Improved Estimation of Trilateration Distances for Indoor Wireless Intrusion Detection

Philip Nobles[1], Shahid Ali[2] and Howard Chivers[3]
[1,3]*Cranfield University*
Defence Academy of the UK
Swindon, UK
[2]*National University of Sciences and Technology*
Pakistan
p.nobles@cranfield.ac.uk[1] and h.chivers@cranfield.ac.uk[3]

Abstract

Detecting wireless network intruders is challenging since logical addressing information may be spoofed and the attacker may be located anywhere within radio range. Accurate indoor geolocation provides a method by which the physical location of rogue wireless devices may be pinpointed whilst providing an additional option for location-based access control. Existing methods for geolocation using received signal strength (RSS) are imprecise, due to the multipath nature of indoor radio propagation and additional pathloss due to walls, and aim to minimise location estimate error. This paper presents an approach to indoor geolocation that improves measurements of RSS by averaging across multiple frequency channels and determining the occurrence of walls in the signal path. Experimental results demonstrate that the approach provides improved distance estimates for trilateration and thus aids intrusion detection for wireless networks.

1 Introduction

Wireless local area network (WLAN) technology based upon the IEEE802.11 standard, often referred to by the industry accreditation "WiFi", is now as much a part of corporate networks as Ethernet, is the predominant networking technology in the home and is integrated into computers, smartphones and games consoles [1]. Wireless is ubiquitous, but is not without security risks [2]. A WLAN device is as likely to be a network attacker, or victim, as any other network device but rather than being physically attached to a port on a network switch, the wireless device could be located anywhere within range of the wireless network. This makes physically locating an attacker a difficult task.

Since Medium Access Control (MAC) addresses and Internet Protocol (IP) addresses can be spoofed, it is not possible to distinguish between an authorised device and a spoofed, or insider, copy using network traffic data alone [3]. If the physical location of the devices can be determined then this additional information may be used to distinguish between them.

In the most common configuration, IEEE802.11 WLAN client network Stations (STA) communicate via an Access Point (AP) using 2.4GHz radio frequency (RF) signals. The AP might also provide access into a corporate network and/or the Internet. WLAN networks may be configured such that clients must authenticate with the AP and data traffic may be encrypted, but in certain cases the authentication and encryption keys may be obtained by cryptanalysis [4]. For the purposes of this paper we will assume, however, that the attacker is an insider who possesses the correct authentication credentials. Even without the correct credentials a number of attacks are possible, such as denial of service, and thus it is desirable to be able to locate any unauthorised WLAN device [5].

If accurate geolocation is available then additional security mechanisms may be implemented. As one example, devices could be denied access to the network when inside, or outside, specific areas, such

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 1, pp. 93-102

as the perimeter of a building. Accurate location tracking also has uses within warehousing and for autonomous vehicles [6].

2 Location Estimation

Location estimation of wireless devices inside a building is a challenge. The Global Positioning System (GPS) works very well in outdoor environments. GPS receives signals from multiple satellites and can calculate position with a 10m accuracy [7]. GPS is rendered ineffective within a building, however, due to wall and ceiling losses. In addition, client devices must be equipped with GPS receivers and must be correctly reporting their location. Infrared and ultrasonic location systems have also been proposed, but these require additional components. It is thus desirable to use the RF communication capabilities of the WLAN devices themselves to provide the required functionality for geolocation.

Traditional methods for geolocating a RF transmitter include angle of arrival (AoA) using antenna arrays, time of arrival (ToA) and received signal strength (RSS) [8]. Angulation refers to the use of angles to calculate positions whereas lateration uses distances derived from ToA or RSS measurements. For location in two dimensions at least three distances from known points, or "anchors", is necessary and the term trilateration is thus used. Given perfect distances, the device's location is at the intersection of three circles centred around the anchors.

