jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2011, VOL. 57, NO. 4, PP. 447–450
Manuscript received August 21, 2011; revised November 2011. DOI: 10.2478/v10177-011-0062-3

System Concept of WIFI Based Passive Radar

Stanisław Rzewuski and Krzysztof Kulpa

***Abstract*—In this paper idea of passive radar system based on popular wireless networks commonly named WIFI is presented. In such an networks many transmitters operates in the same channel using multiple access. Wireless networks operating on frequencies 2.4GHz and 5GHz are very common today (IEEE 802.11 a/b/g/n). Classic passive radar determines bistatic distance and velocity by using cross-ambiguity function. To seek target position in XYZ space at least illumination of 3 different transmitters is required. In that paper it was assumed, that all transmitters operate on the same band frequency and the passive radar receiver has to couple each transmission burst with transmitter position by decoding the physical address of transmitter from captured data stream. Having most of the signal sources in our passive radar environment it is possible to detect and to localize objects of interest.**

***Keywords*—Passive radar system, WIFI signal decoding, frame detection, processing signal from wireless networks.**

I. Introduction

THE classical radar illuminates the targets using pulse or continuous wave illumination and receives the target echoes. At the present time the electromagnetic environment is full of different emission, and it is harder and harder to find the free window in which a new radar can operate without interferences with presently working devices. While we do not have to use the flashlight in sunny day, it is no longer necessary to emit own energy for remote sensing, while we can capture other emissions such as FM radio, DVB television, GSM networks, WIFI networks. It is possible to build radar that is not emitting any electromagnetic waves to excite surrounding environment. These radars are named passive, as they only listen and analyze what is around them using signals emitted by other systems. In this paper subject of interest is passive radar based on WIFI networks signals.

WIFI technology (IEEE 802.11 a/b/g/n) implemented in almost all currently produced laptops and smartphones is very widely available. In urbanized areas there is a problem of building WIFI network that will not be interfering with other networks on 2.4 GHz band. In case of 5GHz band it is a matter of time when that situation will happen.

According to regulations power transmitted by wireless network nodes devices that operate in 2.4 GHz should not exceed 50 mW and in case of 5GHz frequency it should not exceed 1W for outdoor equipment. In real life most wireless outdoor equipment is using external antennas that allows for long range operation – up to 30km. The world record for long distance WIFI link was 382 km done by Ermanno Pietrosemoli in Venesuela in May 2007 [1]. It means that environment for such a passive radar already exists.

S. Rzewuski and K. Kulpa are with Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland (e-mail: stach81@tlen.pl, K.Kulpa@ise.pw.edu.pl).

WIFI technology based on IEEE 802.11 a/b/g/n standard operates in two bands 2.4 GHz and 5 GHz. In case of 2.4 GHz band there are 11-14 non orthogonal channels. Number of channels depends on geographical region. Each channel according to standard should be 20 MHz wide. In some cases vendors produce software that forces RF hardware to operate on narrower bandwidths like 5-15 MHz (decreasing transmission speed). This functionality was implemented to help Wireless Network Operators avoiding channel overlapping or other electromagnetic disturbances in their operability environment. We are assuming that devices will use 20MHz channel for communication. It is possible to calculate bistatic resolution of a radar system from (1) which is 15 meters.

$$\frac{C}{B} = r \tag{1}$$

where:
r – resolution of a radar system [m],
C – speed of light [m/s],
B – bandwidth of a radar system [Hz].

This 15 m resolution determines that classical passive radar based on range-Doppler processing can be done for the outdoor WIFI networks with coverage form few hundreds to thousands of square meters. Such a networks are owned by Wireless Internet Service Providers (WISP) and are very common worldwide. The indoor applications are also possible, but they should rely mostly on Doppler processing and power budget analysis and were presented by Viani, Olivieri, Massa [2].

II. Radar Concept

Passive radar locates the target by finding a point of cross-section of bistatic ellipsoids. In our case presented in Fig. 1 the transmitter's opportunity are wireless networks nodes devices located in the radar environment.

System concept is following: passive radar is equipped with several directional antennas (one in simplest case) and one omnidirectional antenna. Directional antennas should be directed towards area of interest (possible location of targets). Omnidirectional antenna is collecting direct signals from the? transmitters. Analysis of signal directly form transmitters (reference signal) and reflected from targets and clutter from directional antennas will be used to detect objects and estimate their bistatic range and velocity.

