

# War and Peace: A Practical Study of Wi-Fi Related Issues

Stuart Cunningham and Vic Grout

**Abstract** — The facility of having wireless access to networks and the Internet has grown significantly in recent years. The advent of Wi-Fi and Wireless Access Points (APs) allows huge degrees of flexibility and easy access to information and resources. To this effect, it is now common to find multiple access points in public areas, in the home, and in the working environment. The security of APs is now an issue of paramount importance. However, as the technology has spread throughout such a diverse market of users, the security aspects have not been so quickly adopted. This has led to numbers of unsecured private and corporate APs being left open to abuse and given scope for *war driving*. In this work we investigate and establish the uptake of wireless networking facilities in a common urban area and establish to what extent security vulnerabilities are indicated within these varied constituent environments. As a counter to the general malicious perception implied by the term *war driving*, we propose the title of *peace driving* for such surveys intended, not to exploit but to increase awareness and provide information for academic research.

The results from our study show significant uptake of wireless networking in both the residential and business areas surveyed. The number of access points present in some residential areas is large, and given the relatively small distances between access points there is undoubtedly traffic which is crossing private boundaries. We show that a large proportion of access points, particularly in residential and suburban areas, have little or no security, and are at high risk of being exploited. As additional advice, we briefly outline simple security measures which are easily employed to attempt to address this critical issue.

**Index Terms** —

Security, wireless networks, wireless access point distribution.

---

**1 INTRODUCTION**

Wireless networking is becoming an increasingly popular and frequently used method of connecting to internal networks and also the Internet. This is true across industry, academia, and in home networks. More and more users are choosing portable and laptop computers as their preferred method of 'getting connected' and wireless network access has already become commonplace [1, 2]. ISPs are increasingly including wireless routers and adapters with their home and business broadband, DSL and cable network services, which has doubtless helped to increase the uptake in wireless networking with home users in particular.

Whilst there has been extensive work carried out into the study of user behaviour,

roaming, and service utilisation in wireless networks across large geographic areas [1, 3, 4], fewer results are available for determining the proliferation and uptake of wireless capability and consideration given to the security of those people who deploy wireless technology in their homes and businesses. In this work we determine the uptake of wireless networking within a limited geographic area, ascertain to what extent security mechanisms have been implemented, and attempt to derive correlations between the density and grouping of APs and the area within which they are situated.

In the next section, we briefly describe the scenario of our case study and the methods used for data collection. We then present and analyse the results in section 3. In section 4, we highlight and discuss issues and present succinct recommendations for mechanisms to improve security at the point-of-delivery in wireless networks. Finally, in section 5, we conclude and discuss issues and challenges raised for consideration in future work.

- 
- *Stuart Cunningham is a Lecturer in Computing and member of the Centre for Applied Internet Research (CAIR), University of Wales, NEWI, Plas Coch Campus, Mold Road, Wrexham, LL11 2AW, North Wales, UK E-mail: s.cunningham@newi.ac.uk*
  - *Vic Grout is a Reader in Computer Science and Director of the Centre for Applied Internet Research (CAIR), University of Wales, NEWI, Plas Coch Campus, Mold Road, Wrexham, LL11 2AW, North Wales, UK E-mail: v.grout@newi.ac.uk*

## 2 A REAL-WORLD CASE STUDY

In order to establish to what extent wireless networks have been adopted in the community, we undertook a study of a small town area, incorporating commercial and residential zones. Our primary method of investigation was constituted by following the road network over this zone and detecting the presence of APs. The size of the investigated field was approximately 16km<sup>2</sup>, although as is to be expected, it was not possible to totally cover absolutely every part of the area given the nature and scope of this study. Instead, we attempted to replicate conditions and equipment which would be available to an everyday user. This point in particular is given in a scenario known as the “parking lot attack”, which defines how an AP can be used to gain access to internal and external networks, and the ease with which this can be executed with even the simplest of equipment. This is illustrated in Figure 1.

