December 2004

Accidental Wireless Networks: An Initial Study

Sameer Verma
San Francisco State University

Paul Beckman
San Francisco State University

Accidental Wireless Networks: An Initial Study

Sameer Verma
San Francisco State University
sverma@sfsu.edu

Paul Beckman
San Francisco State University
pbeckman@sfsu.edu

ABSTRACT

This research project attempts to prove that there are community wireless networks in existence that are formed accidentally as a result of consumer macro-behavior. Specifically, certain combinations of brand and technology implementations can result in extensive and overlapping wireless networks that allow users to roam seamlessly in residential neighborhoods.

We examined the distribution of wireless nodes across three such residential neighborhoods. Our hypothesis is that a majority of these wireless access points (APs) run on a small number of commercial brand devices using default settings and no encryption. Given a certain density, such nodes can overlap and provide, in effect, a seamless community wireless network, purely by the accidental behavior of individuals. The macro-behavior of consumers gravitating toward inexpensive and popular brand devices allows such networks to come about. Data analysis shows interesting patterns of node distribution by Wi-Fi channel, commercial brand, and configuration, including encryption settings. It is not the intention of this paper to establish any recommendations about the future direction of such accidental networks, or to speculate on the security issues related to wireless networks.

Keywords

Wi-Fi, Ubiquitous Computing, Consumer Macro-Behavior

INTRODUCTION

The research project described in this paper investigates factors that enable the creation of multi-node neighborhood area wireless networks that may arise by the accidental or incidental actions of completely uncoordinated groups of individuals. These "accidental wireless networks" (AWNs) are built using standard consumer products that let end-users implement home high-speed wireless computer networks. In such AWNs, each individual, by their independent choice, installs a Wi-Fi access point (AP) for their own personal use. The most common general purpose of each of these APs is to let the owner of that AP wirelessly connect to the Internet[1].

However, due to several factors involved in the purchase and installation of home APs, it is possible, and in some instances, quite likely, that the group of unrelated APs in a neighborhood may together form a continuous and generally seamless wireless network. These factors are:

1. There are a relatively small number of commercial providers of AP hardware who control most of the market share of residential AP hardware (Synergy, 2004).
2. Commercial providers of AP hardware do not vary the hardware or software configuration of individual APs that are sold to end-users (Stevenson, 2002).
3. Individuals installing APs in their homes are either unsophisticated in their knowledge of wireless computer networking or they are lazy (Vichr and Malhotra, 2003).

From the perspective of a casual passer-by, or "AWN exploiter", attempting to connect to the Internet via an AP in a residential neighborhood, the result of the combination of these three factors is that it may be possible to stay wirelessly and continuously connected to the Internet over a large geographic area with little or no work breaking into and staying connected to the wireless network.

[1] A much less common use is to wirelessly connect computers and peripherals in a home network without connecting that network to the Internet.

The result of the first factor is that end-user consumers who purchase commercial APs are likely to have a product similar to that of their neighbors. This means that an AWN exploiter attempting to connect to the Internet through a residential AP need not worry about hardware incompatibilities across many vendors, as there are relatively few. The result of the second factor is that the hardware and software configuration used by one residential AP is likely to be the same as the configuration used by other residential APs. The impact on the AWN exploiter is that they need not worry about changing their own network connection configurations as they change connections from one AP to the next. The result of the third factor is that, since almost all residential APs are sold by the manufacturer with security disabled (Verma and Beckman, 2002, Arbaugh, 2002); almost the entire wireless network is open to anyone who wishes to connect. The impact on the AWN exploiter is that they don't have to worry about hacking into the wireless neighborhood network – it is essentially wide open for their initial and continued use.

The Wi-Fi protocol

The Wi-Fi protocol was designed as a point-to-multipoint solution wherein the hardware owner would set up one AP to which many remote devices could simultaneously connect. Most commercially sold APs that are targeted at the residential user have an effective physical radio range of about 100 meters (Fleishman, 2001), which makes them very suitable for connecting computer devices within one residence. These types of APs are sold as COTS (commercial off-the-shelf) products that are available in all typical computer and consumer electronic products stores. A complete home setup, including the AP and 2 to 3 laptop or desktop wireless network cards will cost in the range of $100-200. The first commercially popular wireless networking protocol, called 802.11b, allows data transmission rates up to 11 megabits/second. Later generations of this protocol (802.11g) have increased the data transmission rate to about 54 megabits/second (Shoemake, 2003).

The typical home user installs this type of AP so that they can wirelessly connect several computers and peripherals such as printers to the wireless network and then to the Internet. Less commonly, a home user may install an AP purely with the intent of connecting their personal computer devices in a home network but without any connection to the Internet.

