Glyndŵr University
Glyndŵr University Research Online

Computing   Computer Science

11-1-2008

Peace Driving: Case Studies of Wi-Fi Usage

Stuart Cunningham
Glyndwr University, s.cunningham@glyndwr.ac.uk

Vic Grout
Glyndwr University, v.grout@glyndwr.ac.uk

Follow this and additional works at: http://epubs.glyndwr.ac.uk/cair

Part of the Computer and Systems Architecture Commons, Digital Communications and Networking Commons, Hardware Systems Commons, and the Systems and Communications Commons

Recommended Citation

Peace Driving: Case Studies of Wi-Fi Usage

Abstract

Wireless networking technologies, under the umbrella of the IEEE 802.11 suite of standards and commonly referred to as Wi-Fi, is now commonplace technology in both the home and office. In this work, we present the results of studies into wireless networking uptake and security within two town communities in the UK. Our work concentrates on the geographical positioning of wireless access points (APs) and the security measures used to protect these liberating technologies from unwanted misuse, often referred to as war driving, we employ the title peace driving, for wireless networking surveying which aims to address security issues in wi-fi networks. 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. These findings are corroborated across both the communities which were studied. We suggest that similar sized and constituent communities are representative of others in the UK and find similar trends between the two studied as part of this work.

Keywords

Wireless, wi-fi, networking, security, war driving, peace driving

Disciplines

Computer and Systems Architecture | Digital Communications and Networking | Hardware Systems | Systems and Communications

Peace Driving: Case Studies of Wi-Fi Usage

Stuart Cunningham and Vic Grout

Centre for Applied Internet Research (CAIR), Glyndŵr University, Wrexham
{s.cunningham | v.grout}@glyndwr.ac.uk

Abstract

Wireless networking technologies, under the umbrella of the IEEE 802.11 suite of standards and commonly referred to as Wi-Fi, is now commonplace technology in both the home and office. In this work, we present the results of studies into wireless networking uptake and security within two town communities in the UK. Our work concentrates on the geographical positioning of wireless access points (APs) and the security measures used to protect these liberating technologies from unwanted misuse, often referred to as war driving, we employ the title peace driving, for wireless networking surveying which aims to address security issues in wi-fi networks.

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. These findings are corroborated across both the communities which were studied. We suggest that similar sized and constituent communities are representative of others in the UK and find similar trends between the two studied as part of this work.

Keywords

Wireless, wi-fi, networking, security, war driving, peace driving

1. Introduction

Wireless networking is now commonly employed in a range of applications and scenarios, ranging from industry, business, education, and home and personal use. The freedom of mobility and widening network access across a limited physical area is highly attractive when providing an easy-access network infrastructure.

There has been extensive work carried out into the study of user behaviour, roaming, and service utilisation in wireless networks across large geographic areas (Arbaugh & Shankar 2002, Kotz & Essien 2005, Tang & Baker 2000, Tang & Baker 2002) 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.

2. Peace Driving

In these investigations we focussed on two distinct community areas. In order to realistically and practically assess the accessibility of APs within these communities we did not opt to employ any special equipment in our studies (aside from the inclusion of a Global Positioning System (GPS) which is not directly involved in the detection of APs). Our main intention in employing non-specialist equipment was to emulate the kind of equipment and conditions which could be easily acquired; to simulate closely the materials and environment of the casual war driver. To this end we did not use any external, extended range antennae or amplifiers to boost the signal in any way. We also made the assumption that only the most determined of war drivers would probably remain within the confines of a vehicle as this provides an element of urban camouflage, power for equipment and shelter.

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. In all of our studies we followed the road network in each area over several days during the hours of 09:30 to 12:00 and 13:30 to 17:00.

The first investigation took place across a $16km^2$ area which, from our own prior observations, we knew to contain residential, commercial and industrial zones. The total population within the area surveyed is approximately 60,000. 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.

