Increased Security Level using Space-division Approach in Wireless Computing Network

Zhaohui Sun, Junwei Lu and David Ireland
School of Microelectronic Engineering, Griffith University, Australia

Abstract—**This paper presents a new Space-division Approach for solving the security problems in infrastructured wireless network and Ad-Hoc wireless network using smart directional antennas. The security level definition according to this Approach in WLAN is also proposed, the corresponding experiments in a typical office environment is obtained to evaluate its practicability.**

I. INTRODUCTION

Mobile wireless networks have become not only increasingly popular but inevitable in the computing industry. Except for its advantages of freedom, simplicity of installation and ease of use, the security problem in WLAN is more seriously than in traditional wired network. More and more wireless experts recognized of this and designed several software encryption solutions such as WEP2 standard and IEEE 802.11i [1-2]. However, the result is not as successful as expected due to WLAN's inherent specialty of space signal sharing. When the smart directional antenna is used in WLAN, the space can be divided into signal area and non-signal area, or secure area and non-secure area, outside the secure area the eavesdroppers will get only noise signal, thus the security level will be further improved.

II. NUMERICAL RESULTS

As to the purpose of research, one can use the distance from Access Point (AP) to terminal as radius to draw a circle, only the signal within this area will be concerned, and its dimension called S1. The security area is defined as the area that have both AP and terminal's signal because short of any one the information will be considered incomplete, and its dimension called S2, beam bandwidth for directional antenna used in AP called θ, in terminal called α. In order to accord with our ordinary notion, security level can be defined as

$$\eta = \log(\frac{10 \times S1}{S2}) \qquad (1)$$

To ensure a reliable wireless link, Line of sight (LOS) conditions is assumed, Friis free-space propagation equation can be used to calculate the transition distance of directional antenna or online calculator at: http://www.signull.com/fsc.php.

Free Space Loss=20log10 (Frequency in MHz) +20log10 (Distance in Meters) -27.5 [3]

Totally four scenarios are discussed below:

1. *AP: omni-directional antenna*
   Terminal: omni-directional antenna

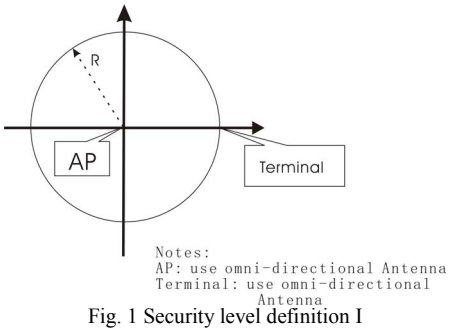
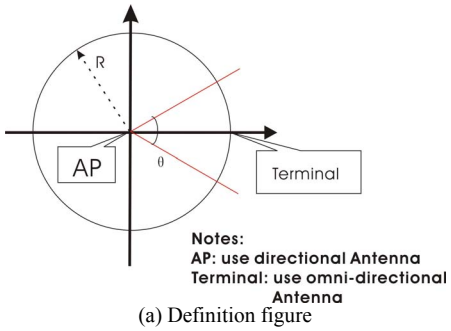


Fig. 1 Security level definition I

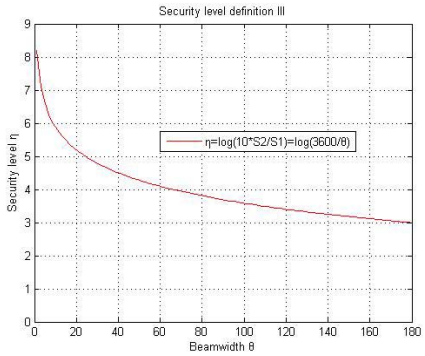
Obviously, this is traditional way; one can use the equation (1) to figure out the security level, that is 1.

2. *AP: directional antenna*
   Terminal: omni-directional antenna

Because usually the signal pattern of directional antenna is ellipse-shape, it is very difficult to calculate its dimension. The simplified case can be achieved by using a sector instead of ellipse whose two side border is defined by 3-db point to represent its signal area and the angle of the sector is defined the AP's beamwidth θ. From Figure 2, one can see that security area is decreased from a circle to a sector and its diagram in Matlab program.