METHODOLOGY

Data collection

Since the goal of the research project was to determine the physical extent and characteristics of any accidental wireless networks, three representative residential neighborhoods in the northern San Francisco peninsula were selected for data collection. A fourth industrial area was also chosen for data collection as a comparison to the residential areas. To make AP density comparisons easier, each area was driven for a total of 4 street miles (as measured on the automobile odometer) at normal street speed limits of approximately 20 miles/hour.

Data was collected using a Fujitsu Lifebook P2120 laptop PC, a Lucent Orinoco 802.11b card, and a Delorme Earthmate global positioning system unit, all running in a 1993 Pontiac Sunbird convertible. Together, these three pieces of hardware, and Network Stumbler 3.30 software (Milner, 2003), were able to collect data about the manufacturer, Service Set Identifier (SSID), and general configuration of the APs that were within radio range of the vehicle as it was driven down the streets of several residential neighborhoods in the San Francisco area. Three different neighborhoods were used for data collection, although no attempt was made to analyze the collected data based on the characteristics of those neighborhoods.

The Network Stumbler software, using the signal input from the GPS unit, recorded every detectable AP's: MAC address (that uniquely identifies that AP's wireless card), SSID, name, broadcast channel, vendor name, infrastructure mode, encryption type (if any), signal strength, noise level, latitude, longitude, time of first AP detection, and time of last AP detection. These data items were stored in a Network Stumbler log file that was then converted for import in an Excel spreadsheet for data analysis.

Data analysis

After collecting 4 linear street miles of data from three residential areas and one industrial area, the four sets of records stored by the Network Stumbler software were transferred to spreadsheet files for easier data manipulation. Since the goal of the research project was to determine the existence and possible extent of AWNs, the collected data was analyzed along the dimensions that allow and support the appearance of AWNs. As mentioned above, these factors are: the brand of the AP manufacturer, the configuration of each individual AP, and the extent that the end-user changes the original configuration of their AP.

Each of these factors can be measured with the data that was collected. The first factor (the AP manufacturer) appears in the record of each AP. If there are a large number of APs that use the same manufacturer, an AWN is more likely to be operational, as AWN exploiters will have to worry less about hardware incompatibilities that often arise even within industry adopted standards. The second and third factors (the extent of variance of AP configuration when sold/distributed by the manufacturer and the extent that end-users deliberately change their AP configuration) are shown in each AP record as a set of values that comprise that AP's configuration. With regard to the viability of an AWN the relevant elements of the configuration of an AP are the manufacturer, the SSID (default vs. non-default), the broadcast channel, and the encryption used (if any). Each of these values appears in the stored data record for each AP. The data collected was therefore sufficient to enable at least a preliminary evaluation into the existence and extent of any AWNs.

AGGREGATE DATA PROFILE

Raw data files

The contents of the data files show the following results for the factors that influence the existence and extent of an AWN:

Manufacturer	# of APs	% of APs
D-Link	22	6.6
Linksys	85	25.6
NetGear	50	15.1
Other	175	52.7
Total	332	100%

Table 1. AP by Manufacturer

SSID	# of APs	% of APs
Default	110	33.1
Non-default	222	66.9
Total	332	100%

Table 2. AP by SSID (Default vs. Non-default)

Channel	# of APs	% of APs
1	6	1.8
2	3	.9
3	10	3.0
4	3	.9
5	1	.03
6	211	63.5
7	5	1.5
8	6	1.8
9	5	1.5
10	14	4.2
11	69	20.7
Total	332	100%

Table 3. AP by Channel

Encryption	# of APs	% of APs
WEP	151	45.5
None	181	54.5
Total	332	100%

Table 4. AP by Encryption (WEP vs. None)

AP density

The density of the access points varies by area. Over the four linear street miles in the residential areas, there were 45, 70, and 193 detectable APs. In the four linear street miles in the industrial area, there were 24 detectable APs. For the residential areas, this results in a minimum of about 1 AP/block up to a maximum of about 4 APs/block. In the industrial area, there was about one AP per 2 blocks. Since the size of city blocks varies somewhat, it is not possible to derive exact comparisons of the density of APs/block.

AP characteristics

For the purposes of studying the existence and extent of an AWN, the combination of several of the aforementioned factors is relevant. Specifically, an AWN will be most readily accessible if it is comprised of APs where all of the following characteristics are true: 1) they are from one of the major manufacturers, 2) they use that manufacturer's default SSID, 3) they are running on the default channel set by the manufacturer, and 4) they do not use any encryption. Table 5 shows the results of the raw data records indicating the APs that would reasonably support the infrastructure of an AWN.