The bistatic parameters of the targets (bistatic range and bistatic velocities) estimated by finding the coordinates of the peaks of crossambiguity function (2) surveillance beam (directive antenna output) and reference channel obtained by regenerating selected data batches received by omnidirectional antenna.

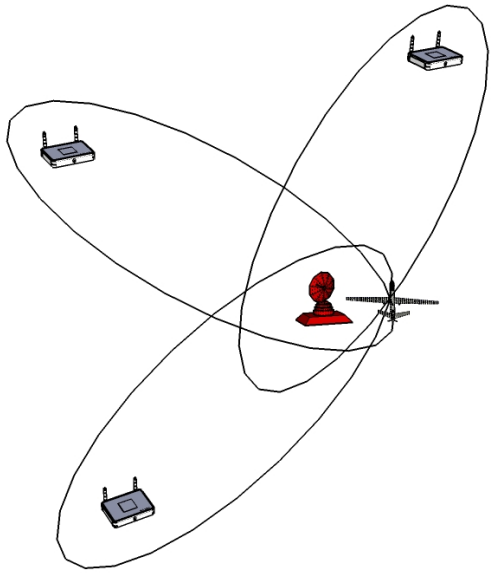

Fig. 1. Passive radar system geometrical concept.

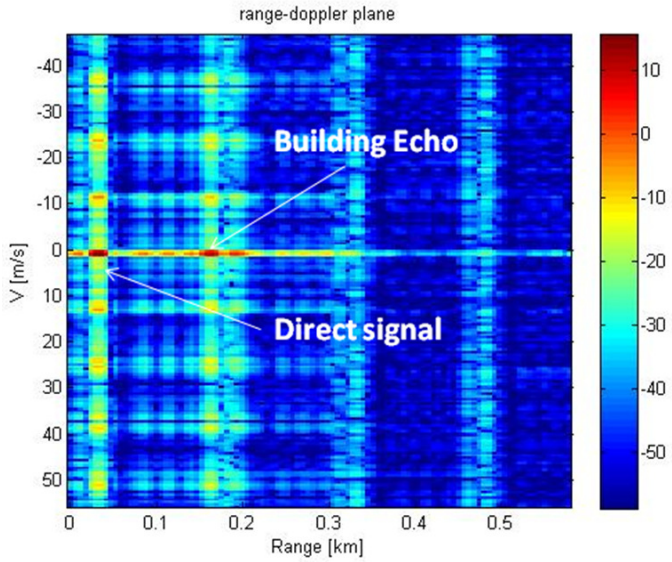

Fig. 2. Crossambiguity function of recorded WIFI signal from balcony of DSP lab of Warsaw University of Technology – color coded in dB.

$$y(R, v_r) = \int_{t=0}^{t_i} x_R(t) * x_T\left(t - \frac{2R}{c}\right) * e^{(-j2\pi(-\frac{2v_r F}{c})t)} dt \quad (2)$$

where:
R – distance from radar,
F – carrier frequency,
v_r – radial velocity,
c – speed of light,
t – time,
t_i – integration time,
x_R – received signal,
x_T – transmitted signal.

The example results of corssambiguity function calculated using real-life signals is presented in Fig. 2. It is easy to see, that strong direct signal and an echo of stationary target (building) is visible. Echoes of the targets are accompanied by the side lobes, which limits the visibility of the small targets. The direct signal together with accompanying side lobes may be removed using CLEAN methods [3], which are beyond the scope of the paper and will not be discuss in details.

To calculate presented crossambiguity function whole signal stream received by all antennas should be divided into substreams originated from all transmitters available in the surroundings. While the WIFI communication is based on the data packages, the whole transmission can be divided into several intervals. Each interval corresponds to one of following events: idle event, where there is no transmission from the transmitters, transmission event, where TN it is transmission from N-th transmitter and collision event where more than one transmitter try to transmit their data.

By receiving and decoding the data stream from omnidirectional antenna it is possible to settle the start and time duration of all events and selects only TN events for given N. As the result it is possible to produce the time windows for all transmitters in the area as presented in Fig. 3.

