Eavesdropping near-field contactless payments: a quantitative analysis

Thomas P. Diakos[1], Johann A. Briffa[1], Tim W. C. Brown[2], Stephan Wesemeyer[1]

[1]*Department of Computing, University of Surrey, Guildford GU2 7XH, UK*
[2]*Center for Communication Systems Research, University of Surrey, Guildford, GU2 7XH, UK*
E-mail: t.diakos@surrey.ac.uk

Published in *The Journal of Engineering*; Received on 22nd August 2013; Accepted on 11th September 2013

Abstract: This paper presents an assessment of how successful an eavesdropping attack on a contactless payment transaction can be in terms of bit and frame error rates, using an easily concealable antenna and low-cost electronics. Potential success of an eavesdropping attack largely depends on the correct recovery of the data frames used in the ISO 14443 standard. A near-field communication inductive loop antenna was used to emulate an ISO 14443 transmission. For eavesdropping, an identical inductive loop antenna as well as a shopping trolley modified to act like an antenna were used. The authors present and analyse frame error rates obtained with the authors equipment over a range of distances, up to 100 cm, well above the official maximum operating distance depending on the magnetic field strength.

1 Introduction

Contactless transactions ranging from access control and ticketing [1, 2] to financial payments [3, 4] are becoming increasingly popular in Europe, Asia and the United States. It is estimated that there are at least 23 million such contactless cards in circulation in Britain [5] and mobile devices equipped with near-field communication (NFC) account for 13.32% of worldwide web traffic [6]. The idea is that for relatively low values the point of sale (POS) may not need an online transaction approval, making contactless an attractive solution for transactions that need to happen quickly, such as ticketing and low-value payments. Reasons for this rise in popularity include the promotion of contactless cards by banks and the decision of popular mobile phone manufacturers to equip their handsets with NFC technology [7]. Big players in electronic payments such as VISA [8], Mastercard [9] and Google [10] have already developed platforms for contactless payments.

There is, however, a growing concern about the security risks. Vulnerability to skimming attacks, where an attacker extracts information from the victim's contactless device without him realising have been identified in [11]. Additionally, the ISO 14443 standard states that a contactless card should respond to any device generating a magnetic field capable of powering it up. Based on this, an attacker could build a rogue transmitter that could power up and interrogate the target extracting information such as the unique identifiers (UID) [12] that could be used as means of tracking the owner of the target device. Skimming attacks are not the only potential threat to contactless systems. There is also the threat of relay attacks, which involves activating the victim's card from a distance and transmitting the probed information to a legitimate reader to complete a transaction [13]. Google's Wallet application, despite being in its infancy, has already been put under scrutiny in [14] in the context of relay attacks. Finally, eavesdropping, where the attacker attempts to listen in on an ongoing transaction between a contactless device and reader, has already been demonstrated as a possible attack on contactless cards. In [15, 16], eavesdropping on contactless communications from distances well over 20 cm was shown, invalidating the claim that the operating range of high frequency (HF) radio frequency identification (RFID) is within the near field only.

However, published results show a wide variety of eavesdropping distances. This, to some extent, can be attributed to the different experimental set up each researcher used. In [16], an off-the-shelf receiver and eavesdropping antenna were used on a Philips Mifare token and the attacker observed uplink communication (token to reader) on an oscilloscope from up to 4 m. What is unclear, although, is how much of the originally transmitted data can be recovered from the signal observed on the oscilloscope. In [17], raw signals were observed from up to 6.5 m using a single 1 m loop as an eavesdropping antenna, but there is no mention of any specific details on the receiver set-up. A reader generating a measured magnetic field of 3.1 A/m and an ISO 10373–6 compliant smartcard were used. Eavesdropping was carried out with single-loop antennas with diameters of 30 and 50 cm. Respectively, binary data were recovered from up to 3.5 m. In [18], a similar signal processing approach was used along with commercially available receiver and receiving antenna to recover binary data from 1 to 3 m depending on the environment in which the attack was carried out. In [19], theoretical work was shown that aims to give a measure of eavesdropping success given a certain distance in the form of achievable bit error rates (BER). A variety of noise environments were modelled, but no practical results were given. Bit recovery in [19, 20] was achieved using synchronous demodulation (i.e. a coherent receiver) in software. In [17], on the other hand, no bit recovery was attempted. In [19], it was shown that there is a 15% difference in performance between a coherent demodulator and a non-coherent one.

All previously listed attacks achieved a range of eavesdropping distances from 1 to 6.5 m. This variation can be attributed to the different equipment and operating conditions. What is missing, although, is practical results showing how reliably eavesdropping can be carried out, quantifying how much of a transmitted sequence can be recovered at the eavesdropping end at various distances. Measurements from [16–20] relied on often expensive or bulky equipment that cannot be easily replicated in a portable system. In our paper, we determined how reliably information from an ISO 14443 Type A device could be recovered by an eavesdropper, in a way that could be used to obtain sensitive information from the victim using a covert antenna and low-cost electronics. Emphasis was on frame error rate (FER) as in order to recover meaningful information that could lead to compromising a victim's financial security or privacy, data need to be recovered in the form and structure that was originally transmitted.