Manufacturer	APs with Default SSID and default channel and no encryption	% of APs
D-Link	10	3.0
Linksys	44	13.3
NetGear	28	8.4
Total	332	100%

Table 5. "AWN Supporting" APs

FINDINGS

Raw data files

The records in the raw data files show that, on the northern San Francisco peninsula residential neighborhoods for which data was collected, the number of high-speed wireless network access points varies from about 1/block up to about 4/block. The question posed in this research project, that "accidental wireless networks" may currently exist, is generally answered in the affirmative. The factors that are relevant to the existence of an AWN are shown to be present:

1. Three top manufacturers (D-Link, Linksys, and NetGear) account for slightly under half (47%) of all of the APs that were found (see Table 1). There may be other APs from these manufacturers that appear in the raw data files, but that do not show up directly as supplied by those three manufacturers, due either to actions taken by the manufacturer or by a more sophisticated user. Therefore, the total number of APs that appears from these three suppliers is a minimum value; the total may be higher.
2. The default SSID set by the manufacturer is used in one-third (110/332) of the APs that were detected (see Table 2). This shows that an AWN exploiter would not need to be very highly sophisticated to break into the AWN. Simple knowledge (or even simple software like Network Stumbler) will give the exploiter the information they need about the SSID to connect to the AWN.
3. The default channels selected by the major manufacturers are obviously 6 and 11, as indicated by the vast majority of APs operating on those channels (see Table 3). With regard to an AWN, this suggests that an exploiter will not

have to worry about channel changes as they pass through the AWN, as many of the APs will be operating on the same channel. However, this fact has implications beyond the existence of an AWN. Specifically, if there are many APs in the AWN that are operating on the same channel, such as channel 6, as shown in this dataset, there are likely to be more problems with interference on those highly-used channels. This will affect the exploiter of the AWN and the owner of the AP, as they will be simultaneously competing with many other local APs for the bandwidth within the same channel.

4. Perhaps most important to the existence of the AWN is the use (or non-use) of encryption. Although it has been shown that WEP as an encryption mechanism is far from robust or secure, it is a first step to prevent an unsophisticated AWN exploiter from entering the AWN. However, as the raw data file shows, more than half (about 55%) of the detected APs were not using any encryption mechanism (see Table 4). To the AWN exploiter, the advantage of this fact is obvious; they do not have to expend any effort, time, or resources to use the AWN. As long as the density of the APs is high enough, they can enter the AWN at any point without knowing anything about network security, much less about how to hack into the AWN.

AP density

The density of the APs ranged from about 1/block to about 4/block. In the residential neighborhoods where this data was collected, the number of blocks/mile ranged from about 10 to 12, indicating an AP density ranging from about 1/500 feet to 4/500 feet. With an effective physical radio range of about 100 meters, it is possible that, in the more dense AP zones, an AWN exploiter could stay fully connected over the range of many blocks.

Figure 1 shows an example of the APs plotted in one of the residential areas in which data was collected. As can be seen from the figure, there are many APs in this particular neighborhood. To protect the identity of the owners of those APs, no data is given on the AP's MAC address, SSID, manufacturer, or other AWN-relevant characteristics.

