Noisy Carrier Modulation for HF RFID

Gerhard P. Hancke
ISG Royal Holloway, University of London
Egham, UK
gerhard.hancke@rhul.ac.uk

***Abstract* - Radio-frequency tokens are vulnerable to eavesdropping. Several schemes have been proposed that use additional devices to generate cover noise, or bit collisions, in order to protect communication between a reader and a token. We discuss the practical weaknesses in current bit-blocking schemes and propose an alternative implementation where the tokens modulate their reply onto a noisy carrier provided by the reader. We believe that this modification resolves some weaknesses of bit-blocking protocols and is also easier to implement as it does not require additional blocking devices. This method can also be used to simply add noise to the backward communication channel in order to complicate the recovery of eavesdropped data.**[1]

I. Introduction

RFID devices have been shown to be vulnerable to eavesdropping and a number of parties have raised privacy concerns with regards to personal data being leaked or specific devices being tracked [1]. Cost constraints limit the amount of logic than can be accommodated and often devices simply contain data storage elements with no security mechanisms. In certain cases key exchange is not possible as the device has no cryptographic means to do so and without a shared key no data can be exchanged confidentially. Deriving a session key from the token's identifier, by using a master key, is also not feasible in some cases since the token responds with a random identifier in order to address privacy issues.

The idea of exchanging data securely by using characteristics of noise on the communication channel, and without the need for a shared secret, has been around for decades following on from the work of Wyner [2]. Here the sender transmits some data, $y(t)$, which is corrupted by noise, $N'(t)$ and $N''(t)$, on the communication channel. The intended recipient receives $x(t) = y(t)+N'(t)$ while the attacker receives $z(t) = y(t)+N''(t)$. The basic idea is that $N'(t) << N''(t)$ and as a result, based on the information theory regarding noise and channel capacity, the intended recipient can recover the data while the attacker cannot. Several ideas, following this model, have been proposed in the RFID environment [7] [8]. The problem with these proposals are that, even though they are theoretically shown to be secure, there are no real-world assurances that $N''(t)$ will always be sufficient to prevent an attacker from recovering the data.

It is therefore a logical progression to protocols that intentionally add noise to the communication channel. A number of protocols have been suggested in the last few years that use bit-collisions, or blocking, in the communication channel to protect the token's privacy [3] [4] and as a method to exchange keys, or data, between a reader and a token [5] [6]. Two devices, which are theoretically identical in terms of their communication channel, transmit a data sequence at the same time. If both transmit a '1' we get symbol S_{11} and if both transmit '0' we get symbol S_{00}. If the devices transmit a '1' and a '0' respectively we get either S_{01} or S_{10}. Bit-blocking works on the assumption that the attacker cannot distinguish between these two symbols. Previous authors argue that distinguishing between different devices is hard, and that it would require special hardware, collusion between different attackers or 'fingerprinting' of tokens.

In the NTP protocol [5] a noisy token, which is similar to the other tokens, is used to ensure that $S_{01} \approx S_{10}$. The NKA protocol [6] suggests that each device synchronizes phase and amplitude before starting the protocol. We looked at several ISO 14443A tokens, all containing a NXP Mifare 1K IC. Tokens have the ability to synchronize relatively well – as illustrated by the anti-collision procedure in ISO 14443A cards. The tokens we tested all responded within 0.1 μs of each other, which is roughly equivalent to 1% of a bit period. A determined attacker could probably fingerprint a card using phase differences, but variability in the amplitude of S_{01} and S_{10} is an easier option. A difference in amplitude occurs if there is a difference in the modulation depth of the two devices. The modulation depth, or the change in amplitude of the carrier during data modulation, is determined by antenna inductance, the resonant capacitor, modulation impedance and even orientation (since it effects antenna coupling). Matching the modulation depth is tricky, since it involves changing the RF carrier's amplitude, or tuning parameters. Figure 1 shows a synchronized response of two tokens that clearly has four distinct amplitudes for S_{01}, S_{10}, S_{11} and S_{00} respectively. As a result an attacker with eavesdropping equipment, in our case a simple tuned copper loop antenna and amplifier, might be able to distinguish between the two sequences. In the case of NKA, where two active devices transmit simultaneously, an attacker might find amplitude differences as a result of being closer to one devices than the other.