2 System description

2.1 Transmitter

An NFC device can operate in three modes. In peer-to-peer mode as specified in ISO 18092 [21] where such devices can exchange data files (e.g. images) or set up a wireless link between them. Additionally, an NFC device can also operate in reader/writer

mode, also known as proximity coupling device (PCD). The PCD is acting as the reader that generates the electromagnetic field required to power passive transponders $f_s = 13.56$ MHz which in turn responds by load modulating the carrier signal with a $f_s = f_c/16 =$ 847 kHz subcarrier. In PCD mode, an NFC device is able to read passive poster tags [22] or contactless smartcards. Finally, the last mode of operation is that of contactless smartcard emulation. In this mode, the NFC device assumes the role of a smartcard typically used for contactless payments or ticketing applications. Implementation of this mode is dictated and governed by the ISO 14443 standard, where two types of smartcards (referred to as proximity integrated circuit card or PICC) are specified, Type A and Type B. For the purpose of our work, we chose to concentrate on smartcard emulation mode because this is the de facto mode for contactless payments used today on the high street. We also chose to focus on Type A emulation as this is the most common type used in contactless payments. From this point forward, when we refer to the standard, we mean the ISO 14443 standard.

In order to be able to measure the FER of an eavesdropping attack, the transmitted data need to be known at the receiving end. To accomplish this, standard compliant frames were generated in software. We chose to transmit only PICC frames because we wanted to focus on studying the uplink communication because this is more likely to contain information useful to an attacker. The standard states that for data exchange between devices, frames referred to as 'standard frames' are to be used. These frames are longer than the 'short frames' used to initiate and establish communication. As our emphasis is on obtaining sensitive information from the PICC, only 'standard frames' were transmitted. Each 'standard' frame consists of $9n$ bits (8 data + parity bit for each of n bytes) along with the start of frame (SOF) and end of frame (EOF) bits. SOF is a Manchester encoded binary '1' and the EOF is specified as an unmodulated carrier with a duration equal to 9.44 µs. After examining the trace file of a financial contactless transaction, we found that the majority of standard frames were between 40 and 80 bytes long. For this reason, we chose to use a 'standard' frame size of 60 bytes. A random binary sequence was generated and Manchester encoded as per standard guidelines shown in Table 1. The 847 kHz subcarrier was generated in software using an external trigger signal at 1.7 MHz. This frequency was chosen to ensure we would have at least two samples for each subcarrier cycle. This sampling frequency resulted in each modulated bit consisting of 16 samples and having a duration of 9.41 µs. The standard specifies the bit duration as $128/f_c$ and abbreviates it to 9.4 µs. The process of encoding the baseband signal and then on-off keying (OOK) modulating it on the subcarrier is illustrated in Fig. 1.

At the end of each frame, an extra 160 guard samples, equivalent to 94.1 µs, were inserted. This was done to meet the requirement of at least 86.4 µs between the last transmitted PICC frame and the next PCD response, with the carrier field being on for the whole duration. The transition delay between two PICC frames transmitted consecutively is illustrated in Fig. 2.

Table 1 ISO 14443 type A modulation

	PICC–PCD	PCD–PICC
modulation	OOK modulated 847 kHz subcarrier, load modulated carrier	100% ASK
baseband	Manchester code	modified Miller code
synchronisation	SOF, EOF bits	SOF, EOF bits

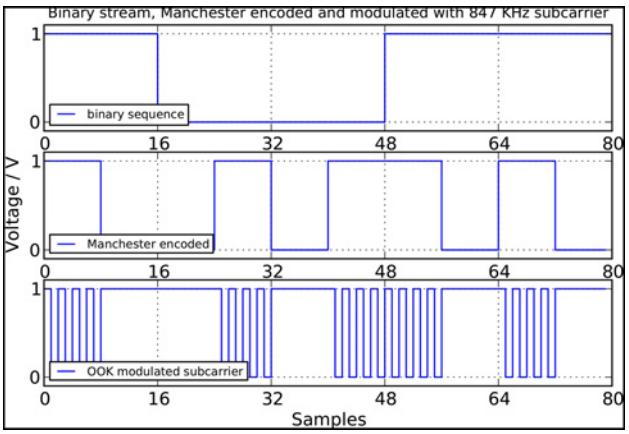

Fig. 1 *Sequence of 5 bits, Manchester encoded and then loaded onto the 847 kHz subcarrier*

