


浙江大学电气工程学院
College of Electrical Engineering Zhejiang University

网络安全导论

物联网终端安全

1. 概述、基础知识
2. 加密与认证技术
3. 软件与通讯安全
4. 电力工控系统安全
5. **物联网终端安全**
6. 智能无人系统安全

5.1 定义、组成、分类、主要特性

物联网终端之传感器

物联网终端安全之传感器与执行器安全

5.1 传感器概述

1. 传感器的定义

2. 传感器的组成

3 .传感器的分类

4. 传感器的特性

5. 传感器的标定

5.1 传感器概述

- 传感器在物联网中的作用相当于人体的“**五官**”。

- 目前，传感器早已渗透到诸如智能制造、车辆控制、海洋探测、环境保护、资源调查、医学诊断、生物工程等领域。

- 随着物联网的快速发展，传感器技术在发展经济、推动社会进步方面的重要作用越来越明显，但其存在的安全问题也不容忽视。

5.1 传感器概述

- AI以大数据为支撑，传感器数据如各类**视频、图片、声音、加速度**等数据是算法的基石；
- **AI2.0时代，跨媒体AI**将更加依赖传感器数据的输入，如智能手机、自动驾驶汽车；
- 智能系统的**“五官”安全**是安全的决定性因素，而目前对其研究不充分。

自动驾驶汽车中传感器问题
导致安全事故（特斯拉）

波音737空难中
传感器安全问题

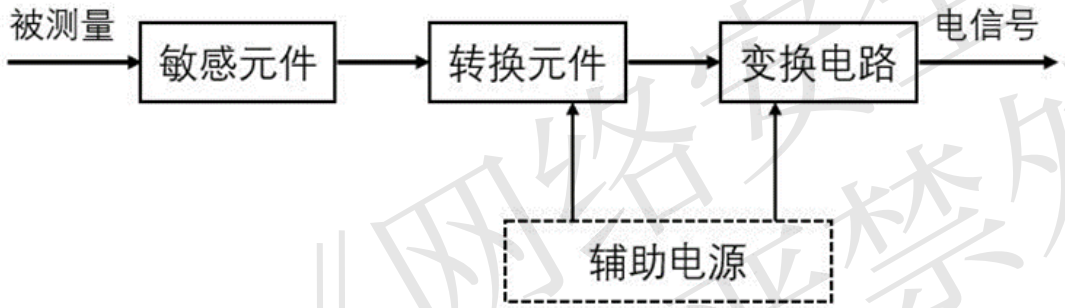
5.1.1 传感器的定义

- 传感器是一种检测装置，能感受到被测量的信息，并能将检测感受到的信息，按一定规律变换成为电信号或其他所需形式的信息输出，以满足信息的传输、处理、存储、显示、记录和控制等要求。被测量的信息可以是光、热、运动、湿气、压力，或许多其他环境现象中的任何一种。
- 传统的水银温度计，就是一种传感器，利用水银的热胀冷缩原理，感知环境的温度，并通过读取水银到达的刻度来获取温度值，如下图所示。

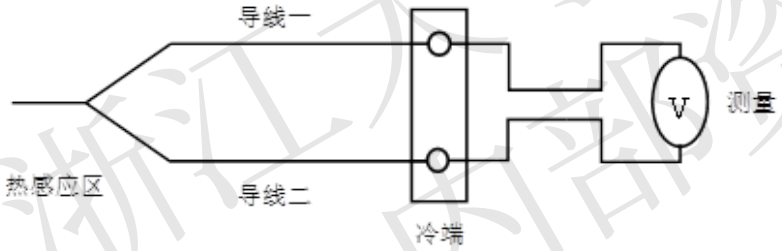
- **国家标准GB7665-87**对传感器下的**定义**是：“**能感受规定的被测量并按照一定的规律转换成可用信号的器件或装置**，通常由敏感元件和转换元件组成”。

5.1.2 传感器的组成

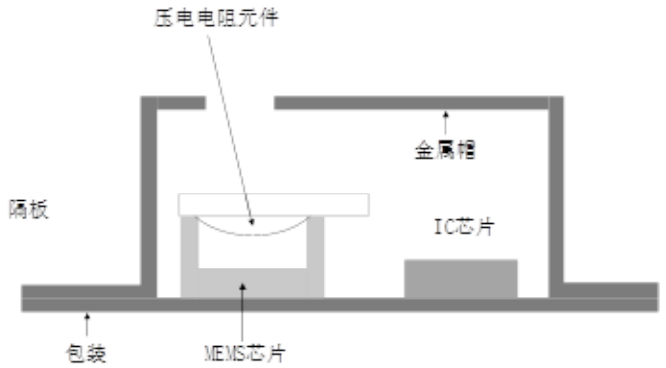
- 传感器一般由**敏感器件、转换元件、变换电路和辅助电源**四部分组成，如下图所示。



- 有些传感器很简单，有些则较为复杂。



• 图a 热电偶
由一个敏感元件（兼转换元件）组成，它感受被测量时直接输出电量



• 图b MEMS压力传感器
不但包括敏感元件和转换元件还包括后续信号处理的IC电路

5.1.3 传感器的分类

- 由于传感器应用领域众多，适用范围又广，其品种和规格繁多，根据不同的原则可以将传感器分成不同类型。比较常用的分类方法有以下几种。

- 1 按工作原理分类
  - 物理传感器和化学传感器

- 2 按构成原理分类

- 3 按能量转换情况分类
  - 能量控制型传感器和能量转换型传感器

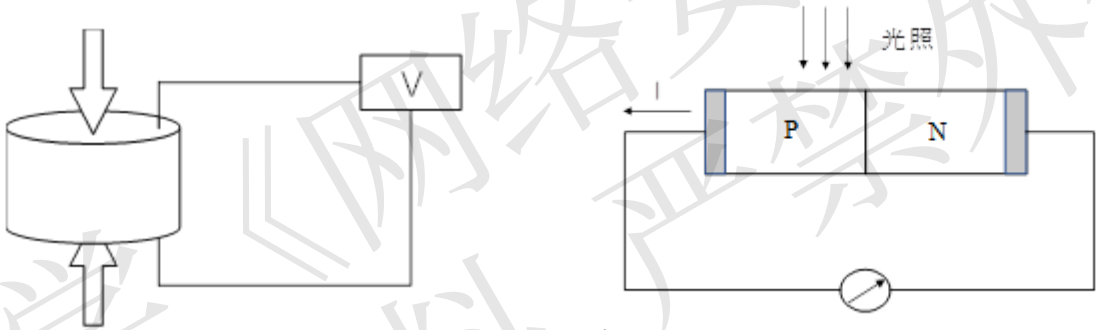
- 4 按输出信号分类
  - 模拟传感器
  - 数字传感器
  - 膺数字传感器
  - 开关传感器

5.1.3 传感器的分类

5.1.3.1 按工作原理分类

物理传感器

- 物理传感器可以按其工作原理的物理效应进行分类，诸如压电效应、磁致伸缩现象、离化、极化、热电、光电、磁电等效应。**被测信号量的微小变化都将转换成电信号。**



5.1.3.1 压电、光电效应图

化学传感器

- 化学传感器包括那些以化学吸附、电化学反应等现象为因果关系的传感器，被测信号量的微小变化也将转换成电信号。

有些传感器**既不能划分到物理类，也不能划分为化学类。**

- 大多数传感器是以物理原理为基础运作的。化学传感器技术问题较多，例如可靠性问题，规模生产的可能性，价格问题等，解决了这类难题，化学传感器的应用将会有巨大增长。

5.1.3 传感器的分类

5.1.3.2 按传感器的构成原理分类

结构型传感器

结构型传感器是基于物理学中场的定律构成的，包括动力场的运动定律、电磁场的电磁定律等。物理学中的定律一般是以方程式给出的。对于传感器来说，这些方程式也就是许多传感器在工作时的数学模型。这类传感器的特点是传感器的工作原理是以传感器中**元件相对位置变化引起场的变化**为基础。

物性型传感器

物性型传感器是基于物质定律构成的，如虎克定律、欧姆定律等。物质定律是表示物质某种客观性质的法则。这种法则，大多数是以**物质本身的常数**形式给出。这些常数的大小决定了传感器的主要性能。因此，物性型传感器的性能随材料的不同而不同。如光电管就是物性型传感器，它利用了物质法则中的外光电效应。此外，也有基于守恒定律和统计定律的传感器，但相对较少。

5.1.3 传感器的分类

- **5.1.3.3 根据能量转换情况**

  - 能量控制型传感器
    - 能量控制型传感器，在信息变化过程中，其能量需要外电源供给。如电阻、电感、电容等。电路参量传感器都属于这一类传感器。基于应变电阻效应、磁阻效应、热阻效应、光电效应、霍尔效应等的传感器也属于此类传感器。

  - 能量转换型传感器
    - 能量转换型传感器，主要由能量变换元件构成，他不需要外电源。如基于压电效应、热电效应、光电动势效应等的传感器都属于此类传感器。

5.1.3 传感器的分类

5.1.3.4 按输出信号分类

- **模拟传感器：**
  - 将被测量的非电学量转换成模拟电信号。
- **数字传感器**
  - 数字传感器输出信号为数字量(或数字编码)的传感器。是指将传统的模拟式传感器经过加装或改造A/D转换模块，使之输出信号为数字量(或数字编码)的传感器，主要包括：放大器、A/D转换器、微处理器（CPU）、存储器、通讯接口电路等。
- **膺数字传感器**
  - 将被测量的信号量转换成频率信号或短周期信号的输出（包括直接或间接转换）。
- **开关传感器：**
  - 当一个被测量的信号达到某个特定的阈值时，传感器相应地输出一个设定的低电平或高电平信号。

5.1.4 传感器的主要特性

5.1.4.1 静态特性

定义：

传感器的静态特性是指对静态的输入信号，传感器的输出量与输入量之间所具有相互关系。

因为这时输入量和输出量都和时间无关，所以它们之间的关系，即传感器的静态特性可用一个不含时间变量的代数方程，或以输入量作横坐标、把与其对应的输出量作纵坐标而画出的特性曲线来描述。

主要参数：

表征传感器静态特性的主要参数有：**线性度、灵敏度、迟滞、重复性、漂移**等。

5.1.4 传感器的主要特性

5.1.4.1 静态特性

（1）线性度：

传感器的线性度是指其输出量与输入量之间的关系曲线偏离理想直线的程度，又称为非线性误差。在不考虑迟滞、蠕变等因素的情况下，其静态特性可用下列多项式代数方程来表示：

$$y = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{5.1}$$

其中，y-输出量，x-输入量，a_0-零点输出，a_1-理论灵敏度，a_2，$a_3 \ldots a_n$-非线性项系数。

由于存在二次、高次项，所以传感器的输出是非线性的，这将导致传感器会存在一定的安全风险，在传感器安全的章节中，会对此进行详细介绍。

5.1.4 传感器的主要特性

5.1.4.1 静态特性

（2）灵敏度：

灵敏度是传感器静态特性的一个重要指标。其定义为传感器在稳态信号作用下输出量变化对输入量变化的比值。用S表示灵敏度。

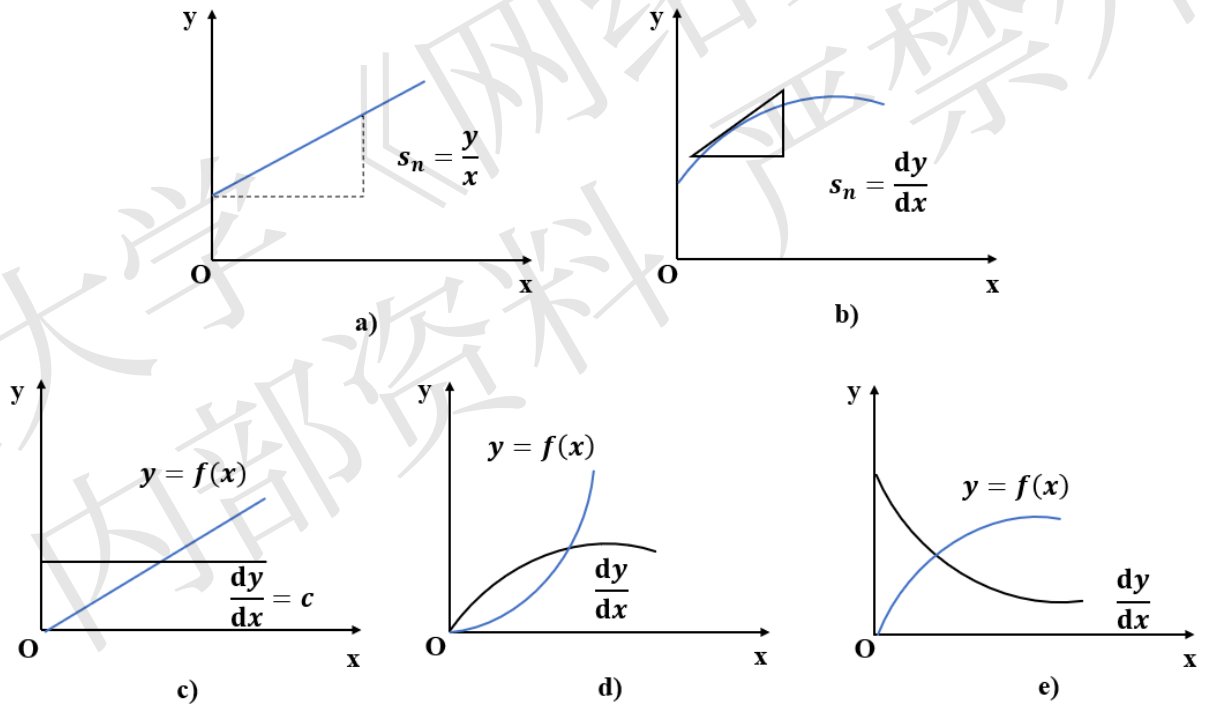


图5.1.4.1(2) 传感器的灵敏度

5.1.4 传感器的主要特性

5.1.4.1 静态特性

（3）迟滞：

传感器在输入量由小到大（正行程）及输入量由大到小（反行程）变化期间其输入输出特性曲线不重合的现象成为迟滞。

对于同一大小的输入信号，传感器正反行程的输出信号大小不相等，这个差值称为迟滞差值ΔH_max，迟滞误差一般以满量程输出的百分数表示。

$$\gamma_H = \frac{\Delta H_{max}}{y_{FS}} * 100\ \%$$

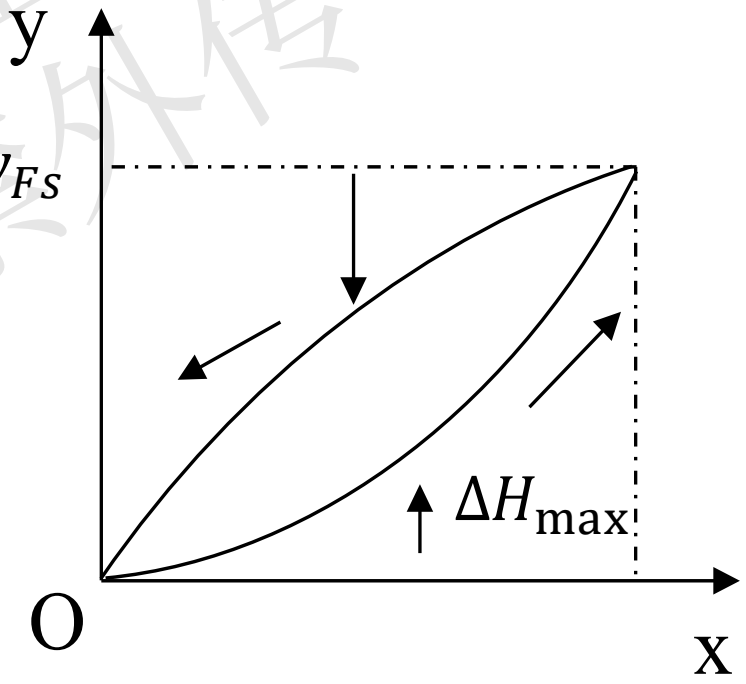


图5.1.4.1(3) 传感器迟滞特性

5.1.4 传感器的主要特性

5.1.4.1 静态特性

（4）重复性：

重复误差表征的是传感器在输入按同一方向作全量程连续多次变动时所得特性曲线不一致的程度。其反映的是测量结果偶然误差的大小，而并不表示与真实值的差别。

$$\text{重复误差：}\ \gamma_R = \frac{\Delta R_{max}}{y_{FS}} * 100\ \% \tag{5.3}$$

（5）漂移：

传感器的漂移是指在输入量不变的情况下，传感器输出量随着时间变化，此现象称为漂移。产生漂移的原因有两个方面：一是传感器自身结构参数；二是周围环境（如温度、湿度等）。

