Practical Message Manipulation Attacks in IEEE 802.15.4 Wireless Networks

Matthias Wilhelm[1], Jens B. Schmitt[1], and Vincent Lenders[2]

[1] Disco Labs, TU Kaiserslautern, Germany
[2] armasuisse, Thun, Switzerland
{wilhelm,jschmitt}@cs.uni-kl.de, vincent.lenders@armasuisse.ch

Abstract. We assess the ability of adversaries to modify the content of messages on the physical layer of wireless networks. In contrast to related work, we consider signal overshadowing to achieve such manipulations during transmission. We present preliminary experimental results, which suggest that our approach enables deterministic message manipulations, even in unpredictable radio environments.

1 Introduction

In this research project, we consider message manipulation attacks in wireless networks. The attacker's goal is to violate the integrity of a message, tricking a victim receiver to accept a message of the attacker's choice, while the sender considers its original message to be delivered successfully. While such attacks can also be realized on higher layers (e.g., modifications by forwarding hops or memory manipulations on sender or receiver), we focus on attacks on the physical layer of wireless communications. A recent study by Pöpper et al. [1] shows that such message manipulations are possible if an attacker emits well-chosen RF waves that combine with the original signal to a new signal, which is then received as a packet of the attacker's choice; this method is called *symbol flipping*. However, the results also show that this attack is challenging in practice because a correct timing and matching amplitude and phase at the receiving antenna are required, which is hard to attain in realistic radio propagation environments.

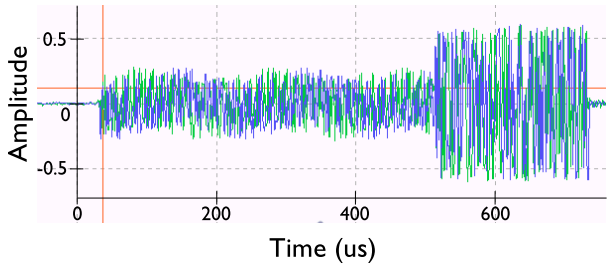
We consider an alternative manipulation method using *signal overshadowing*, i.e., the property that in angular modulation schemes only the stronger of two colliding signals is received. The expected benefit of our approach is that it is less sensitive to the physical properties of the victim signal, making it more practical and reliable. However, the technical challenges of tight timing and phase synchronization requirements still remain. We aim to analyze our method in IEEE 802.15.4 networks, implement a system that manipulates messages over the air deterministically, and evaluate its attack performance against off-the-shelf receivers in realistic scenarios.

2 System Challenges and Implementation

Challenges. Correct reception requires that the attacker matches its timing and phase closely to the legitimate sender. While the sender does not suffer from symbol errors because the receiver uses preamble and SFD (start-of-frame delimiter)

Sender	Preamble	SFD	Header	0	0	0	0	0	0	0	0	CRC				
+ Attacker				d	e	a	d	b	e	e	f	4	f	b	d	
Receiver	Preamble	SFD	Header	d	e	a	d	b	e	e	f	4	f	b	d	

(a) The attacker synchronizes with the packet and alters the received content.



(b) The attack at the physical layer: signal replacement by overshadowing.

Fig. 1: Physical layer message manipulation attack.

to synchronize with the signal, the attacker cannot exploit this. Especially the phase offset may play a major role because the used MSK modulation generates symbol flips if the relative phase deviates by more than $\frac{\pi}{2}$. Since this relation between original and attack signal at the receiver is hard to control by the attacker, we might face the challenge that the attack is still unreliable, even with optimal timing. However, as the standard uses spread spectrum modulation, we may hope that receivers can compensate such deviations. Fig. 1a shows that the attacker can directly send the desired symbols when using overshadowing, but must time its attack precisely to be successful (with a deviation of less than 1 µs in IEEE 802.15.4). This requires the attacker to detect and synchronize with the victim signal with tight timing constraints.

Attack system implementation. We use RFReact [2] to implement the attack. This USRP2-based software radio system implements an IEEE 802.15.4 transceiver in FPGA logic and uses programmable firmware to control its operation. The system detects the preamble of an incoming packet, achieving symbol synchronization and timing recovery, and enables the attacker to start transmitting arbitrary waveforms after a tunable delay, with a timing precision of 10 ns.

3 Initial Experimental Results

Experimental setup. We use three USRP2s in our experiment, taking the role of attacker (using RFReact), legitimate sender, and as a signal scope for RF monitoring. The victim receiver is a COTS device, an Atmel RZ Raven USB stick. The experiment takes place in an indoor office environment with distances of 2 m–3 m between the antennas. No attempts to match the carrier phase at the receiver are made in the setup. The attack depicted in Fig. 1a is performed 10000 times: the attacker attempts to replace the last 12 symbols of a packet, altering 8 symbols of payload (to `0xdeadbeef`) and 4 symbols of CRC (to `0x4fdb`). A physical layer view of the overshadowing attack is shown in Fig. 1b.

Rel. frequency	Received symbols	#errors	Rel. frequency	Received symbols	#errors
66.97 %	deadbeef4fbd	0	0.94 %	deadbe7f4fbd	1
2.95 %	00000bc8b9cc	12	0.91 %	d7adbeef4fbd	1
2.68 %	4eadbeef4fbd	1	0.76 %	deadb7ef4fbd	1
2.19 %	0deadbeef4fb	11	0.72 %	000000000000	12
1.23 %	7eadbeef4fbd	1	0.57 %	00000bc8b9ce	12
1.12 %	0fbecff858ce	12	18.96 %	Rel. freq. $< 0.5\%$	var.

Table 1: Experimental results: modified payload as received by the victim. Symbols errors are underlined and highlighted in red.

Experimental results. The results are shown in Table 1; the attack succeeds in 6697 attempts of 10000. We can divide the observed errors into two classes: *(C1)* the timing error is less than one symbol duration (16 µs) such that no leading zero symbols are present (23 % of the cases), and *(C2)* completely missed symbol timing (> 16 µs, 10 %) that may be attributed to problems in the attack system.

These results show that such a manipulation attack is indeed feasible. We see a good timing synchronization and small timing errors, and achieve a deterministic manipulation outcome in the majority of attempts. Surprisingly, phase errors seem to play a minor role. As the attacker does not synchronize with the carrier phase, the phase error should be distributed uniformly in the range 0 to 2π. When considering the used MSK modulation and a constant phase offset during the attack, this should lead to a significant number of 12 symbol errors observations in *C1*, even with optimal timing. However, we notice that the receiver is able to correctly detect the attacker's symbols in most cases, and that single symbol errors are prevailing in the others. Symbol timing seems to be the decisive factor to attack success.

4 Conclusion

Our experimental results suggest that the described message manipulation attack method is reliable, even in unpredictable indoor radio environments. Therefore message integrity measures must be taken, even when sender and receiver are in transmission range and closely monitor the channel state and packet timing.

We plan to analyze this attack for IEEE 802.15.4 networks, extend our experimental study to various COTS receivers and radio environments, and devise methods to detect and mitigate such attacks.

References

1. C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Čapkun. Investigation of signal and message manipulations on the wireless channel. In *Computer Security — ESORICS 2011*, volume 6879 of *LNCS*, pages 40–59. Springer Berlin Heidelberg, Sept. 2011.
2. M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. WiSec 2011 demo: RFReact—a real-time capable and channel-aware jamming platform. *SIGMOBILE Mobile Computing and Communications Review*, 15:41–42, Nov. 2011.