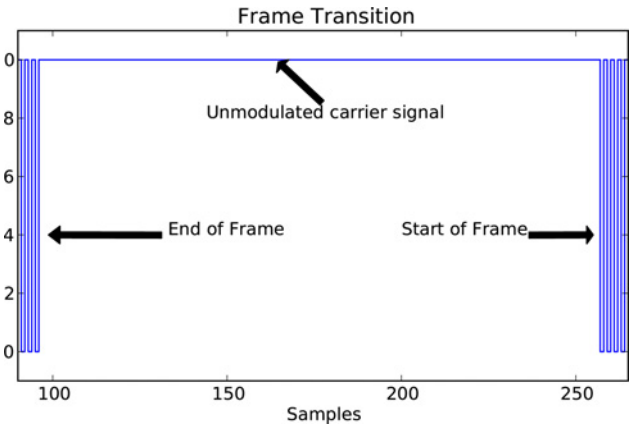

Fig. 2 *Transition between two PICC frames*

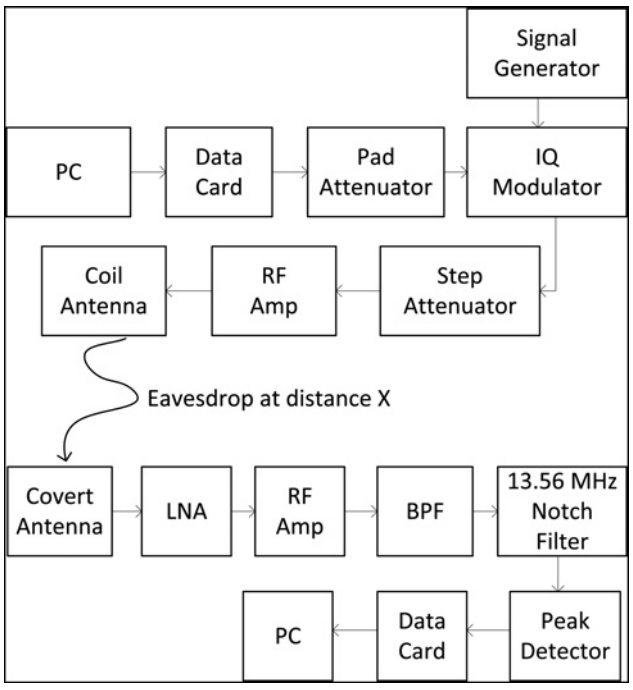

Fig. 3 *Transmitter and receiver arrangement*

J Eng 2013
doi: 10.1049/joe.2013.0087

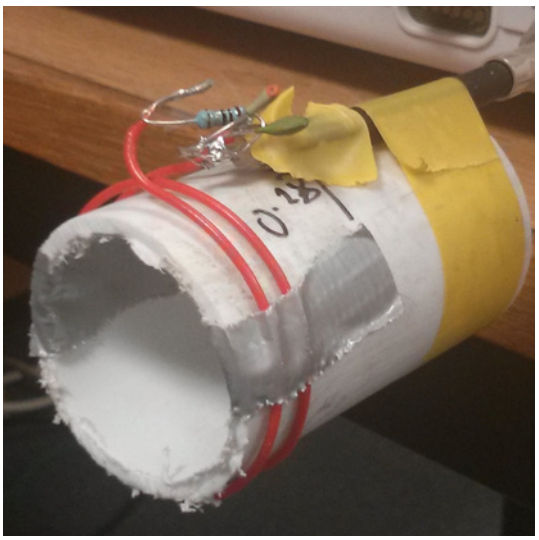

Fig. 4 *Loop antenna used for transmission and reception*

For the transmission and reception of our frames, the arrangement shown in Fig. 3 was used. The subcarrier modulated output of the data acquisition (DAQ) card was passed to an IQ modulator for modulation with the carrier signal at 13.56 MHz. An attenuator in-between was used to control the baseband voltage at the input of the modulator. A signal generator was used to generate the 13.56 MHz sinusoidal carrier and the resulting modulation was 100% ASK (OOK). In order to obtain enough current at the transmit antenna to transmit the standard specified magnetic field (1.5–7.5 A/m), an RF amplifier was used along with a step attenuator to control the magnetic field strength. Our work in [23] showed that eavesdropping distances vary significantly based on the H-field strength. Unlike the work shown in [17, 18], with our arrangement the strength of the H-field was fully adjustable and not dependent on a given commercial PCD device. This is an important alteration since the generated H-field strength is at the discretion of the PCD's manufacturer, as long as it is within the broad range specified by the standard. For transmission, a single-loop cylindrical antenna similar to the one that could be found in an NFC device was used, shown in Fig. 4. However, unlike conventional NFC antennas, the inductive loop was matched to 50 Ω to be compatible with the power amplifier. The match was achieved using a low-value series resistor and parallel capacitor, which ensured minimal loss [24]. The antenna's resonant frequency was at 13.56 MHz with a bandwidth of 2 MHz to include the modulation sidebands.

2.2 *Hardware receiver*

Two antennas were used for reception that are easily concealable, unlike in previous work that relied on either commercial products [18] or large diameter antenna [17] that would make covert eavesdropping impractical. For further details on the design of the eavesdropping antennas refer to [23, 24]. The eavesdropped signal was fed to an LNA (to maximise signal-to-noise ratio (SNR)) and then another RF amplifier followed by a bandpass and notch filters to suppress side band noise and the unwanted 13.56 MHz carrier, which can be up to 90 dB higher than the PICC's response [25]. The second RF amplifier was used to compensate for the losses because of the two filters. This ensures that the peak detector used for Type A demodulation will be able to distinguish the modulating sidebands without interference from the carrier.

