

Using Smart Mobile Terminal Antennas to Achieve Optimal Wireless Network Performance and Security

Ian Scriven, Junwei Lu, David Ireland

(Griffith University Centre for Wireless Monitoring and Applications, Brisbane, Australia)

Abstract: In this paper, a complete smart mobile terminal antenna system (SMTA) is presented. This system uses a radiation beam switching approach in an attempt to achieve optimal wireless network performance while increasing network security. Test results are presented that demonstrate the ability of the SMTA system to maintain consistently high wireless signal levels in a dynamic, noisy environment.

Keywords: Smart Antennas, Wireless Networking, Security

1 Introduction

Smart antennas are becoming increasingly popular in mobile computing because they can give longer battery life, more reliable connectivity and better security than conventional omni-directional antennas. Unlike traditional omni-directional antennas, where radiation and information is transmitted equally in all directions, smart antennas are able to direct the majority of the transmission towards the intended receiver. Likewise, they are able to alter their directional sensitivity in such a way that noise reception can be greatly reduced. Lower antenna gain or lower transmission power can then be used, lowering the power requirements of the system, and increased noise resistance leads to more reliable wireless network connections. Heavily utilized frequency spectrum can be more easily reused thanks to the spatial diversity introduced through the use of such smart antennas. Perhaps most advantageous however is the increased security that smart antennas can provide. One of the key security weaknesses of wireless networks is the possibility of ‘eavesdroppers’ sniffing packets sent and received over the wireless

network. By directing the radiation towards the intended target and limiting transmission in other directions, it becomes much harder for eavesdroppers to obtain the received signal strength required to accurately intercept packets. This is demonstrated in Figure 1.

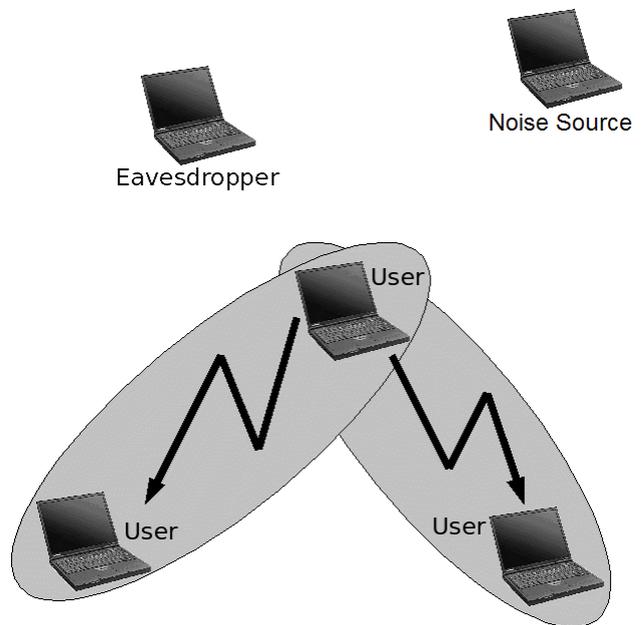


Figure 1 - Smart antennas in use in an ad hoc wireless network

The IEEE 802.11a/b/g protocol for wireless networks is a robust protocol, and is able to scale connection speeds depending on the connection quality by altering the modulation scheme [1]. In Figure 1, the connections between the legitimate users of the network will be made at a high speed. While the eavesdropper will be able to receive some of the transmission, their received signal power will be much lower, introducing a large number of errors in

demodulation, greatly reducing the eavesdroppers' ability to accurately crack into the network or steal sensitive information.

2 The Dielectrically Embedded Smart Mobile Terminal Antenna (DE-SMTA)

The smart mobile terminal antenna (SMTA) is a parasitic monopole array consisting of a single, central driven element surrounded by a number of passive elements in a number of concentric circles [2]. The configuration used in this application consists of six passive elements located in a single circle on a ground plane surrounding the central element, as in Figure 2. The complex impedances of the six passive elements determine the directionality of the SMTA.

The SMTA antenna functions on the principle of mutual coupling, a fundamental principle in multi-element antenna systems describing the interchange of electromagnetic radiation between the radiating elements of the antenna array [3].

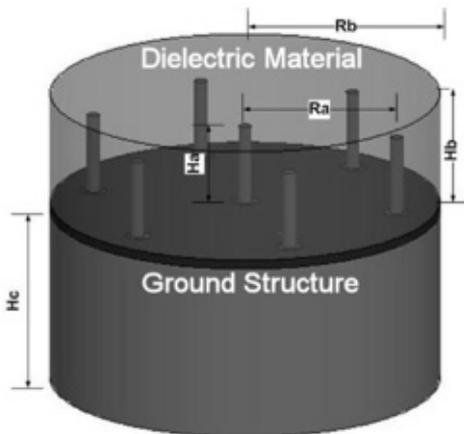


Figure 2 – The DE-SMTA

SMTA antennas designed to operate at the 2.4GHz frequency range required for 802.11a/b/g wireless computer networks are generally too large to be practical. Lu et al recently developed a novel new SMTA design, the dielectrically embedded SMTA (DE-SMTA) [4]. By embedding the antenna dipole elements in a ceramic material with a relative

permittivity of 4.5, Lu et al were able to reduce the volume of the antenna by 80% and its footprint by 50%. The DE-SMTA is shown in Figure 2. As with the SMTA, the directivity of the DE-SMTA is determined by the impedances of the six passive antenna elements.