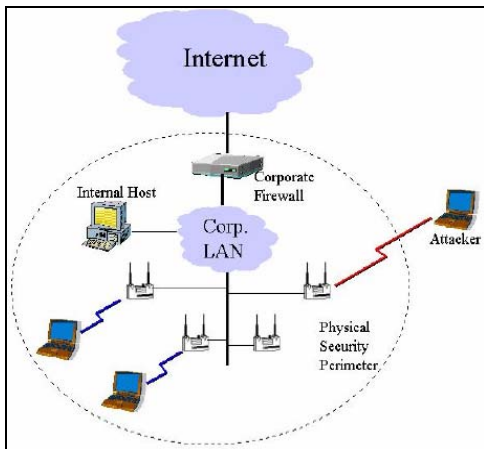


Fig. 1 The Parking Lot Attack [6]

To this end, we followed the road network across the area and employed a Toshiba laptop computer with an integrated wireless adapter and a Global Positioning System (GPS) to ensure that we were able to make an accurate mapping of the APs, and most crucially, the relative density of APs within this limited area. This allows for the detection of available wireless networks, both secure and insecure (and the ability to discriminate between them), and an associated GPS location for the point where the AP was discovered. The *NetStumbler* software package was used for the detection of APs. Though it could be argued that more sophisticated technology would provide greater detail and granularity in this exercise, it is important to remember that normal users,

and potential intruders, would not normally employ such equipment.

Our study was undertaken over a time period of approximately 10 hours of actively covering the geographic area, which was split across two weekdays in April 2007. To maintain consistency of results, all surveying was carried out within locally defined ‘office hours’, i.e. between 9.30am – midday and 1.30pm to 5pm. The area surveyed has a population of approximately 60,000.

## 3 DISCUSSION OF RESULTS

Initially, we are concerned with investigating the density and distribution of the access points across the area concerned. Perhaps of most interest, given the scope of this work, is the adoption of basic security or restricted access to these wireless networks (or lack thereof). It is also intriguing to establish exactly how many APs are detected in this area, which provides an indication of the uptake of wireless technology within the surveyed community. It should be noted that, for the purposes of anonymity, the orientation, exact scale, and identifiable parameters will be removed from all information presented in this section. Where appropriate, we indicate broad areas and classifications from actual knowledge of the area surveyed and data retrieved, but we feel it is not appropriate to detail particulars.

To this end, Figure 2 shows the mapping of access points across the 16km<sup>2</sup> area, in a representative Cartesian space, and indicates whether each AP is detected as being secure or insecure. Table 1 provides a summary of the information gathered.

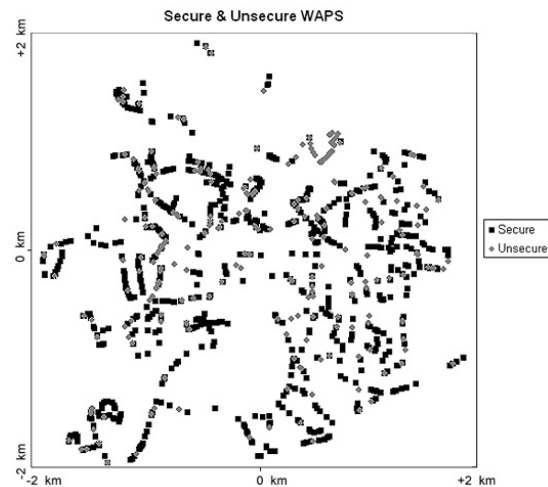


Fig. 2 Mapping of Access Points and Security Covering 16km<sup>2</sup> Geographic Area

TABLE 1  
AP Survey Details

<b>Security</b>	
Secure APs	891 (77%)
Unsecure APs	262 (23%)
<b>Data Rates</b>	
54 Mbps	1027 (89%)
11 Mbps	126 (11%)
<b>Total APs</b>	1153

As Figure 2 shows, there is a fairly similar spread of both secure and unsecure APs over the area which was surveyed. It is also clear that some areas have much denser concentrations of access points than others, and this is discussed in more depth later in this section. Whilst the percentage of secure APs is considerably higher, there is still almost a quarter of all access points which are not secure, which, when we consider the actual number of access points this refers to, is a point of concern. However, upon reflection against a notional study undertaken in 2002 [5], which revealed that approximately two thirds of networks were unsecure, the number of unsecure access points has decreased. As expected, the majority of networks employ the IEEE 802.11g standard (54 Mbps), and much fewer use the IEE 802.11b standard (11 Mbps).