Although, in theory, a coherent receiver offers superior performance, its implementation is not straightforward. If done in hardware, in order to maintain phase synchronisation, a PLL circuit is needed which would increase the complexity of the design significantly. Without phase lock there would be intersymbol interference (ISI) caused by the difference in phase between the local clock and the received carrier [26]. If, on the other hand, a software implementation is used as in [20], the necessary high-speed sampling would increase data and processing requirements considerably. For example, Hancke in [18] used a (coherent) hardware receiver which mixed the eavesdropped signal up to 30 MHz which was captured at 100 MS/s for just 320 ms. This is not a compact or portable solution and high-speed sampling equipment is very expensive. One could replace our DAQ card with an field programmable gate array (FPGA)-based solution at reasonable cost and end up with an eavesdropping kit small enough to fit in a backpack or briefcase. In order to obtain accurate error rates, we transmitted a long series of frames. At 100 MS/s with 16-bit sampling, this would require approximately 112 GiB. By implementing a non-coherent receiver in the form of a logarithmic amplifier [27] acting as a peak detector, we were able to overcome the above limitations.

2.3 *Software decoder*

The output of the peak detector was captured on the analogue input of the DAQ card at 1.7 MHz. Decoding of the eavesdropped data were done offline. The idea was that the attacker would capture a number of transactions and then decode them later.

As the eavesdropping distance gets longer or background interference gets stronger, the SNR will reach a point where the captured samples can no longer be decoded without further software processing. The top half of Fig. 5 shows the effect noise has on the transmitted data. The vertical line indicates the SOF, with anything before that being just an unmodulated 13.56 MHz carrier signal, emulating the PCD's magnetic field. In order to minimise the impact of noise, we chose to use the variance of the captured samples as a way of achieving frame synchronisation. The nature of Manchester encoding ensures that the variance of the carrier signal loaded with an encoded subcarrier will always be higher than that of the carrier corrupted by AWGN.

A sliding window of length 32 samples (2 bits) was used to compute the variance of the captured samples. The reason this particular size was chosen is illustrated as follows: a binary sequence is first Manchester encoded and then modulated with the 847 kHz subcarrier. Owing to the nature of Manchester encoding, a sequence of '1 0' or '0 1' will always cause a dip in variance after Manchester encoding because of the prolonged lack of state transitions since '1 0' → '1 0 0 1' and '0 1' → '0 1 1 0'. With a sliding window of 16 samples during the occurrence of these two sequences, the variance drops to a minimum between samples 0–16 and 64–80 falsely indicating a SOF/EOF. With a window of 32 samples, this problem is avoided. This is illustrated in Fig. 6.

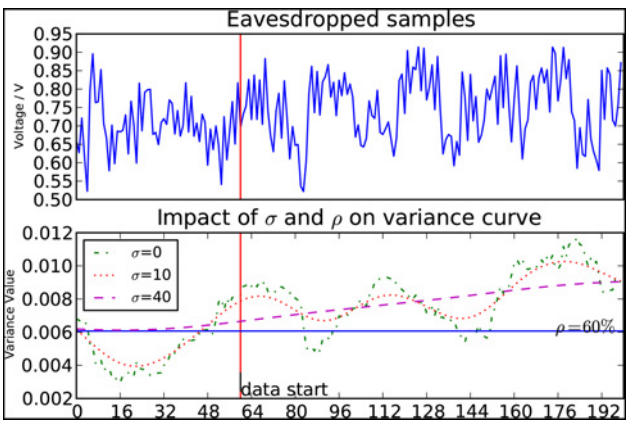

Fig. 5 *Variance smoothing and threshold*

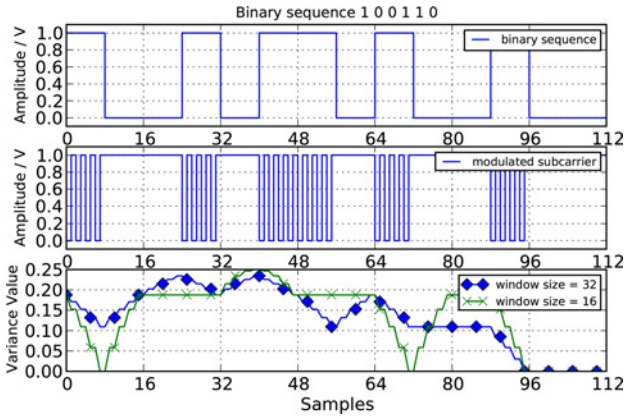

Fig. 6 *Variance window size*

This approach provides us with preliminary frame synchronisation by detecting the sample positions where a drop in variance above or below a certain threshold value occurs. We define this threshold, ρ, as a fraction corresponding to a value between the most frequent high and low variance values. Crossing ρ signals the start and end of a frame.