$$\text{温漂} = \frac{\Delta_{max}}{y_{FS}\,\Delta T} * 100\ \% \tag{5.4}$$

5.1.4 传感器的主要特性

5.1.4.1 静态特性

（6）分辨率：

定义：分辨率是指传感器能够感知或检测到的最小输入信号增量。

分辨率可以用绝对值或与满量程的百分比来表示。分辨率高是精度高的必要条件而非充分条件。

（7）阈值：

定义：当传感器的输入从零开始缓慢增加时，在达到某一值后输出发生可观测的变化，这个输入值称传感器的阈值电压。（能检测的“最小”输入）

5.1.4 传感器的主要特性

5.1.4.2 动态特性

定义：

传感器的动态特性是指传感器对动态激励（输入）的响应（输出）特性，即其输出对随时间变化的输入量的响应特性。

主要参数：

传感器的动态特性可以从**时域和频域**两个方面分别采用**瞬态响应法和频率响应法来分析**。

- 在采用**阶跃输入**研究传感器的时域动态特性时，常用延迟时间、上升时间、响应时间、超调量等来表征传感器的动态特性。
- 在采用**正弦输入**信号研究传感器的频域动态特性时，常用幅频特性和相频特性来描述传感器的动态特性。

5.1.4 传感器的主要特性

5.1.4.2 动态特性

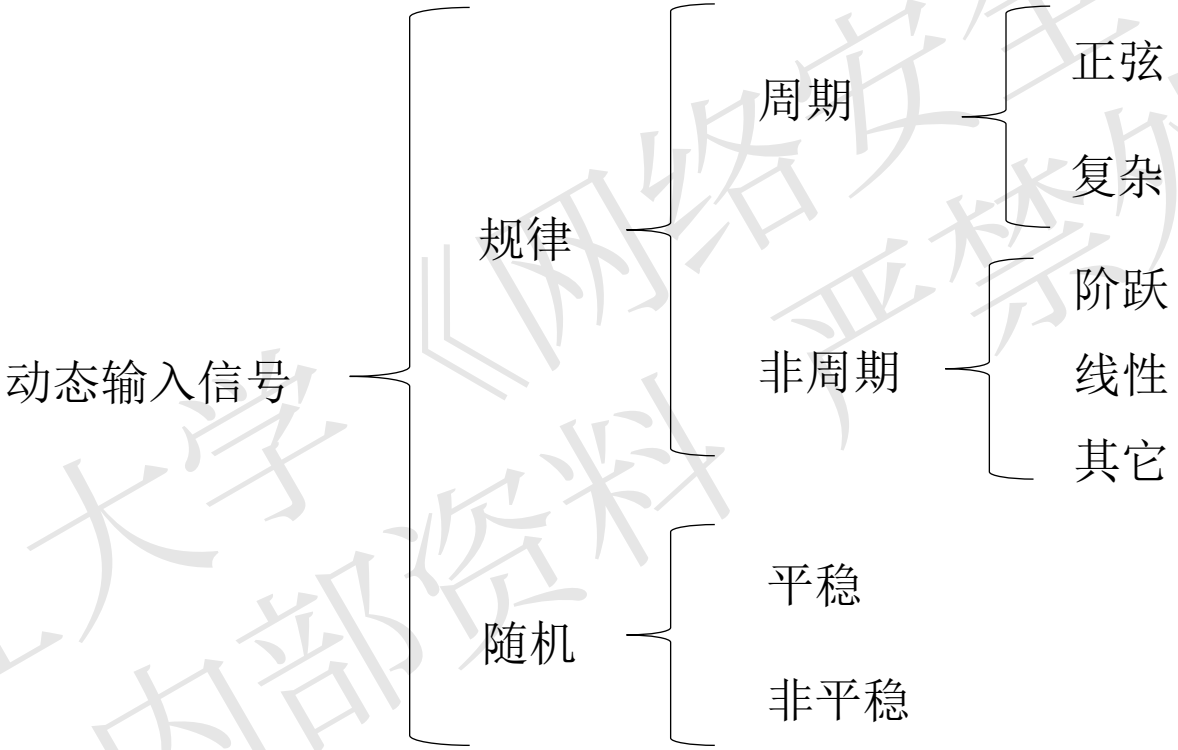


图5.1.4.2 动态输入信号的种类

5.1.4 传感器的主要特性

5.1.4.2 动态特性

（1） 传感器的数学模型

通常可以用线性时不变系统理论来描述传感器的动态特性。从数学上可以用常系数线性微分方程（线性定常系统）表示传感器输出量与输入量的关系：

$$a_n \frac{d^n y}{dt^n} + a_{n-1} \frac{d^{n-1} y}{dt^{n-1}} + \cdots + a_1 \frac{dy}{dt} + a_0 y$$

$$= b_m \frac{d^m x}{dt^m} + b_{m-1} \frac{d^{m-1} x}{dt^{m-1}} + \cdots + b_1 \frac{dx}{dt} + b_0 x \qquad (5.5)$$

式中：$a_n, \cdots, a_0$ 和$b_m, \cdots, b_0$ 与系统结构参数有关的常数。

5.1.4 传感器的主要特性

- **5.1.4.2 动态特性**

  - **（2） 传递函数**

对式（5.5）作拉氏变换，并认为输入和输出及它们的各阶时间导数的初始值为0，则得：

$$H(s)=\frac{L[y(t)]}{L[x(t)]}=\frac{Y(s)}{X(s)}=\frac{b_m s^m+b_{m-1}s^{m-1}+\cdots+b_1 s+b_0}{a_n s^n+a_{n-1}s^{n-1}+\cdots+a_1 s+a_0} \quad (5.6)$$

其中：$s=\beta+jw$

式（5.6）的右边是一个与输入无关的表达式，它只与系统结构参数（a，b）有关，正如前文所言，**传感器的输入-输出关系特性是传感器内部结构参数作用关系的外部特性表现**。

5.1.4 传感器的主要特性

5.1.4.2 动态特性

（3）频率响应函数

对于稳定的常系数线性系统，可用傅里叶变换代替拉氏变换，相应地有：

$$H(jw) = A(w)e^{j\phi(w)} \tag{5.7}$$

模（称为传感器的幅频特性）：

$$A(w) = |H(jw)| = \sqrt{[H_R(w)]^2 + [H_I(w)]^2} \tag{5.8}$$

相角（称为传感器的相频特性）：

$$\phi(w) = \arctan\frac{H_I(w)}{H_R(w)} \tag{5.9}$$

5.1.4 传感器的主要特性

5.1.4.2 动态特性

（4）传感器的动态特性分析

一般可以将大多数传感器简化为一阶或二阶系统。

一阶传感器的微分方程为：

$$a_1 \frac{dy(t)}{dt} + a_0 y(t) = b_0 x(t) \tag{5.10}$$

它可改写为：

$$\tau \cdot \frac{dy(t)}{dt} + y(t) = S_n \cdot x(t) \tag{5.11}$$

式中：τ - 传感器的时间常数（具有时间量纲）

这类传感器的幅频特性、相频特性分别为：

幅频特性：$A(w) = 1/\sqrt{1 + (w\tau)^2}$ (5.12)

相频特性：$\phi(w) = -\arctan(w\tau)$ (5.13)

5.1.4 传感器的主要特性

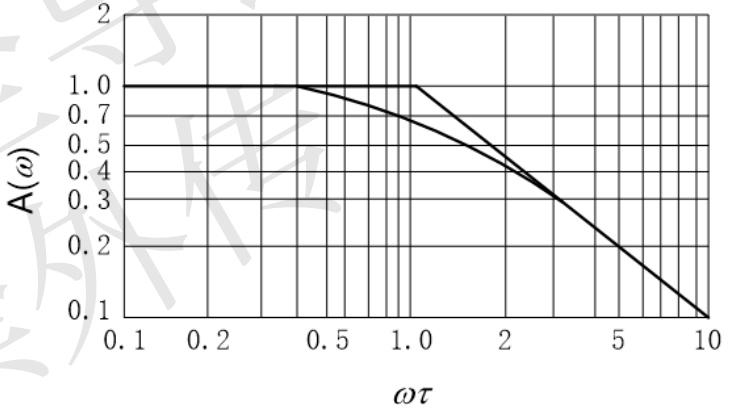
5.1.4.2 动态特性

（4）传感器的动态特性分析

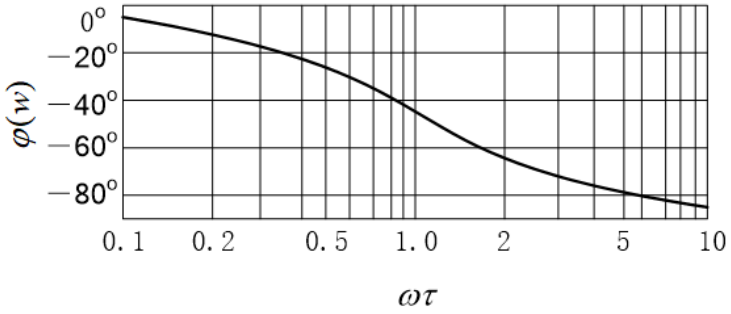
$$A(w) = 1/\sqrt{1+(w\tau)^2} \quad (5.12)$$

$$\phi(w) = -\arctan(w\tau) \quad (5.13)$$

从式（5.12）、（5.13）和右图看出，时间常数越小，此时A(w)越接近于常数1，ϕ(w)越接近于0，因此，频率响应特性越好。当wτ<<1时：
A(w)≈1，输出与输入的幅值几乎相等，它表明传感器输出与输入为线性关系。ϕ(w)很小，tan(ϕ)≈ϕ，
ϕ(w)≈-wτ，相位差与频率成线性关系。



(a)幅频特性



(b)相频特性

图5.1.4.2 一阶传感器的频率特性

5.1.5 传感器的共有特性

- **1. 对物理信号的敏感性。**

传感器测量的基本方法（换能原理）就是利用换能器将某种类型的物理信号转换为电信号进行处理。因此传感器的设计导致其会至少对某种物理信号具有敏感性，无论这种物理信号是来自何处和如何产生的。

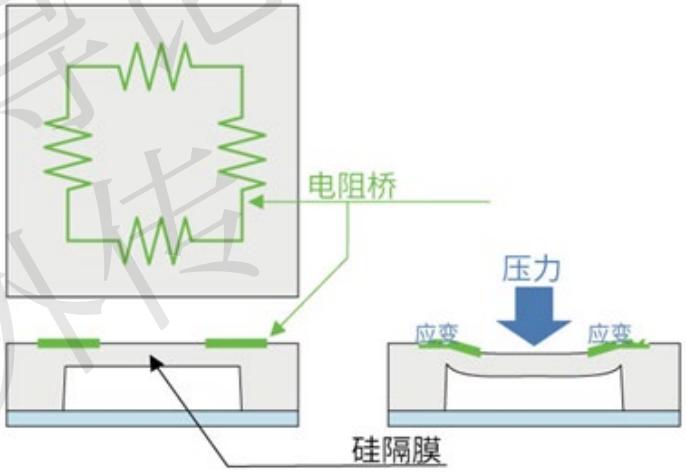


图5.1.5.1 压阻式气压传感器。对压力（气压）的变化具有敏感性

- **2. 相似的模拟信号处理。**

虽然传感器依赖于各种各样的换能器，但它们对换能后产生的模拟信号的处理具有一定的相似性，例如通常都使用放大器和滤波器。

虽然电路设计可能会由于不同换能器产生的电信号特点具有较大的差异，相似的电子器件可能会导致其相似的物理特性被攻击者利用。

5.1.5 传感器的共有特性

- **3. 相同的信号模态转换。**

  信息在感知过程中会经历由物理信号形态到模拟电信号形态和数字电信号形态的转换。

  这种相同的信号模态转换导致攻击者可能在对不同传感器的攻击利用各个信号模态形同的特性来构造恶意信号。

- **4. 盲目信任链。**

  传感器测量的本质是对真实物理世界的电信号替代。大部分传感器都使用一系列的电子器件对换能后电信号进行处理，并且所有的器件都假设它的输入信号（其他器件的输出）是可信的，因此形成了一条“盲目信任链”。

  这条盲目信任链可能导致恶意信号可以在整个信号链中传播而不被检测到。

5.1.6 传感器的标定

- **定义：**

  传感器的标定是利用某种标准仪器对新研制或生产的传感器进行技术检定和标度；它是通过实验建立传感器输入量与输出量间的关系，并确定出不同使用条件下的误差关系或测量精度。

  传感器的校准是指对使用或储存一段时间后的传感器性能进行再次测试和校正，校准的方法和要求与标定相同。

- **传感器的标定分为静态标定和动态标定两种。**
  - **静态标定**的目的是确定传感器静态特性指标，包括线性度、灵敏度、分辨率、迟滞、重复性等。
  - **动态标定**的目的是确定传感器的动态特性参数，如频率响应、时间常数、固有频率和阻尼比等。
  - 对传感器的标定是根据**标准仪器与被标定传感器的测试数据**进行的，即利用标准仪器产生已知的非电量并输入到待标定的传感器中，然后将传感器的输出量与输入的标准量进行比较，从而得到一系列标准数据或曲线。

