**Empirical Channel Model for 2.4GHz IEEE 802.11 WLAN[[1]](#endnote-1)**

**Stanley L. Cebula III, Aftab Ahmad, Jonathan M. Graham, Cheryl V. Hinds, Luay A. Wahsheh, Aurelia T. Williams, and Sandra J. DeLoatch**

**{s.l.cebula@spartans.nsu.edu}, {aahmad, jmgraham, chinds, lawahsheh, atwilliams, sjdeloatch}@nsu.edu**

Information Assurance Research, Education, and Development Institute (IA-REDI), College of Science, Engineering and Technology (CSET), Norfolk State University (NSU)

700 Park Avenue, Norfolk State University, Norfolk VA 23504

**Contact Author:** Stanley L. Cebula III

**Conference:** ICWN’11

**Keywords:** WiFi, IPsec, WLANs, Information Assurance, Channel Models

**Abstract**

In order to design robust systems for security and forensics of Wireless LANs (WLANs), real-time channel measurements are imperative. We introduce a WLAN Forensics (WiFo) system that uses a grid of WiFi sensors to generate a real-time channel model as well as locate each user within one of the grid areas surrounded by four sensors (or two sensors and the access point). With the help of measurements spread over an extended period of time, we show that these real channel profiles do not follow any recommended model. We conclude that only real-time, empirical channel models can benefit a WiFo system, where users are required to be identified with respect to their location and the signal needs to be contained for environments such as classified ones.

1. **INTRODUCTION**

One way to look at the extent of security provided in the IEEE 802.11 standard is by comparing it with a more trusted protocol suite, such as IPsec. As reported in [1], WiFi is not quite a match for the flexibility and robustness of IPsec. Specifically, there is no security on the physical layer of WiFi. With wired LANs, one can physically trace each packet’s source and destination machine. This is the definition of privacy in a LAN environment. However, there is no way to physically trace a packet on a WiFi network to see the source or destination machine. Also, wired LANs contain physical connections that can be controlled (via physical cable). There is no way provided to control or view the WiFi signal in the 802.11-2007 standard. In classified environments, signal spilling can occur when a WiFi signal is transmitted further than intended. This makes it possible for attacks to occur outside of the physical building where the WiFi network is operated. A tool that allows system administrators to view each machine connected to the WiFi network on a map would provide the ability to identify attackers, thus increasing security. Such a tool will create a map of the signal strength of the WiFi network. With the help of a power control loop, it can be used to restrict the WiFi signal to desired physical boundaries. In order to map the signal strength of a WiFi network, a real-time channel model is required to predict the signal strength at any given distance. Such a system is shown in Figure 1. The system consists of a grid of WiFi sensors that provide signal strength feedback to the access point (AP) to determine a LIVE channel profile. Such a system can also be used to locate users within the grid, thus providing the same level of privacy as a wired LAN would provide. In this paper, we report on research results of one aspect of this system. Instead of using WiFi sensors we based our channel model on actual measurements in a lab that was moderately populated with students and faculty using regular computing equipment. The measurements were made for several days on fixed locations around an Actiontec GT704WG access point. Besides providing our own empirical channel model, we will also compare it with popular existing models.

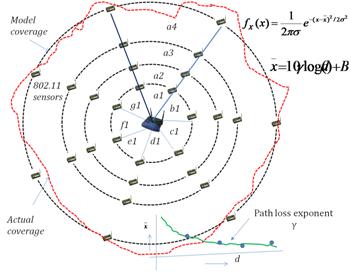


Figure 1. WiFo System Architecture

* 1. **WiFo System Model**

We introduce a new term, WiFo system, in this paper. WiFo is an acronym for WiFi Forensics. The system architecture is shown in Figure 1.The WiFo system consists of an access point surrounded by a grid of low-power, inexpensive (low-memory, low-processing) WiFi sensors. There are two main algorithms that run in the AP: one for plotting and consequently controlling the signal power coverage and the other for location determination. These algorithms can take two types of inputs from each sensor:

1. the signal level of the sensor itself, and
2. a list of user stations (STA) sorted by the RSSI as seen by the sensor.

The quantity in (i) is employed in obtaining a LIVE signal coverage map by measuring the signal path loss exponent and modeling the signal power, either using an empirical probability density function (pdf) of the signal or using a well-known distribution, such as *lognormal*, as shown in the Figure 1. The purpose of this paper is to report one aspect of this system, the empirical channel model.

The remainder of this paper is organized as follows: obstacles that affect signal strength are discussed in Section 2. Existing channel models are outlined in Section 3. We discuss how we found the path loss and developed our channel model in our environment in Section 4. Lastly, we conclude the paper in Section 5.