Fig. 5 illustrates another problem that we faced. When the SNR becomes low enough, the variance of the captured samples can still falsely dip below $\rho = 60\%$. This value of ρ was chosen because after some preliminary testing, we found it to be performing consistently well for a variety of SNR. In this example, data start at sample 60 and continues until the end of the plot. In order to solve this problem of false dipping, we applied Gaussian smoothing to the variance curve. The degree of smoothing was determined by, σ, the standard deviation for the Gaussian kernel. The lower half of Fig. 5 illustrates the effect of different σ values. With no smoothing ($\sigma = 0$), the variance curve crosses ρ between samples 80–96 and 130–150 causing the software to interpet this as three different frames when only one was transmitted. With $\sigma = 10$, the variance curve stays above ρ. Owing to the length of the sliding window being equal to 32 samples (2 bits) the variance curves cross the threshold 16 samples (1 bit) earlier than where they should had done, but since this is a constant difference it is easily addressed by adding an offset of 16 samples to the variance detected frame start positions. In the case of $\sigma = 30$, this applies excessive smoothing causing the variance curve to never fall below the value of ρ and consequently the SOF.

Robust frame synchronisation is achieved with a combination of cross-correlation and frame length check. Frames start with a set SOF sequence and end with an EOF sequence as defined in the standard. The SOF being a Manchester encoded binary '1' would cause the variance to rise and cross ρ. This position plus 16 samples (the offset mentioned earlier because of the chosen window size) give us the SOF position. The EOF, being an unmodulated carrier, is a bit trickier to accurately detect. For this reason, a frame length check is used. According to the standard, the shortest possible frame is a 'short frame' consisting of seven data bits and the SOF/EOF markers. Given our sampling rate of 1.7 MHz, such a frame would have a length of 144 samples. However, a 'short frame' is only used for a few commands. The standard specifies that 'standard frames' are used for the rest of communication. Such frames consist of $9n$ bits (8 data + parity bit for each of n bytes) along with the SOF and EOF markers (each being 1 bit long) with each bit encoded as 16 samples. Based on this, the shortest possible standard frame ($n = 1$) will consist of $(9 \times 16) + 32$ samples. Since we are able to accurately detect the SOF, the correct EOF is found by adjusting the rough frame end position until the resulting frame length minus the length of SOF/EOF markers is a multiple of 144. Manchester encoded bits are decoded using a cross-correlator and the FER is finally computed.

3 Experimental set-up

The aim of our work was to determine the reliability with which an eavesdropper could recover information from a contactless payment based on the ISO 14443 standard. To do so, some known frames had to be transmitted according to the specifications detailed in the previous section and eavesdropped at the receiving end. In order for our results to be reliable, a number of frames had to be transmitted that was large enough to allow sufficient errors to occur. As we also wanted to simulate different power levels for an eavesdropping distance of 20–170 cm hence requiring a lot of experiments to be carried out, we chose to transmit 5000 frames. This number was large enough to cause errors and at 20 minutes per run allowed us to finish a set of experiments in a single day.

In order for the results to be entirely based on the capabilities and performance of our receiver design, we wanted to experiment in a controlled environment. By running our experiments inside an anechoic chamber, we ensured that no external interference was affecting our results. Most of the equipment was kept outside the chamber and an RF cable was used to feed the signal to the transmitter antenna inside the chamber. This approach allowed us to avoid any risk of cross-coupling between measurement equipment. Tests were conducted to verify such coupling was not present. Fig. 7 illustrates the whole arrangement. Inside the chamber, the transmitting antenna was kept at a fixed position. The receiving antenna connected to the receiver circuit (Fig. 8) was moved at various distances, in increments of 5 cm. Power levels resulting in H-field strength of 1.45, 3.45 and 7.45 A/m were used. These values allowed us to emulate the minimum, maximum and in-between values of what is specified in the standard.

For reception, two different antenna designs were used. The single-loop cylindrical antenna shown in Fig. 4 and a shopping trolley [22]. The trolley was positioned 2–30 cm away from the transmitting antenna. Once all captures were completed, they were processed offline. A first set of experiments was performed with 500 transmitted frames. This was carried out to determine a suitable pair of σ and ρ within reasonable time. Eavesdropped data at each distance and H-field strength was processed with a