5.1.6 传感器的标定

- **在国内，标定的过程一般分为三级精度：**
  - 国家计量院进行的标定是**一级精度**的标准传递。
  - 在国家计量院标定出的传感器叫标准传感器，具有**二级精度**。
  - 用标准传感器对出厂的传感器和其他需要校准的传感器进行标定，得到的传感器具有**三级精度**，这就是我们在实际测试中使用的传感器。

5.2 概述、安全模型、换能攻击、防护方法

传感器测量安全

物联网终端安全之传感器与执行器安全

5.2 传感器测量安全

1. 测量安全概述

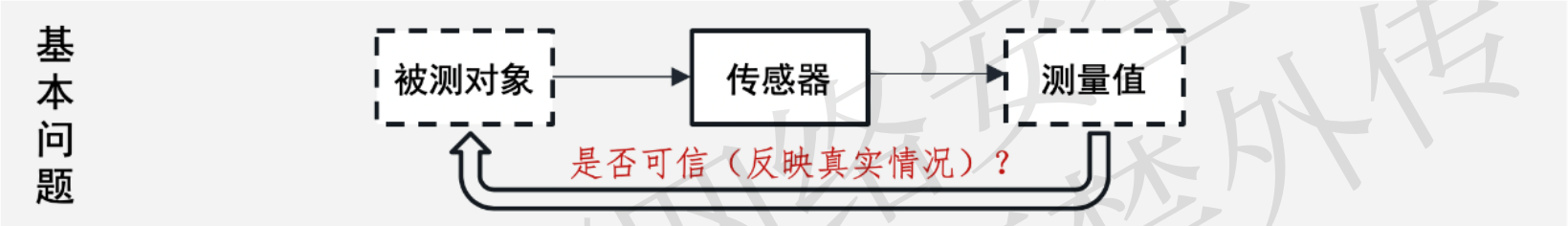
2. 传感器简单安全模型

3. 换能攻击方法

4. 换能攻击的防护方法

5.2.1 测量安全概述

5.2.1.1 基本问题与意义



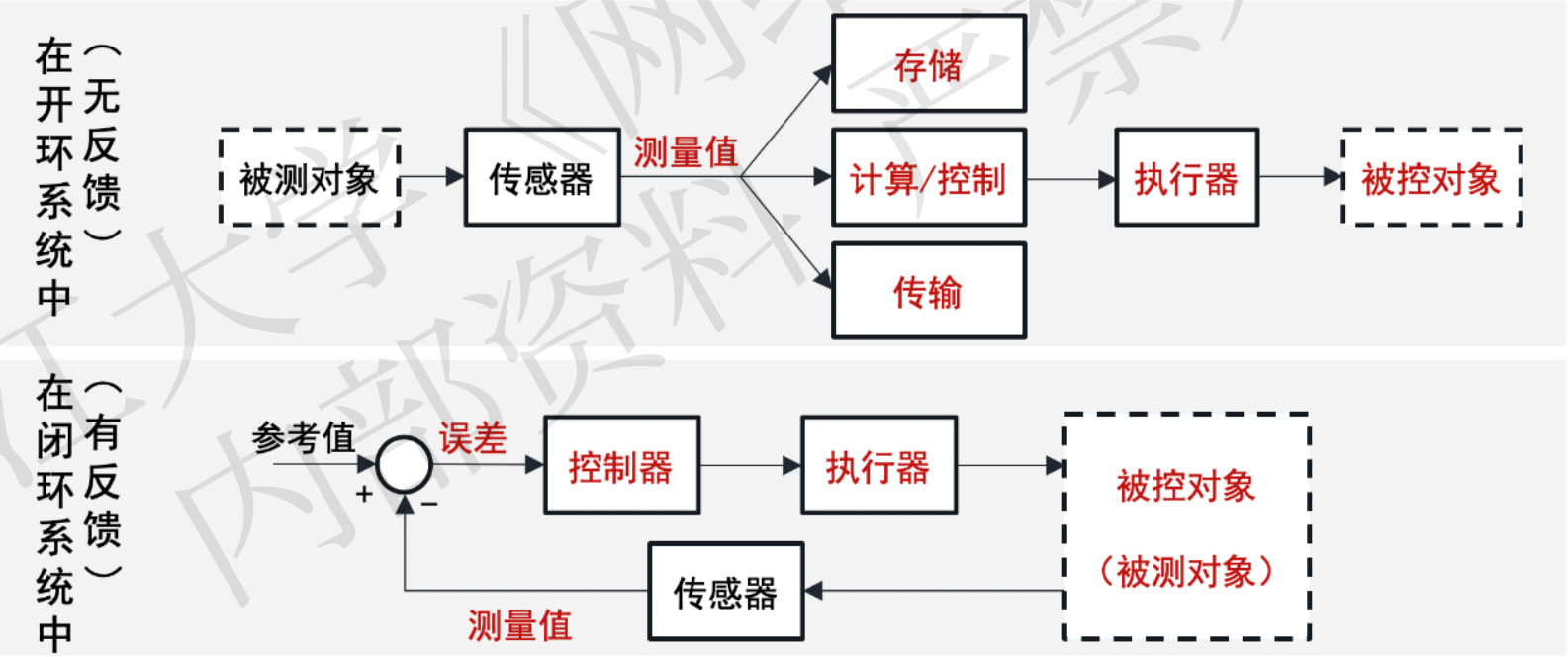
传感器测量安全的基本问题可以描述为，**传感器的测量值能否可信地反映真实的被测对象。**

举例：在实际温度为20摄氏度的情况下，热电偶测量的温度为 -100摄氏度；在一个安静的环境中，麦克风记录到了人耳听不到的声音；静置的加速度计测量到了运动时的加速度等等。

5.2.1 测量安全概述

5.2.1.1 基本问题与意义

思考：如果传感器的测量值不可信，那么对于使用这些不可信测量值的系统和设备会有什么样的影响？



5.2.1 测量安全概述

5.2.1.1 换能攻击的概念

- **定义**：换能攻击（Transduction Attack）是一类利用传感器的设计缺陷，通过产生并发射物理信号来影响传感器测量的攻击。

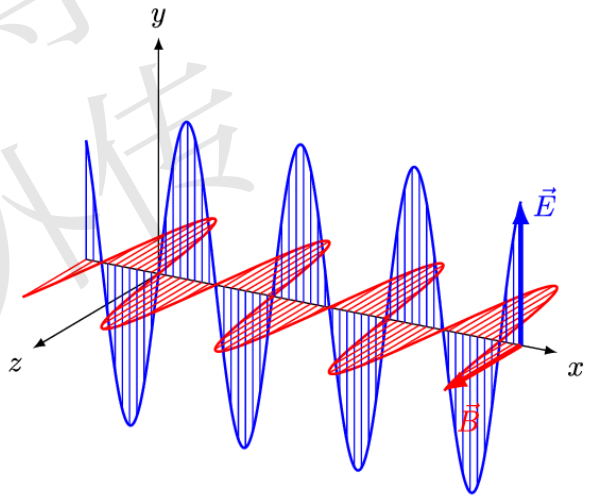
- **解释**：攻击者产生的物理信号可以通过有意或无意的换能过程（transduction）转换为传感器内部的模拟电信号，从而影响传感器的输出。这类攻击不需要和传感器有实际的物理接触，因此具有较高的隐蔽性。

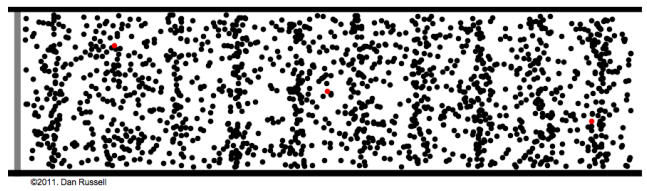
5.2.1 测量安全概述

5.2.1.2 换能攻击的物理信号

包括但不限于以下几类：

- **电磁波**是指同相振荡且互相垂直的电场与磁场，在空间中以波的形式传递能量和动量。电磁波的传播不需要依靠介质，其在真空中其传播速度为光速。按照频率可以将电磁波分为无线电波、微波、红外线、可见光、紫外线、X射线和伽马射线。
- **声波**是一种可以在气体、固体、液体中传播的机械波。按照频率可以分为次声波、可听声波和超声波。



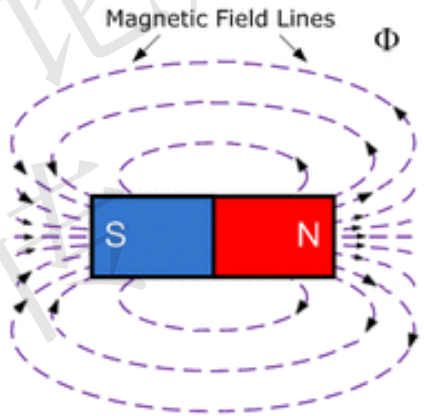


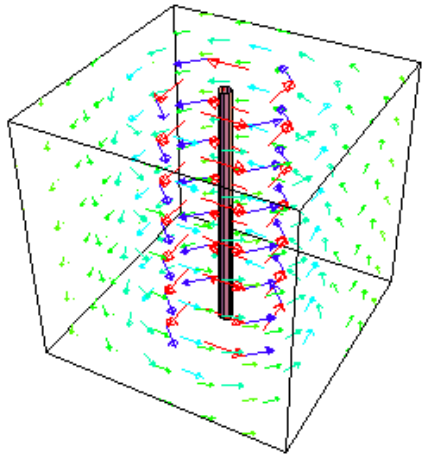
5.2.1 测量安全概述

5.2.1.2 换能攻击的物理信号

- **磁场**是由磁体、运动的电荷或电场的变化而产生的物理场。处于磁场中的磁性物质或电流会因为磁场的作用而感受到磁力。

- **电场**是存在于电荷周围能传递电荷与电荷之间相互作用的物理场。电场对场中其他电荷有作用力。





5.2.1 测量安全概述

5.2.1.3 换能攻击的分类

换能攻击可能对传感器的测量值实现两种程度的控制：

1. 拒绝服务攻击（Denial-of-Service, DoS）

- **定义**：此类攻击的目的是阻止传感器输出可用的测量值。在此类攻击下，传感器的测量值通常是攻击者无法控制或预测的。

- **举例**：一个非常强的声音干扰，如果**其频率与陀螺仪固有的谐振频率一致**，可能导致陀螺仪输出一个看似随机的角速度测量值。对于依赖陀螺仪进行飞行姿态控制的无人机来说，这种攻击会导致其无法维持稳定的飞行，可能导致无人机的坠毁。

5.2.1 测量安全概述

5.2.1.3 换能攻击的分类

2. 欺骗攻击（Spoofing）

- **定义**：此类攻击的目标是造成传感器输出一个看似正确实则错误的测量值。与拒绝服务攻击的区别是，在此类攻击下攻击者通常可以部分或完全控制传感器的测量值。

- **举例**：一段特殊制作的声音信号可以欺骗手机中加速度计的输出，从而实现对与其绑定的遥控汽车行为的控制。

5.2.1 测量安全概述

5.2.1.5 攻击者假设

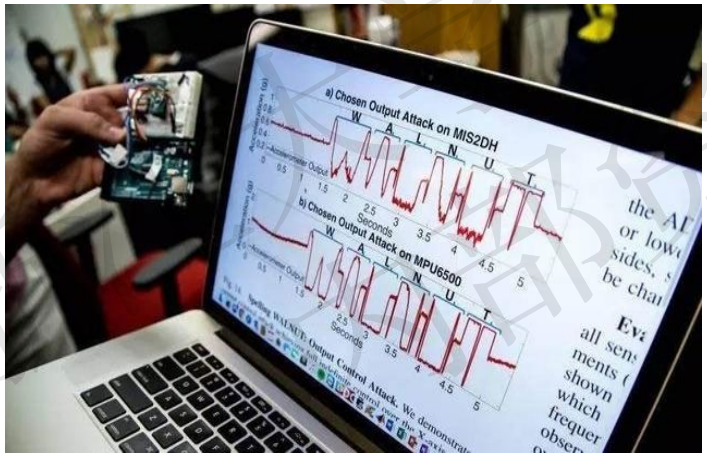
- **影响模拟信号。**攻击者通过产生和发射恶意物理信号直接影响传感器电路中的模拟信号，而非数字信号，例如数据的处理和传输过程。
- **传感器分析。**虽然攻击者在攻击之前不能对目标传感器进行任何改动，但他可以在攻击之前可能接触到类似或相同型号的传感器并进行分析和评估，**通过逆向分析的方式获取传感器的工作频率、带宽、信号波形、电路组成和特性等重要设计参数**。这些分析结果可以被用于实际的换能攻击中。
- **攻击距离。**换能攻击的攻击距离通常是由恶意物理信号的发射功率决定的，因此攻击者可能通过增大发射功率来增加攻击距离，因此本节重点讨论攻击距离之外的攻击可行性要素。

5.2.1 测量安全概述

5.2.1.6 换能攻击的例子

1. MEMS加速度传感器和陀螺仪

美国密歇根大学&浙江大学的一项研究成功利用声波攻击了MEMS加速度传感器，并且成功入侵智能手机和智能可穿戴设备Fitbit手环。通过播放不同的恶意音乐文件，控制加速度传感器，让三星Galaxy S5 手机的芯片输出信号拼出单词“WALNUT”，或控制遥控玩具汽车。



图a. "WALNUT"攻击实验

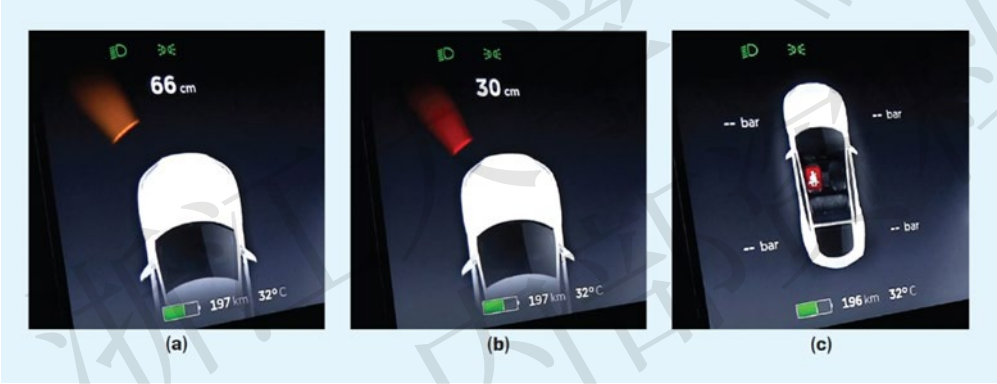
图b. 对玩具汽车的攻击

5.2.1 测量安全概述

5.2.1.6 换能攻击的例子

2. 超声波传感器

2016年就出现了针对Tesla汽车传感器的攻击案例，研究人员欺骗传感器使车载系统对物体的距离判断错误，或识别到影子障碍物，导致遇到障碍物未能停车或者在没有障碍物的情况下紧急制动，从而造成事故的发生。



图a. 特斯拉自动驾驶汽车在攻击下未能检测到障碍物

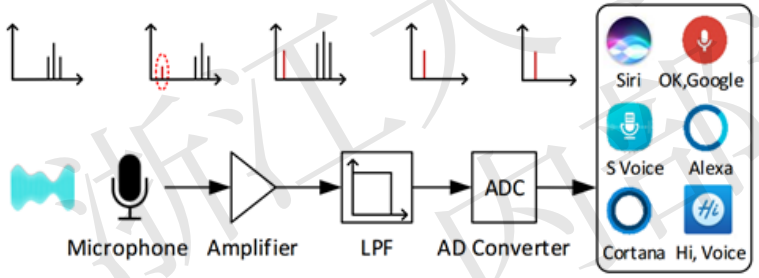
图b. 特斯拉Model S在该停车时不停车

5.2.1 测量安全概述

5.2.1.6 换能攻击的例子

3. 麦克风传感器

随着Siri、Google Now、Alexa等语音助手变得越来越流行，其面临的安全问题也日益突出。“海豚攻击”等利用智能设备（例如手机）麦克风电路的漏洞，无声地控制其执行相应的操作。例如：拨打付费或者监听电话，操作汽车导航系统、购物、无声解锁智能手机等。因此，攻击者可以在用户不知道的情况下操纵其智能设备，造成隐私泄露、财产损失等安全问题。



图a. 海豚音攻击原理图

图b. 远距离攻击演示

主观题 1分

设置

思考：

如何理解和分析传感器的测量安全问题?