1. **OBSTACLES**

In any type of WiFi signal transmission, the output signal from the transmitting STA or AP will differ from the signal that is received. There are many factors that affect the signal while it is in transit. These include attenuation, free space loss, fading, reflection, diffraction, scattering, refraction, and noise. Attenuation occurs when the strength of a signal falls off with distance [2]. Basically, the further the signal travels, the weaker the signal will get. This can be represented logarithmically [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. The rest of this section has made heavy use of [2]. Free space loss is a form of attenuation that means the signal disperses with distance. In other words, the further the signal travels, the more the signal spreads out in other directions. The spread of the signal makes the signal weaker. When variation of the signal power occurs due to changes in the transmission medium or path, fading occurs. Basically, any interruption in the transmission medium (atmospheric changes) or path (objects) can affect the strength of the signal. Reflection exists when the signal bounces off large objects causing the signal to change. These changes can increase or decrease the signal strength. This usually happens when the signal reflects off walls, floors, or ceilings. Diffraction is produced when the signal runs into a large object. The secondary waves resulting from the obstructing surface are present throughout the space and behind the large object negatively affecting the strength of the transmitted signal. This can occur when the signal runs into a wall partition or cubicle. Scattering exists when the transmitted signal passes through many small objects that cause the signal to go in many different directions. Scattered waves are produced by rough surfaces, small objects, or by other irregularities in the channel. Refraction is defined as a change in direction of a transmitted signal resulting from changes in velocity. This usually occurs when only part of the line of sight transmitted signal reaches the destination. Noise can be characterized as various distortions imposed by the transmission medium or additional unwanted signals. Noise is usually caused by interference or reception of unwanted signals from other electronic devices. Due to the large number of obstacles that affect the strength of a transmitted WiFi signal, the channel models used to represent the environment must be very specific to each environment.

1. **SOME EXISTING PATH LOSS MODELS**

The channel models that are discussed in this section include the Okumura-Hata model, Log-distance Path Loss model, and JTC Indoor Path Loss model. We will briefly describe each model and determine its suitability for the environment under consideration.

* 1. **Okumura-Hata Model**

The Okumura-Hata model is a combination of the Okumura model and empirical models developed by Masaharu Hata [3]. The Okumura-Hata model is represented below:

where is the 50th percentile median path loss, is the centre frequency in megahertz, is the base station antenna height in meters, is the receiver station antenna height in meters, is a vehicular station antenna height-gain correction factor that depends on the environment, and is the link distance in kilometers [3, 4, 5].

The Okumura-Hata model is extremely accurate, because it is based on measurements in a specific environment. However, while the Okumura-Hata model is popular and accurate, it is mainly used in outdoor, urban environments [3, 4, 5]. The Okumura-Hata model would work well if we were determining path loss in network located outdoors. We should not use the Okumura-Hata model in the development of our signal strength monitoring system, because we are conducting measurements inside an office environment.

* 1. **Log-distance Path Loss Model**

The Log-distance Path Loss model is a very popular logarithmic model that is based on a linear dependence between the path loss in decibels and the logarithm of the distance between the transmitter and receiver [2, 4, 6, 7, 8]. This model predicts path loss inside a building or in densely populated areas. There also exist many studies that use a variation of the Log-distance Path Loss model [3, 5, 8, 9, 10, 9, 12]. The Log-distance Path Loss model is represented below:

where is the measured path loss in decibels one meter from the transmitted signal, is a path loss exponent dependant on the surroundings and building type, is the distance between the transmitter and receiver in meters, is typically one meter, and is a normal (Gaussian) random variable in decibels that has zero mean and standard deviation of decibels [2, 4, 6, 7]. This model also takes into consideration different obstacles in the transmitter to receiver path (also known as log normal shadowing). Table 1 lists the path loss exponents based on different environments [2, 5, 12].

|  |  |
| --- | --- |
| Environment | Path Loss Exponent, |
| Free Space | 2 |
| Urban area cellular radio | 2.7 to 3.5 |
| Shadowed urban cellular radio | 3 to 5 |
| In building line-of sight | 1.6 to 1.8 |
| Obstructed in building | 4 to 6 |
| Obstructed in factories | 2 to 3 |

Table 1. Log-distance Path Loss Exponent

According to many studies which used the Log-distance Path Loss model or a variation of this model, the Log-distance Path Loss model is accurate and simple to use [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. The Log-distance Path Loss model also will work in our environment and could be used in the development of our signal strength monitoring system.

