Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards

Tim W. C. Brown
Centre for Communication Systems Research
University of Surrey
Guildford, GU2 7XH, UK.
twcbrown@theiet.org

Thomas Diakos, Johann A. Briffa
Department of Computing
University of Surrey
Guildford, Surrey, GU2 7XH
t.diakos@surrey.ac.uk, j.briffa@surrey.ac.uk

***Abstract*—Measurements results are presented to evaluate the distance at which a carrier signal of 13.56MHz can be eavesdropped by a "rogue" antenna, which is transmitted by an inductive loop H-antenna, thus representative of a contactless payment device employing near field communication (NFC). Results are evaluated based on the magnetic H-fields used in the ISO14443 standard, while the ability to receive a carrier is based upon the minimum noise floor achievable by a radio receiver at such frequencies and bandwidths. Depending on the size of H-field and the antenna design, measurements indicate that in general the maximum eavesdropping range with practical radio apparatus is largely due to the background noise, which larger antennas were susceptible to in the laboratory environment.**

***Index Terms*—NFC, eavesdropping, interrogation, H-antenna**

I. Introduction

With the fast emergence of near field communications (NFC) being used for contactless payment devices for convenience and ease of buying small items, there is growing concern over the security risks associated with transmitting such information wirelessly. Two particular threats, where the propagation of radio as well as design of antennas in the high frequency (HF) band is of interest, is that of eavesdropping and interrogation [1][2], whereby it is possible that data can be "listened" to while a transaction is taking place. More importantly however, there are also "skimming" attacks possible whereby a contactless payment device can be interrogated to send data back to an eavesdropper as it is passing by. Finally there are also the risks of "man in the middle" attacks, whereby it is assumed two contactless payment devices are communicating with each other, but in reality they are both communicating with the device acting as a man in the middle and bogusly appearing to be each device separately. In all these cases, the eavesdropping antenna may be at some distance away from both devices and its success will depend on how easily it is able to receive information transmitted by the inductive loop H-antenna used in the mobile device for NFC [3].

While other publications have shown existing NFC devices to achieve a successful eavesdrop [2], they have addressed the topic from an end to end perspective, whereby the device is transmitting real data and it is evaluated as to whether the eavesdropped data can be quantified in any particular fashion. What is not known in such tests is the degree of H-field that the device transmits. It is only assumed that the reader device is transmitting within the ISO14443 standard, which requires a minimum H-field of 1.5A/m and a maximum of 7.5A/m, though the mobile device which receives from the reader is expected to emulate a passive card, which would normally backscatter the response back to the reader and is likely to be significantly less than 1.5A/m. Therefore the results presented in this paper evaluate the eavesdropping distance achievable from a H-antenna for H-fields between 0.5A/m and 7.5A/m. The results are divided into two parts, the first set of measurements verify the expected path loss using a spectrum analyser and different antenna designs, while the second set of results evaluate the distance at which a type A NFC signal using on off keying (OOK) modulation can be successfully recovered.

II. Measurement Setup

The NFC antenna was set up as a circular coil antenna of one turn with a radius, r_{ant}, of 1.5cm. This resulted in a low inductance antenna of 0.3μH, which cannot be easily matched by reactive components alone and provide a wide bandwidth due to the high Q-factor such a circuit creates. Therefore a small resistance of 10Ω was placed in series with the inductive antenna as illustrated in figure 1, such that by using a Smith Chart [4], it was possible to suitably match the input to 50Ω at 13.56MHz using a parallel capacitance of 420pF, giving a return loss of greater than 10dB and a sufficient bandwidth.