Triangulation and trilateration have been considered in some detail for wireless sensor networks [9]. The location methods previously proposed in the literature have concentrated upon reducing the estimate error of combined measurements rather than considering the error mechanisms due to the indoor radio propagation environment itself, as is done in this paper. One method for improving location estimates is to track the movement of wireless devices and then apply tracking algorithms, such as Kalman filters, to the multiple estimates [10]. This approach is useful in the case of moving robotic sensors but is less applicable in the case of a typical WLAN where devices are not necessarily in motion when being used. The following subsections consider the use of ToA and RSS methods as applied to WLANs.

2.1 Time of Arrival

Very accurate measurements of signal arrival time are required to estimate the distances encountered in an indoor environment. WLAN devices typically do not report signal arrival times without additional custom external hardware [11]. This approach is thus not considered further.

2.2 Received Signal Strength

The reduction in received power with distance of a radio frequency signal transmitted in free space, or pathloss, follows an inverse square law and is usually calculated using the Friis equation [12]

$$L_p = \frac{P_r}{P_t} = G_t G_r \left[\frac{\lambda}{4\pi d}\right]^2 \tag{1}$$

where L_p is the pathloss at distance d. P_t is the power supplied to the transmitting antenna with a gain of G_t in the direction of the receiving antenna. P_r is the power at the receiving antenna of gain G_r. λ is the wavelength of propagation.

For a transmission frequency of 2.4GHz and unity gain, free space path loss in dB may be given by

$$L_p = 40.23 + 20log(d) \tag{2}$$

Received signal strength (power) (RSS) provides good estimates for line-of-sight scenarios with no multipath, where a direct relationship is present between received signal strength and distance from the transmitter. The indoor propagation environment, however, is complex and received signals suffer from a combination of free-space pathloss, signal attenuation primarily due to walls and multipath. Thus, the received signal strength has a complex relationship with distance, causing errors for geolocation.

IEEE802.11 WLAN devices report received signal strength in the form of Received Signal Strength Indication (RSSI) values. RSSI is used by the WLAN to decide if the radio channel is free for transmitting and also to decide when to switch, or "roam", to a different access point. Different vendors implement RSSI in various ways [13]. The Linksys WRT54G APs used in the experiments described in Section 4 report RSSI values in dBm. In this paper the term RSS is used to refer to theoretical received signal strengths and RSSI to refer to received signal strengths as reported by the WLAN AP firmware. The WRT54G RSSI values are effectively referenced to 0dBm and are thus equivalent to pathloss measurements giving $RSSI(dBm) = -L_p$.

Multipath in the indoor environment is caused by multiple signal reflections from walls, ceilings, furniture and other objects. The impact of multipath upon received signals is frequency selective fading. For a typical indoor environment, frequency selective fading causes fades of as much as several tens of dBs that vary with location. This directly effects the measured RSSI. A typical measured indoor radio channel frequency response is shown in Figure 1. This response was obtained by sampling RSS at 501 individual frequencies across a 500MHz bandwidth [14].

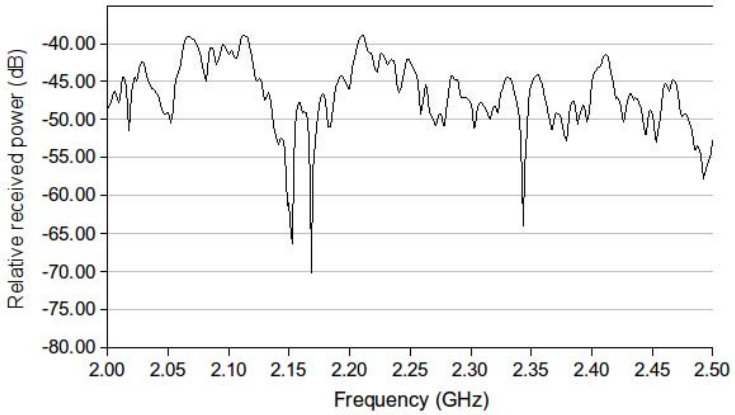

Figure 1: Measured indoor 2.0-2.5GHz radio channel frequency response

One indoor geolocation method that has been proposed is to match signal "fingerprints" obtained by measurements of RSS at locations throughout the building(s) of interest to received signals [15]. The problem with this approach is that the indoor environment is sufficiently complex with low correlation between closely spaced locations, of the order of wavelengths, that it would not be practicable to measure a building to a resolution sufficient for accurate estimation [16]. The accuracy of then matching stored samples from previous off-line measurements to real-time RSSI values has been shown to be poor [17].