We know, from observations of the areas surveyed, that the area incorporates residential/suburban areas as well as smaller amounts of commercial and industrial regions. Although there is an inherent interwoven nature across a real geographic area between the residential and commercial areas, it is interesting to see if the results of our mapping exercise reflect the designation of these areas, particularly through the density and clustering of the access points which have been detected. This can be achieved by plotting the location of the APs on a map of the area, which reveals that the majority of access points reside in the areas which are mainly residential. This is only to be expected, given the much larger number of individuals who would be present in these locations. Somewhat surprisingly however, is the number of access points within the commercial regions which do not appear to have adopted a security mechanism on their network access point. In one of the larger residential areas there is sparse distribution of secure access points, whilst in some others, there are higher concentrations. It is speculated that this might be due to a stronger sense of community in these areas, which could be classed as being areas of higher-value within the community.

However, to approach this from a statistical analysis perspective, and to strengthen the

assumptions made from visual analysis of the AP locations on a map of the area, we need a more formal statistical analysis. Unfortunately, looking for multi-dimensional correlations in such, somewhat indeterminate, data is a difficult process. There are generally two heuristic approaches in these circumstances. We can either take the data and look for trends that come to fit known zones within the overall area or start with a knowledge of defined zones, then look to find patterns in the nature of the APs within them. The latter approach is discussed at the end of this section. To achieve the former, we employ a simple  $k$ -means analysis across our detected points [7].

$$J = \sum_{i=1}^k \sum_{x_j \in S_i} |x_j - \mu_i|^2 \quad (1)$$

We present the results of two iterations of the standard  $k$ -means algorithm on our dataset with values of  $k=3$  and  $k=4$ . The results are presented in Figure 3 and Table 2, and Figure 4 and Table 3 where each point's cluster membership is represented by a different symbol on the graph.

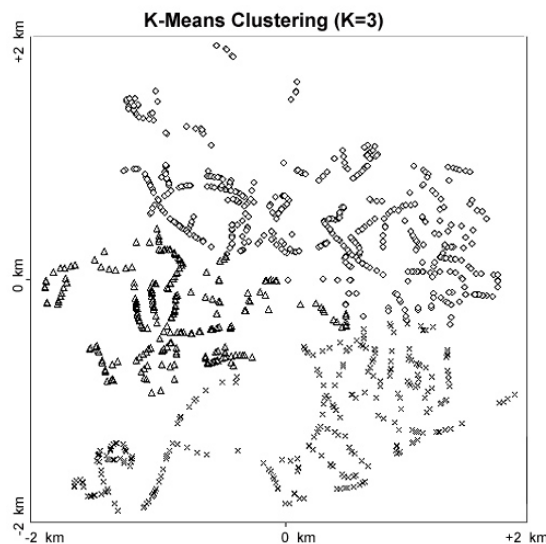


Fig. 3  $k$ -Means Clustering of APs ( $k=3$ )

TABLE 2  
Overview of Cluster Membership ( $k=3$ )

Cluster	Number of APs
x (Cross)	308 (26.71%)
o (Circle)	561 (48.66%)
Δ (Triangle)	284 (24.63%)

The execution of the  $k$ -means algorithm helps to reveal specific areas of concentration within the mapping of access points. In this iteration, where we determine

three clusters of points, the algorithm helps to highlight the main concentrations of APs, mainly as a result of the high concentration of residential areas. However, we know from knowledge of the location that the three categories do not accurately represent the distinct residential and commercial/industrial areas. There is definite cross-inclusion of these to different types of access point usage. In particular, the cluster with the largest population (circles) includes significant membership from two distinct residential areas, as well as several small commercial and industrial sites. However, the other two clusters perform a reasonable approximation of two separate communities of users. To this extent, further separation is required, and we apply the *k*-means algorithm again, this time splitting the data into four clusters.

intermingled slightly with the cluster indicated by the squares and slightly with the cluster indicated by the circles. However, given the much lower number of APs detected in these areas, it is natural to expect this, and this also accounts for this cluster having the highest membership. This aside, the remaining categories (triangles and crosses) identify almost exclusively residential areas and those which are considered locally to be distinct. This is also helped due to the lack of any detected access points in the often open or more rural areas which are inclined to separate residential areas in particular. It is worth noting the significant difference between the number of APs present in the triangle cluster, cross cluster and the circle cluster; this may be indicative of socio-economic similarity and differences between these areas.