(a) Definition figure



(b) Trendline in Matlab

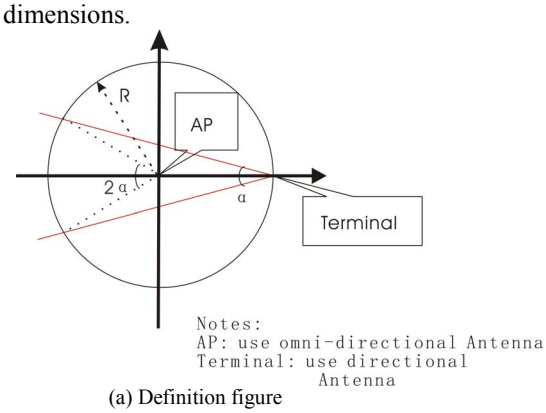
Fig. 2 Security level definition II

Therefore, security level can be calculated by equation (2):

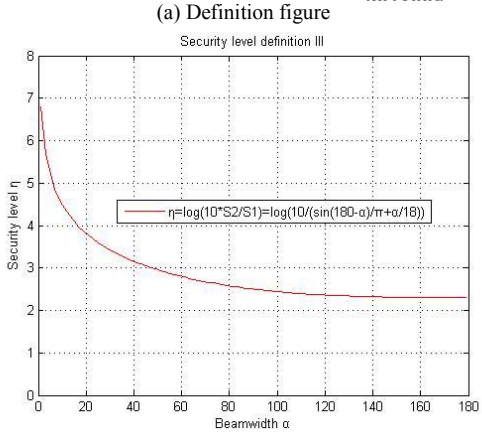
$$\eta = \log(\frac{10 \times S1}{S2}) = \log(\frac{3600}{\theta}) \qquad (2)$$

3. AP: omni-directional antenna
Terminal: directional antenna

This scenario is more complicated compared with I or II. Now the security area changes to a caky figure. One can think the dimension of security area is the sum of sector's dimension and two triangles' dimensions.



(a) Definition figure



(b) Trendline in Matlab

Fig. 3 Security level definition III

$$S2 = S_{sector} + S_{triangle} = R^2 \sin(180 - \alpha) + \pi R^2 \frac{\alpha}{180}$$

Security level is obtained as:

$$\eta = \log(\frac{10\pi}{\sin(180-\alpha) + \frac{\pi\alpha}{180}}) \qquad (3)$$

4. AP: directional antenna
Terminal: directional antenna

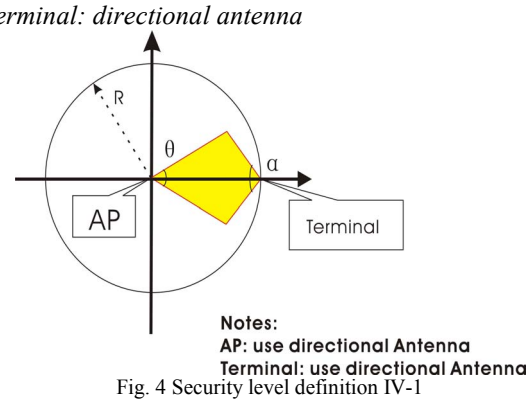


Fig. 4 Security level definition IV-1

This is the most secure way that the security area changes to a regular quadrangle.

$$S2 = \frac{tg\frac{\theta}{2} \times tg\frac{\alpha}{2}}{(tg\frac{\theta}{2} + tg\frac{\alpha}{2}) \times \pi} \times R^2$$

Therefore security level

$$\eta = \log(\frac{10 \times S1}{S2}) = \log(\frac{(tg\frac{\theta}{2} + tg\frac{\alpha}{2}) \times 10\pi}{tg\frac{\theta}{2} \times tg\frac{\alpha}{2}}) \qquad (4\text{-}1)$$

Along with the increase of two antennas' beamwidth, θ and α, these two lines will intersect outside the circle (see Figure 5). At this stage, the dimension of security area changes into the sum of two sectors' dimensions and two triangles' dimensions.

