精读

Detection of Electromagnetic Interference Attacks on Sensor Systems (Oakland'20)

First Author

Youqian Zhang

Summary

1. Proposed a detection method for low-level (low-power) EMI attack (target on the wire between the sensor and the microcontroller).
2. Basic idea: The attacking signal is more obvious when the sensor is turned off. By turning on/off the sensor periodically (Manchester encoding), we can detect the attack signal during the off period and keep the sensor working in the mean while.
3. Method: modulate the sensor output in a way that is unpredictable to the attacker (turn on/off the sensor according to randomly Manchester encoding), if controller detects fluctuations (both during the on and off period), then the attacking signal can be detected.
4. Evaluation: both on a temperature system and a microphone system (whose physical quantity is constant during a short measurement).

Challenge (technical)

No big challenges but some regular practical ones.

- how to synchronize the digitized signal and teh secret Manchester code sequence: By introducing preamble
- how to handle samples in the rising or falling edges: Remove
- how to determine the voltage level of zero samples: set threshold (noise tolerance)

Main idea

The attacking signal is obvious when the sensor is turned off (e.g., disturbance on 0V level). So the authors turn on/off the sensor according to randomly Manchester encoding which is unpredicted by the attacker. (A normal sensor is working with a fixed bias level?)

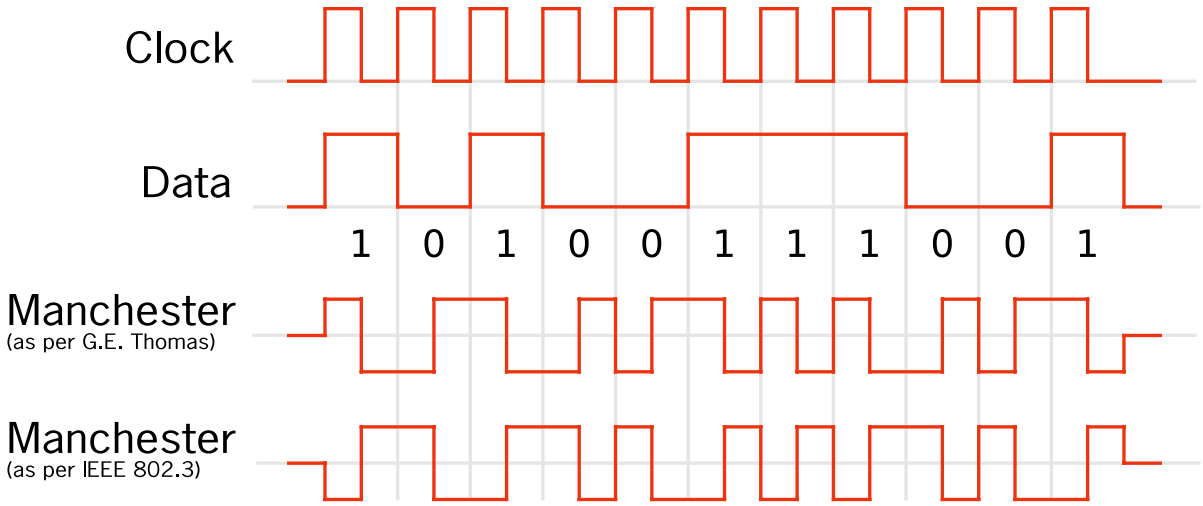
Strength

1. Existing method: shielding and EMI filters (cannot full block interference, cannot detect)
2. separate the work period into working and detecting by switching on/off to achieve normal working and attack detection during each working period.

Weakness

1. Whether turn on/off the sensor frequently will impact the usability of the sensor?

2. Unreasonable assumption: "we assume that the attaker knows voltage levels, but she does not know wether the voltage level transitions from high to 0V or from 0V to high..." Manchester encoding 是可以根据每一个周期的起始值来判断该周期是0还是1(例如接连两个周期不变的话，周期间隙会有跳变沿)，因此攻击者可以先需要观察一定数目的周期，估计出Bias Voltage Generator进行Manchester encoding的周期，然后在监听接下来的信号的起始值来判断该周期是0还是1，从而完成更为准确的预测。



3. Experiment: limited attacking distance (10cm for microphone and 1cm for thermistor) to inject the malicious signal. (the authors demostrated that they "want to realize the remote injection with a low power of the ... signal generator.")
4. Singular frequency auido signal; the doubtable significance of the attack using a single frequency audio signal to inject, in other words, is it convincing to use only singular frequency audio signal to evaluate the detection performance?
5. Cannot recover the physical quantity from the cases of being attacked.(univeral problem?)

Inspiration

1. Spoofing attack detection + Manchester encoding or sth. else?
2. Remote EMI attack (by some accumulate effects or persistant fault injection?)

泛读 1

BIAS： Bluetooth Impersonation Attacks (Oakland'20)

First Author

Daniele Antonioli

Solved problems

Present the master and slave impersonation attacks on both the legacy and secure authentication procedure during secure connection establishment (without knowing the shared long term key between Alice and Bob).

Main Idea

Leveraging the volunerabilities of bluetooth (BR/EDR) including the lack of mandatory mutual authentication, overly permissive role switching, and an authentication procedure downgrade.

What can be learned from this paper

1. The procedure of secure connection establishment about the bluetooth. Bluetooth Basics
2. Security connection establishment procedure which lacks mutual authentication may expose attack surface (Man-in-the-Middle attack).

泛读 2

Millimeter-Wave Full Duplex Radios (MobiCom'20)

First Author

Vaibhav Singh

Solved problems

Proposed mmFD, the first SDR-driven comprehensive system of a mm-wave full-duplex platform (28GHz) to achieve 1.7X througput gain over equivalent half-duplex systems.

- solid hardware design
- digital self-interference cancellation algorithms

Contribution

1. Exploit the small wavelength of mm-wave to achieve strong signal isolation between the transmit and receive antennas.
2. Solid hardware design (a custom IC, antennna, analog and digital frontends design).

What can be learned from this paper

Some knowledge about the mmwave platform design and common problems in full duplex communication (e.g., self-interference).