We did perform iterations of the *k*-means algorithm with 5 and more cluster areas, but found that the results started to become less and less representative of the natural distinctions present within the local area, and that communities and areas perceived as being cohesive would be separated by the algorithm at this stage.

To approach the problem from the other direction, requires a formal definition of zones within the overall area. This can be difficult but not impossible. We require a knowledge of *m* zones,  $Z_1, Z_2, \dots, Z_m$ , in the sense of being able to recognise when an access point, *a*, is geographically within a given zone, *Z*, that is, in set terms,  $a \in Z$ . Denote, by  $A_j$ , the set,  $\{a : a \in Z_j\}$ , of access points in zone  $Z_j$ . For any set of access points, *A*, denote the set of secure points by  $S(A)$  and the set of unsecure points by  $U(A)$ . We can then calculate the security index,  $SI_j$ , for zone  $Z_j$  as

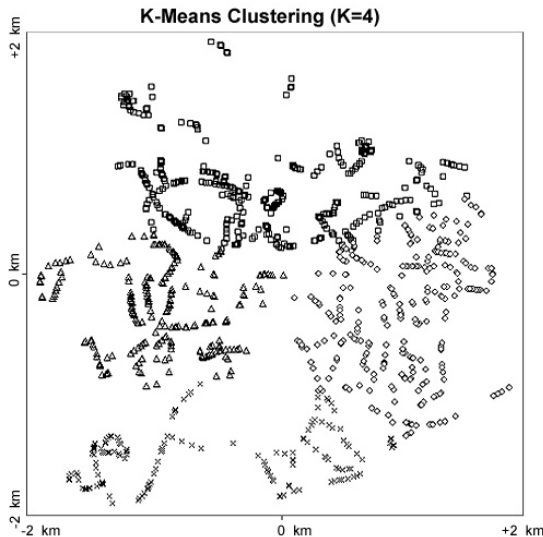


Fig. 4 *k*-Means Clustering of APs (*k*=4)

TABLE 3  
Overview of Cluster Membership (*k*=4)

Cluster	Number of APs
□ ( <i>Square</i> )	418 (36.25%)
○ ( <i>Circle</i> )	288 (24.98%)
△ ( <i>Triangle</i> )	268 (23.24%)
x ( <i>Cross</i> )	179 (15.52%)

In employing 4 cluster regions, the *k*-means algorithm displays promising results in considering the density and concentration of access points in respect to the areas they cover. The new graph now successfully highlights four broadly distinct areas within the community surveyed. Still, the commercial and industrial areas are

$$SI_j = \frac{S(A_j)}{S(A_j) + U(A_j)} \quad (2)$$

We then require a scoring, or ordering, of each zone. These may be based upon independent features such as property value, level of industrial activity, etc. or upon features of the access points themselves within each zone such as density, type, etc. Each such scoring or ordering will give a *value*,  $V_j$  or *rank*,  $R_j$ , for each zone,  $Z_j$ . Calculating coefficients of correlation or rank correlation across zones will show different levels of dependence between features.

This aspect of this investigation is ongoing

and final figures are not available at the time of going to press.

#### 4 SECURITY CONFIGURATION

Given the rather unique nature and 'openness' of this type of network access, it would be reasonable to expect that potential threats to a network would probably take the form of either those who wanted to 'piggyback' onto the network to gain no-cost access to the Internet and those who have more malicious intent. Whatever the intention or threat, there is a clear need for robust security, as the repercussions could range from reduced bandwidth to total system failure and even information loss.

It is important to stress the importance of physical security measures which can be used to reduce unwanted access to APs. This is particularly pertinent to industry and commercial use, where, unlike home or leisure users, wireless access may only be required within the confines of a building or enclosed private area. The installation of wireless capabilities in these scenarios is more likely to be to allow roaming and cable-free access inside the building. The simplest solution in preventing unwanted access to a wireless network is to prevent the network from being detected beyond the confines of a designated space. This can be addressed through physical measures, such as careful antenna positioning, consideration of the antenna type (and importantly the footprint of the antennae), and considering dampening or blocking the signal at the extremities where practical. For example, Figures 6 and 7 compare the footprints / radiation patterns of an omni-directional and directional Wi-Fi antenna.