The critical condition is: $\alpha + \frac{\theta}{2} = 180$

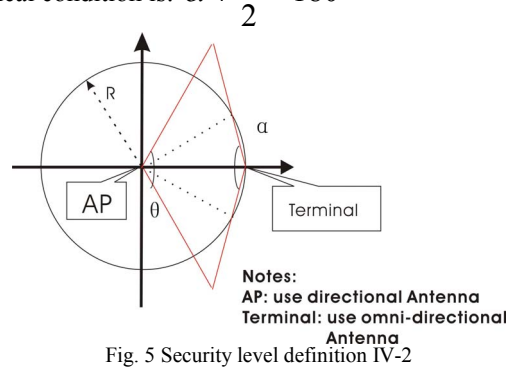


Fig. 5 Security level definition IV-2

Table 1: Parameters of adopted antennas

	Antenna Type	Directivity	Gain	F/B	Beamwidth
Transmit Antenna	D_Link 900AP+ embedded	omni-directional	2.5dbi	0	360
	M.gear MGR-OS-05A	omni-directional	5dbi	0	360
	M.gear MGR-DS-06B	directional	6dbi	18	120
	New ESMB	directional	6dbi	20	95
Receive Antenna	D_Link DWL-660 embedded	omni-directional	2dbi	0	360
	New ESPAR	directional	4.5dbi	22	85

When $\alpha + \frac{\theta}{2} \geq 180$

$$S2 = S_{sector} + S_{triangle} = \pi R^2 \frac{\frac{\theta}{2} + \alpha - 180}{180} + R^2 \sin(180 - \alpha)$$

So security level

$$\eta = \log(\frac{10 \times S2}{S1}) = \log(\frac{10\pi}{\pi(\frac{\theta}{2} + \alpha - 180) + \sin(180 - \alpha)}) \quad (4\text{-}2)$$

Figure 6 is the viewdata of security level scenario 4 in Matlab:

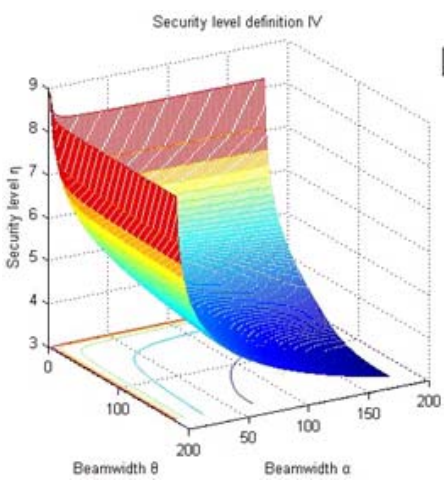


Fig. 6 Security level definition IV in Matlab

Based on the aforementioned results, one can define security level according to the space use as Table 2:

Table 2: Security level standard definition

Security level	Standard
1	low security
1~3	light security
3~4	medium security
4~	high security

Using directional antenna in AP or terminal, both can greatly improve the security level in WLAN, while the influence in AP's case is more distinct. The narrower the bandwidth is, the better effect will be achieved.

III. Experimental Results

To examine the WLAN's directivity performance both in LOS case and real environment (non-LOS case), the following experiments were presented. The wireless equipments were adopted as:

AP: D_Link DWL_900AP+ (Firmware: rev. B 2.61)
Terminal: COMPAQ PII notebook
with D_Link DWL_660 802.11b wireless card

In order to enable comparability of the result, six different antennas were used. Two of them are D_Link equipment embedded; two benchmark antennas come from M.gear Co., and the left two are new-designed ESPAR [4] and ESMB [5] directional antennas. Network Stumbler 0.4.0 software, http://www.netstumbler.org/, was adopted to record the signal strength.

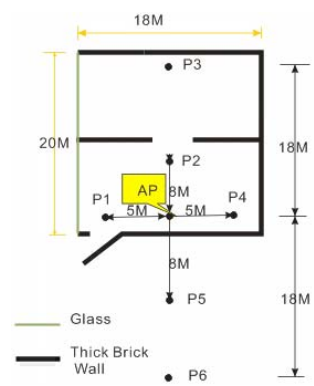


Fig. 7 Layout of Antenna experiment environment

LOS condition was achieved in a big open yard. To compare with it, the real experiment environment is in a typical office area comprising two rooms depicted in Fig. 7. The dimensions of the examined region are 20 × 18 m, where three walls are made of 40 cm brick block and the fourth is large glass window. And six different positions were chosen to compare the signal strength result.