The method presented in this paper uses RSSI as reported by the AP plus additional methods, including some knowledge of the indoor environment, to reduce the RSS error and thus improve geolocation accuracy.

3 Improving RSS accuracy

Measurements of RSS from a single 25MHz WLAN channel will be subject to multipath fading. Averaging measurements taken across multiple 802.11 WLAN channels provides an implementation of frequency diversity that provides a more accurate RSS measurement and obviates much of the effect of frequency selective fading upon RSS.

Now that a useful measurement of RSS is available, the next indoor propagation mechanism to tackle is the presence of walls and their effect upon the measured RSSI. The effect of walls upon averaged RSSI values is to present a fixed attenuation depending upon the construction material of the wall [14]. Given the typical range of a WLAN, it is likely that there will be none to several walls between the AP and STA. Assuming a maximum of n walls between each AP and STA gives $n+1$ possible distance values for any measured RSSI value, one of which represents the true distance.

Taking RSSI values from multiple APs with overlapping coverage areas, desirable in any case for roaming, it is possible to produce a set of possible distances for each AP. When plotted on a floorplan, these distances may be represented as $n+1$ concentric circles for each AP. Given that RSS measurements from at least three APs are required to provide a location estimate, there exists at least $(n+1)^3$ possible combinations of measurements to provide the location estimate, which in addition are likely to have some remaining error associated with each measured RSSI value. The accuracy of these position estimate depends partly upon the accuracy of the wall loss estimate, the measurement accuracy of the AP's RSSI mechanism and the geometry of the APs and the STA. Residual errors remain after the multi-channel averaging process and include other losses such as furniture.

If we now make some assumptions then we may reduce the number of possible combinations of RSSI measurements to be considered.

3.1 Relationship between RSS and room geometry

Referring to Figure 2, consider a square room with infinitely thin sides of length $2Xs$, with an AP placed at the centre of the room. Assuming free-space pathloss for a 2.4GHz signal, for any client STA if $RSS > -(40.23 + 20log(Xs))$ dBm then the STA must be located within the same room as the AP.

If $2Xd$ is the diagonal length across the room then for any $RSS < -(40.23 + 20log(Xd))$ dBm the STA must be located outside the room.

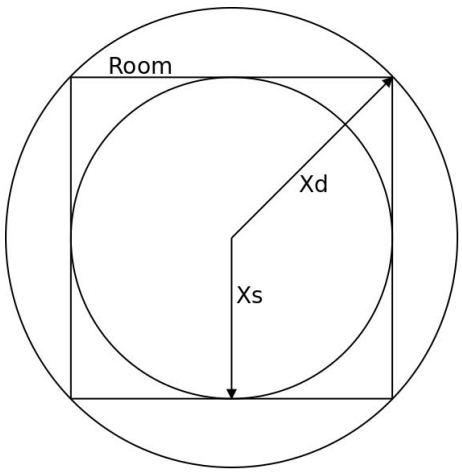

Figure 2: Square room.

If we consider that the walls of the room have a wall loss associated with them, then providing this

loss is greater than 3dB (the diagonal of a square is $\sqrt{2}$ times the length of a side resulting in a 3dB difference in RSS), then for any $RSS < -(40.23 + 20log(Xs) + 3)$ dBm the STA must be located outside the room. The difference between 3dB and the wall loss allows the condition to also hold true for some rectangular rooms.