* 1. **JTC Indoor Path Loss Model**

The JTC (Joint Technical Committee) Indoor Path Loss model is the official path loss model for office environments presented by the International Organization for Standardization (ISO). This model has traits from the Okumura-Hata model (based on specific measurements of different factors) and the Log-distance Path Loss model (based on the relationship between the logarithm of the distance between the transmitter and receiver to the path loss in decibels). The JTC Indoor Path Loss model is represented below:

where is an environment dependent fixed loss factor in decibels, is the distance dependent loss coefficient, is the distance between the transmitter and receiver in meters, is a floor/wall penetration loss factor in decibels, is the number of floors/walls between the transmitter and receiver, and is a normal (Gaussian) random variable in decibels that has zero mean and standard deviation of decibels (log normal shadowing) [3, 5, 13]. Table 2 contains the corresponding variables dependent on the type of environment [3, 5, 13].

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Residential | Office | Commercial |
|  | 38 | 38 | 38 |
|  | 28 | 30 | 22 |
|  | 4n | 15 + 4 (n-1) | 6 + 3 (n-1) |
| Log Normal Shadowing Std. Dev. | 8 | 10 | 10 |

Table 2. JTC Indoor Path Loss Model Variables

The JTC Indoor Path Loss model will work in our environment. According to [3], the JTC Indoor Path Loss model may be more accurate than the Log-distance Path Loss model due to the addition of the function. The JTC Indoor Path Loss model could be used in the development of our signal strength monitoring system.

The Okumura-Hata, Log-distance Path Loss, and JTC Indoor Path Loss models are all accurate and reliable in different environments. Based on our environment of an indoor office setting, the Log-distance Path Loss and JTC Indoor Path Loss models could be used in the development of our signal strength monitoring system.

1. **DEVELOPING A CHANNEL MODEL**

In order to develop our own channel model, we took many measurements in our custom environment and find the predicted value line based on our data. This predicted value line acts as a path-loss model in our environment. The area that we used for testing and developing our own channel model is a portion of the Information Assurance Research, Education, and Development Institute (IA-REDI) located on the sixth floor of the Marie V. McDemmond Center for Applied Research (MCAR) at Norfolk State University. This area is a computer lab (approximately twenty feet by sixty-five feet) next to an office, three conference rooms, and one long hallway. We used commercially available hardware and software. The access point we used was an Actiontec GT704WG router on default settings. The wireless card we used to connect to the access point was an Intel® PRO/Wireless 3945ABG Network Connection built-in a Dell Latitude D830 laptop running Windows XP on default settings. The program we used to measure the signal strength is called inSSIDer (freeware) [14]. We measured the signal strength at eighteen locations on every hour between 9:00 a.m. and 5:00 p.m. (EST) for one week. Figure 2 displays the experiment area, measurement locations, and access point (AP). The access point is the circle in the upper right hand corner. The letter ‘x’ represents the measurement locations, and the arcs represent measured distances (ten feet) from the access point. Table 3 contains the measurement locations and their distance from the access point.

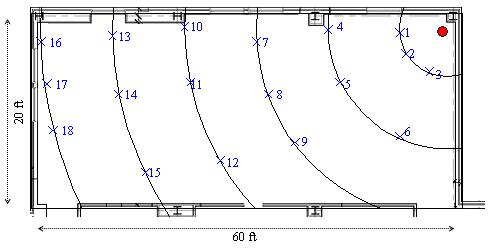


Figure 2. Environment Overview

|  |  |  |
| --- | --- | --- |
| Location | Distance from AP (ft) | Distance from AP (m) |
| 1 | 10 | 3.408 |
| 2 | 10 | 3.408 |
| 3 | 10 | 3.408 |
| 4 | 20 | 6.816 |
| 5 | 20 | 6.816 |
| 6 | 20 | 6.816 |
| 7 | 30 | 10.224 |
| 8 | 30 | 10.224 |
| 9 | 30 | 10.224 |
| 10 | 40 | 13.632 |
| 11 | 40 | 13.632 |
| 12 | 40 | 13.632 |
| 13 | 50 | 17.04 |
| 14 | 50 | 17.04 |
| 15 | 50 | 17.04 |
| 16 | 60 | 20.448 |
| 17 | 60 | 20.448 |
| 18 | 60 | 20.448 |

Table 3. Distance of Locations from AP

The access point was sitting on a desk approximately three feet from the ground. When measuring the signal strength, the laptop was held approximately five feet from the ground with the screen facing away from the access point. The program inSSIDer was used to collect data, and a total of 810 measurements were taken over a one-week time period.

Displayed in Figure 3 is the cumulative distribution function (CDF) of the measured signal strength versus distance. Figure 3 shows the data collected (displayed in Figure 4) can be classified as normal.