III. Signal Reception and Decoding

WIFI networks nodes based on IEEE 802.11 b standard [4] were taken into account as source of a signal in this article. Such a signal is in area of interest because currently in urbanized areas this technology became very popular – globally. From frame data that are sent it is possible to extract MAC address of a source and destination wireless network node (STA). Encryption algorithms used in WIFI do not impacts that, because they encrypt data field's. Fig. 4 presents frame structure and data encoded inside it (simplified view).

PPDU (PLCP protocol data unit) containing PLCP Preamble and PLCP Header. PLCP – Preamble in and Header case of IEEE 802.11b standard are always transmitted with 1 Mbps speed and DBPSK modulation. They always have constant time length which is 192 microseconds. PLCP – Preamble contains: SYNC – synchronization field – 128 encoded ones, SFD – start frame delimiter and SIGNAL – signal type field. This Preamble is used to allow receiver to synchronize with signal, detect end of synchronization phase (SFD) and identify what will be data speed and modulation of PSDU (PLCP service data unit) container. Next in the frame is PLCP Header which contains: SERVICE – Field reserved for future use, LENGTH – unsigned 16-bit integer that indicates the number of microseconds from 16 to (2^{16} – 1) that determine in simplification PSDU occurrence time, CRC16 – check sum that is calculated form previous PLCP HEADER fields to protect data consistency.

PSDU – PLCP service data unit which in simplification contains MSDU – MAC service data unit. MAC frame contains following fields: Frame Control, Frame Duration, Address 1,2,3 Sequence Control, Address 4, QoS (Quality of Service) Control, Frame Body, FCS – frame check sequence. From perspective of information usability for passive radar system MAC frame fields are interesting, because each Address field contains a MAC 48-bit address which explicitly defines each

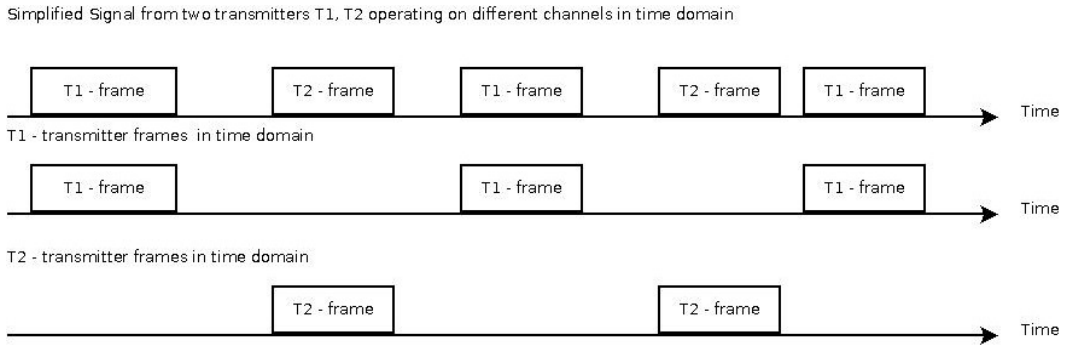

Fig. 3. Signals from different WIFI networks and channels in time domain. T1,T2 – transmitters.