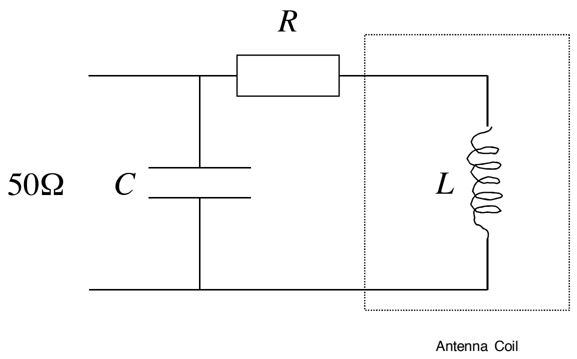


Figure 1 – Tuning of an NFC antenna for measurement

Knowing the loss caused by the introduction of the series resistance at 13.56MHz, which calculated to be less than 1dB and thus negligible, it is possible to ascertain the power and hence maximum current, *I* in the H-antenna, from which the magnetic H-field can be calculated by [5]:

$$H = \frac{I}{2r_{\text{ant}}} \qquad (1)$$

In the measurements, sufficient current was induced in the H-antenna using a signal generator and power amplifier (with pad attenuators for protection) in order to achieve fields up to 7.5A/m.

The first rogue antenna consisted of a 5m wire, comparable to a quarter wavelength at 13.56MHz, which was placed over the eavesdropper's body as illustrated in figure 2 and connected to a handheld spectrum analyser.

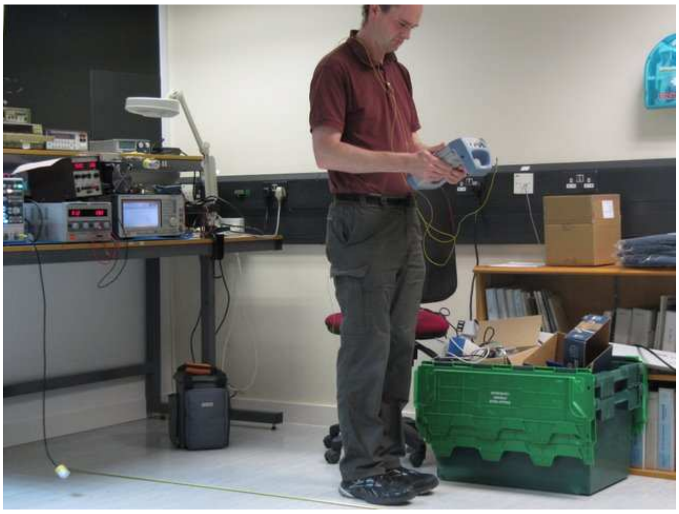


Figure 2 – Photograph of the measurement setup and eavesdropper wearing a rogue antenna

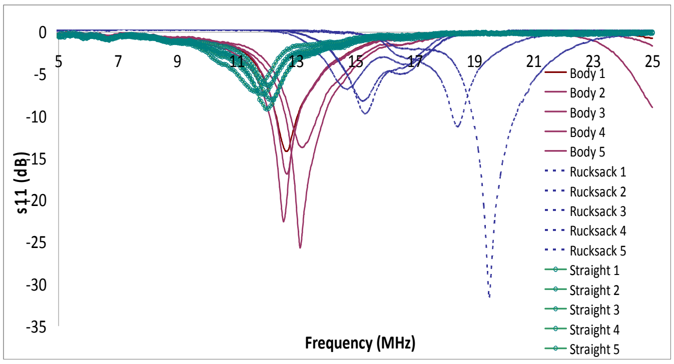


Figure 3 – Comparison of the reflection coefficient, s_{11} of a 5m wire on the body, a rucksack and laid on the ground

It is useful to study the vulnerability that such an antenna has with regards to de-tuning in different scenarios. Figure 3 illustrates such cases where the wire was mounted onto the body in five different ways, then secondly it was mounted to a rucksack in another five ways while finally it was laid straight on the floor in five different positions to evaluate how the reflection coefficient, s_{11}, measured with a network analyser, changes. Clearly it can be seen that in the case of the rucksack, the antenna is subject to much de-tuning and it is hard to keep its resonant frequency at a constant position. However in the case where the antenna is laid on the ground and round the body, there is little difference and thus the wire antenna can be considered to be more reliable when used in such a way. Though the antenna is not tuned to 13.56MHz for the ground case, a shorter wire could easily rectify this problem though it is not so practical to have a 5m long wire placed along the ground for eavesdropping purposes. The antenna being wrapped round the body of an eavesdropper is a more practical scenario where the tuning can be maintained, though undoubtedly efficiency will be compromised due to the water content of the body.