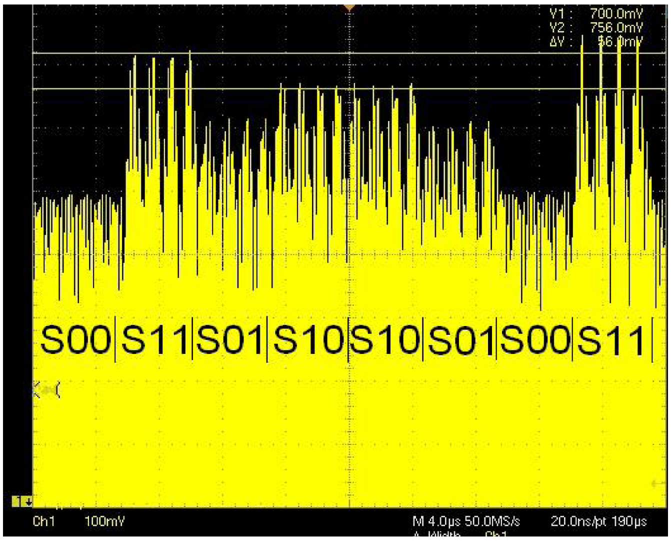

Figure 1 - Bit collision between the replies of two ISO 14443A tokens

II. Noisy Carrier Modulation

We propose that the blocker uses a layer of band-limited AWGN (Additive White Gaussian Noise) in addition to bit-blocking to hide differences in the physical characteristics of the tokens' communication. Figure 2 shows an example of how this works: (a) and (b) are the blocking sequence and data and (c) is the combination of the two. The fact that (c) has two distinct levels for S_{01} and S_{10} is hidden by adding random noise (d) but the data can still be recovered (e). In a way this merges bit-blocking with the concept of hiding data in random noise. We also propose that the reader itself acts as the blocker.

[1] Appears in the Proceedings of RFID 2007, Vienna, Austria, 24–25 September 2007.

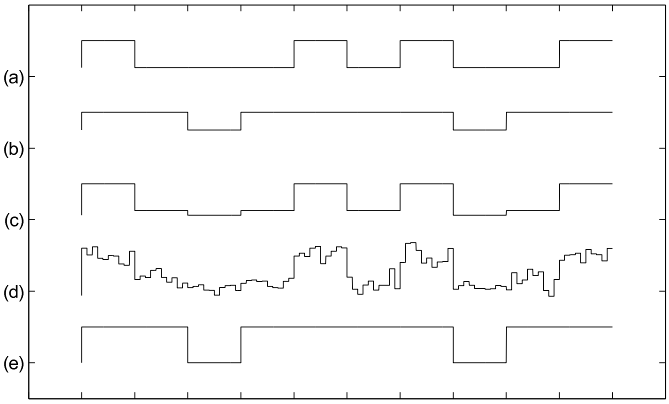

FIGURE 2 - EXAMPLE OF NOISY CARRIER MODULATION

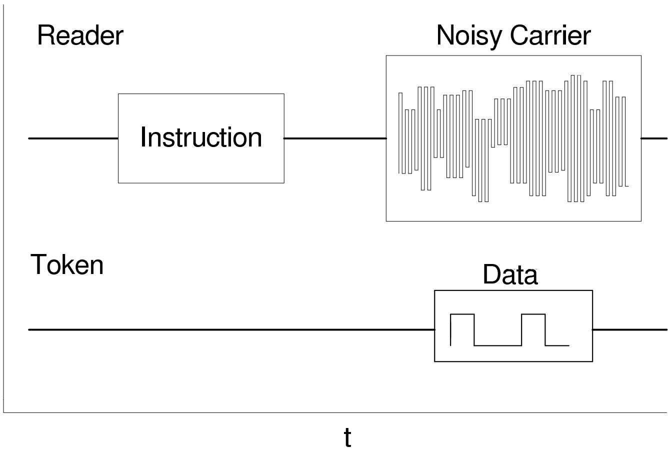

FIGURE 3 - SYSTEM IMPLEMENTATION

A RFID token modulates its data onto the reader's carrier by varying its impedance, and as a result the coupling of the antennas. We do not create bit-collisions by making two sources transmit at the same time, but rather by generating a noisy carrier onto which the token's data is modulated. The reader combines the output of a PRN, that can generate the bit-blocking sequence, and an AWGN noise source. The result is modulated onto the carrier in addition to the token's data. After the reader removes the carrier and subtracts the noise the data can be recovered. This system is simpler as the user does not need to carry an additional device, which shares a secret with all readers that are encountered. The exchange phase of our protocol is shown in Figure 3. This is followed by a resolution phase where S_{11} and S_{00} are discarded and a key, K_T, is refined from the remaining symbols. This phase is the same as described in the NTP and NKA protocols.