The geographical mapping of the results of the first study is presented in Figure 1 which indicates APs that are secure (by using WEP encryption) and those deemed insecure (not using WEP). In this first study, undertaken in 2007, a total of 1153 APs were discovered across the geographical area of which 77% employed WEP security and the remaining 23% did not use WEP.
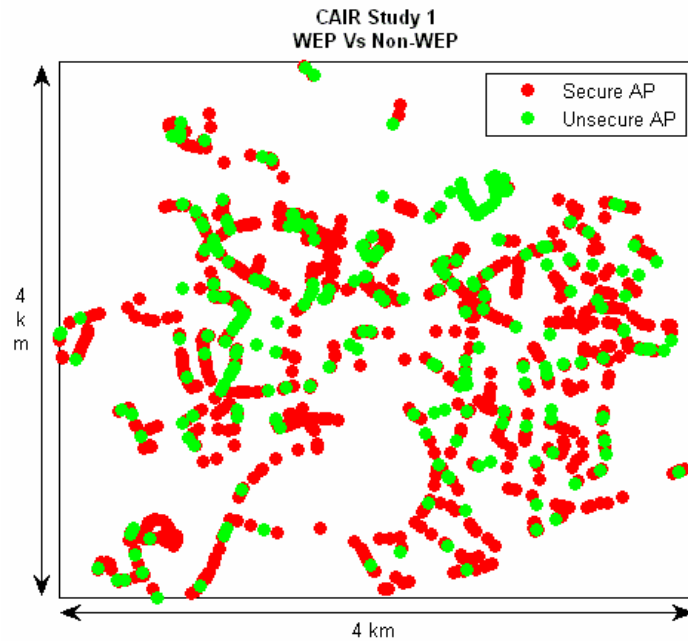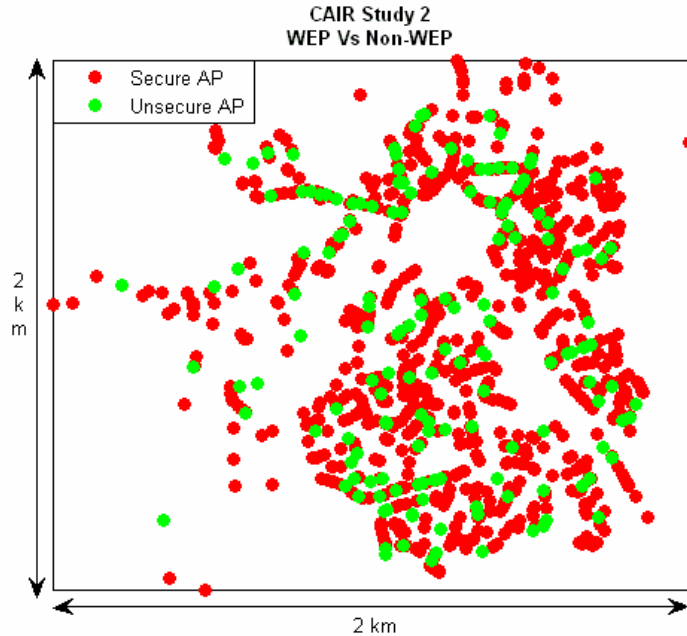
Figure 1: AP Mapping from 1st Study

As Figure 1 shows, there is a fairly similar spread of both secure and insecure 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 (Ward 2002), which revealed that approximately two thirds of networks were insecure, the number of insecure 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). It is known, from observations of the areas surveyed, that the area incorporates residential/suburban areas as well as smaller amounts of commercial and industrial regions (Cunningham & Grout 2007).

The second study was undertaken some time after the first in order to strengthen the findings of the original study and to draw comparisons with the results of the first investigation. Figure 2 shows the mapping of the results from the second study. Though only eight months separated the two studies, and a different region would be surveyed, it is interesting to look at the number of APs encountered and how many of these are considered to be secure. The second investigation was carried out over a similar area constituted of the same type of zones. The main difference in this second survey was that the area was approximately 4km^2. The population of the area in this second investigation is approximately 15,600. This second investigation was carried out on two separate days, the first in December 2007 and the second in January 2008.

The mapping results from the first study provide interesting contrast to that of the second study. If we initially consider the distribution of APs across each square area, the first study shows APs which are sparser and more evenly spread that those in the second study. We must remember the differences in size and approximate population between the two areas, however, this is also an interesting point to note when we take into account the fairly similar number of APs despite the size of the second study being smaller. Of course, the mappings do have an underlying structure to them, which is most clearly seen in because of the road network followed to allow discovery of APs.