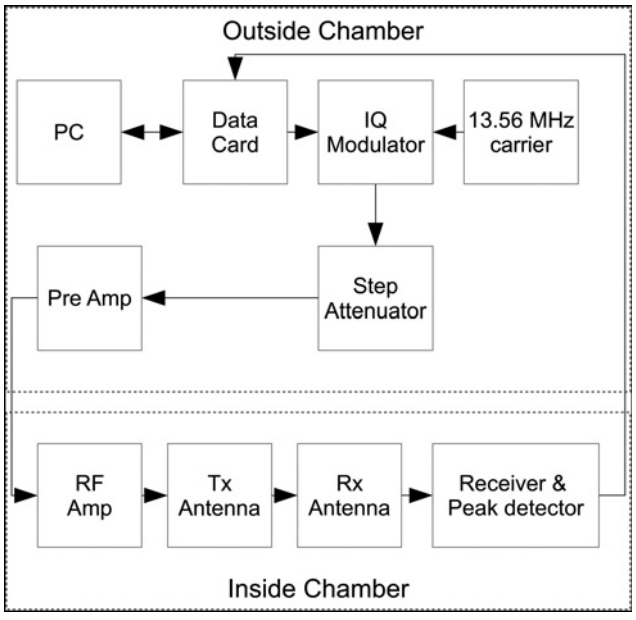

Fig. 7 *Experimental set up*

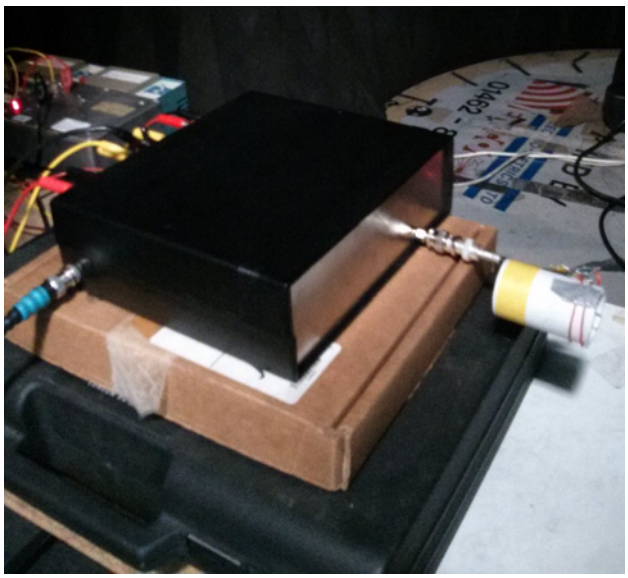

Fig. 8 *Receiver circuit and eavesdropping antenna*

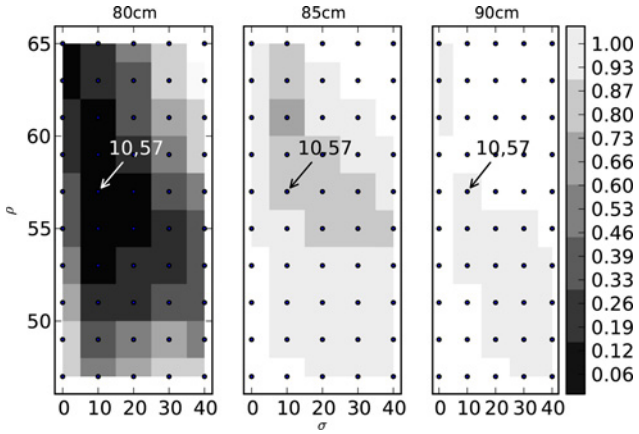

Fig. 9 *7.45 A/m 85 cm σ and ρ selection*

range of Gaussian smoothing factors, with σ in the range of 0–40, and ρ in the range of 49–65. Error rates obtained were then plotted as shown in Fig. 9. This was done to determine whether a single pair of σ, ρ values could be used at all distances and H-field strengths. Empty spaces on the pseudo-colour plots indicate instances were no frames were detected at all or frames were received at a length that was not a multiple of the 'standard frame' size as described earlier.

We found that $\sigma = 10, \rho = 57$ gave consistently good results. We took the worst-case scenario, for example, the furthest distance at a particular H-field strength that we could eavesdrop and looked for a pair there that worked at all distances regardless of the H-field strength. This pair was not always the ideal choice, for example, at 85 cm $\sigma = 10$ and $\rho = 61$ gave a lower FER. However, this set of values performed consistently well across all distances. Establishing this pair of values is important because the attacker will not have knowledge of the eavesdropped H-field strength or distance, let alone the current SNR.

4 Results

All results presented in the following section are for transmissions of 5000 frames. Experiments were performed on two separate days to ensure that our results were reproducible. Experiments confirmed that eavesdropping distance depends on the transmit power and the resulting H-field strength. Distances achieved were between 20 and 90 cm in the case of the maximum H-field strength (7.45 A/m). From our own work with commercial PCD devices, mobile phones and ISO 14443 Type A smartcards by various manufacturers, we found that the generated H-field varies drastically from product to product. It is not unrealistic for a victim's device that is <1 cm away from a PCD to generate a high H-field up to the maximum 7.5 A/m to ensure reliability for a transaction.

FERs that were achieved with various H-field strengths and eavesdropping distances are illustrated in Fig. 10. To ensure the consistency and reliability of our results, experiments were repeated on a second day. In the case of 3.45 A/m, an experiment on a third day was also performed. Using normal approximation, interval levels with 95% confidence were also plotted for each result. Even with the minimum H-field, reliable eavesdropping was possible up to 40 cm. This is still a distance an attacker could easily find himself from his victim without raising any suspicion. For example, this could be the case in a crowded underground station or at the checkout queue of a supermarket. Another interesting finding is the rate at which the FER degrades after a certain point. It can be seen that FER increases very sharply in the space of 5–10 cm regardless of the H-field strength.