Providing the dimensions of the room housing the AP are known, for a given RSSI value it is thus possible to determine the occurrence of a wall between the AP and STA. RSSI values may then have a correction applied when calculating distances based upon free-space pathloss to take into account the additional wall loss. Wall losses for typical building materials are available in the literature, although it is fairly straightforward to measure wall loss by placing the AP on one side of the wall and the STA on the other at a known distance. For brick walls a loss of 5dB is typical.

This theory may be extended to consider the set of rooms adjacent to the room housing the AP. In this manner, the number of walls between the AP and the STA for a given RSS may be determined. Clearly for this extended method to be applied a floorplan of the building must be available.

4 Experiments

4.1 Experiment Setup and Location

A 15x30m section of a building at Cranfield University, the Heaviside Laboratory, was used as the location for a series of experiments to test the indoor geolocation methods described in the above sections. The test area comprised seven rooms and is predominantly of brick construction.

The Linksys WRT54G AP allows for an updated open source firmware, DD-WRT [18], to be installed that provides RSSI measurements in dBm and thus these APs were chosen for the experiments. A 3com WLAN PCMCIA card was chosen as the client STA device, but any WLAN STA client device would have been suitable.

4.2 Relationship Between RSS and Distance

Preliminary experiments were carried out to investigate the relationship between RSS and distance for line-of-sight locations. These experiments have been described in a previous paper [19]. Figure 3 reproduces measured RSSI values for four WLAN channels measured at various distances from an AP. The theoretical free-space loss is included for comparison. As expected, multipath causes fading which produces significant deviation of RSS from free-space loss.

Results for averaging across WLAN channels are presented in Figure 4. The averaging process produces estimates which are close to the theoretical free-space loss and thus will provide more accurate geolocation estimates.

4.3 Geolocation Experiments

APs were placed in the centre of four rooms as marked by numbers 1 to 4 on Figure 5. A client STA was then connected, or "associated" to use the IEEE802.11 terminology, with the WLAN network and moved between multiple locations throughout the test area. Since an STA will automatically reassociate to the strongest available signal as part of the roaming process, by switching the AP's RF signal on and off in turn it was possible to obtain an RSSI reading for the STA at each location from all four APs. For each association the reported RSSI was recorded for each of the 13 frequency channels available on the AP.

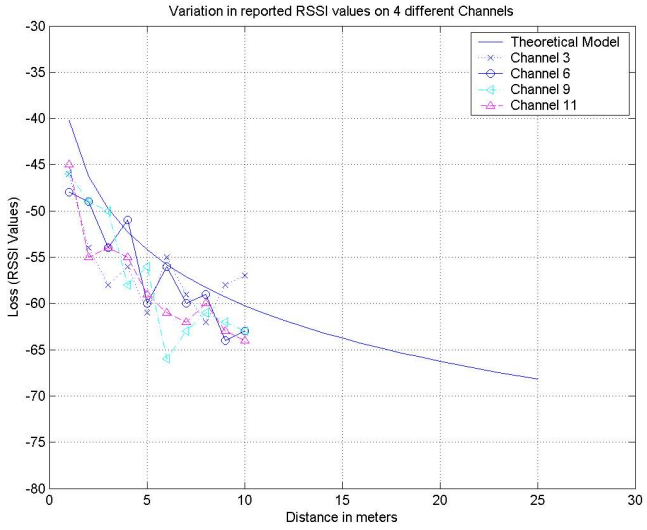

Figure 3: Variation in RSSI for 4 different WLAN channels.

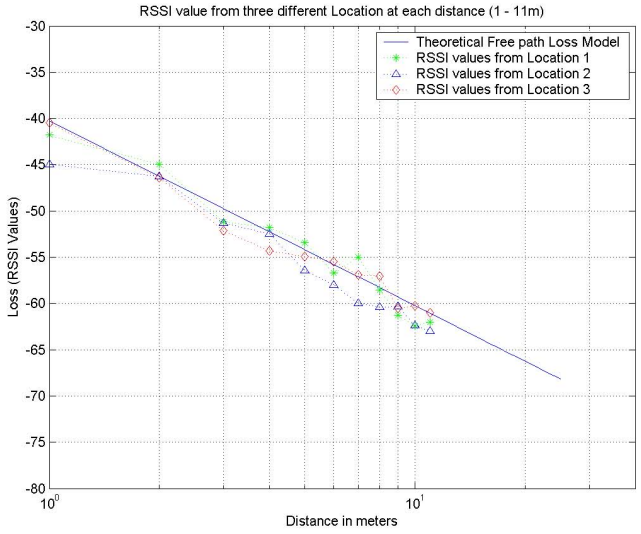

Figure 4: RSSI averaged across 13 WLAN channels against distance for multiple STA locations and three AP locations.