Figure 2: AP Mapping from 2nd Study

It is of particular interest to note that the majority of APs are encountered within residential zones. This was supported by noting the occurrence of default SSID (Service Set Identifier) names on many of the access points. In the second study, many more APs were encountered with the default names associated with Internet Service Providers and equipment manufacturers. For example, SSIDs such as "BTHomeHub", "BT Fusion", "NETGEAR", "BTVoyager", "DLINK_WIRELESS", "linksys", and "Wanadoo" frequently appeared. In the second study especially there was a marked increase in other providers which had recently launched broadband Internet services such as "LiveBox", "SpeedTouch", "TalkTalk", and "Sky".

To directly compare the summary of results between the two studies, Table 1 examines the two studies undertaken.

Table 1: Summary of Both AP Studies

Study	Area	# APs	Average # APs / km^2	# Non-WEP APs	# WEP APs
Study 1	16 km^2	1153	72.06	262 (23%)	891 (77%)
Study 2	4 km^2	1113	278.25	159 (14%)	954 (86%)

Given the size differences in the areas covered we can assume that on average, there has been growth in the uptake of wireless networking within the community. The number of users aware of the need for security, even if that might only be by using WEP, has also increased, although this is not entirely conclusive for reasons mentioned elsewhere in this paper. However, in the areas covered during the second study it was noted that there was a much larger amount of residential and suburban zones encountered, along with smaller commercial and industrial areas, than in the first study. The zones also differed in terms of the surroundings which were not covered as part of the study (to incorporate these outlying zones in the original study would have considerably increased the size and time required to methodically the additional areas). Beyond the square area in the first study there remained some other residential and industrial areas whereas in the second study almost all of the entire community was concentrated within the square area, which has the effect of making the results of this study somewhat more reliable and representative of the community under investigation rather than purely the sampled area.

3. Community Survey

To gain further insight into the awareness of security issues and actual usage of wireless technologies on a more specific level we undertook a small survey involving a sample of participants who were mainly based within the geographical area investigated as part of the first study. The main aims were to determine more information about the usage of wireless networks and the type of security configuration which might be in place. At the time of going to press there were a total number of 22 participants involved in the survey, which begins to represent a reasonable sample of the population covered by the peace driving network surveys. The results from this survey are presented in Table 2, Figure 3 and Figure 4.

Table 2: Survey Details

Wi-Fi Internet Usage		
Personal (68.2%)	Mix of Personal & Work (31.8%)	
Have you Changed the SSID?		
Yes (68.2%)	No (22.7%)	Don't Know (9.1%)

Figure 3 depicts the number of users who make use of a given access point and it is clearly shown that APs are most commonly used by a small number of individuals (31.8%), most commonly an individual or pair (36.4%) of users, with the maximum number of people using APs being six (4.5%). Given the coverage gained by employing wireless networks, it could be assumed that wi-fi is more commonly put

in place to provide ease of access from various locations around the home, rather than because it is easier to network a number of computer systems together.
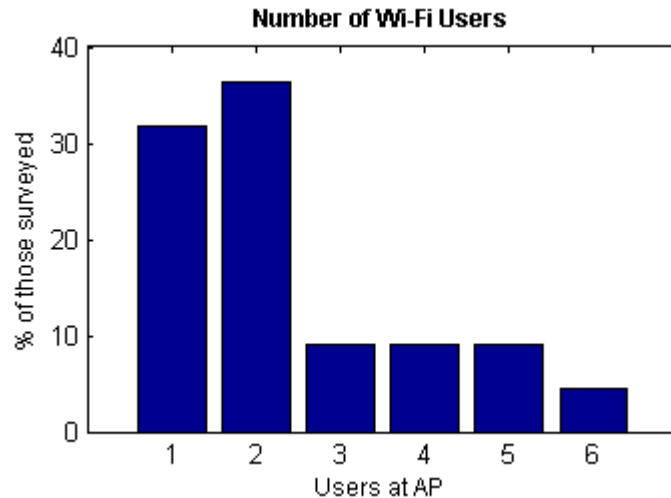