The second rogue antenna was that of a shopping trolley, which could represent any large metallic structure in proximity to a contactless payment terminal such as a basket or shelving. Whatever the structure, a structure with a resistor and a capacitor such as that in figure 1 can be connected to two points on the shopping trolley in close proximity as previous measurements show that it is the most inductive at such a point [3]. The inductance was, however higher at 0.5μH, requiring a resistance of 30Ω and capacitance of 180pF to get close to the required impedance match. However, this will of course bring a further receiving loss to the antenna with the higher resistance required, which will be around 4dB.

Finally the third antenna used more for purposes of comparison in the second set of tests was another inductive loop antenna similar to the one used as the transmit antenna.

III. Path Loss Measurements

The first set of path loss measurements are presented in figure 4 using a rogue antenna wrapped around the body. These results show how the received power from the spectrum analyser in dBm changes over distance when comparing 0.5A/m, 1.5A/m and 7.5A/m. Obviously for lower fields, the measured power levels fall below the noise floor of the spectrum analyser at a large distance. A minimal resolution bandwidth was also used in order to ensure maximum dynamic range of the measurements.

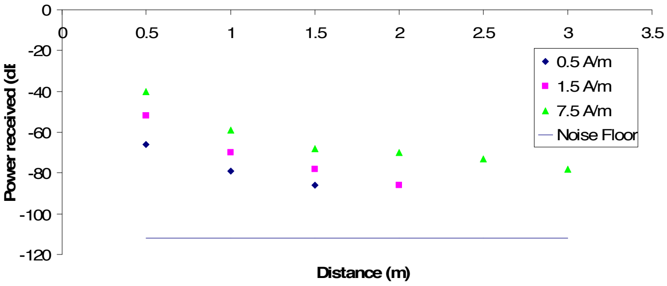


Figure 4 – Results comparing the propagation range against transmitted H-field

A -111.9dBm noise floor is also inserted as a base line since it is assumed that for NFC, with two subcarriers 847kHz either side of the 13.56MHz carrier, that an eavesdropper would require a system bandwidth of approximately 1.6MHz with such minimum noise floor. It should be noted however, that in practice the noise floor of any receiver will be higher than this, not only due to noise in the radio and the noise figure of the receiver amplifier, but other background noise radiated by nearby electrical devices and also broadcast signals in the high frequency (HF) band [3]. The degree of such interference is highly dependent location.

Concentrating on the 0.5A/m results, plotted in figure 5, further measurements are taken where they compare the power received versus distance but at different angles from the antenna, being 0° when directly in front of the loop of the H-antenna and at 45° and 90° where it is tangential to the loop. Clearly there is little change in the received power. Thus at any radius away from the H-antenna, the power decays with a $1/r^3$ proportionality as would be expected theoretically [5], where r is the distance from the loop.

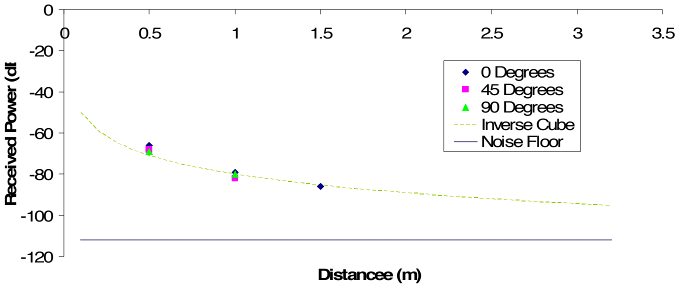


Figure 5 – Results comparing the propagation range against angle for 0.5A/m and comparison to $1/r^3$ curve

Similar measurements were carried out using a shopping trolley, though in this case, only H-fields of 0.5A/m, 1.5A/m and 4.5A/m were possible to carry out due to limitations of equipment used. Figure 5 shows the results of the measurements taken, where for 4.5A/m, the measurement was taken two times with the front of the trolley (where it was connected to the spectrum analyser) was facing the loop antenna, while in the second case the side of the trolley was facing the loop antenna.