4.4 Geolocation Using Single-Channel RSSI Measurements

A typical geolocation result using uncorrected single channel RSSI measurements is presented in Figure 6 for comparison. The figure represents the test area, showing the location of walls as lines and the actual location of the STA as a small square. The estimated distances of the STA from each AP as calculated from reported RSSI is depicted as circles.The combination of multipath and wall loss means that estimated distances are wildly inaccurate with the only intersection of circles within the area covered by the floorplan appearing outside of the test area. Two of the circles lie completely outside the area covered by the floorplan and thus do not appear in the figure.

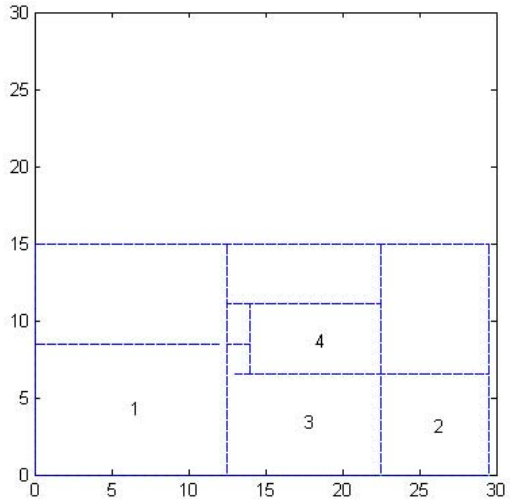

Figure 5: Floorplan of the area used for experiments showing the location of APs 1-4. Scale is metres. The upper half of the figure represents locations outside of the building.

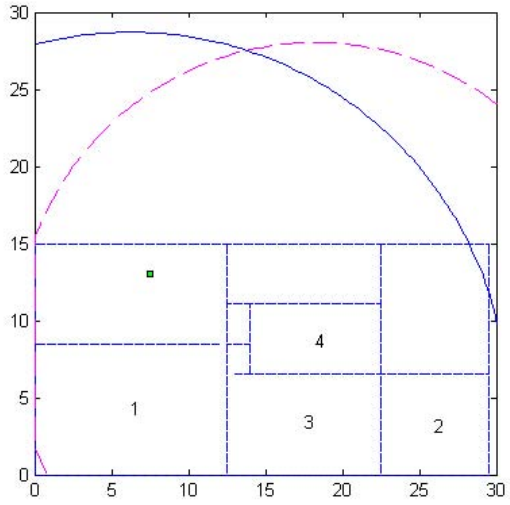

Figure 6: Estimated geolocation curves based upon uncorrected RSSI measurements.

4.5 Geolocation Using Averaged RSSI Values

A typical geolocation result using averaged RSSI values is presented in Figure7. The intersection of two circles is closer to the true location but without the wall losses taken into account the distance estimates remain inaccurate.