Figure 3: Users per AP

Figure 4 illustrates the security measures which those users who indicated that they had employed some kind of security (77.3% of the sampled population, according to the survey) use. In this question, participants were allowed to choose multiple answers, since more effective protection of APs is commonly achieved by employing a combination of security techniques, such as filtering and encryption, for example. The options permitted were WEP encryption, WPA encryption, MAC address filtering, IP address filtering, hiding the SSID, and changing the default router password. An 'other (please specify)' option was also provided, though none of the participants used it). As Figure 4 shows, the largest amounts of uptake are towards WPA encryption and changing the default password used to configure the router.

4. Future Work

A major addition required in future studies is to employ software which is able to provide more detailed information regarding the security mechanisms in place at APs. Clear determination of the type of security being used will provide much more accurate results with a greater granularity. However, this also presents some issues regarding the amount of penetration which is considered acceptable when undertaking wireless surveying. Whilst encryption technologies are generally visible upon viewing the wireless networks available, testing to see of mechanisms such as MAC address filtering require attempts to be made to connect to the AP.

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. Even in studies where the road network is used, the researcher is presented with the challenge of navigating the best path through the area in order to minimise overlap and repetition, in other words the *route inspection* or *chinese postman problem*. This challenge goes beyond the aims of this work, although its investigation would be especially beneficial in scenarios where large geographic areas are to be studied.
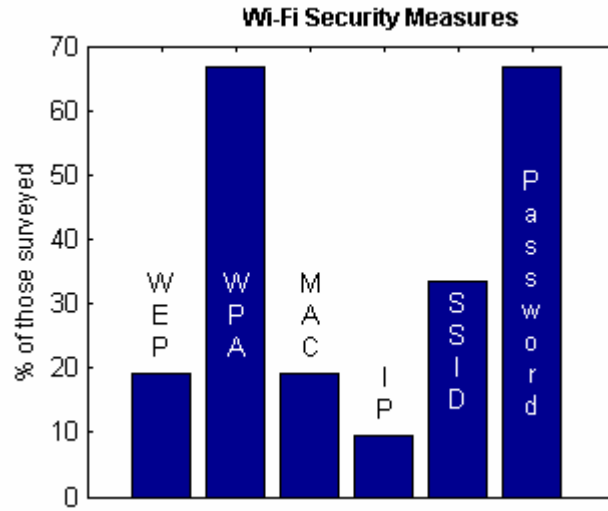
Figure 4: Security Measures Employed

To approach the problem from the direction of attempting to match distinct geographic or communal areas in the mapping with security aspects 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, ..., 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 insecure points by $U(A)$. We can then calculate the security index, SI_j, for zone Z_j as

$$ SI_j = \frac{S(A_j)}{S(A_j) + U(A_j)}. \quad (1) $$

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 the investigation is ongoing.

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 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.

5. References

Arbaugh, W.A., N. Shankar, N. (2002), Y.C.J. Wan: "Your 802.11 Wireless Network has No Clothes", *IEEE Wireless Communications*, Vol.9 , pp. 44-51.

Cunningham, S & Grout, V. (2007), *War & Peace: A Practical Study of Wi-Fi Related Issues*, Proceedings of the International Conference on E-Activity and Leading Technologies (E-ALT 07), Porto, Portugal, December 2007, pp. 393-399.

Kotz, D., Essien, K. (2005), Analysis of a Campus-wide Wireless Network, *Wireless Networks*, Vol. 11, pp. 115-133, Springer, Netherlands.

Tang, D., Baker, M. (2000), *Analysis of a Local-Area Wireless Network*, Proceedings of the 6th annual international conference on Mobile Computing and Networking, Boston, Massachusetts, USA.

Tang, D., Baker, M. (2002), Analysis of a Metropolitan-Area Wireless Network, *Wireless Networks*, Vol. 8, pp. 107-120, Springer, Netherlands, 2002.

Ward, M. (2002), *Hacking with a Pringles tube*, BBC News – Science & Technology, British Broadcasting Corporation. Available at: http://news.bbc.co.uk/1/sci/tech/1860241.stm [Accessed 25/7/2008]