3 DE-ESPAR Control System

As stated previously, DE-SMTA radiation directionality is achieved by setting the impedances of the passive antenna elements. A wide range of impedances can be set through the use of varactors (voltage controlled variable capacitors) however these require a wide range of control voltages (up to twenty volts) in order to obtain a full range of impedances [3]. A simpler and less expensive method is to control radio frequency switch connections between the passive antenna elements and the ground plane [5].

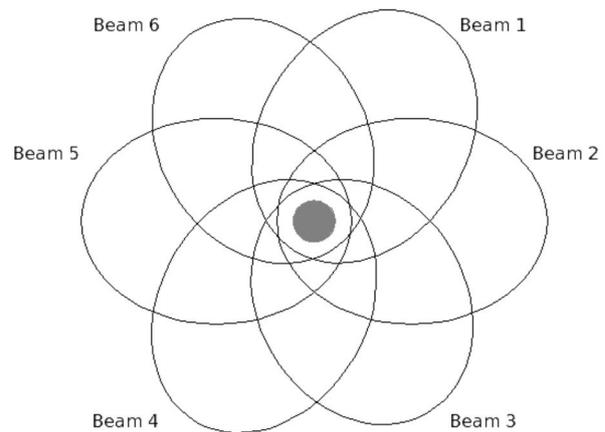


Figure 3 - Example of a beam switching system employing 6 fixed beam positions to cover a 360 degree area

Using this set up, it is possible to obtain a number of useful radiation patterns with good directivity and gain. Simulations have shown that the best radiation pattern (the best compromise between gain and radiation beamwidth) was achieved by connecting three adjacent passive elements to ground, while leaving the opposite three elements disconnected (that is, open circuited). This configuration can be replicated utilising the

symmetrical nature of the DE-SMTA to provide six possible radiation beams with 3dB beamwidths of approximately 80 degrees to completely cover the 360 degree azimuthal plane with minimal overlapping, as can be seen in Figure 3.

A beam switching system has been developed to select the most suitable beam from this group of six possibilities after performing a scan where the performance of each beam is measured. This method has a great advantage in that it is remarkably simple, resulting in very low power requirements, in terms of both computational power and electrical power. The beam switching method is not without its disadvantages, however. As the beam positions are fixed, uniform gain cannot be maintained exactly in all directions. The variation in gain can be reduced by adding more beam positions, however this would result in a linear increase in the amount of time required to scan all beams. It would also make it necessary to increase the frequency of scanning and beam switching operations in order to maintain the optimum beam position.

The software for this control system utilises Microsoft's Network Driver Interface Specification (NDIS, currently version 5.1). NDIS is an Application Programming Interface (API) for network interface cards under Microsoft Windows. Version 5.1 in Windows XP supports 802.11 wireless network cards, and provides access to a wide range of information and statistics on wireless network connectivity under Windows. Windows Management Instrumentation (WMI) provides an easy to use interface through which applications can obtain a wide range of system management information, including NDIS statistics [6]. The DE-SMTA control system software uses WMI to access NDIS wireless information and obtain details of all available wireless networks, access points and the received signal level of each access point, allowing the user to specify which wireless network or access point they connect to and track.

4 Testing Results

An external application, Network Stumbler [7]

(or more commonly NetStumbler) was used in during testing to provide regular, accurate received wireless signal strength measurements. Two tests were performed, both involving moving a laptop using the smart antenna system around in an environment containing a wireless access point. In the first test, the smart antenna control application was running and actively tracking the wireless access point, performing scans at ten second intervals. The results, taken from NetStumbler (and showing received signal strength on the Y axis and time on the X axis), can be seen in Figure 4, and show that the system does a good job of maintaining the best possible connection when tracking a wireless signal. In some cases small (approximately 5 dBm) dips in signal strength can be observed when scanning is taking place, or when the laptop has moved a significant distance before the system has rescanned, however these drops are small in both magnitude and duration, and as such pose no problem to connection integrity.