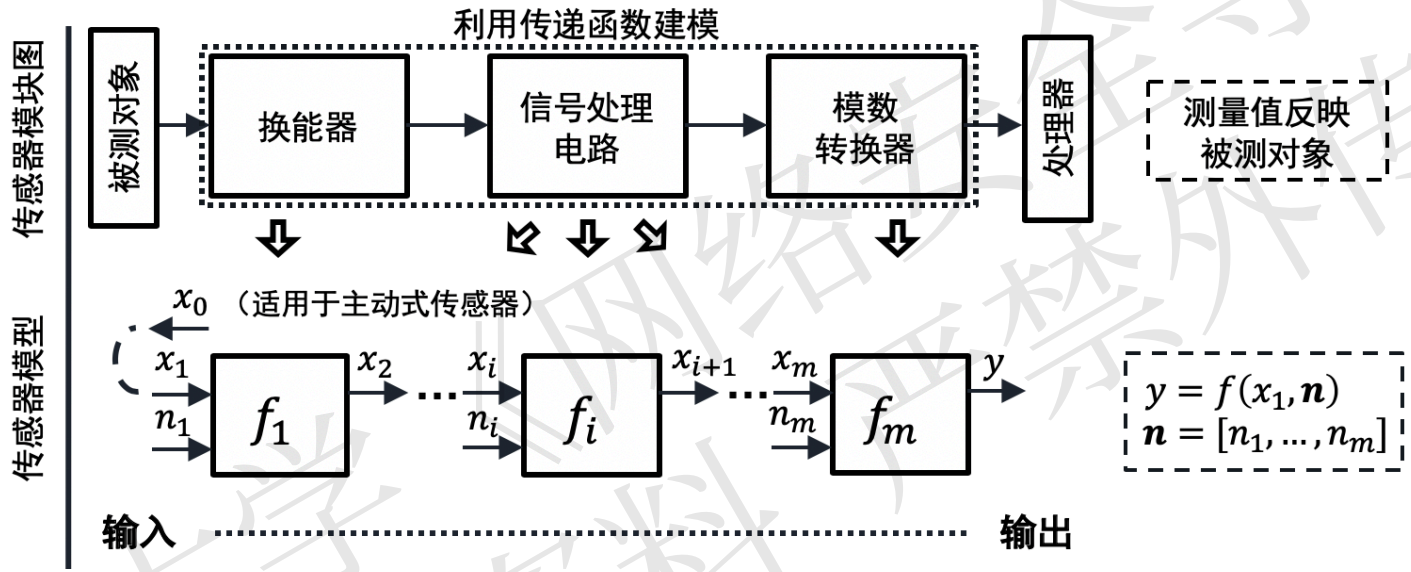
换能攻击是怎样实现的?

该如何防护换能攻击?

作答

5.2.2 传感器简单安全模型

5.2.2.1 传感器模型



可以将传感器的第 i 个组件的输入输出关系用其(时域)传递函数 f_i 描述:

$$x_{i+1} = f_i(x_i, n_i)$$

其中传递函数的输入包括正常信号 x_i 和噪声信号 n_i，输出信号为 x_{i+1}。本节将传感器简化为一个由其主要构成组件的级连模型，因此 x_{i+1} 同样是下一个（第 $i+1$ 个）组件的输入。

5.2.2 传感器简单安全模型

5.2.2.1 传感器模型

- **举例**：一些传感器常用的传递函数，以最常用的加性噪声为例:

  - 一个**线性的传递函数**可以表示为 $x_{i+1}= c_0 + c_1(x_i + n_i)$，其中 c_0 是函数的截距， c_1 是斜率。线性的传递函数被用于描述很多传感器组件的理想或简化状态，例如位置换能器和放大器。

  - **非线性的传递函数**适用于描述大部分传感器组件的实际工作状态。常用的包括：对数函数 $x_{i+1}= c_0 + c_1 \ln(x_i + n_i)$(光电二极管)、指数函数 $x_{i+1}= c_1 e^{k(x_i+n_i)}$(热敏电阻)、幂函数 $x_{i+1} = c_0 + c_1(x_i + n_i) + c_2(x_i + n_i)^2$（硅电阻传感器）等。其他情况可以用更高阶的幂级数描述。

5.2.2 传感器简单安全模型

5.2.2.1 传感器模型

我们可以将级连的传感器组件表示为如下所示级连的传递函数：

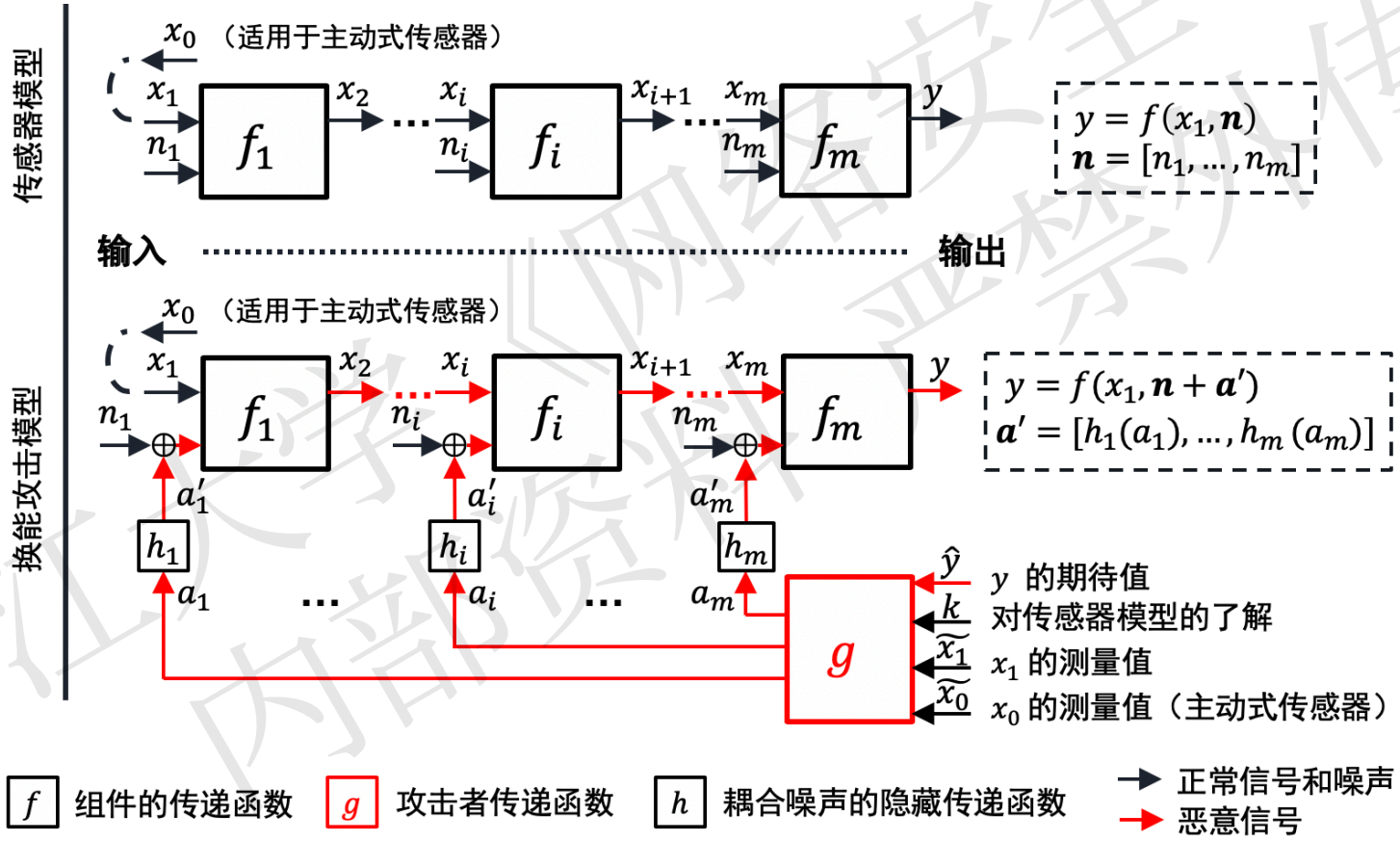
$$y = f_m(\cdots f_2(f_1(x_1, n_1), n_2)\cdots, n_m)$$

其中最终输出 y 是传感器的测量值，m 是级连的传感器组件数量。因此传感器的输入包括换能器处接收的物理激励 x_1 以及每个组件处收到的噪声。如果我们将所有组件收到的噪声表示为一个向量 $\boldsymbol{n} = [n_1, n_2, \ldots, n_m]$，将整个传感器的传递函数表示为 f，那么级连的传递函数可以简化为：

$$y = f(x_1, \boldsymbol{n})$$

5.2.2 传感器简单安全模型

5.2.2.2 换能攻击模型



5.2.2 传感器简单安全模型

5.2.2.2 换能攻击模型

在传感器模型的基础上，**换能攻击可以定义为通过向物理信号或电信号形态的正常信号 x_i 注入恶意噪声最终实现对传感器测量值 y 的篡改**。在换能攻击下的传感器测量值可以表示为：

$$y = f(x_1, \boldsymbol{n} + \boldsymbol{a}')$$

其中 $\boldsymbol{a}' = [a_1', a_2', \ldots, a_m'] = [h_1(a_1), h_2(a_2), \ldots, h_m(a_m)]$ 是攻击者向传感器注入的恶意噪声的向量，a_i' 是向第 i 个传感器组件注入的噪声，它来自于攻击者产生的物理信号a_i，$\boldsymbol{n} + \boldsymbol{a}' = [n_1 + a_1', n_2 + a_2', \ldots, n_m + a_m']$。**$\boldsymbol{h}_\mathbf{i}$ 是第 i 个传感器组件前的描述外部噪声传递与耦合过程的隐藏传递函数**，它同时描述来自外部的正常噪声信号 n_i 和恶意噪声信号a_i' 的耦合过程。

5.2.2 传感器简单安全模型

5.2.2.2 换能攻击模型

注入的信号 a_i' 和正常的噪声信号 n_i 是同种类型的信号，它们结合（通常为叠加）后的信号作为噪声可影响被干扰组件的输出和传感器的测量值。攻击者产生的物理信号也可以用一个传递函数表示：

$$a = [a_1, a_2, \ldots, a_m] = g(\hat{y}, k, \widetilde{x_1}, \widetilde{x_0})$$

$\hat{y}$ 是攻击者想要制造的传感器测量值，k 代表攻击者对目标传感器模型的了解，$\widetilde{x_1}$ 是攻击者对目标传感器所测量的物理量的测量值，当目标传感器为主动式传感器时，攻击者还需要测量目标传感器发出的物理激励 $\widetilde{x_0}$ 以实现对其测量值的完全控制。

5.2.2 传感器简单安全模型

5.2.2.4 讨论

我们可以看出一个换能攻击可能涉及到两类基本步骤：

1. **信号注入步骤**涉及恶意物理信号转换为传感器中的恶意电信号的换能过程，主要包括可能影响换能（即信号注入）的一系列特性，例如信号注入点和信号参数等。
2. 仅仅有高效的信号注入不一定能造成攻击者期待的传感器测量值。因此，换能攻击可能还需要一系列的**测量构造步骤**。这些步骤涉及如何构造期待的传感器测量值的一系列特性与方法，考虑的是如何进一步构造恶意物理信号使得注入的信号可以保留在传感器的信号调理电路中并造成传感器输出期待的测量值。

5.2.3 换能攻击方法

5.2.3.3 构造换能攻击

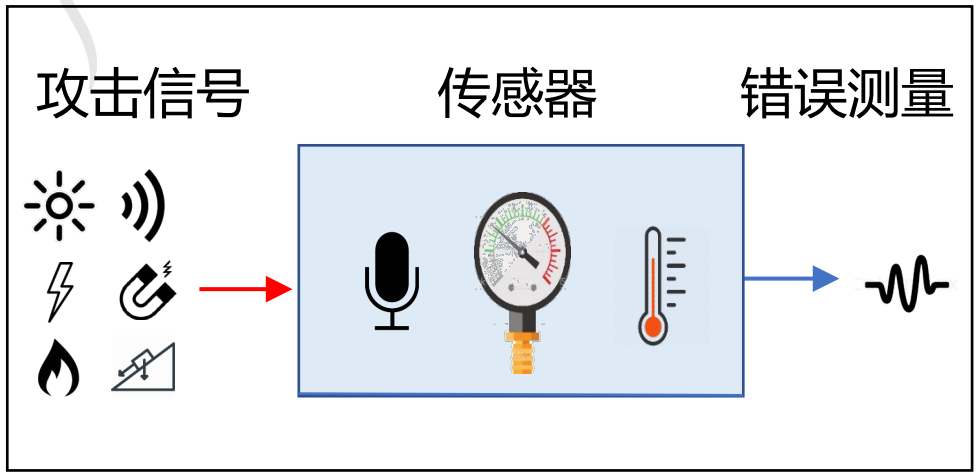
攻击者可以根据目标传感器和希望实现的后果，将不同的信号注入和测量构造步骤串联形成换能攻击的攻击链。在设计换能攻击时，攻击者可以通过分析目标传感器的信号调理链路确定可能利用的信号注入和测量构造步骤，并基于此构造恶意的物理信号。因此，对**传感器系统组件、模型和传递函数的了解**对于建立简单传感器安全模型是至关重要的。

5.2.3 换能攻击方法

5.2.3.1 信号注入步骤

为成功且高效地向传感器中注入恶意信号，攻击者需要同时考虑信号的注入点和包括信号的**类型、幅度、频率**等可能影响信号注入效率的因素

1. 信号注入点和信号类型
   a) 换能器之前的注入点
   b) 换能器之后的注入点
2. 高效注入和信号频率
   a) 幅度
   b) 频率
3. 带内信号和带外信号



5.2.3 换能攻击方法

5.2.3.1 信号注入步骤

1. 信号注入点和信号类型

   思考：注入信号的类型由什么决定?

