ON THE DESIGN OF NFC ANTENNAS FOR CONTACTLESS PAYMENT APPLICATIONS

T. W. C. Brown T. Diakos, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, GU2 7XH, UK. Email: t.brown@surrey.ac.uk, t.diakos@surrey.ac.uk

Introduction: The increasing interest in using Near Field Communications (NFC) technology [1] at 13.5MHz is growing rapidly in the area of contactless payments, as well as numerous other applications, between devices that are within 10cm distance apart. However, there is growing concern that the use of such devices for contactless payments invites problems with regards to using metallic objects in the vicinity of the two devices to act as "rogue" antennas, which eavesdrop information during a financial transaction is taking place. This paper presents aspects of designing H-antennas both for the two devices communicating while also identifying the means by which rogue antennas can be created by exploiting real life metallic structures. In this paper, a shopping trolley is taken as an example.

The first part of this paper will focus upon the design of NFC antennas for communication between two devices within proximity less than 10cm apart. Such example in the case of contactless payments would be a mobile handset communicating with a vending device, such as a ticket machine or credit card payment terminal in a café. Applying theory analysed for such antennas, the paper will then go on to analyse the potential use of a shopping trolley to act as a rogue antenna from which information could potentially be eavesdropped.

NFC Antenna Design Theory: A typical example of magnetic coupling loop antennas, otherwise known as "H-antennas", is illustrated in figure 1. The two ends of such an antenna are connected to a radio frequency (RF) transceiver with a capacitor placed across in parallel. The DC resistance at the input can be assumed to be zero while as the frequency increases, it will create an inductance such that a circuit model for such an antenna can be represented as that shown in figure 2 where the antenna is represented as an inductor [2]. The parallel capacitor is then connected to the load of the transceiver, which will in this case be assumed to be purely resistive. Were there to be a reactive component at the transceiver input, it can be easily cancelled out by applying a series negative reactance so therefore need not be considered.

Many publications in the literature assume the inductance to be constant over frequency, though observations from measurement using a network analyser find it to be the case that inductance will change at lower frequencies.

Figure 3 shows measured results using a vector network analyser, where the inductance reduces to a constant value after about 1MHz. Where the frequency is low, the loop is effectively resembling a short circuit where the inductance would be expected to fall to zero. However, due to precision required in such circumstances, an accurate value of inductance cannot be resolved. In this paper the inductance will be considered as frequency dependent and is therefore denoted, $L(f)$ or $L(\omega)$ where relevant, where f is the frequency and ω is the angular frequency equal to $2\pi f$. This will become more important when the inductance values for a rogue antenna are considered.

For any loop antenna to resonate, it is well known that the parallel capacitance to be applied can be derived as follows:

$$C = \frac{1}{(2\pi f_0)^2 L(f_0)} \tag{1}$$

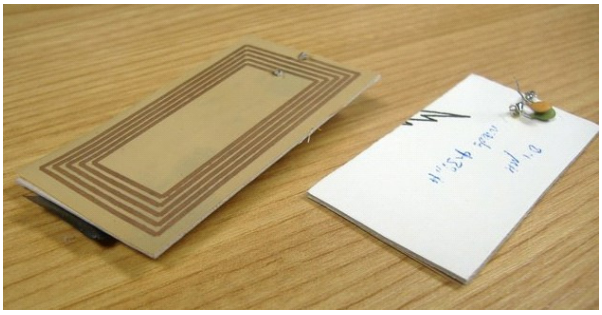

Fig.1: Illustration of tuned NFC antennas used in a contactless transaction

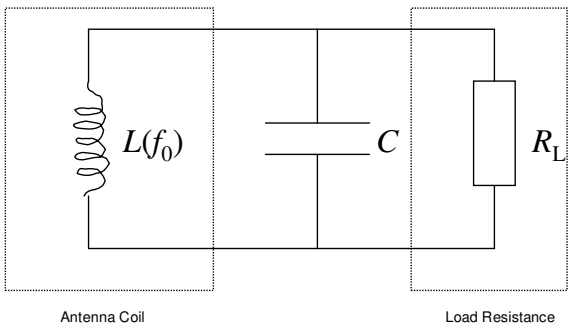

Fig.2: Circuit model of a H-antenna

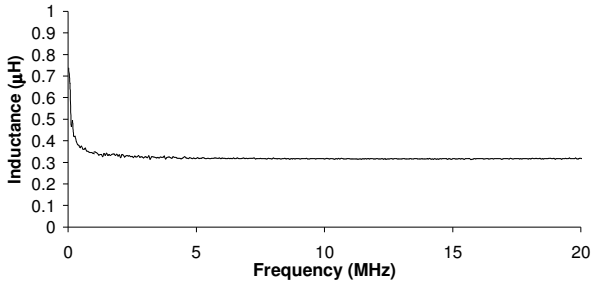

Fig.3: Measured values of inductance over frequency

At the resonant frequency, the transceiver connected to the antenna has a load resistance, R_L, where in receive mode it will have the following system frequency response function, based on the ratio of the load voltage, V_L, across the load resistance compared to the input voltage effectively resulting from the current flowing in the loop antenna, V_{in}, is defined as follows:

$$\frac{V_L}{V_{in}} = \frac{1}{1 + \frac{j\omega L(\omega)}{R_L} - \omega^2 LC} \tag{2}$$

One important point to realise from this is that maximum power transfer at the resonant frequency, ω_0, will reduce to:

$$\frac{V_L}{V_{in}} = \frac{R_L\sqrt{C}}{j\sqrt{L(\omega_0)}} \tag{3}$$

thus requiring a low inductance in order to maximize gain with as high load resistance as possible. The magnitude of this equation is also equal to the Q factor of the system, that will depend on a low value of L and a high value of R_L.

For transmit mode, the transfer function relating the voltage across the antenna, V_A, which is now a reactive load, to the source voltage, V_S, that is now in parallel with R_L, is as follows:

$$\frac{V_A}{V_S} = \frac{1}{jR_L\left(\omega C - \frac{1}{\omega L(\omega)}\right) + 1} \tag{4}$$

which by inspection shows that it will always have a value of 1 at the resonant frequency. The Q factor is derived in the same way, thus emphasising the need to design quality NFC antennas with low inductance and having a high load resistance at the transceiver.

Rogue antenna characteristics: A further point of interest is now to consider the ease with which a criminal would have the ability to use a large metallic structure as a rogue antenna which they would be able to connect a transceiver device from which data could be eavesdropped. The case of a shopping trolley is a useful example in this instance given that such an item could be positioned in close proximity to a ticket machine in a railway station from which a contactless payment transaction is taking place. Characteristics that were measured from this example case are likely to be similar for other metallic structures of such size.

The shopping trolley tested is illustrated in figure 4 where the trolley's characteristics were measured at four separate locations. In all four cases, the ground connection to the network analyser (i.e. the outer part of the coaxial cable) was attached to the same point on the trolley, while the inner core of the coaxial cable was connected to the four different locations. The "Near End" connection was made where the two ports were connected within close proximity to each other, the "Leg End" connection was to the bottom of the leg of the trolley while the "Middle End" and "Far End" connections of the trolley were considering the middle point and furthest point at which a connection could be made. In all cases, some extra wire was required to enable the connection to be made and in all cases the effect of this wire was not calibrated out of the measurement because this would in the real case be considered as an integral part of the rogue antenna. Another point worthy of noting is that it was necessary to use a file to take off a waterproof coating where the connection was made so that a valid measurement could be taken. These four test positions therefore give a good overview of how the characteristic change when a large metallic structure is used.

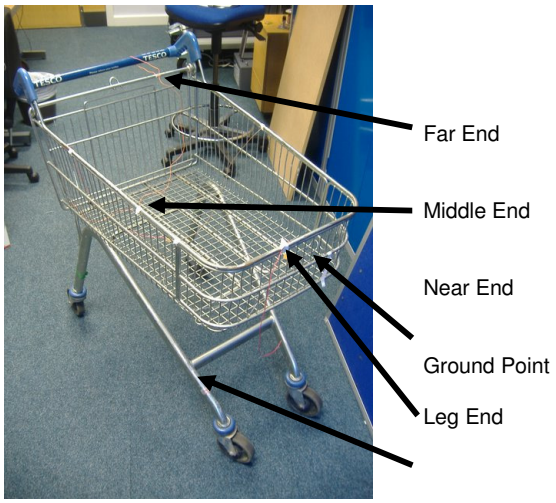

Fig.4: Photograph showing the positions on a trolley for measurement.