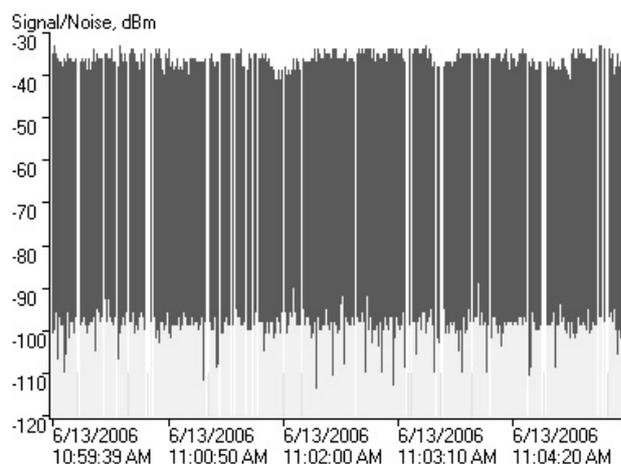


Figure 4 - Measured received signal strength, control application actively tracking

A second control test was performed to provide a comparison for the above results. In this test, a fixed beam position was maintained, while the laptop was moved around in the same manner as before. The results from NetStumbler, as shown in Figure 5, show that this time there were significant drops in received signal strength, in some cases approaching 20 dBm. Obviously, areas with higher received signal strength

occur when the position of the laptop in the testing space results in the fixed beam position being close to the optimal position, while the lower regions occur when the fixed beam position is close to opposite of the optimal direction. While in the majority of cases these changes did not result in the connection being dropped, prolonged drops in signal strength cause the wireless system to change modulation schemes and scale down the connection speed.

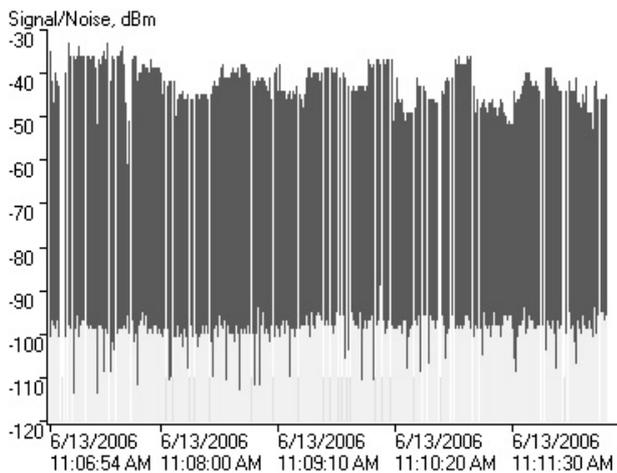


Figure 5 - Measured received signal strength, fixed beam position

4 Conclusion

The smart mobile terminal antenna system presented in this paper has been shown to have considerable benefits in regards to wireless network performance and security. By using a steerable directional antenna it is possible to maintain a consistently high wireless connection strength in a noisy real-world environment, even whilst moving. By directing wireless transmissions towards their intended recipient instead of broadcasting them (and strongly) in all directions. Testing results have been presented which demonstrate the effectiveness of the SMTA system in this regard.

The SMTA system also allows for increased noise immunity, as, from Lorentz reciprocity, the smart mobile terminal antenna's directivity is the same for receiving as it is for transmitting. This means that the effect of relatively powerful (and common) noise signals in the 2.4 GHz band can be minimized

providing the noise source is not in the same direction as the target of communications.

Finally, any potential 'eavesdroppers' who are not located directly between the SMTA transmitter/receiver and its counterpart (whether another mobile computer or a wireless access point) will have problems demodulating and transmissions due to their lower received signal strength.

Reference

- [1] Information technology-- Telecommunications and information exchange between systems-- Local and metropolitan area networks-- Specific requirements-- Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999)
- [2] R. Schlub, "Practical Realization of Switched and Adaptive Parasitic Monopole Radiating Structures," PhD Dissertation, School of Microelectronic Engineering, Griffith University, Brisbane, Queensland, Australia, 2004.
- [3] D. Ireland, "Realization of Dielectric Embedded Monopole Radiating Structures For Wireless Computing," Masters Dissertation, School of Microelectronic Engineering, Griffith University, Brisbane, Queensland, Australia, 2006.
- [4] J. W. Lu, D. Ireland, and R. Schlub, "Dielectric Embedded ESPAR (DE-ESPAR) Antenna Array for Wireless Communications," IEEE Transactions on Antennas and Propagation, vol. 53, pp. 2437-2443, 2005.
- [5] M. Shah, "Smart Antenna Control System for Wireless Ad Hoc Computing," Masters Dissertation, School of Microelectronic Engineering, Griffith University, Brisbane, Queensland, Australia, 2005.
- [6] Microsoft, "WMI: Introduction to Windows Management Instrumentation," 23/05/06; <http://www.microsoft.com/whdc/system/pnppwr/wmi/WMI-intro.msp>.
- [7] M. Milner, "stumbler dot net," March; <http://www.stumbler.net>.
- [8] I. Scriven, "A Beam Steering Control System for DE-ESPAR Smart Antennas", Honours Dissertation, School of Microelectronic Engineering, Griffith University, Brisbane, Queensland, Australia, 2006.