2. 高效注入和信号频率

   思考：如何通过选择注入信号的幅度和频率提高注入效率?

3. 带内信号和带外信号

   思考：注入带外信号有什么好处？有什么问题?

   （例如，向语音助手的麦克风注入超声波）

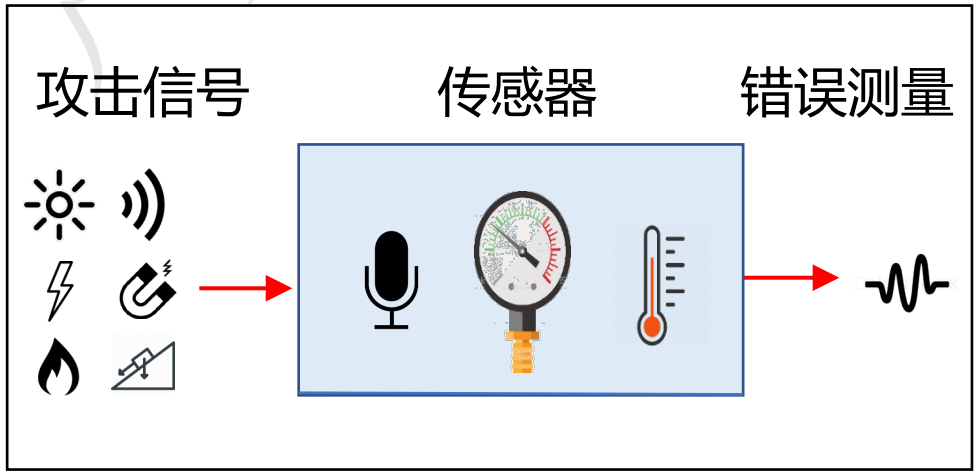
5.2.3 换能攻击方法

5.2.3.2 测量构造步骤

为使得注入的信号可以保留在传感器的信号调理电路中并造成传感器输出期待的测量值，攻击者需要在信号注入的基础上，进一步构造恶意物理信号，利用传感器硬件的特性实现期望的传感器测量值。

常见的测量构造步骤：

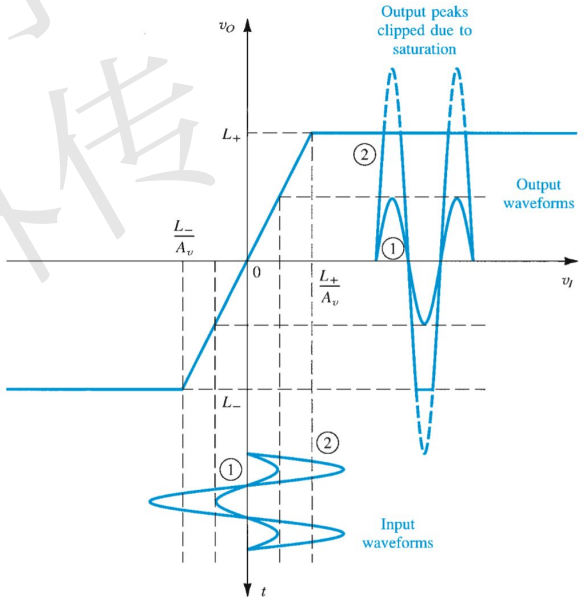
1. 饱和
2. 交调失真
3. 包络检测
4. 混频
5. 滤波



5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——饱和

- **定义**：饱和指某种物理量无法超过一定的阈值，是一种模拟电路中常见的现象。
- **举例**：如下公式所示，当输入超过一定阈值时一个放大器就可能进入饱和状态，此时放大器的输出不会继续随着输入线性增长，因而出现了限幅：



$$f_i(x_i, n_i + a_i') = \begin{cases} c_1\mathcal{A}(x_i, n_i + a_i'), & \text{当}\mathcal{A}(x_i, n_i + a_i') \le k \\ const, & \text{当}\mathcal{A}(x_i, n_i + a_i') > k \end{cases}$$

其中$\mathcal{A}(x_i, n_i + a_i')$指$x_i$和$n_i + a_i'$结合后的信号强度，$c_1$是放大系数，$k$是保和点。

- **利用**：攻击者可以通过饱和现象向电路中注入直流信号。

5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——交调失真

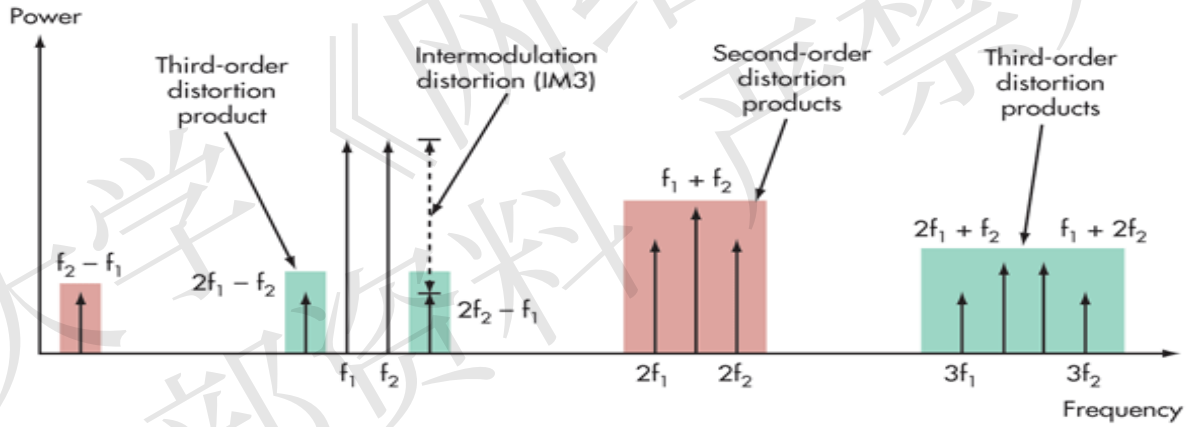
- **定义**：当一个含有多个频率分量的信号经过一个非线性器件时就有可能发生交调失真（Intermodulation Distortion, IMD）。常见的非线性器件包括放大器、二极管、换能器等，甚至模数转换器因为其内部存在的放大器也有一定的非线性。
- **原理**：交调失真会导致输出信号中出现输入信号里不包含的频率分量，它们主要出现在输入信号中频率的和与差以及其倍数。
- **思考**：对于以下非线性传递函数，假设混合后的信号$x_i + n_i + a_i'$包含两个频率，f_1和f_2（$f_1 > f_2$），输出的频率会包括哪些?

$$x_{i+1} = c_0 + c_1(x_i + n_i + a_i') + c_2(x_i + n_i + a_i')^2$$

5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——交调失真

假设混合后的信号$x_i + n_i + a_i'$包含两个频率，f_1和f_2（$f_1 > f_2$），此时输出x_{i+1}包含频率f_1、f_2、$f_1 - f_2$、$f_1 + f_2$、$2f_1$、$2f_2$，以及直流分量。

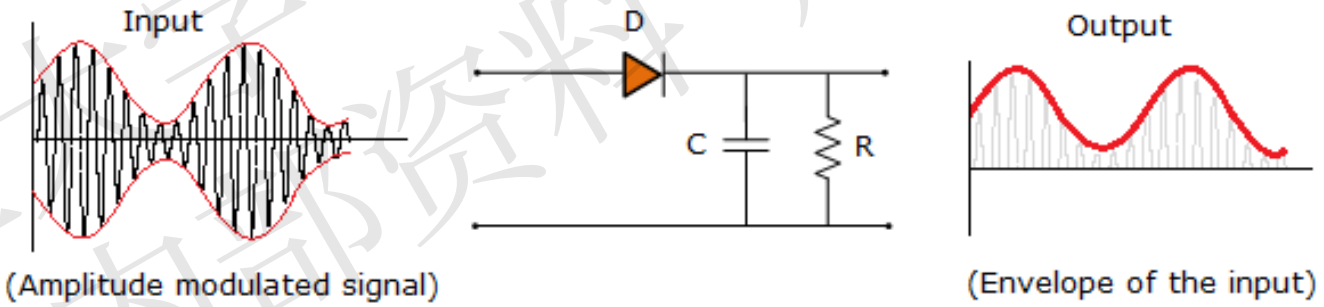


利用：注意其中$f_1 - f_2$是可能小于f_1和f_2的，因此攻击者可能利用交调失真将恶意的带外信号转化为带内信号。例如，一个调幅（AM）信号经过交调失真可以无意中实现类似解调的效果。事实上，交调失真在混频器等射频电路中已被设计用于降频的目的。

5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——包络检测

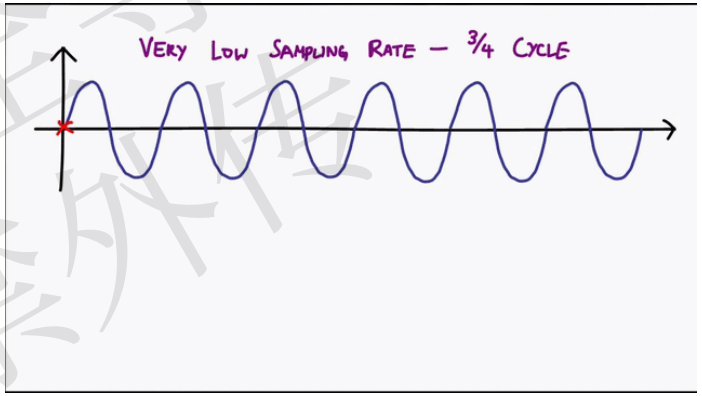
二极管和电容是模拟电路中非常常见的器件，特别是用于静电放电保护。然而它们也可能成为简单的包络检测器，从而解调调幅信号。Foo Kune等人在麦克风电路中发现了能够解调调幅信号的二极管和电容对。



5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——混频

- **定义**：根据奈奎斯特-香农采样定律，如果一个信号的频率高于采样率的一半，那么这个信号将与其他频率的信号无法区分，这种现象被称为混频（Aliasing）。

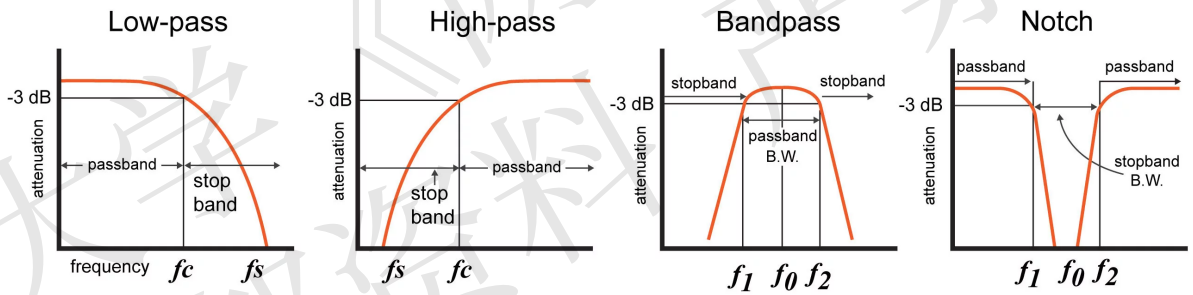


- **举例**：如果模数转换器的采样率是F_s，那么频率为f $(f < F_s)$的信号将与频率为$F_s - f$的信号无法区分。
- **利用**：攻击者可能利用混频现象将恶意的带外信号转换为带内信号。例如，Trippel等人和Tu等人通过调整声音信号的频率、幅度、相位实现对MEMS加速度计或陀螺仪的模数转换器输出的控制。Foo Kune等人通过将载波频率设为与模数转换器的采样率相同来解调注入的信号。

5.2.3 换能攻击方法

5.2.3.2 测量构造步骤——滤波

- **现象：**在理想情况下，一个模数转换器前的滤波器应当去除所有的带外信号并避免混频的发生。然而在现实中大部分的滤波器都有一个截止频率范围，在这个范围中带外信号只会被部分衰减。



- **利用：**攻击者可以利用滤波器的这一特性构造能够经过滤波器但是会影响其他传感器组件的信号。Trippel等人发现许多MEMS加速度计中的滤波器都有极宽的截止频率范围，因此无法完全去除攻击者注入的高频信号。

5.2.4 换能攻击的防护方法

- 对换能攻击的防护可以分为两类，分别是**攻击检测**与**攻击抵御**。攻击检测旨在检测到换能攻击的存在，而攻击抵御则是为了抵御攻击对传感器测量值的影响，让传感器即使在攻击发生时也可以有可信的输出。

- 攻击检测方法
  - 检测信号注入步骤
    - 带外信号检测
    - 验证执行
    - 输出随机
  - 检测测量构造步骤
    - 饱和检测
    - 交调失真的特征检测

- 攻击抵御方法
  - 屏蔽
    - 物理隔离
    - 攻击面缩减
  - 滤波
  - 随机化
  - 改进组件质量
  - 传感器融合

5.2.4 换能攻击的防护方法

攻击检测方法

检测信号注入步骤——带外信号检测

防御者可以利用额外的换能器有针对性地对注入的带外信号进行检测。例如，使用额外的麦克风就可以检测到攻击MEMS加速度计和陀螺仪的共振频率声音。因为传感器的正常工作只依赖于带内信号，对带外信号的检测并不会影响传感器的工作。

检测测量构造步骤——交调失真的特征检测

研究表明利用交调失真进行信号解调的攻击可能会在模拟信号中留下可识别的特征。Zhang等人通过检测高频语音信号（500 Hz – 1 kHz）的强度来识别利用交调失真解调的无声语音指令，类似的，Roy等人提出计算50 Hz以下的频段与高频信号的相关性。由于这些特征是由交调失真引入的，攻击者无法轻易在传感器的模拟信号中消除这些特征。