4.6 Geolocation Using Averaged RSSI Values and Predicted Wall Occurrences

Including the predicted number of walls between AP and STA improves the estimated distances and provides geolocation estimates that lie close to the true location of the client STA. Figure8 shows a typical

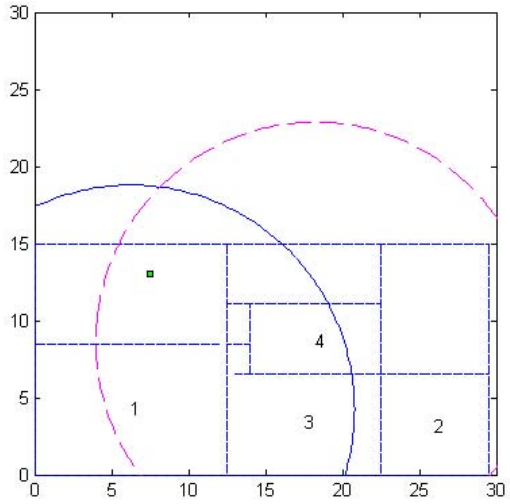

Figure 7: Improvement in geolocation estimates due to averaging of RSSI values across WLAN channels.

example where results from all four APs have been combined using trilateration to reduce the geolocation error to a mere 1.25 metres. Geolocation estimates are plotted as small crosses. The experiment was repeated for additional STA locations to validate the method.

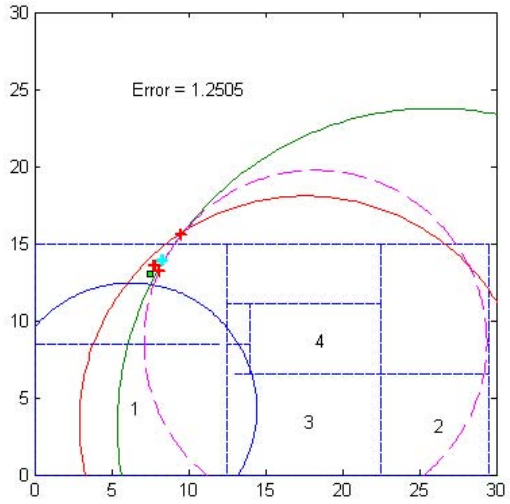

Figure 8: Accurate geolocation estimates using prediction of wall occurrences.

5 Conclusion

The complexity of the indoor radio propagation environment makes accurate geolocation of wireless devices challenging. This paper has presented a novel approach to improving geolocation accuracy by considering the dominant propagation mechanisms that cause errors for RSS measurements, namely mul-

tipath and wall loss. The effect of multipath on RSS is reduced by averaging RSSI values across multiple WLAN channels. A method has been presented to determine the occurrence of walls between APs and STAs to improve RSS measurements, based upon knowledge of the indoor room layout, and hence to improve estimated distances for trilateration. Experimental results demonstrate that the approach provides accurate geolocation within the indoor environment and thus aids detection of WLAN insider attacks.

References

[1] "IEEE 802.11, the working group setting the standards for wireless LANs," http://www.ieee802.org/11/. [Online]. Available: http://www.ieee802.org/11/

[2] J. Park and D. Dicoi, "WLAN security: current and future," *Internet Computing, IEEE*, vol. 7, no. 5, pp. 60–65, 2003.

[3] P. Nobles and S. Ali, "Evil twins, wi-phishing and other wireless threats," in *Proc. of the 4th IET Secure Mobile Communications Forum, London*, December 2006.

[4] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," *IEEE Wireless Communications*, vol. 9, no. 6, pp. 44–51, 2002.

[5] P. Nobles and P. Horrocks, "Vulnerability of IEEE802.11 WLANs to MAC layer DoS attacks," in *Proc. of the 2nd IEE Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, 2004. (Ref. No. 2004/10660)*, 2004, pp. 14/1–14/5.

[6] F. Thomas and L. Ros, "Revisiting trilateration for robot localization," *IEEE Transactions on Robotics*, vol. 21, no. 1, pp. 93–101, 2005.

[7] P. Enge and P. Misra, "Special issue on global positioning system," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 3–15, 1999.

[8] R. Stansfield, "Statistical theory of DF fixing," *IEE Journal of Electrical Engineers*, vol. 94, no. IIIA, pp. 762–770, 1947.

[9] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. Wiley-Interscience, Sep. 2007.

[10] C. Rohrig and M. Muller, "Indoor location tracking in non-line-of-sight environments using a IEEE 802.15.4a wireless network," in *Proc. of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS'09), St. Louis, MO, USA*. IEEE, October 2009, pp. 552–557.

