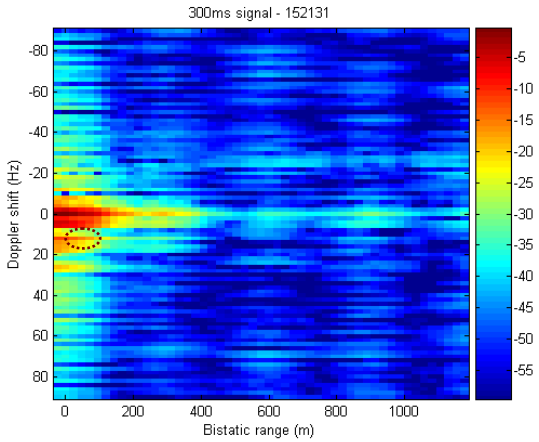

Figure 6 – Cross Ambiguity diagram for 300 ms integration time when two targets (12m) is moving towards the receiver

As mentioned in previous text, the two targets were measured. However, because of the sidelobe effect, even the distance between two targets is long enough, it still impossible to separate the targets based on the resolution analysis (Figure 7), except for the stronger power which is due to one of the target was moving closer to the receiver.

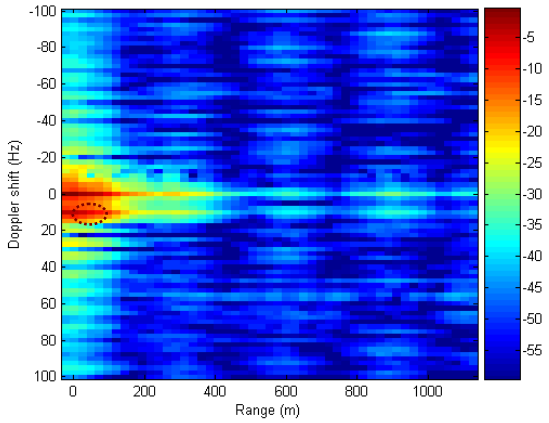

Figure 7 – Cross Ambiguity diagram for 300 ms integration time when two targets (35m) is moving towards the receiver

3. *Discussion*

The preliminary results presented in this paper show that the 802.11 Beacon transmission can potentially be used as a transmitter of opportunity for a passive radar system. The Doppler resolution appears to be suitable for detection of moving human targets although interference from direct signal breakthrough is a potential problem as previously seen in other studies [7]. This can be quantified for this experiment to give an idea of the suppression needed. In this case the ratio of the received power to the direct signal breakthrough power is as follows:

$$\frac{P_R}{P_D} = \frac{\sigma_B L^2}{4\pi (R_T R_R)^2} \cdot \frac{G_{Rmain}}{G_R} \qquad (10)$$

where P_R and P_D are the power of the reflected signal and the power of direct signal both received by echo antenna, L is the bistatic baseline. R_T and R_R are the distance between the transmitter and target, receiver and target, respectively. G_{Rmain} is the peak gain of the surveillance antenna, G_R is the antenna gain at 60° away from the peak which is -30dB in our experiment. Therefore, for the geometry shown in Figure 1, this ratio is -24dB which seems to be promising for detection with the direct signal interference in the reflected signal. However, although the SIR ratio of the passive radar is acceptable, the target is still invisible because of the sidelobe from the Doppler-range figure above. Besides, in a typical indoor application it can be expected that multipath and clutter would be significant. Therefore, the clutter and multipath

interference cancellation will be essential to achieve the clear target information.

This study considers only one transmitter. In a real situation echos could be received from a number of transmitters. However in general wireless LAN systems are designed such that each transmitter covers a certain area and multiple transmitter interference is avoided by the medium access control (MAC) mechanism utilised. Nevertheless some target echoes related to distant transmitters could be returned and this will require further investigation. This study had only examined the situation of an idle network emitting the Beacon signal only. This would be the scenario in quiet areas and periods so has relevance to, for example, night security applications. However further work on typical user active environments is also required.

V. CONCLUSIONS

We report an investigation into the performance of the 802.11 Beacon transmissions in a wireless based passive radar system. The 802.11 beacon frame has been used as an example transmission and simulated ambiguity analysis show that range and Doppler resolutions agree quite well with simple theoretical predictions based on bandwidth and integration time. Preliminary experimental studies in a field environment have then been carried out and detection of moving human targets has been achieved for the first time using wireless LAN transmissions. Further work is now underway on improving target visibility by reducing direct signal breakthrough effects. Further studies in real indoor wireless scenarios using combined beacon and data transmissions are also planned to investigate the effects typical complex transmission environments and address multipath and target resolution and localisation issues.

Acknowledgements

The authors would like to give special thanks to Fabiola Colone (INFOCOM Dept., University of Rome "La Sapienza"), Shaun Doughty and Graeme Smith for their assistance with this work. The work presented here was supported by the UK Engineering and Physical Sciences Research Council (EPSRC). Hui Guo is sponsored by a Dorothy Hodgkin Postgraduate Award (DHPA).

REFERENCES

[1] H. Guo, S. Coetzee, D. Mason, K. Woodbridge and C. Baker, "Passive Radar Detection Using Wireless Networks", European Radar conference, Edinburgh, 2007

[2] IEEE Std 802.11-1999, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[3] F. Colone, K. Woodbridge, H. Guo, D. Mason, and C.J. Baker, "Measurement and analysis of the ambiguity functions of wireless LAN transmissions", submitted for publication *IEEE Trans, Signal Proc., 2008*.

[4] H. D. Griffiths and C. J. Baker, "Passive coherent location radar systems. Part 2: Waveform properties", IEE Proc., Radar Sonar Navig., 2005, 152.

[5] IEEE Std 802.11b-1999, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the2.4 GHz Band.

[6] G. E. A. Franken, H. Nikookar and P. van Genderen, "Doppler Tolerance of OFDM coded Radar Signals", Proceedings of the 3rd European Radar Conference (EURAD 2006), Manchester, pp 108-111, 2006.

[7] Willis, Nicholas J. *Bistatic Radar*, SciTech Publishing, 2005.