5.2.4 换能攻击的防护方法

攻击抵御方法

屏蔽——物理隔离

防御者可根据实际的应用场景增加物理隔离以衰减进入传感器的外部物理信号，例如使用法拉第笼来屏蔽电磁波。常见的物理隔离包括屏蔽导线、隔音、光屏蔽。

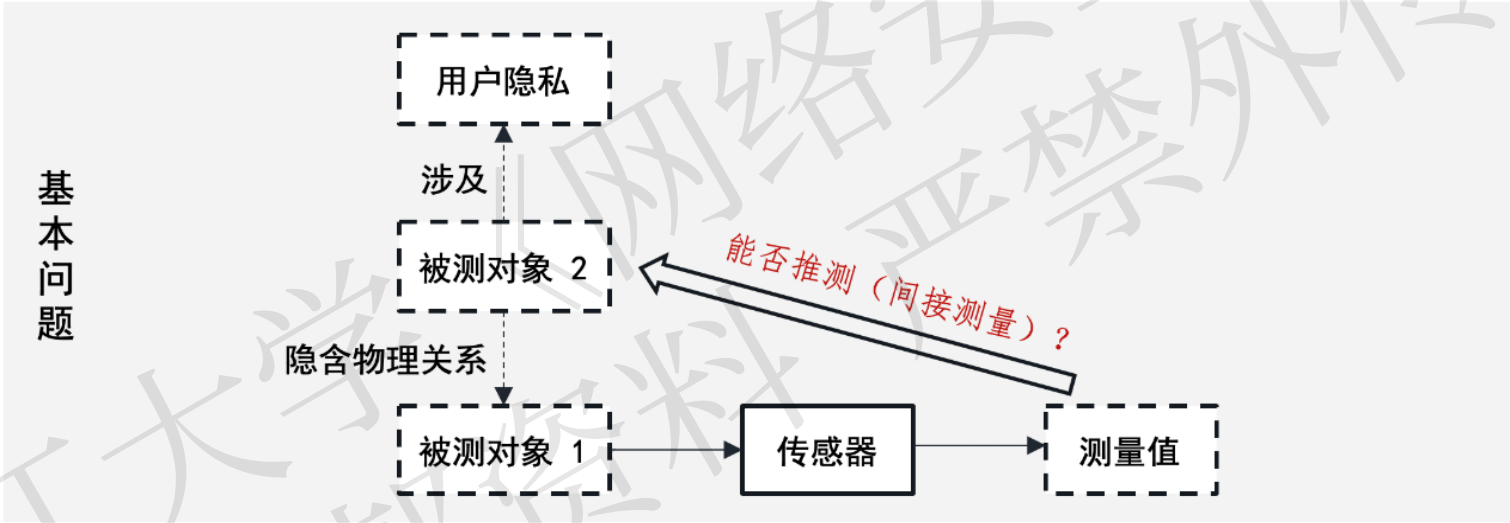
随机化——输出随机化

当主动式传感器的输出波形变得随机化之后，传感器就可以集中搜寻输入信号中与输出的随机性匹配的有用信号，而由于攻击者并不了解该如何产生与之匹配的随机信号，攻击对传感器的影响变得有限。Xu等人为汽车超声波传感器提出的波形随机化方法可以在攻击存在的情况下获得可信的测量值。Petit等人和Shin等人也为激光雷达防护提出了随机探测的方法。

5.3 传感器隐私安全概述

- **概述：**传感器的隐私安全是攻击者利用传感器的信息推测出用户非直接测量的附加信息，这些信息会导致用户隐私的泄露，如图所示。

  由于传感器数据获取的权限并不是很严格，所以能被攻击者利用。



- **传感器隐私安全可以分为三类：**
  - 1.利用感知信息推测用户行为；
  - 2.利用感知信息推测设备指纹；
  - 3.利用感知信息推测用户身份。

5.3.1 推测用户行为

5.3.1.1 追踪用户位置信息

- 与运动传感器相关的一个问题是位置信息的泄漏。

  即使用户关闭了手机的位置跟踪服务，例如GPS和通信接口，陀螺仪传感器也可以定位和跟踪用户，其它可以用于位置追踪的传感器还包括：麦克风传感器，光传感器，加速度传感器，磁力传感器等。

- 案例：

  利用智能手机运动传感器获取用户的旅行路线和位置。该研究通过大量实验表明，用户非常容易受到追踪。运动传感器不仅可以跟踪人的位置，还可以预测旅行路线。例如，通过收集加速度计数据以推断用户的轨迹。

5.3.1 推测用户行为

5.3.1.1 追踪用户位置信息

案例：

利用智能手机运动传感器获取用户的旅行路线和位置。该研究通过大量实验表明，用户非常容易受到追踪。运动传感器不仅可以跟踪人的位置，还可以预测旅行路线。例如，通过收集加速度计数据以推断用户的轨迹。

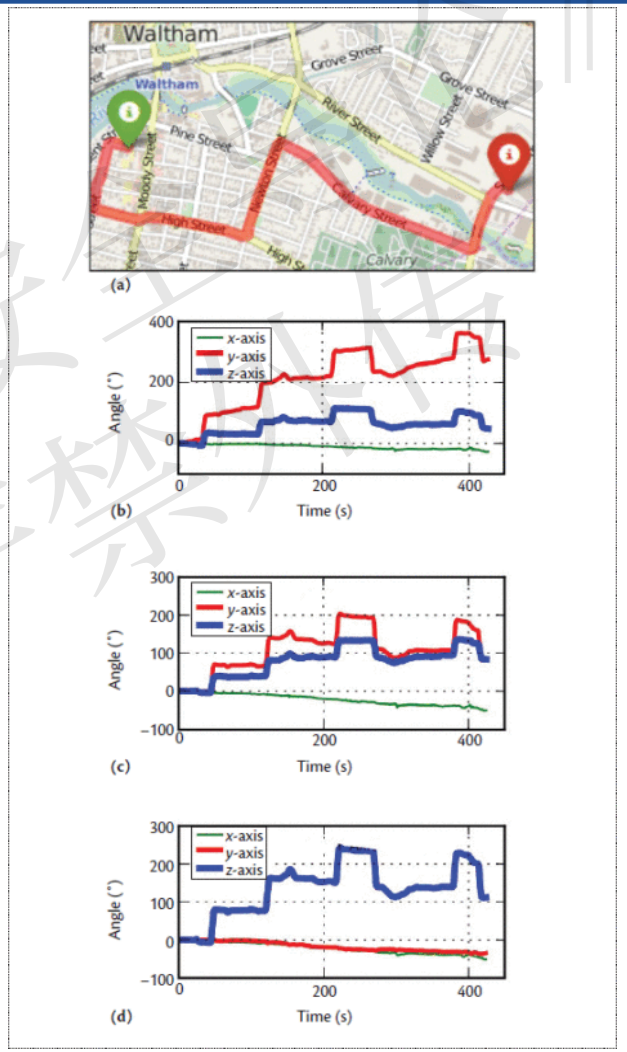


图5.3.1.1 通过误差补偿等措施，陀螺仪的数值可以反推行进路线

图片来源及参考文献：Narain, S., Vo-Huu, T.D., Block, K., Noubir, G.: The perils of user tracking using zero-permission mobile apps. IEEE Security and Privacy 15(2), 32–41 (2017)CrossRefGoogle Scholar

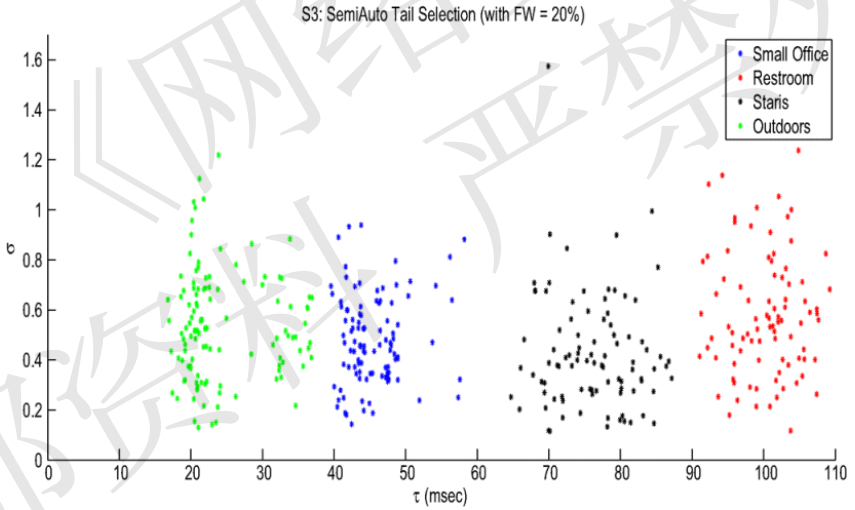
5.3.1 推测用户行为

5.3.1.2 推测用户活动和场景

传感器数据不但可以用于追踪用户的位置，还可以用来推测用户的活动或者所在的场景。

- 案例：

Audio Forensics开发的声学环境识别系统（AEI）可以推测出用户所在的环境。他们构建了一个模拟环境噪声的系统，在四个常见地点（小型办公室，洗手间，楼梯和室外等）的评估表明，它能够很好地实现场景的区分。



图片来源及参考文献： Malik, H.: Acoustic environment identification and its applications to audio forensics. Information Forensics and Security IEEE Transactions on 8(11), 1827–1837 (2013)

5.3.1 推测用户行为

5.3.1.3 窃取用户密码

与传感器相关的另一个安全问题是推测用户的密码、PIN（个人识别号）

案例：

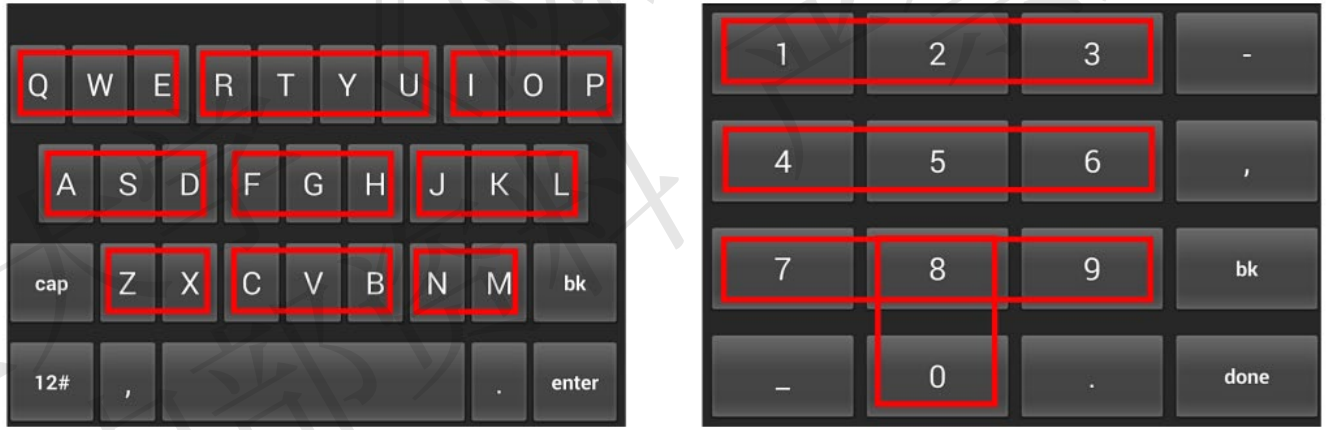
Olejniket 等人提出通过光传感器来窃取QR码，它可以使用内置的环境光传感器API从多台笔记本电脑或智能手机的浏览器中窃取敏感数据。环境光传感器安装在智能电子设备中，以自动改变屏幕亮度。当用户访问站点时，光线的颜色会相应更改。因此，攻击者可以通过**环境光传感器检测这些变化并获得用户的历史访问记录。**

该研究表明，攻击者可以使用此方法分析基于环境光传感器的亮度变化，从而能够窃取敏感数据，例如网页的QR码和身份验证机制。

5.3.1 推测用户行为

5.3.1.4 推测用户输入（键盘，手写）

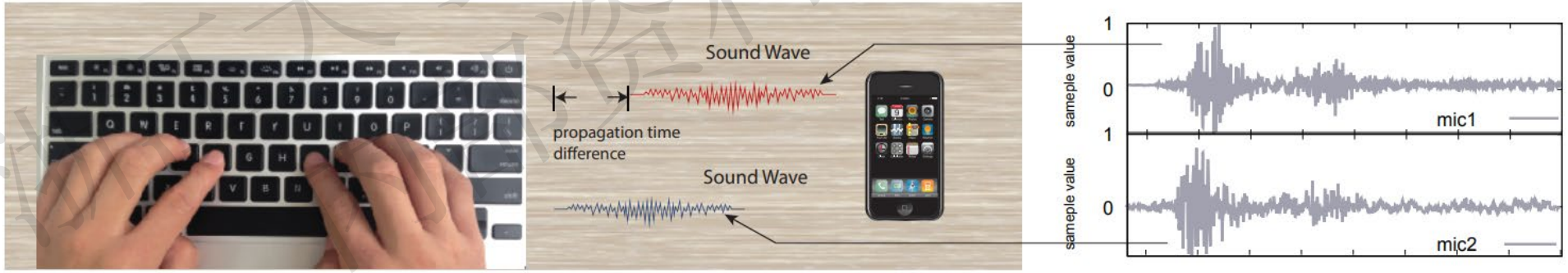
- 除了推测用户输入的密码信息，传感器数据还可以用来进一步推测用户输入的其它内容。使用运动传感器数据结合机器学习算法，不但可以推断移动设备触摸屏上触摸点的位置信息而且还可用于在智能手机触摸屏键盘上提取输入文本的整个序列。
  - 案例： Narain 融合了立体声麦克风和陀螺仪的数据，推断出用户触摸点的位置。



图片来源及参考文献：Narain, S., Sanatinia, A., Noubir, G.: Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning. In: Proceedings of the 2014 ACM conference on Security and privacy in wireless and mobile networks, pp. 201–212 (2014)

5.3.1 推测用户行为

- **5.3.1.4 推测用户输入（键盘，手写）**
  - **另一种攻击类型只使用声音信号来推测用户输入**
    - 案例：例如手写输入攻击，该类攻击通过麦克风收集手写的声音信号，基于深度学习算法，在不知不觉中识别用户书写的文字。
  - **通过主动发射声音信号并收集回声进行用户输入推测**
    - 案例： 利用手机扬声器不断发出听不见的超声波脉冲，麦克风收集受害者手写的回声，通过计算音频信号到达麦克风的时间差来恢复击键的物理位置。实验显示，打字位置的估计的准确度约为72.2%。



5.3.2 推测设备指纹

- **设备指纹概述：**

指纹原本作为一种生物统计技术用于识别身份。这个概念在20世纪60年代被引入到设备识别中。当时的设备指纹是使用具有外部可观察特征的信号构造了一个特殊的发射器识别系统，起初用于辨别雷达。此后，多种从软件或者硬件中提取指纹并用于识别、追踪网络设备的方法被提出。传感器的硬件指纹不但可以对设备进行身份识别和认证，还可以成为不法分子进行攻击的手段，例如，追踪用户导致用户信息泄露等安全问题。