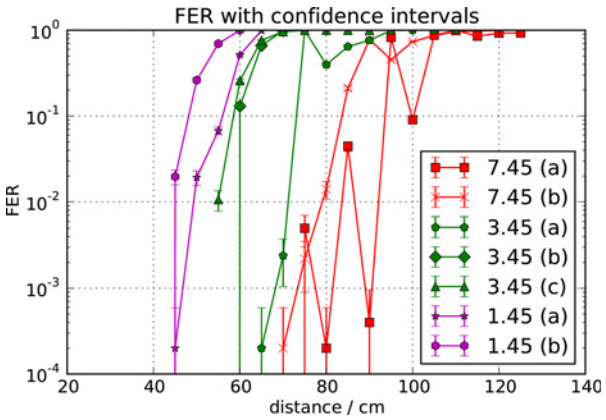

Fig. 10 *Summary of FER results with σ = 10 and ρ = 57*

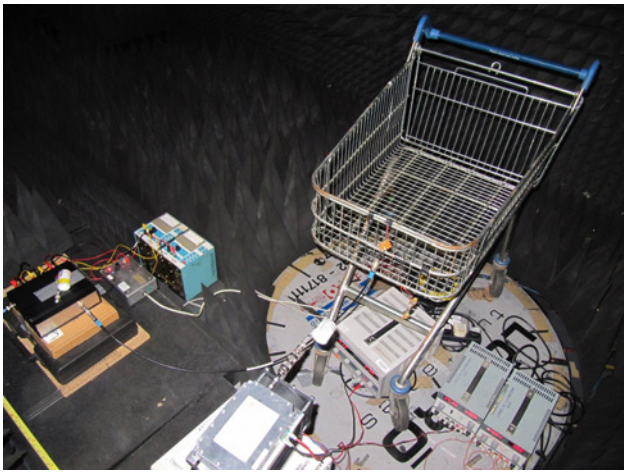

Fig. 11 *Shopping trolley eavesdropping arrangement*

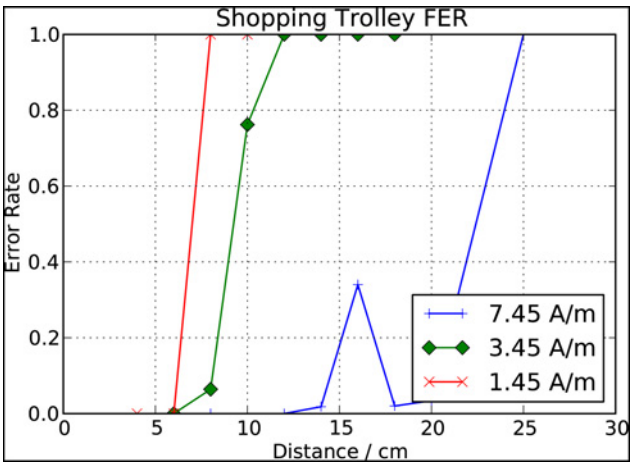

Fig. 12 *Shopping trolley FER with ($\sigma = 10$ and $\rho = 50$)*

Based on the results shown in Fig. 10 achieved FERs vary to a small extent. FER for 1.45 A/m remained consistent and reproducible through all of the experiments. A 7.45 A/m on the other hand was less consistent as can be seen from the first run at that field strength. We attribute this to the fact that as the eavesdropping distance gets longer, correct alignment of the two antennas becomes more difficult to accomplish and at the same time it has a much greater impact on the results. The reason for this behaviour is the very low SNR at these distances, so even the slightest deviation has a big impact. For 3.45 A/m, with the exception of the first experiment the rest returned nearly identical results. We also experimented with the shopping trolley (Fig. 11) to see whether a large metallic structure such as a trolley or metallic shelving found in an environment where eavesdropping is likely to happen could have any effect. The key difference compared with our inductive loop is that the trolley is a lossy antenna [24], and generates its own noise. This lowers the SNR and because of it the σ, ρ pair used before is no longer applicable to this antenna. By repeating the same process as described in the previous section, we found that the trolley gave the lowest FER with $\sigma = 10$ and $\rho = 50$, and these results are illustrated in Fig. 12. The difference in FER between H-field strengths is similar to what we achieved with the inductive loop, in terms of the relative eavesdropping distances, although they are all shorter. A key difference was the FER at minimum field strength, was in steps of 2 cm, no errors occurred from 4 to 6 cm and then at 8 cm the FER shot to 100%. This is because the transmitted H-field strength was already very low at 1.5 A/m and given that H-field strength is inversely proportional to the cube of the distance, a very small change in eavesdropping distance will have the drastic effects, as observed here. Owing to the lack of intermediate points, a logarithmic scale was not used in this case.

5 Conclusions

We have shown that eavesdropping on HF RFID contactless communication is largely dependant on the strength of the magnetic field generated by the victim device. Depending on the H-field strength, eavesdropping distance can be within the 20–90 cm range in a shielded environment. Such an environment is not unrealistic as similar conditions could be found in an underground station. All of our work has been carried out using inexpensive and off-the-shelf electronics along with a DAQ card. This card costs £1500, but in a system designed to be deployed, it can be replaced with a considerably less expensive FPGA-based system or a laptop-based DAQ. An attacker could assemble our receiver at low cost and easily conceal it in a backpack. In addition to this, by making use of Gaussian filtering and variance computation in software an attacker can achieve frame synchronisation in a robust way. We have shown that a good pair of fixed parameters works consistently regardless of the eavesdropping distance or the H-field strength and only depends on the characteristics of the eavesdropping antenna.