[11] F. Izquierdo, M. Ciurana, F. Barcelo, J. Paradells, and E. Zola, "Performance evaluation of a TOA-based trilateration method to locate terminals in WLAN," in *Proc. of the 1st International Symposium on Wireless Pervasive Computing ISWPC'06, Phuket, Thailand*, January 2006, pp. 1–6.

[12] H. Friis, "A note on a simple transmission formula," *Proceedings of IRE*, vol. 34, 1946.

[13] J. Bardwell, "Converting signal strength percentage to dBm values," WildPackets Inc., White paper, Nov. 2002. [Online]. Available: http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf

[14] P. Nobles and F. Halsall, "Delay spread and received power measurements within a building at 2 GHz, 5 GHz and 17 GHz," in *Proc. of the 10th International Conference on Antennas and Propagation (Conf. Publ. No. 436), Edinburgh, UK*, vol. 2, April 1997, pp. 319–324.

[15] P. Bahl and V. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proc. of IEEE INFOCOM 2000, Tel-Aviv, Israel*, vol. 2. IEEE, March 2000, pp. 775–784.

[16] P. Nobles and F. Halsall, "Spatial correlation analysis of indoor radiowave propagation measurements for wireless LANs," in *Proc. of IEE Colloquium on Radio Communications at Microwave and Millimetre Wave Frequencies (Digest No. 1996/239), Savoy Place, London*, December 1996, pp. 10/1–10/5.

[17] A. G. Dempster, B. Li, and I. Quader, "Errors in determinstic wireless fingerprinting systems for localisation," in *Proc. of the 3rd International Symposium on Wireless Pervasive Computing (ISWPC'08), Santorini, Greece*. IEEE, May 2008, pp. 111–115.

[18] "DD-WRT," http://www.dd-wrt.com. [Online]. Available: http://www.dd-wrt.com

[19] S. Ali and P. Nobles, “A novel indoor location sensing mechanism for IEEE 802.11 b/g wireless LAN,” in *Proc. of the 4th Workshop on Positioning, Navigation and Communication 2007 (WPNC’07), Hannover, Germany*. IEEE, March 2007, pp. 9–15.

Philip Nobles is a lecturer within the Centre for Forensic Computing and Security, Cranfield University, at the Defence Academy. Since 1991 he has led research and teaching in telecommunications and computer networks. Philip joined Cranfield University at Shrivenham in 1999 where his teaching, research interests and publications cover information security, wireless networks and cyberdefence. Philip has led successful research projects sponsored by Government, Research Councils and industry. These projects include the development of wireless cameras for the BBC (a Royal Television Society award winning project), a recent study on critical national infrastructure security for CPNI and the current TSB project Integrated Model for the Management of the Complexity, Risk and Resilience of Secure Information Infrastructure. He has also contributed to international working groups, including ETSI standards. Philip has been interviewed on national and international media, including BBC News, providing an expert view on cybercrime, wireless networks and internet security.

Shahid Ali is employed at National University of Science and Tehnology (NUST) Pakistan. He completed his PhD in year 2007 from Cranfield University (UK). His thesis title was “ Indoor Geolocation Using Wireless LANs”. At present, he is actively involved in research and teaching assignments at the university. He also interface with the industry to conduct research. His active research areas have been Underwater Propagation losses, RF Propagation Losses, Indoor Geo Location, Antennas (Underwater and Above water) and controls.

Howard Chivers is Professor of Information Systems and Director of the Centre for Forensic Computing and Security at Cranfield University, within the Defence Academy of the United Kingdom. His research interests are in system security and computer forensics, and current security projects include risk management in dynamic collaborative networks, the identification of subtle intrusions within computer networks, and the security of industrial GRID applications. He is also a security practitioner, providing security advice and methodology for various projects, including air traffic management within the EEC. His previous career includes time in Industry, developing cryptographic products, and Government, managing the computer security research program of the UK National Authority for Information Security.