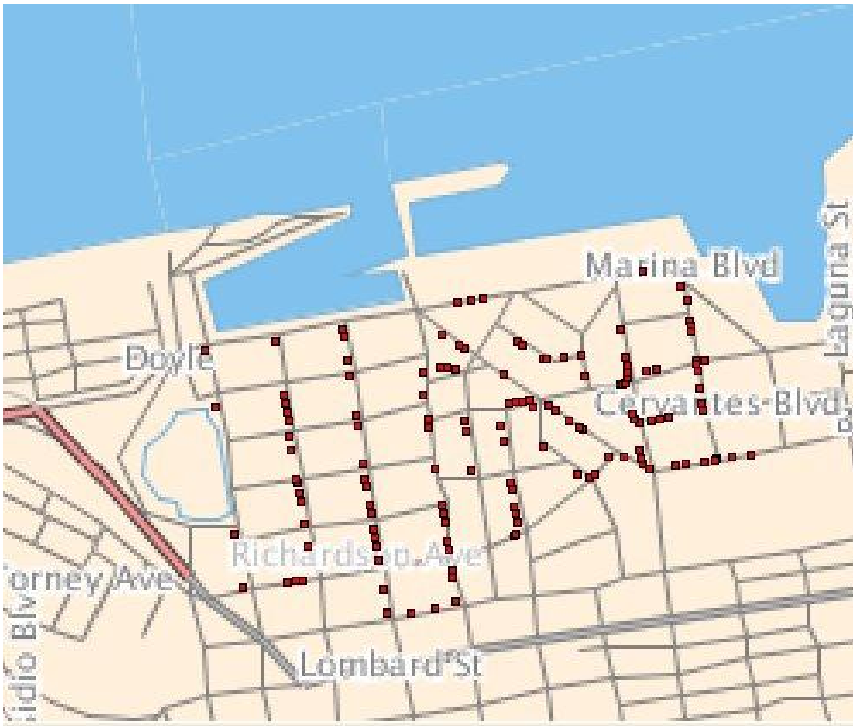

Figure 1. APs in One Residential Neighborhood

AP characteristics

The data from Table 5 shows that almost one out of four (82/332, or 24.6%) APs is: from one of the three major manufacturers **and** is running with the default SSID set by that manufacturer **and** is running on the default channel set by that manufacturer **and** is running with no encryption. That the combination of these four characteristics is true for almost one-fourth of the detected APs is good for those who wish to exploit the existence of an AWN, but it is not good for those AP owners who do not wish to have their APs provide the infrastructure for an AWN.

It is also important to point out that the figure of 24.6% of "AWN-supporting" APs is a conservative estimate. An AP can support the infrastructure of the AWN merely by being plugged in and running. Even a relatively unsophisticated AWN exploiter will not be severely hindered by having to connect through an AP built by a lesser-known manufacturer or by an AP running with an SSID or on a channel other than the manufacturer's default. The truly sophisticated AWN exploiter will not even be stopped by an AP owner employing WEP encryption (the only type of encryption that was encountered during the data collection process for this research project). Therefore, the effective existence of an AWN is far more established than even the data for this research project has indicated.

CONCLUSIONS

AP characteristics

The data collected for this research project support the contention that the four factors mentioned are present and can contribute to the existence of an "accidental wireless network". The characteristics of the access points shown by the data also indicate that a small number of manufacturers of high-speed wireless access points account for a significant number of APs that are detectable in residential areas. The data also show that those manufacturers do not vary the configuration of the APs that are purchased by residential users and that those users, for whatever reason (ignorance or laziness or some other reason), do not alter the manufacturer's default configuration enough to prevent the emergence of an AWN.

Accidental wireless networks

It has been argued above that a system called an "accidental wireless network" can come into existence, and will be supported and enhanced in strength and geographic extent by factors related to the independent actions of manufacturers and consumers. Those three factors are: 1) there are a relatively small number of AP manufacturers, 2) AP manufacturers do not vary the configuration of the APs that they sell to residential customers, and 3) residential customers who purchase APs are not technologically sophisticated and/or are lazy.

Data collected in three residential and one industrial area indicate that the three factors appear to be generally true, and the combination of those three factors does seem to support the creation of an AWN. Since this large group of residential (and occasional commercial) AP owners is obviously acting individually, it can be seen that AWNs are a result of the macro-behavior (meaning the collective consumer behavior that arises from the uncoordinated actions of individuals) of a set of consumers. This large-scale macro-behavior is driven by the low price-point of Wi-Fi hardware, and a near-ubiquitous support in mainstream operating systems and software. The macro-behavior of this set of consumers with regard to technical knowledge and sophistication also show that someone with the intent of exploiting the existence of the AWN can do so with very little effort, knowledge, or resources. The knowledge of an AWN exploiter on a consumer's AP is largely non-existent. Since there is an increasing number of residential wireless APs being purchased and installed, it is also likely that the existence and extent of AWNs will correspondingly increase.

REFERENCES

1. Arbaugh, W. (2002), Security: Technical, Social, and Legal Challenges, *IEEE Computer*, vol. 35, pp. 109 - 111.
2. Fleishman, G. (2001) New Wireless Standards Challenge 802.11b, 2003. Available at: http://www.oreillynet.com/cs/user/view/cs_msg/7817
3. Milner, M. (2003) Network Stumbler Software, Netstumbler, Available at: http://www.netstumbler.net
4. Shoemake, M. B. (2003) Status of Project IEEE 802.11g, Available at: http://www.IEEE.org
5. Stevenson, D. (2002) In Tech Live Wardriving for Wireless Connections. Available at: http://www.techtv.com/news/computing/story/0,24195,3396517,00.html
6. Synergy (2004) 4Q 2003 WLAN Market Shares, Synergy Research Group, Inc., Available at: http://www.srgresearch.com/
7. Verma, S and Beckman, P. (2002) A framework for comparing wireless internet service providers with neighborhood area networks, *Proceedings of the Americas Conference on Information Systems,* Dallas, TX
8. Vichr, R. and Malhotra, V. (2003) In DeveloperWorks' Securing 802.11 transmissions, Part 1: 802.11x's elusive security, 2003. Available at: http://www-106.ibm.com/developerworks/wireless/library/wi-80211security.html