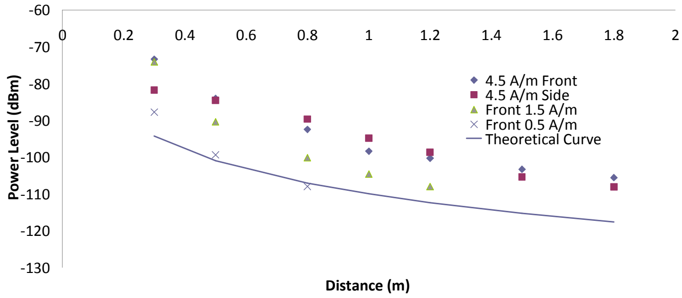


Figure 6 – Comparison of path loss for measurements taken using a shopping trolley

Measurements were out of dynamic range where the back of the trolley was facing the loop antenna. For 1.5A/m and 0.5A/m measurements to the side of the trolley were excluded because they were out of dynamic range to obtain a meaningful set of results. For the 4.5A/m measurements, orientation of the trolley has little effect, while reducing the H-field to 0.5A/m reduces the received power by as much as 20dB.

IV. Measurements with a Demodulator

The second set of measurements took a full evaluation of the distance at which a type A modulation from an NFC device, which uses OOK modulation at a rate of 108kbps, thus a square wave with a frequency of roughly 108kHz was chosen to represent such a signal and evaluate whether it is recoverable by use of an oscilloscope. The measurement setup is shown in figure 7, where a rogue antenna (a shopping trolley in the case illustrated) is matched to 50Ω and connected to a low noise amplifer, which is then further amplified together with a filter within the 1.6MHz bandwidth used in NFC, thus creating a representative noise floor with additional system noise from the low noise amplifier and the peak detector, which acts as the demodulator in the case of OOK. This form of demodulator was chosen as it will result in the least amount of additional noise, which would otherwise occur from demodulation using a mixer, where the local oscillator will have additional phase noise. The operational amplifer was only required for purposes of compensating out losses in the filter and increasing the signal to a level detectable by the peak detector.

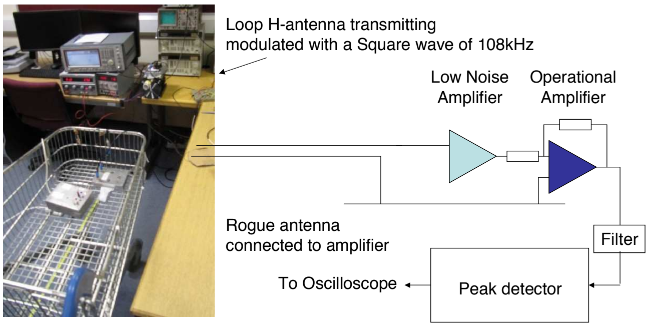
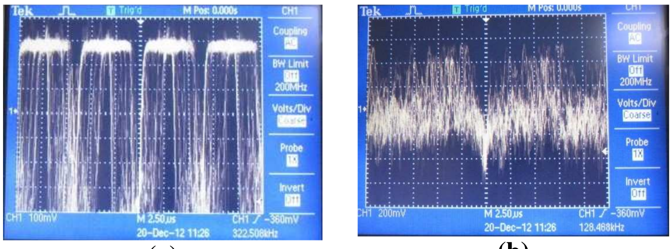


Figure 7 – Diagram of the measurement setup for measuring the range at which a type A NFC signal can be successfully demodulated

In carrying out the measurements, the output was observed on the oscilloscope with an output similar to those shown in figure 8 (a) where the output of the peak detector can be identified to detect the square wave rising from zero to 1 as would be expected in OOK. In the case where the rogue antenna was moved too far away from the transmitting loop antenna, only a noise floor as observed in figure 8 (b) resulted from which it was deduced at the maximum distance that any detection would be possible.