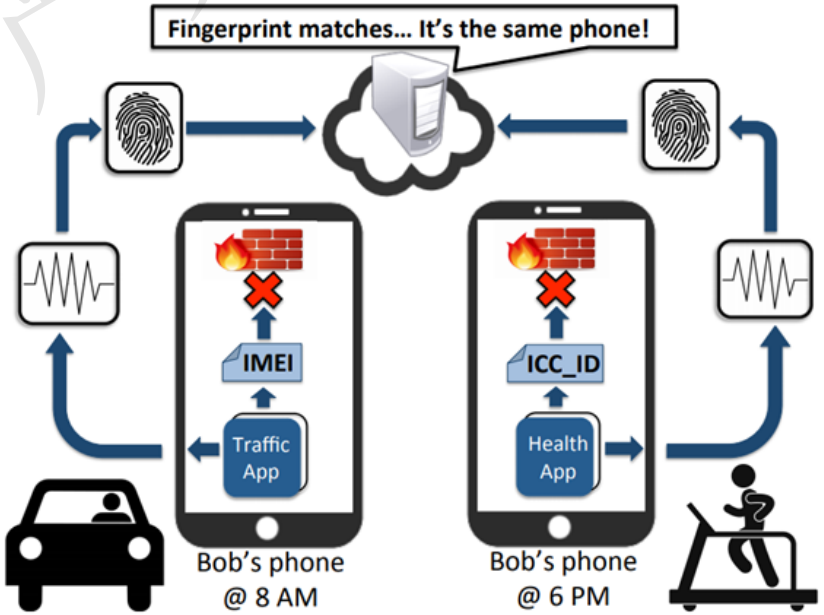


图5.3.2：小明使用由同一云后端支持的不同应用程序。 即使设备ID被阻止，导出传感器数据切片也可以使云推断出它是同一用户。

图片来源及参考文献：S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi. ccelPrint: Imperfections of Accelerometers Make martphones Trackable. In Proceedings of the 21st Annual etwork and Distributed System Security Symposium (NDSS), 2014

5.3.2 推测设备指纹

- **设备指纹原理：**

  设备指纹运用了智能手机的传感器，即便是同一型号，也存在差异的原理。

- **传感器的设备指纹：**

  硬件的细微差异在传感器制造过程中非常容易发生，这为传感器的设备指纹的存在提供了可能。可用于设备指纹的传感器包括：加速度传感器，陀螺仪，麦克风-扬声器等。

- **防御手段：**

  对于传感器指纹攻击，一个防御手段是在不影响传感器数据的精度下，将传感器的原始数据添加噪声使得传感器的唯一性被掩盖

5.3 定义与组成、安全问题

执行器安全

物联网终端安全之传感器与执行器安全

5.3 执行器

1. 执行器的定义和组成

2. 执行器安全问题

5.4.1 定义和组成

- **对于执行器最广泛的定义是：**

一种能提供直线或旋转运动的驱动装置，它利用某种驱动能源并在某种控制信号作用下工作。执行机构使用液体、气体、电力或其它能源并通过电机、气缸或其它装置将其转化成驱动作用。其基本类型有部分回转(Part-Turn)、多回转(Multi-Turn)及直行程(Linear)三种驱动方式。设备指纹运用了智能手机的传感器，即便是同一型号，也存在差异的原理。

- **执行器在自动控制系统中的作用：**

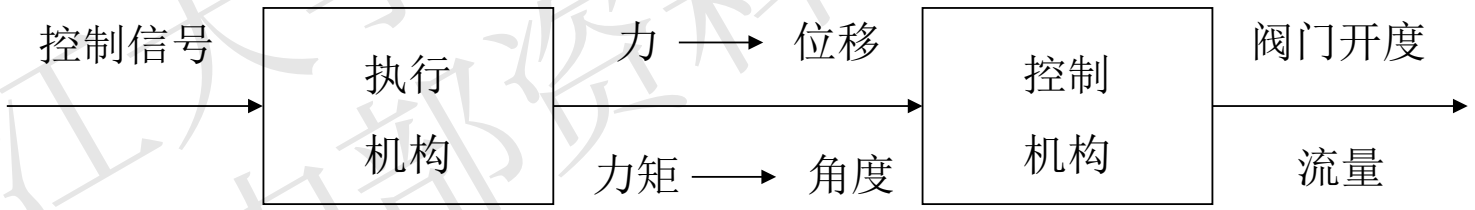
接受调节器发出的控制信号，改变调节参数，把被调节参数控制在要求的范围，从而达到生产过程化。因此，执行器是自动控制系统中极为重要且必不可少的组成部分。简单来说，驱动器是指从能源转为功率的输出，进而产生旋转、直进等机械运动的机器，藉由驱动器的带动，便可以驱动物体执行其所订定的动作行程。

5.4.1 定义和组成

- **组成：**

一般来说，执行器是由执行机构和控制机构来组成的。

其中，执行机构是执行器的推动装置，它按控制信号压力的大小产生相应的推力或扭矩， 推动控制机构动作。它是将压力信号的大小转换为阀杆位移的装置。控制机构是执行器的控制部分，它直接与被控介质接触，控制流体的流量，最常见的是调节阀，它是将阀杆的位移转换为流过阀的流量的装置。

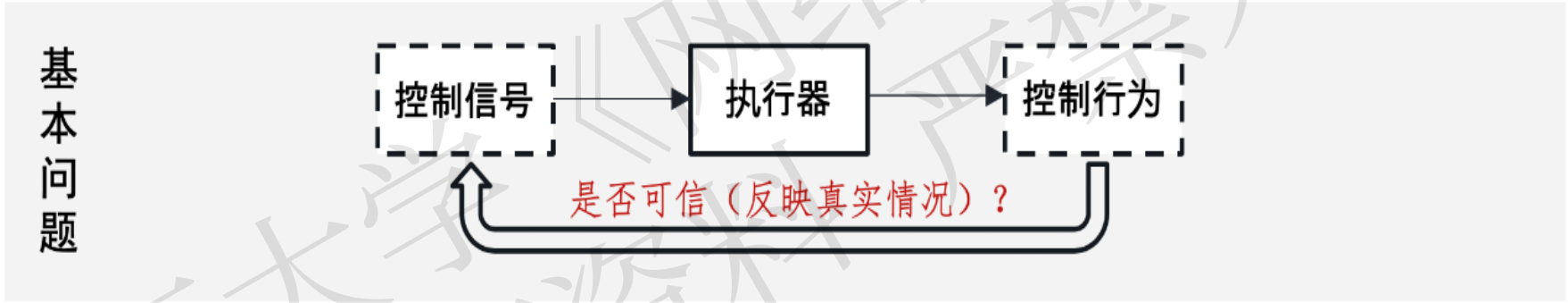


5.4.1 执行器的组成

5.4.2 执行器安全问题

执行器测量安全的基本问题可以描述为，**执行器接受的控制信号是否是可信的。**

执行器安全问题包括：**传统网络攻击**和**物理攻击。**



5.4.2 执行器安全的基本问题

5.4.2 执行器安全问题

5.4.2.1 传统网络攻击

（1）变频驱动器

黑客将注意力始终聚焦于大型的变频驱动器。因为这种驱动器在风力发电，水下作业，采矿以及供热供暖系统中有着普遍的应用，处于工业生产的核心位置。

驱动器是一种数字设备，用于设置电机的频率，控制电机的运转速度，防止电机因转速过快而抛锚。进一步，这些电机又控制着水泵，移动式系统设备，空气压缩机等的运行。

Reid Wightman，一名Digital Bond Labs实验室的安全研究员。他指出：到目前为止，我们发现至少有四个变频驱动器制造商，在他们所生产的驱动器上都有一个相同的漏洞：**驱动器能够随意读写数据，最致命的是，当一个未经授权的操作者要重新设定驱动器马达转速时，他可以直接进入系统进行更改，无需任何的身份验证。**黑客可通过远程攻击，获得设备运行的频率，进行更改，进而控制设备。

5.4.2 执行器安全问题

- **5.4.2.1 传统网络攻击**
  - （2）驱动系统攻击
    - 典型的固定翼飞机的执行器sUAS由伺服电机和直流电机组成。伺服电动机和直流电动机的形式为脉冲宽度调制（PWM）信号，是有模拟信号经过编码后的数字信号。
    - 由于执行器不与外部的任何系统相互作用，相比于其他系统，它们被认为不太容易受到网络攻击。然而，就像与外部系统隔离的传感器陀螺仪一样，是非常**容易受到物理攻击**的。

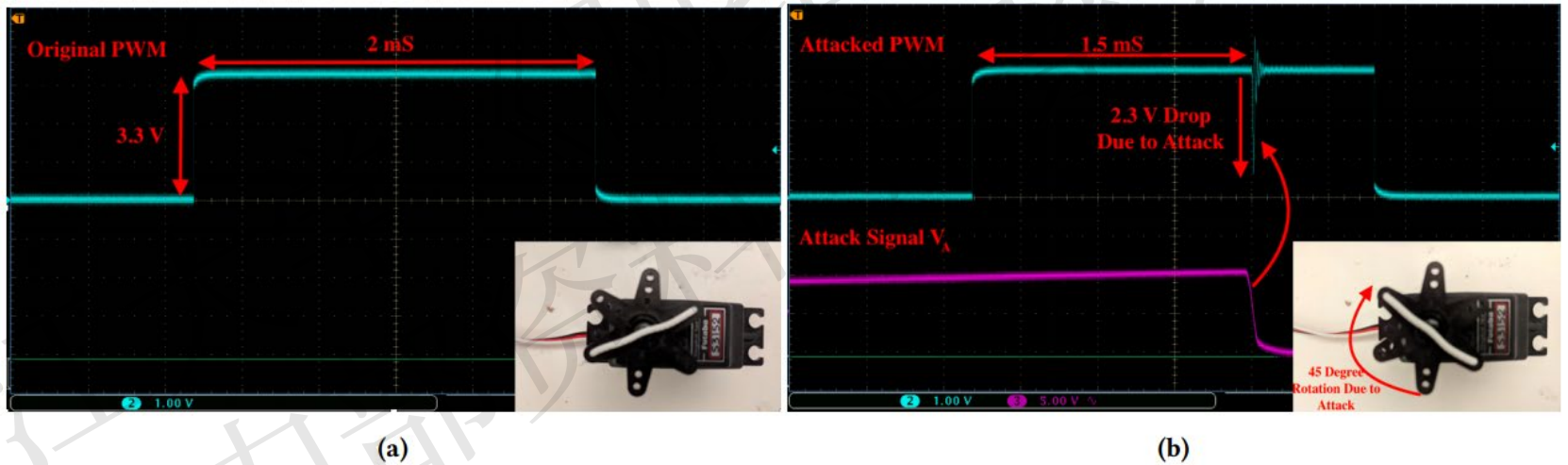
5.4.2 执行器安全问题

5.4.2.1 传统网络攻击

（2）驱动系统攻击

案例：

利用电磁干扰信号改变PWM来实现对执行器的控制，任意改变系统的输出。



(a) 原始PWM 信号和对应的伺服电机的位置

(b) 攻击信号V_A （紫色）； 被攻击的PWM信号（蓝色） 和对应的伺服电机位置

图片来源及参考文献： J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems"

5.4.2 执行器安全问题

5.4.2.2 电磁注入攻击

汽车电机控制器攻击

现有的电动汽车电机控制器的外部只有一层很厚的金属壳体。受到外界的强电磁场干扰后，电磁场在金属壳体上瞬间达到磁饱和，电磁场攻破金属壳体后瞬间就攻击电动汽车电机控制器集成电路中的核心电子器件，使电机控制器不能正常工作。