Fig. 6 Omni-Directional Antenna Footprint [8]

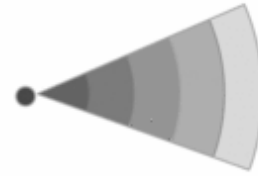


Fig. 7 Directional Antenna Footprint [9]

These types of measures and considerations are still pertinent when implementing home or leisure networks, for example although network access may be required in a user's own garden, they do not necessarily want to network to 'leak' outside of those bounds if possible. However, this is a contentious method of deploying a wireless service and its merits often argued. This is mainly because an attacker can find ways around such measures, by using larger antennae or signal boosters, for example. In this case software-based and encryption solutions become necessary.

In any case, wireless networks are primarily designed and implemented to permit degrees of freedom with computer communications, which are not normally available under the constraints of wired networking. Where networks have been installed deliberately to allow users access beyond physical bounds and in open spaces, limiting the actual signal, or availability of the AP, will not always be a suitable first-line security measure. In these scenarios, and we assume these to be far more common than the commercial scenario described previously, software-based security needs to be employed. Of note is the work carried out by Arbaugh and Shankar in 2001, which highlighted many of the problems and security vulnerabilities present in wireless networks and deficiencies of the WEP (Wired Equivalent Privacy) protocol [6] and the other security features and protocols available in 802.11 networks. There are alternatives, of course, the obvious one being use of Wi-Fi Protected Access (WPA) in preference to WEP. There are also more advanced techniques such as Smart Cards, USB and Software Tokens. Neither should simple techniques, such as hiding the SSID or applying Access Control Lists (ACLs) based on IP or MAC address, be overlooked. Whilst, none offer much security in isolation (most can be spoofed), they can all make a contribution to a secure overall combination.

It is expected that through revisions to the IEEE wireless standards, stronger encryption techniques, and sensible precautions, a reasonable and appropriate level of security can be attained for most scenarios [5, 6].

## 5 CONCLUSIONS & FUTURE WORK

Our study provides a useful insight into the uptake of wireless networks across a representative area. It shows that wireless networks have been implemented across a range of social, residential, commercial, and industrial locations, with little bias being found regardless of social or financial status in these areas. The uptake of, at least, basic security mechanisms in wireless networking has been shown to be effected within a high majority of the APs we encountered. The use of clustering techniques on the retrieved data is of particular interest in this, and for future, work. The distribution of access points does help to indicate where communities exist, and comes close to approximating the bounds of different categories of community. Further refinement and investigation of other clustering and pattern recognition algorithms for these purposes, including further development of the analysis that concludes section 3, may well yield further interesting results and be useful in other application scenarios.

Although the results of our study are localised to the particular area investigated, we believe that this is indicative and a representative of the adoption and awareness of wireless technologies in other communities in the UK. The results of this study provide insight and highlight issues related to the community and their implementation of wireless networking technology.

Clearly, there are limitations in using the road network when surveying available access points. However, given the size of the area and time time-scale of the project, it would have been impractical to cover the area in any other way with the existing resources. This is something which could be improved upon in future studies, however, a valid argument stands that where there are no roads, there are most likely no access points. The other limitation of using the road network is that the GPS mappings do not provide a precise level of detail, and consequently mappings appear regimented. However, this is still valuable and indicative of the available APs. A final interesting point of note was the sideline of determining the

quickest path, with lowest cost, whilst covering the required area on the roads. In short, we refer to a variant of the *Route Inspection Problem* (originally known as the *Chinese Postman Problem*) during the undertaking of the study. However, this is a well-documented problem and pursuit of this in further study, whilst relevant from a practical perspective (the problem is *NP-Complete* after all), is beyond the current scope.

Currently, our network detection software is only able to distinguish secure networks as those which employ WEP to secure the network. Therefore, one limitation in the current set of results is that, without attempting to actually authenticate or use an access point, we are currently unable to distinguish access points which appear unsecure but may use a server-based method of authentication, such as that of BlueSocket for enterprise-wide systems and personal and small user systems for home users, for example. The use of such authentication mechanisms is popular with public access pay-as-you-go hot spots to be found in public or communal areas, and within leisure providers, such as hotels. Further investigation is required in this area to determine if it is possible to ascertain greater detail of the security mechanisms in place, without having to manually attempt to access the network behind each access point. However, the legality of this last proposal must be considered.