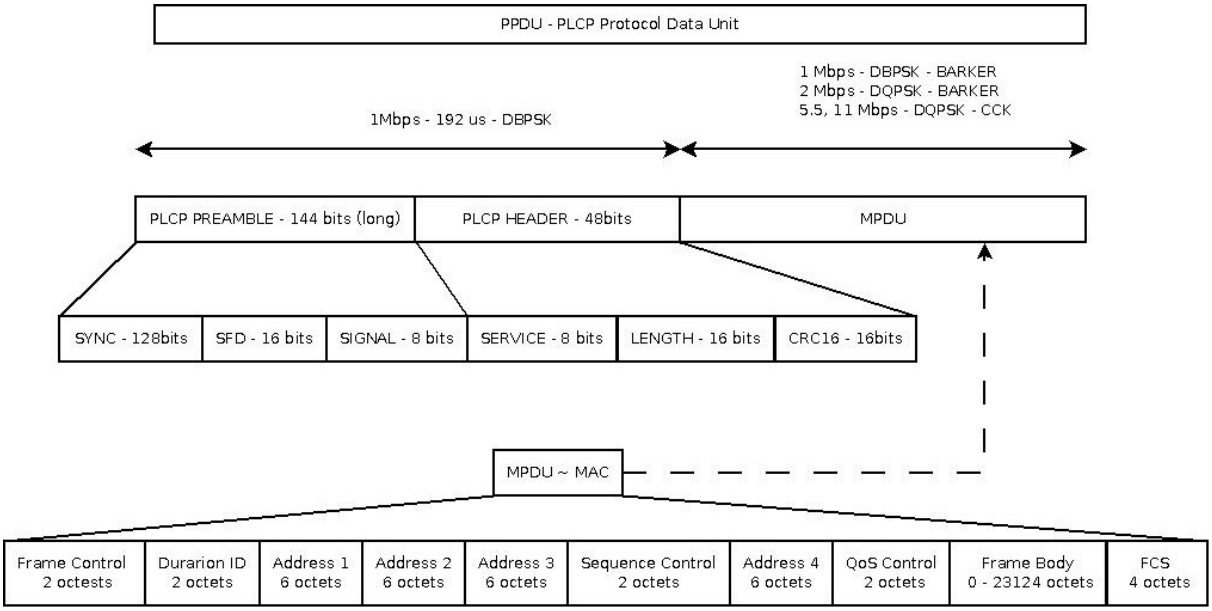

Fig. 4. Frame structure – where: PLCP – physical layer convergence procedure, PPDU – PLCP protocol data unit, MPDU – MAC Protocol Data Unit, MAC – Media Access Control.

Fig. 5. Signal detection.

WIFI network node. Having information from decoded frame it is possible to locate source and destination of the transmitted signal and place it in environment in which radar operates.

PLCP Header and Preamble is modulated using DBPSK (Differential Bipolar Phase Shift Keying) and transmitted with speed of 1 Mbps. PSDU can be sent using DBPSK for transmission DQPSK (Differential Quadrature Phase Shift Keying). Each bit of information that is sent into air is chipped with Barker code (1-2 Mbps) or CCK (5.5-11 Mbps). In our research works only Barker coding was taken into analysis.

The signal detection mechanism is showed on Fig. 5. Signal acquisition is performed at the beginning. On such a collected signal mechanism of Frame detection is performed. Whenever frame is detected this part of signal is submitted to resample process after that signal is demodulated and than de-chipped (coding words are converted into bits). Finally PLCP Preamble and Header decoding can be done. Having correct information from PLCP a MAC address extraction can be performed. Finally MAC address of a source and destination node can be collected. After getting MAC address triangulation algorithm can be started for source and destination node localization.

The concept of the passive radar utilising WIFI communication was verified experimentally at DSP Laboratory of Warsaw University of Technology. The system consists of two WIFI nodes (Mikrotik RB 600 equipped in WMIA-123 MiniPCI Wireless Network Card) and the two channel vector analyser Agilent 89640 Vector Signal Analyzer presented in Fig 6 (left). To simplify the setup the signal from the node T1 was split by 20 dB directional splitter and the attenuated copy was register as first channel of vector signal analyser. This signal played the

Fig. 6. Measuring Equipment – Agilent and High Gain 2.4 GHz antenna on the right.

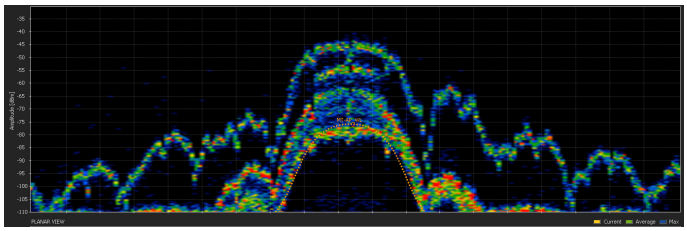

Fig. 7. Spectrum of signal of two communicating WIFI nodes – measurement directly from wire – measured by WiSpy 2.4 dbx – side lobes are clearly visible.

role of reference signal. The surveillance antenna, presented in Fig. 6 (right) collected echo signals vial main lobe and direct signals via side lobes. To analyse the actual spectrum in WIFI region and the presence of other transmitter emission the WiSpy 2.4 dbx was used. Fig. 7 show spectrum of signals exchanged between two network nodes (measurement done in the cable).