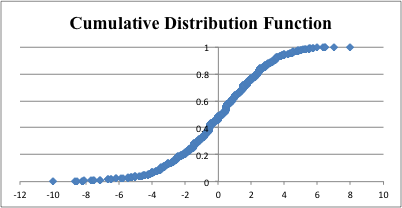


Figure 3. Cumulative Distribution Function of Collected Data

Table 4 represents the average signal strength compared to distance from the access point. Figure 4 displays this relationship along with a predicted value line.

|  |  |  |
| --- | --- | --- |
| Distance from AP (ft) | Average RSSI (dB) | Variance |
| 10 | -28.82 | 7.55 |
| 20 | -33.89 | 6.93 |
| 30 | -37.31 | 7.4 |
| 40 | -40.77 | 7.51 |
| 50 | -42.44 | 5.14 |
| 60 | -47.61 | 12.42 |

Table 4. Average Signal Strength Compared to Distance



Figure 4. Signal Strength Compared to Distance

The equation for the predicted value line is:

where is the predicted signal strength and is the distance from the access point in feet. This equation could serve as a channel model for this specific environment.

1. **CONCLUSION**

The research presented in this paper identified three existing channel models and one new channel model to consider for implementation in this signal strength monitoring system. The new empirical model gives a path-loss exponent of about 2.1, which is closer to the free-space path-loss exponent. In most experiments by other researchers, this value is much higher than the one we obtained. Since custom models can be more accurate in custom environments, a permanent, universal model may not be employed in designing signal mapping systems for 2.4 GHz IEEE 802.11 networks. Upon further review, we also conclude that one should not use the Okumura-Hata model, because we are conducting measurements inside an office environment. The Log-distance Path Loss model and JTC Indoor Path Loss model also will work in our environment, because they are tailored to be universal models for indoor use. However, upon completing the development of our own model (predicted value line from the measurements), a real-time model would be the most accurate to use in the same environment – as proposed in Figure 1 and Figure 4.

**References**

1. Cebula, S. L. and Ahmad, A. “How Secure is WiFi MAC Layer in Comparison with IPsec for Classified Environments?”. In Proceedings of the 14th Communications and Networking Simulation Symposium, April 2011.
2. Tummala, D. “Indoor Propagation Modeling at 2.4GHz for IEEE 802.11 Networks”. M.S. Thesis, University of North Texas, 2005.
3. Pahlavan, K. and Levesque, A. H. “Wireless Information Networks”. Wiley-Interscience. New York, NY, 1995. 73-112.
4. Vig, J. “ISM Band Indoor Wireless Channel Amplitude Characteristics: Path Loss vs. Distance and Amplitude vs. Frequency”. M.S. Thesis, Ohio University, 2004.
5. Tipper, D. “Wireless Communication Fundamentals”. University of Pittsburgh lecture. 2005. 40-42.
6. Faria, D. B. “Modeling Signal Attenuation in IEEE 802.11 Wireless LANs”. Stanford University, July 2005.
7. Akl, R., Tummala, D., and Li, X. “Indoor Propagation Modeling at 2.4 GHz for IEEE 802.11 Networks”. In Proceedings of the 6th IASTED International Multi-Conference on Wireless and Optical Communications, Banf, AB, Canada, 2006.
8. Borrelli, A. et al. “Channel Models for IEEE 802.11b Indoor System Design”. In Proceedings of IEEE Conference on Communications, vol. 6, 2004. 3701-3705.
9. Andrade, C. B. and Hoeful, R. P. F. “IEEE 802.11 WLANs: A Comparison on Indoor Coverage Models”. In Proceedings of the 23rd Canadian Conference on Electrical and Computer Engineering, 2010.
10. Capulli, F, et al. “Path Loss Models for IEEE 802.11a Wireless Local Area Networks”. In Proceedings of the 3rd International Symposium on Wireless Communications Systems, 2005.
11. Liechty, L. “Path Loss Measurements and Model Analysis of a 2.4 GHz Wireless Network in an Outdoor Environment”. M.S. Thesis, Georgia Institute of Technology, 2007.
12. Phaiboon, S. “An Empirically Based Path Loss Model for Indoor Wireless Channels in Laboratory Building”. In Proceedings of the IEEE TENCON’02, 2002.
13. Joint Technical Committee of Committee T1 R1P1.4 and TIA TR46.3.3/TR45.4.4 on Wireless Access, “Draft Final Report on RF Characterization,” Paper No. JTC(AIR)/94.01.17-238R4, Jan. 17, 1994.
14. http://www.metageek.net/products/inssider

1. *Acknowledgement:* “This material is based upon work supported by the Department of Energy National Nuclear Security Administration] under Award numbered DE-FG52-09NA29516/A000.” *Disclaimer:* “This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.” [↑](#endnote-ref-1)