Table 3: Open-yard experiment result using omni-directional receive antenna
(Receive antenna: 4.5db ESPAR- directional, LOS condition)

Transmit Antenna	Signal/Noise Ratio (dB)					
	P1	P2	P3	P4	P5	P6

	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B
D-Link embedded	32	29	21	20	18	17	11	10	10	37	35	33	18	17	15	10	9	10
MGR-OS-05A	41	39	40	31	29	25	15	14	15	39	40	37	26	23	19	20	19	17
MGR-DS-06B	11	6	none	45	33	14	29	17	3	13	3	none	12	2	none	3	none	none
ESMB_directional	8	4	none	48	42	6	36	23	6	11	none	none	11	2	none	2	none	none

Table 4: Indoors experiment result using omni-directional receive antenna
(Receive antenna: 4.5db ESPAR-directional, non-LOS condition)

Transmit Antenna	Signal/Noise Ratio (dB)																	
	P1			P2			P3			P4			P5			P6		
	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B	F/F	B/F	B/B
D-Link embedded	35	33	31	23	26	26	11	10	13	39	37	40	18	17	15	none	none	none
MGR-OS-05A	41	39	40	31	29	25	15	14	15	39	40	37	26	23	19	none	none	none
MGR-DS-06B	46	43	43	46	36	14	29	19	3	49	45	42	27	16	6	16	10	2
ESMB_directional	50	51	39	48	40	8	35	23	none	51	43	40	27	14	none	12	10	none

(F/F AP antenna's Front beam to terminal antenna's Front beam;
B/F AP antenna's Back beam to terminal antenna's Front beam;
B/B AP antenna's Back beam to terminal antenna's Back beam)

The open-yard and indoors experiment results were presented in Table 3 and Table 4 respectively. To make the result veracious as possible, every experiment was repeated three times and recorded the average value. As expected, our new-designed ESMB and ESPAR antennas acted better than commercial directional antennas.

From the experiment results, one can see:

- Indoors signal propagation is a highly complex process because it occurs within environments possessing a variety of geometric and electromagnetic properties;
- Due to multiple-path and interactions with walls, furniture, equipment and even people, the indoors signal strength fluctuation is not very pronounced as expected, but it should be noted results in open-yard do incarnate the non-signal area comparing to indoors case (refer to the notable signal strength variety in P1 and P4 under different condition);
- Using MGR-DS-06B in AP, ESPAR in terminal; and ESMB in AP, ESPAR in terminal, whose corresponding security level is 3.95 and 4.14, both act more securely in LOS condition and non-LOS condition as in some position, P1, P4, P6 etc, one can hardly receive any signal;
- It should be reminded that the results only show the AP's signal strength fluctuation in different positions. From the aforementioned approach, the security level still get improvement with using directional antenna in terminal;
- In reality, the eavesdroppers usually would not have the physical entrance to target WLAN environment, so mostly he will use the B/F mode described in Position 5 and 6. In such case, using directional antenna do boost the security performance;
- Further security improvement could achieved by follow step:

AP: Decrease the transmit power in acceptable range
Decrease the gain of antenna
Rational position selection
Terminal: Increase the gain of antenna
Rational directional selection

IV CONCLUSION

The Space-division Approach in WLAN to solve the security problem and correlated security level definition has been presented. Additional antenna directivity experiments provided information regarding the signal strength in LOS condition and non-LOS condition. Future work will take the reflection interfering and multi-path fading into account and suitable formulation.

REFERENCES

[1] Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", Feb 6, 2002, available at http://www.csc.gatech.edu/~gte369k/802_1x.pdf

[2] Dennis Eaton, Intersil, "Diving into the 802.11i Spec: A tutorial", November 26, 2002, available at http://www.commsdesign.com/design_corner/OEG20021126S003

[3] Robert F. White, "Engineering Considerations for Microwave Communications Systems", 1990, page 35

[4] J.Lu, D.Ireland and R.Schlub, "Dielectric Embeded ESPAR Antenna for Wireless Communications Systems, IEEE Trans. On Antenna and Propagation, Vol. 53, Aug. 2005

[5] J.Lu, D.Ireland and D.Thiel, "FD-TD Analysis of Dielectric Embeded Electronically Switched Multiple-Beam Antenna Array", IEEE Trans. On Magnetics, Vol. 38, No 2, March 2002, pp701-704