It was found that for all the measurements taken, the resistance was not negligible unlike a typical NFC antenna, though in all cases the trolley was inductive. The inductance and resistance as a function of frequency are plotted in figures 5 and 6 respectively. At low

frequencies the resistance is negligible since the characteristics are moving closer to that of what would be expected for direct current (DC). As frequency increases to 13.5MHz, the resistance begins to rise, and is particularly high for the "Leg End" case while also the inductance is increasing. This would be expected since the connection enables the highest possibility of parasitics to occur thus having significant impact on the input impedance at the trolley connectors. If measurements were to be taken beyond 20MHz, there is inevitably going to come a point where the trolley is a capacitive load as would be expected with large loop antennas. Though the trolley is not a large loop antenna, such an antenna is a useful model case from which to justify that at such frequencies as 13.5MHz, with a wavelength of 22.5m, the size of the trolley will still have a loop size less than 0.15λ, where λ is the wavelength [3]. Were significantly larger structures above 2m in any dimension to be considered then it is likely a capacitive antenna may result.

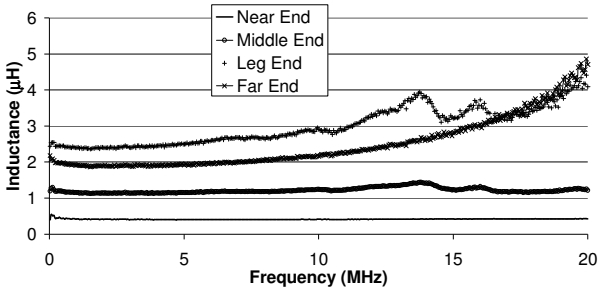

Fig.5: Measured values of inductance over frequency for different positions on the trolley.

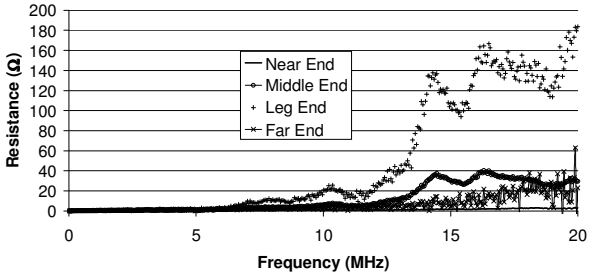

Fig 6. Measured values of resistance over frequency for different positions on the trolley.

Scenario	Inductance at 13.5MHz / μH	Resistance at 13.5MHz / Ω
Near End	0.42	1.31
Middle End	1.42	18.48
Leg End	3.73	70.66
Far End	2.59	7.67

Table 1: Comparison of the inductance values at 13.5MHz for the four test case scenarios.

The values of inductance and resistance for the frequency of interest, 13.5MHz, are shown in table 1. Clearly the values deviate significantly, which will likewise influence the potential of the antenna if it were to be connected at different locations. A new analysis of the antenna's transfer function in receive mode is therefore necessary and a modified circuit diagram is shown in figure 7. In this case, the trolley has inductance, $L_T(f_0)$, with a resistance, $R_T(f_0)$, both of which are dependent on frequency.

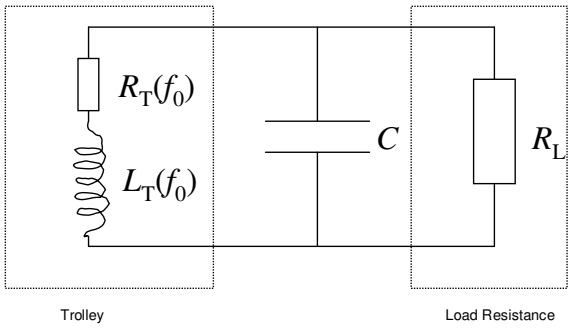

Fig. 7 New circuit representation for a trolley or large metallic object being applied as a rogue antenna.