5.4.2.2.a 电机控制器在电动汽车中的位置

5.4.2.2.b 典型的电机控制器

小结

■传感器概述

定义、组成、分类、主要特性

■传感器测量安全

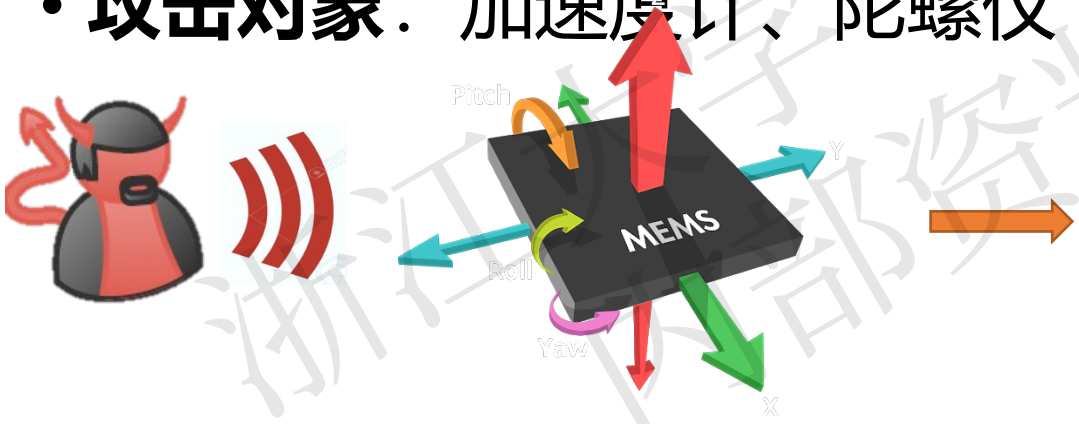
安全模型、换能攻击、安全防护

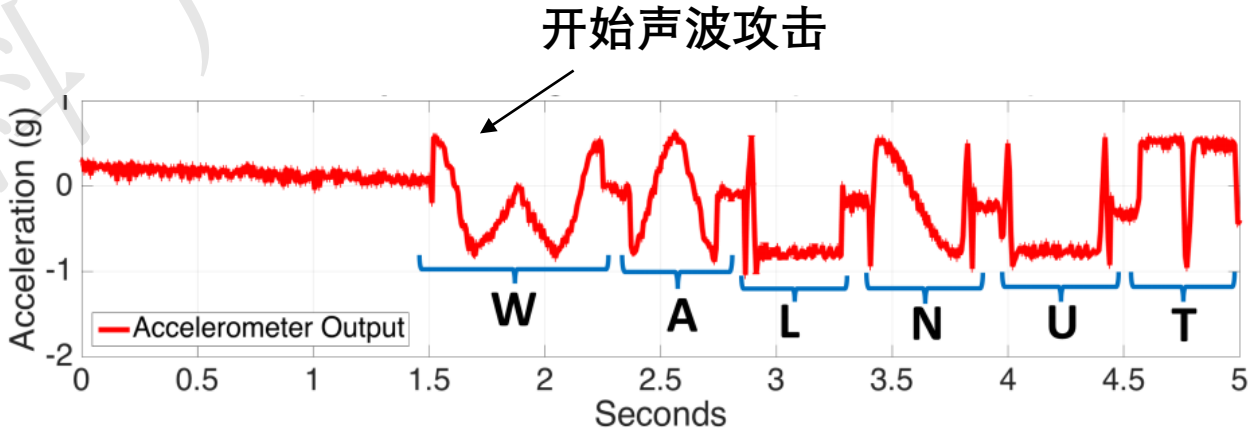
■执行器安全

定义、组成、安全问题

攻击案例1：声波攻击运动传感器

- **攻击原理**：超声波引发运动传感器内部结构**共振**，产生错误或特定读数
- **攻击对象**：加速度计、陀螺仪



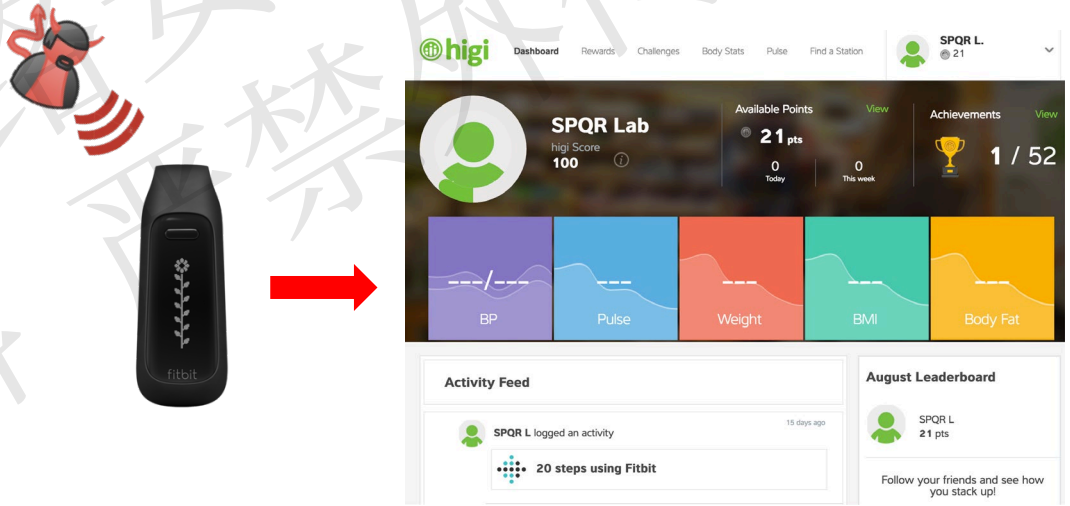


运动传感器-声波攻击

场景一：基于传感器的机器人运动控制

在正常情况下，用户可以倾斜手机至不同的角度来控制小车运动方向。通过声波攻击，小车可以在无需移动手机的情况下运动。

场景二：Fitbit（微信计步器）

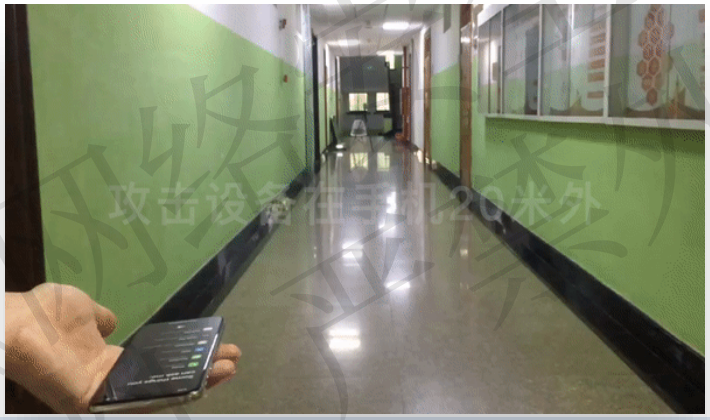


通过声波攻击运动传感器，可以使智能手环误以为人在走路，实现**每日“行走80000步”**，轻松获得步数排行榜的奖励。

攻击案例2：超声波攻击麦克风传感器（海豚音攻击）

- **研究背景：**对智能语音系统如天猫精灵、Siri等进行**无声**指令攻击。
- **研究原理：**利用麦克风具有的硬件**非线性**漏洞，将声音信号调制到超声波，注入语音系统实现无声控制。
- **行业影响：**苹果、亚马逊、谷歌、华为等多家公司披露这个安全漏洞并致谢和合作。

攻击场景



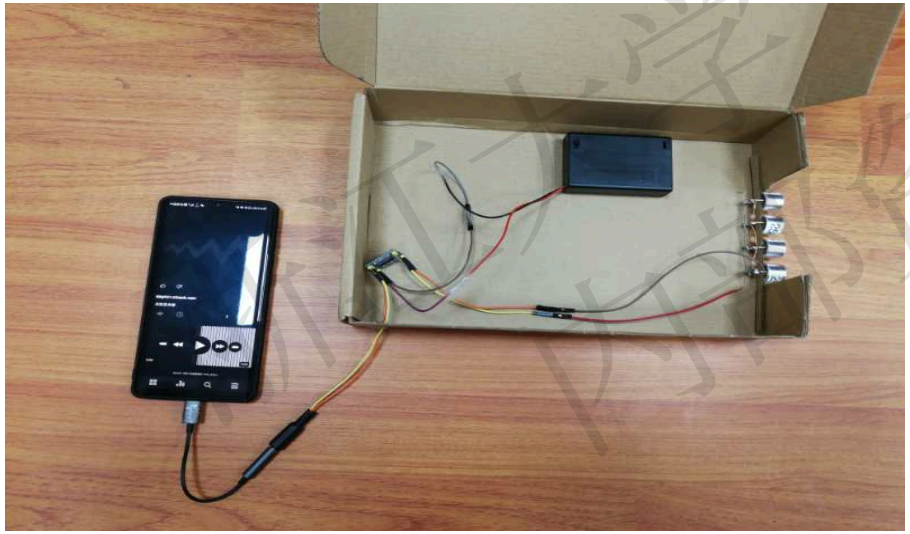
ACM CCS最佳论文奖状

MIT Tech. Review报道

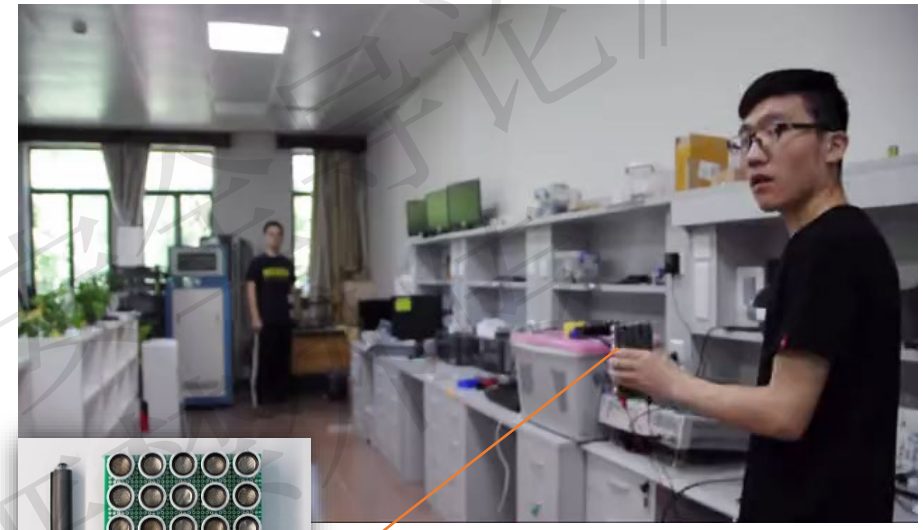
国内外厂商报道合作

更多样化的海豚音攻击

全向攻击



“穷人版”手机实现



长距离攻击 >20m

攻击案例3：激光攻击麦克风传感器

- **研究背景：**通过**激光调制声音**，实现对智能语音设备的无声控制。
- **研究原理：**光信号能够使麦克风的薄膜产生同频率的振动，注入攻击语音。
- **演示案例：**通过激光向远处的麦克风模块播放音乐，并实时重放。

攻击案例4：超声波攻击特斯拉避障传感器

- **研究目标：**自动驾驶汽车避障传感器安全性
- **创新点：**利用超声波传感器换能过程中的**饱和原理**，通过信号处理的方法，实现对超声波信号的消减。
- **影响范围：**获得特斯拉公司官方认可，进入**特斯拉名人堂**；提升特斯拉后续产品的安全性。
- **论文发表：**IEEE IoTJ 2017

分析Tesla 交通事故

Tesla名人堂网站截图

2017	Keen Security Lab	Tencent for CVE-2017-9983
2016	Keen Security Lab	Tencent
	Skygo Team, USSlab	Qihoo360, Zhejiang University
2014	Eusebiu Blindu	@testalways
	Muhammed Gazzaly	@gazly
	Jianhao Liu	Qihoo 360 Adlab
	Wenyuan Xu	Zhejiang University
	Nitesh Bhatter	@nbhatter

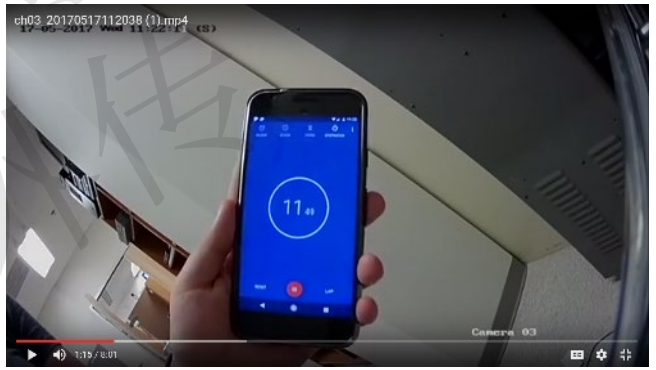
Xu, W., Yan, C., Jia, W., Ji, X., & Liu, J. “Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles” , IEEE IoTJ 2018

攻击案例5：DoS硬盘 – “声音注入DoS机械硬盘”

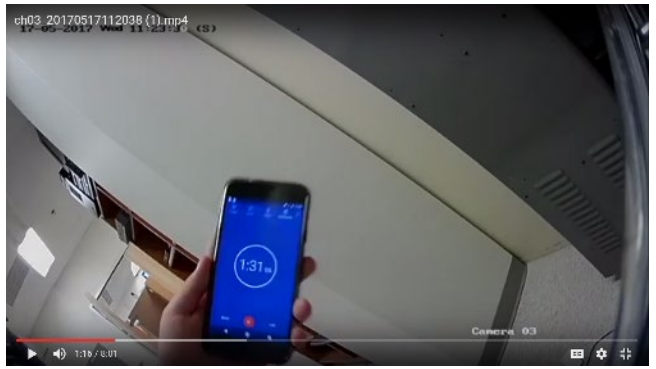
- **研究目标：**声波攻击硬盘，使数据中心宕机
- **创新点：**硬盘中的振动传感器能与**声波耦合共振**，注入特定频率的声波信号，使硬盘停止工作。
- **影响范围：**可导致监控摄像头监控“丢失”。
- **论文发表：**IEEE S&P 2018 (安全四大顶级会议)

Bolton, C., Rampazzi, S., Li, C., Kwong, A., Xu, W., & Fu, K. “Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems,” IEEE Symposium on S&P 2018

攻击案例6：监控画面丢失！



11s

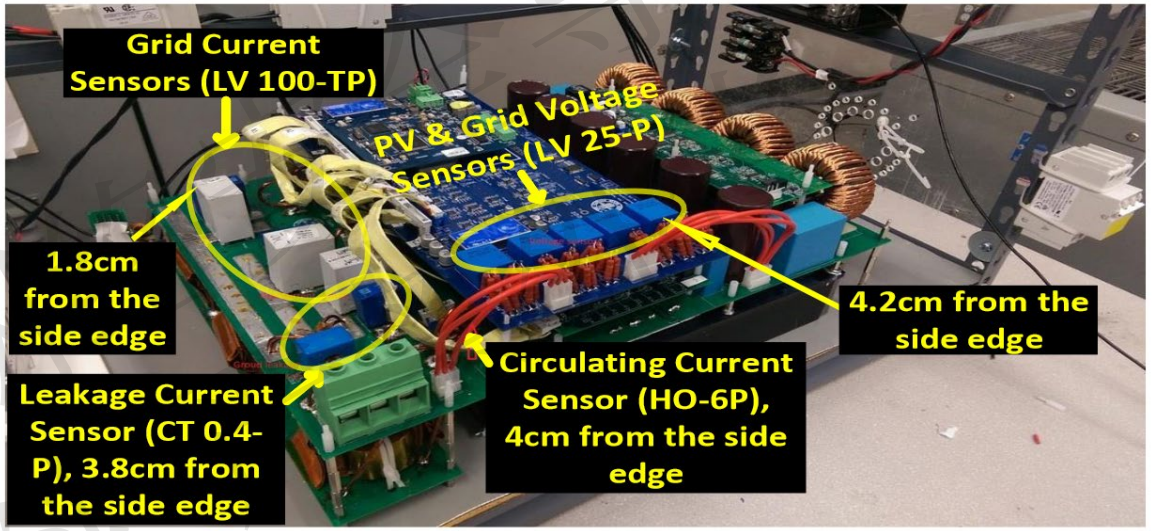


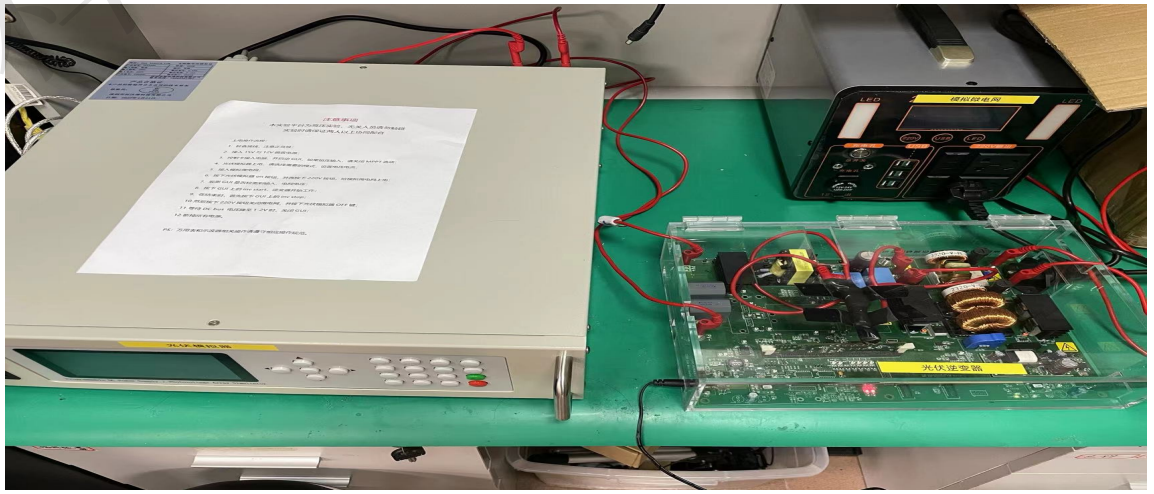
1:31s

约80秒监控录像丢失

攻击案例7：切断光伏逆变器

- **研究目标：**电磁干扰攻击逆变器，使其宕机、烧毁或有功/无功出力出错
- **创新点：**利用电磁干扰攻击光伏逆变器电路中的磁敏传感器和放大电路，使其电压/电流值出错，影响并网。
- **影响范围**：微小电网blackout、大电网频率电压失稳甚至解列。
- **论文发表：**正在投稿
- 应用范围：含磁敏传感器和放大电路终端





攻击案例7：切断光伏逆变器