The Inverse Square Law and Near Field Communication

A. Braeken[1], P. Leemans[1], and Mark Vanophalvens[2]

[1]Department of Industrial Engineering
Vrije Universiteit Brussel
Nijverheidskaai 170, Brussel, Belgium

[2]Atos WorldLine
Brussel, Belgium.

(Submitted 20-06-2014)

Abstract

Near field communication (NFC) is a short-range wireless communication technology, very popular in identification and payment systems. Resistance against different types of security attacks requires the existence of a secure channel. Instead of using operational intensive cryptographic computations, a secure channel can be theoretically obtained based on the superposition principle when sender and receiver send a signal at exactly the same time. In this paper, we show that due to the inverse square law, the attacker can clearly identify the signal of the most nearby device if (s)he is not exactly placed in the middle.

1 Introduction

NFC is based on Radio Field Identification (RFID) technology. It is designed for short and quick transactions, which are reduced to simply touching or bringing devices in close proximity. Due to the success of the smartphone, the NFC technology experiences a tremendous growth, with popular applications such as advertising tags, banking transactions, tickets,...

Despite the fact that NFC only supports short communication ranges, it does not mean that it is resistant against security attacks such as eavesdropping, data corruption, data modulation, denial of services and relay attacks [1],[2]. The existence of a secure channel to share a secret key is an essential re-

quirement for offering resistance against these attacks. It is used as basis for many security protocols to continue the rest of the communication. Instead of using expensive cryptographic operations, Haselsteiner and Breitfu [1], propose the idea of establishing a secure channel based on superposition, but never tested it practically.

In superposition, both devices A and B, send a different bit at exactly the same time by amplitude shift keying (ASK). An attacker cannot distinguish which bit is coming from whom due to superposition of both signals. When both devices send the same value, these bits are discarded. It should be decided upfront, whose bits are collected. Consequently, when a 256-bit signal is sent, an approximately 128-bit secret will be constructed. Fig 1 illustrates this effect.

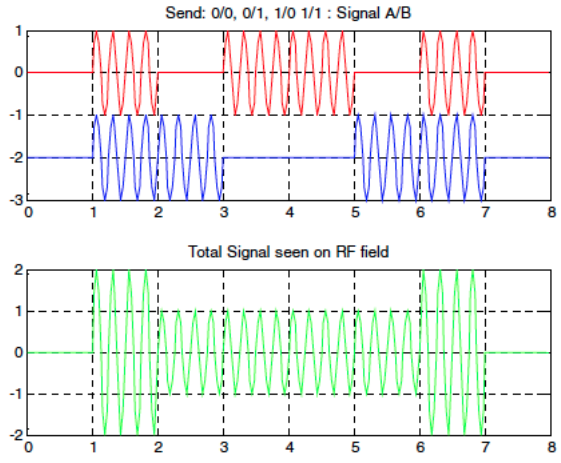

Figure 1: PResult of superposition of two signals, send by ASK [1]

To check the efficiency of the proposed secure channel, we work with the peer-2-peer mode, being both active devices for sender and receiver when sending data. So, there will be no difference in signal strength.

2 Experimental setting

Two devices, A and B, send in active mode and receive when the RF field is deactivated. Consequently, both signals contain the same amplitude, and thus exclude any possible irregularity. Another device S, also called spy, will receive and collect the data of A and B, while A and B are sending simultaneously data. The spy is configured as passive device, does not generate any RF field, and only receives data. Therefore, the spy will have no influence on the RF fields or data send by the terminals A and B. After synchronization, we ensure that the devices constantly send data, so no measurement data losses can occur. Both terminals will continue to fill their FIFO buffer with their respective signals during submission.

3 Results

We consider 4 situations with 25, 20, 10 and 5 centimeters distance between A and B. In all 4 situations, we vary the position of S and analyze the result. From all the experiments, we conclude that if the position of S is closer to either A or B, the exclusive signal of A or B respectively is picked up. Also behind the devices, the result corresponds with the pure signal of that device.

Only in the middle over a range of 5 cen-

timeters, a mix of different signals occurs, where the superposition signal reaches the highest probability. These results are easily explained due to the inverse square law, describing the inversely proportional relation of the signal strength to the square of the distance from its source. Consequently, only in the middle, the same signal strength for the two signals occurs. Fig. 2 presents the intensity curve of the signal between A and B at a distance of 25 centimeters from the experiments. The signal strength at different distances was measured with an oscilloscope. If the distance between S and A equals to 5 centimeters, the signal strength corresponds to 760 mV. At B, the signal strength is already decreased to 43 V. Consequently, it is clear that S will not even notice the signal of B, since the signal strength of A is approximately 16 times larger. As we are dealing with ASK, the amplitude determines the value of the signal.

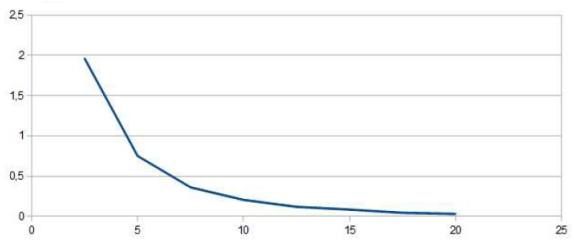

Figure 2: Intensity curve (V) related to distance (cm) for a signal between 2 devices at 25 centimeters distance.

4 Conclusions

Due to the signal strength inverse law, superposition between 2 devices is only obtained in the middle over a range of 5 centimeters. As a consequence, we can conclude that the NFC key agreement protocol, as theoretically proposed in [1], will not be secure. Very recently, Wang et. al. [3] show how randomizing the modulation and the channel can successfully establish a secure channel. Consequently, there seems to exist possibilities to realize a secure channel without cryptographic techniques. However, more research is required in effectively checking these techniques.

References

[1] E. Haselsteiner and K. Breitfu (2006), Security in near field communication (NFC), in Workshop on RFID Security RFIDSec, 2006.

[2] P. S. Halgaonkar, S. Jain, and V. M. Wadhai (2013) NFC: A review of technology, tags, applications and security, IJRCCT, vol. 2, no. 10, pp. 979987.

[3] J. Wang, H. Hassanieh, D. Katabi, T. Kohno (2013) "Securing Deployed RFIDs by Randomizing the Modulation and the Channel", Technical Report, Jan 2013.