Given that it is only of interest to consider the rogue antenna in receive mode, the ratio of load voltage to input voltage will can now be derived as follows:

$$\frac{V_L}{V_{in}} = \frac{1}{1+\frac{j\omega L_T(\omega)}{R_L}+j\omega C R_T(\omega)+\frac{R_T(\omega)}{R_L}-\omega^2 LC} \quad (4)$$

Note that the equation reduces to the original one when R_T is zero. Also at the resonant frequency, the equation becomes the following:

$$\frac{V_L}{V_{in}} = \frac{R_L}{\frac{j(L_T(\omega_0)+R_T R_L C)}{\sqrt{L_T(\omega_0)C}}+R_T(\omega_0)} \quad (5)$$

Therefore a high value of R_L would still be desirable at the receiver though clearly high values of R_T are going to be a disadvantage and effectively act as a damper to the resonant system. To determine the level of Q that would be attainable by a rogue antenna, the values of $L_T(f)$ and $R_T(f)$ have been analysed using equation (4) from which a transfer function versus frequency for the four measurement cases can be output. The data output from this is shown in figure 8 where a load resistance of 1000Ω was chosen and for each of the four cases the capacitance was calculated corresponding to the inductances at 13.5MHz shown in table 1. The dependence of $L_T(f)$ and $R_T(f)$ on frequency will inevitably have impact on the Q factor, while also higher values will degrade the system gain. Clearly the Q is significantly for measurements other locations other than the Near End scenario. Even though a high Q can be

obtained using a small parallel capacitor (which could be fine tuned as a variable capacitor) the trolley does not by any means represent an ideal loop antenna. In fact the feed in effect has a shorting line across it, which means that inevitably the current distribution will be concentrated largely around the feed.

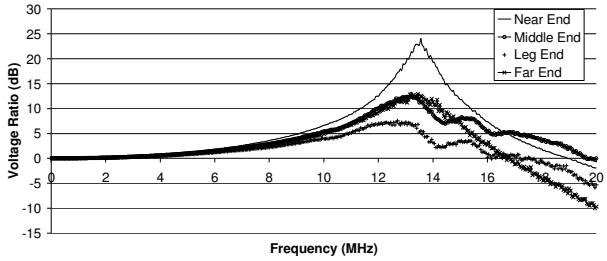

Fig. 8 Comparison of the resultant Q for the different positions on the trolley.

Discussion of the feasibility of building a rogue antenna: This paper has identified that connecting a receiver with high resistance to a metallic device such as a shopping trolley will provide a high Q and as such if the receiver should be connected anywhere, the two ports should be in close proximity. To the criminal, this is a huge advantage because they will have the ability to discretely connect their receiver to a metallic structure using crocodile clips or other means and have the highest chances of achieving eavesdropping. Furthermore it will only require them to adjust a variable capacitor connected in parallel so as to tune the rogue antenna from which a simple device could measure a suitably large Q. A large load resistance has been assumed in this paper because an operational amplifier can be readily used at 13.5MHz, which is assumed to have high input impedance that can be considered a virtual ground **Error! Reference source not found.**. Therefore a criminal has the means to cheaply buy equipment to act as an RF receiver, from which the carrier can be demodulated and then processed at baseband with relatively low cost electronics that can be held within a small rucksack.

Though it would be relatively simple to create the rogue antenna, its reliability is still subject to the efficiency it will have once deployed. Given the high gain of operational amplifiers, however, this lack of efficiency can still be compensated. There are only two major disadvantages that could create difficulty with regards to eavesdropping:

1. The path loss at this frequency and using such antennas is proportional to $1/r^3$, where r is the distance from the source. Therefore the received power will decay rapidly, which would be problematic when using a rogue antenna that is not within a few metres since the allowed transmitted power would begin to hit the noise floor at any further distances.
2. The trolley itself is susceptible to noise, particularly from the wide metallic structure that could mean significantly more noise power is received by the rogue antenna than by the eavesdropped signal. This will be particularly the case where the rogue antenna is in the vicinity of other electrical equipment and therefore it an item of further work to see the potential scale of such noise from a rogue antenna.

Conclusions: The underlying theory behind design of NFC antennas has been presented, with particular interest in the potential use of a shopping trolley to act as a rogue antenna to eavesdrop information a contactless payment using NFC. While it has been shown that building of a rogue antenna with receiver amplifier is relatively simple and low cost, the susceptibility that such a system has to background noise is likely to be the highest obstacle to overcome for a successful eavesdrop.

REFERENCES

[1] NFC Forum, http://www.nfc-forum.org/aboutnfc/

[2] Z.N. Chen et al. "Antennas for Portable Devices", 2007, *Wiley*, UK.

[3] C. A. Balanis, "Antenna theory, Analysis and Design", 3rd Edition, 2005, *Wiley*, USA.

[4] P. Horowitz, W. Hill, "The Art of Electronics", 2nd Edition, 2006.