The time domain representation of the recorded signals is presented on Fig. 8. The signal frames were transmitted with DBPSK modulation, Barker Coding, 11 Mbps transmission

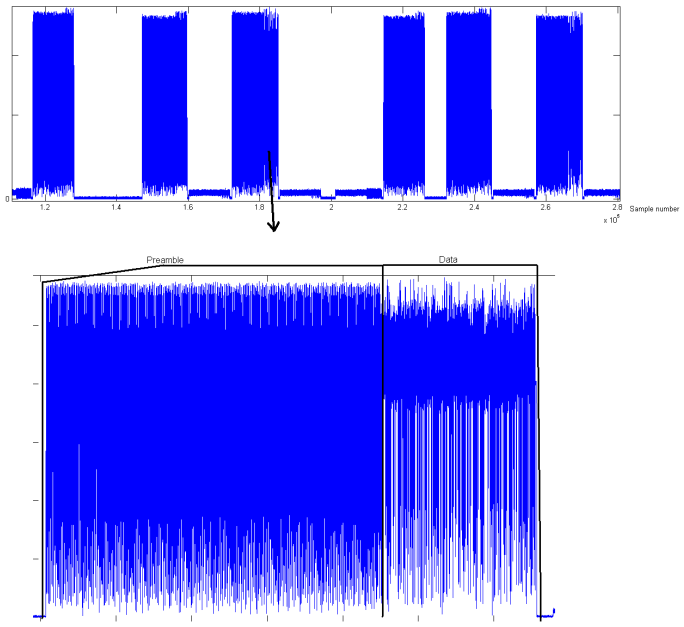

Fig. 8. WIFI network frame in time domain – Horizontal axis – sample number, Vertical scale – Voltage.

speed. Wireless network nodes were sending ICMP (Internet Control Message Protocol) ECHO REPLY and ICMP ECHO REQUEST packets to each other. That data stream was taken for farther analysis using MATLAB. It was possible to decode PLCP data. That signal will be a subject of future research.

In this paper idea of passive radar system based on wireless networks signal was sketched and described. Such a radar can operate in rural area and should detect targets with spatial resolution of 15m. Frame structure for 802.11b standard was presented. It was showed that it is possible to collect and process wireless frame using specialized equipment (directly from antenna cable). By processing we understand decoding PLCP Preamble and Header. It was proved that signal from measurements can be decoded showing CRC16 field decoded and calculated from measurements. In our farther research we would like to focus on farther signal decoding and obtaining MAC address. This will lead to signal source and destination localization. Next step will be signal regeneration so analysis between distorted and sent signal can be done which will lead to locating target's in radar environment.

IV. Conclusions

In this paper idea of passive radar system based on wireless networks signal was sketched and described. Such a radar can operate in rural area and should detect targets with spatial resolution of 15m. Frame structure for 802.11b standard was presented. It was showed that it is possible to collect and process wireless frame using specialized equipment (directly from antenna cable). By processing we understand decoding PLCP Preamble and Header. It was proved that signal from measurements can be decoded showing CRC16 field decoded and calculated from measurements. In our farther research we would like to focus on farther signal decoding and obtaining MAC address. This will lead to signal source and destination localization. Next step will be signal regeneration so analysis between distorted and sent signal can be done which will lead to locating target's in radar environment.

References

[1] Long distance WIFI trial - Ermano Pietrosemoli EsLaRedULA – International Summit for Community Wireless Networks Columbia – http://www.slideshare.net/1ereposition/long-distance-WIFI-trial.

[2] F. Viani, G. Oliveri, and A. Massa, "Real-time Tracking of Transceiver-free Objects for Homeland Security," in *European Radar Conference*. University of Trento Via Sommarive 14, I-38050 Trento, Italy: Department of Information Engineering and Computer Science, 2009.

[3] K. Kulpa, "Application of the CLEAN Class Methods for Detecting Weak Radar Signals in the Presence of Strong Interference Signals," *Prace Naukowe Politechniki Warszawskiej. Elektronika*, pp. 1–158, 2008, z. 164.

[4] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput.

[5] S. D. Deshpande, "Software Implementation of IEEE802.11b Wireless LAN Standard."