(a) **(b)**

Figure 8 – Illustration of the oscilloscope output for a case where the signal is (a) recoverable and (b) in the noise

The measurement was carried out for three different values of transmitted magnetic H-field, 0.5A/m, 1.5A/m and 4.5A/m with the wire antenna around a body, the shopping trolley and another inductive loop all directly facing the transmitting loop. In table 1 the distances at which detection failed by observing the output at the oscilloscope are listed. In the case of the wire antenna there was no success in obtaining any measurements at such bandwidths due to the body causing coupling to the ground, from which high background noise from the surrounding environment (-56.5dBm as measured by the spectrum analyser) was significantly higher than what was detected from the transmitting loop and thus no deducable signal could be output to the oscilloscope.

In contrast, the trolley was also subject to significant background noise though over 10dB less than the case of the wire around the body at -64dBm. This resulted in the possibility to detect using the trolley though for all three cases of transmitting H-field this distance was less than 0.5m due to the fact that the background noise was still significantly high.

Antenna	0.5A/m Dist (m)	1.5A/m Dist (m)	4.5A/m Dist (m)	Background noise (dBm)
Trolley	0.2	0.3	0.4	-64.0
Wire	-	-	-	-56.5
Loop	0.5	0.7	0.9	-91.2

Table 1 – Comparison of the measurement ranges where a demodulated square wave could be recovered and the background noise received by each antenna

Observing the measurements taken by the loop antenna, distances beyond 0.5m were possible to detect. Due to the significantly greater inefficiency of the antenna, the background noise was significantly lower down at -91.2dBm and since the transmitting loop and receiving loop were aligned, the signal to interference ratio compared to the other two antennas was substantially higher, thus allowing a longer detection range. It should be noted that these measurements were carried out in a laboratory environment, which will be subject to a range of background radiation both from broadcast signals in the HF band but also emissions from electrical appliances such as computers that were in the vicinity. Therefore in cases where background radiation is likely to be significantly lower (such as in underground locations) the higher efficiency of the other two antennas will be subject to a lower signal to noise ratio and the possibility of a longer measurement range. However, the results clarify that for retail outlets often based on ground level, the background radiation is significantly high enough that it will make eavesdropping from contactless payment terminals, or interrogation from a nearby distance, to be only possible at distances up to 0.5m using practical antennas and radio apparatus.

V. Conclusion

Results presented here show the first analysis of the propagation range of H-fields from NFC H-antennas using realistic designs of rogue antenna for eavesdropping. These results are limited to scenarios above or on ground level where the eavesdropper is subjected to high levels of background noise from nearby electrical appliances or HF broadcast signals. Clearly the presence of background noise is a good counter measure to prevent interrogation and eavesdropping of NFC devices, though it is certain that the risk is higher from more secluded locations, where there is less availability of background noise.

References

[1] G. Van Damme, K. Wouters, "Practical Experiences with NFC Security on Mobile Phones", *Workshop on RFID Security*, 2009.

[2] G. P. Hancke, "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens", *Journal of Computer Security*, IOS Press, 2011.

[3] T. W. C. Brown, T. Diakos, "On the design of NFC antennas for contactless payment applications", *European Conference of Antennas and Propagation*, 11-15 April, 2011.

[4] D.M. Pozar, "Microwave Engineering", Third Edition, Wiley, 2005.

[5] J. D. Kraus, D. A. Fleisch, "Electromagnetics with Applications", Fifth Edition, 1999, *Wiley*.