Other future work which may result from this dataset is to investigate the variance in signal strength and signal-to-noise ratio (SNR), and thus reliability of connection, of the APs surveyed. This would allow a more detailed investigation in relation to the security and ease of access to these networks. This investigation would help to reveal what importance the effectiveness of access point placement and the effects of interference in the environment have on the ability to detect and retain a signal between a client and a AP. Additionally, when further time is available, another interesting exercise will be to determine the popularity of equipment which is being used in these wireless network installations. This can be easily ascertained from analysing the first three bytes in the MAC address of the access points revealed in the survey. It would also be an interesting follow-up study to undertake another survey in the evening or during the night, to see if the time of day affects the number of networks available, and what discrepancies may occur in the security of

those access points. Finally, it would be useful to carry out the same survey again after a period of time (we believe a year to be suitable), mainly to investigate the growth or decline in the number of access points within the area and the increase or decrease in the security of the available access points.

the British Computer Society (BCS) and the Institution of Engineering & Technology (IET). He chairs the biennial international conference series on Internet Technologies and Applications (ITA).

## REFERENCES

- [1] D. Kotz, K. Essien: "Analysis of a Campus-wide Wireless Network", *Wireless Networks*, Vol. 11, pp. 115-133, Springer, Netherlands, 2005.
- [2] R. Boggs, P. Arabasz: "The move to wireless networking in higher education", *Research Bulletin of the EDUCAUSE Center for Applied Research*, April, 2002.
- [3] D. Tang, M. Baker: "Analysis of a Metropolitan-Area Wireless Network", *Wireless Networks*, Vol. 8, pp. 107-120, Springer, Netherlands, 2002.
- [4] D. Tang, M. Baker: "Analysis of a Local-Area Wireless Network", *Proceedings of the 6th annual international conference on Mobile Computing and Networking*, Boston, Massachusetts, USA, 2000.
- [5] M. Ward: "Hacking with a Pringles tube", *BBC News – Science & Technology*, British Broadcasting Corporation, 2002. Available at: <http://news.bbc.co.uk/1/sci/tech/1860241.stm> [Accessed 10/9/2007]
- [6] W.A. Arbaugh, N. Shankar, Y.C.J. Wan: "Your 802.11 Wireless Network has No Clothes", *IEEE Wireless Communications*, Vol.9, pp. 44-51, 2002.
- [7] C.M. Bishop: "Pattern Recognition and Machine Learning", Springer-Verlag, New York, 2006.
- [8] Allendale Electronics Ltd, "Omni-Directional Antennas", Hertfordshire, UK, 2007. Available at: [http://www.wifi-antennas.co.uk/products/category/omni\\_directional\\_antennas/](http://www.wifi-antennas.co.uk/products/category/omni_directional_antennas/) [Accessed 10/9/2007]
- [9] Allendale Electronics Ltd, "Directional Antennas", Hertfordshire, UK, 2007. Available at: [http://www.wifi-antennas.co.uk/products/category/directional\\_antennas/](http://www.wifi-antennas.co.uk/products/category/directional_antennas/) [Accessed 10/9/2007]

**Stuart Cunningham** was awarded the BSc degree in Computer Networks in 2001, and in 2003 was awarded the MSc Multimedia Communications degree with Distinction, both from the University of Paisley (UK). He is a Member of the British Computer Society and the Institution of Engineering & Technology. Stuart is also a member of the MPEG Music Notation Standards working group.

Stuart is currently a Lecturer in Computing and a PhD student at the University of Wales, studying under the supervision of Dr. Vic Grout.

**Vic Grout** was awarded the BSc(Hons) degree in Mathematics and Computing from the University of Exeter (UK) in 1984 and the PhD degree in Communication Engineering from Plymouth Polytechnic (UK) in 1988.

He has worked in senior positions in both academia and industry for twenty years and has published and presented over 100 research papers. He is currently a Reader in Computer Science at the University of Wales NEWI, Wrexham in the UK, where he leads the Centre for Applied Internet Research (CAIR). His research interests and those of his research students span several areas of computational mathematics, particularly the application of heuristic principles to large-scale problems in network design and management.

Dr. Grout is a Chartered Engineer, Chartered Scientist and Chartered Mathematician, a member of the IMA and ACM, senior member of the IEEE, and Fellow of