Future work involves experimenting with actual mobile phones and contactless cards instead of synthetic data and examining the information that could be eavesdropped and its potential towards a privacy attack on the victim.

6 Acknowledgments

This work was funded by EPSRC and Consult Hyperion. We thank Dr. Peter King for his expertise in the design of the eavesdropping circuitry.

7 References

[1] Boden, R.: NFC transport ticketing service to launch in Valencia. Available at http://www.nfcworld.com/2013/07/01/324851/nfc-transport-ticketing- service-to-launch-in-valencia, 1 July 2013
[2] Dyer, K.: GeoToll uses NFC to manage RFID road toll payments. Available at http://www.nfcworld.com/2013/07/04/324887/geotoll-uses-nfc-to-manage-rfid-road-toll-payments, 4 July 2013
[3] Boden, R.: US Bank expands NFC iPhone payments nationwide. Available at http://www.nfcworld.com/2013/07/03/324861/us-bank-expands-nfc-iphone-payments-nationwide, 4 July 2013
[4] Boden, R.: Hang Seng launches NFC payments service. Available at http://www.nfcworld.com/2013/07/04/324893/hang-seng-launches-nfc-payments-service, 4 July 2013
[5] Payments Council - The way we pay. Available at http://www.paymentscouncil.org.uk/files/payments_council/statistical_publications/the_way_we_pay_-_february_2013.pdf 2013
[6] Boden, R.: NFC devices now account for 13.32% of mobile web traffic. Available at http://www.nfcworld.com/2013/06/26/324795/nfc-devices-now-account-for-13-32-of-mobile-web-traffic, 2013
[7] Samsung: Adopting Near Field Communication. Available at http://www.samsung.com/us/article/near-field-communication-a-simple-exchange-of-information, 2013
[8] Visa payWave. Available at http://www.visaeurope.com/en/cardholders/visa/textunderscore; http://paywave. aspx, 2013
[9] Mastecard payPass. Available at https://www.paypass.com, 2013
[10] Google Wallet. Available at https://www.google.com/wallet, 2013
[11] Cohen, B.: Millions of Barclays card users exposed to fraud. Available at http://www.channel4.com/news/millions-of-barclays-card-users-exposed-to-fraud. 23 March 2013
[12] ISO/IEC 14443. Identification cards – contactless integrated circuit cards – proximity cards. London, GB, 2008
[13] Hancke G.P.: 'A practical relay attack on ISO 14443 proximity cards'. Technical report, University of Cambridge Computer Laboratory, 2005
[14] Roland M., Langer J., Scharinger J.: 'Applying relay attacks to Google Wallet'. Proc. 2013 fifth Int. Workshop on Near Field Communication (NFC), 2013, pp. 1–6
[15] Berger, D.: 'Contactless smart card standards and new test methods'. IEEE Workshop on Smart Card Technologies and Applications, Berlin, 1998, pp. 50–54
[16] Hancke G.P.: 'Practical attacks on proximity identification systems'. Proc. IEEE Security and Privacy Symp., 2006. pp. 6–333.
[17] Novotny D.R., Guerrieri J.R., Francis M., Remley K.: 'HF RFID electromagnetic emissions and performance'. IEEE Int. Symp. Electromagnetic Compatibility, 2008 (EMC 2008), 2008, pp. 1–7
[18] Hancke G.P.: 'Eavesdropping attacks on high-frequency RFID tokens'. Proc. RFIDsec 08. Budapest, Hungary, 2008
[19] Pfeiffer F., Finkenzeller K., Biebl E.: 'Theoretical limits of ISO/IEC 14443 type A RFID eavesdropping attacks'. Proc. 2012 European Conf. Smart Objects, Systems and Technologies (SmartSysTech), 2012, pp. 1–9
[20] Thevenon P.-H., Savry O., Tedjini S., Malherbi-Martins R.: 'Attacks on the HF physical layer of contactless and RFID systems'. Current Trends and Challenges in RFID, 2011
[21] Information technology – Telecommunications and information exchange between systems – Near Field Communica-tion – Interface and Protocol (NFCIP-1). London, GB, 2013

[22] Enlighten Smart Posters. Available at http://www.smartposter.co/enlighten, 2013
[23] Brown T.W.C., Diakos T.P., Briffa J.A.: 'Evaluating the eavesdropping range of varying magnetic field strengths in NFC standards'. Proc. Seventh European Conf. Antennas and Propagation Antennas and Propagation (EuCAP), 2013
[24] Brown T.W.C., Diakos T.: 'On the design of NFC antennas for contactless payment applications'., Proc. Fifth European Conf. Antennas and Propagation Antennas and Propagation (EuCAP), 2011, pp. 44–47
[25] Finkenzeller K.: 'RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication (Wiley, 2010, 3rd edn.)
[26] Proakis J.G.: Digital Communications (McGraw-Hill, 1995, 3rd edn.)
[27] AD8310 Data Sheet Rev F, June 2010