The attacker does not know the noisy-bit blocking sequence so he has to try and recover the data by removing the noise through alternative means. For our simulation we integrate over an entire bit period and make a decision about the symbol based on the result. This is a special case of the correlation demodulator, an optimum receiver used for data recovery in the presence of AWGN. We assume that the attacker knows exactly when the data is sent and that he can guess the bit period for each symbol without performing clock recovery. We also assume the best case for the attacker in terms of environmental noise so we disregard $N'(t)$.The attacker discards symbols S_{11} and S_{00}, and calculates K_A based on his knowledge of S_{10} and S_{01}. Figure 4 shows some results for our scheme: We calculate how much of the 100-bit shared key the attacker guessed incorrectly and plot this against the amplitude of the additional noise for varying amplitude differences, m. We assume that the larger symbol has a range of 0 – 1 and the amplitude of the noise and amplitude difference are scaled relative to this, e.g. in Figure 1 $S_{10} \approx 700$ mV and $S_{01} \approx 660$ mV so $m \approx 40$ mV ≈ 0.055. A bit error rate of 50% is equivalent to the attacker randomly guessing all key bits as statistically he should get half correct.

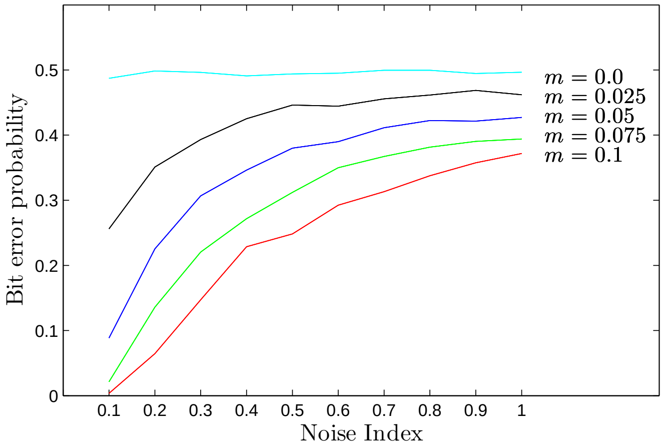

FIGURE 4 - SIMULATED RESULTS FOR NOISY CARRIER MODULATION

III. CONCLUSION

We improve on current proposals for key exchange using bit-blocking. By randomizing the physical communication characteristics, with an additional layer of AWG noise, we make it difficult for attackers to distinguish between the blocking sequence and data through differences in the communication medium. In section II. we show how effective the additional noise is at preventing an attacker from guessing the exchanged key. In our proposal the reader itself acts as the blocker. This simplifies the system as the user does not need to carry a special blocking device. Implementing the scheme requires little additional hardware in the reader, it is transparent to the token and can be extended to any inductively coupled communication, e.g. ISO 14443, ISO 15693. It can also be extended to any system using 'passive' NFC technology and can therefore be applied to ubiquitous computing applications, where pairing and key-exchange often happen between devices that have never interacted before. This method can be used by RFID proxy and blocker systems to hide any differences in their communication medium compared to the tokens they guard. For future work we would like to investigate how this system can be used to directly obfuscate data and to create eavesdropping resistant communication channels for RFID devices.

REFERENCES

[1] G.P. Hancke. *Practical attacks on proximity identification systems (short paper)*. Proceedings of IEEE Symposium on Security and Privacy, pp 328-333, May 2006.

[2] A.D. Wyner. *The Wire-Tap Channel*. Bell Systems Technical Journal, Vol. 54, pp 1355–1387, October 1975.

[3] A. Juels, R. Rivest and M. Szydlo. *The Blocker Tag: Selective Blocking of RFID tags for consumer privacy*. Proceedings of Conference on Computer and Communications Security (CCS), pp 103–111, October 2003.

[4] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman and A.S. Tanenbaum. *A Platform for RFID Security and Privacy Administration*. 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), December 2006.

[5] C. Castelluccia and G. Avoine. *Noisy Tags: Pretty Good Key Exchange Protocol for RFID Tags*. Proceedings of International Conference on Smart Card Research and Advanced Applications (CARDIS), LNCS Vol. 3928, pp 289–299, April 2006.

[6] E. Haselsteiner and K. Breitfuss. *Security in Near Field Communication*. Proceedings of Workshop on RFID Security, pp 3–13, July 2006.

[7] H. Chabanne and G. Fumaroli. *Noisy Cryptographic Protocols for Low-Cost RFID Tags*. IEEE Transactions on Information Theory, Vol 52, No 8, August 2006

[8] J. Bringer and H. Chabanne. *On the Wiretap Channel Induced by Noisy Tags*. Proceedings of European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), pp 113–120, 2006.