论文思路

顾阳阳

2020 年 9 月 23 日

1 关键词

摄像头，定位，流量分析，个人隐私

2 背景

2.1 应用场景

装有摄像头的室内环境，摄像头的工作方式是 WiFi，与路由器无线连接。具体场景如酒店房间，装有无线偷拍摄像头，客人进入房间，并不知道房间内是否有摄像头的存在。可以使用我们的方案来确定是否有摄像头，如果有则进行定位。

2.2 问题陈述

在类似于酒店房间、浴室和更衣室等隐私空间非法安装无线摄像头会造成用户隐私泄露，被偷拍是图片或者视频可能被非法拍摄人进行贩卖或者对受害人进行进一步的权益侵害，给用户的生活造成很大的负面影响。

2.3 相关工作

1. 相关同类型产品或解决方案。

基于红外感知的方法。这种方法依靠捕获夜视模式下的红外光来对摄像头进行检测和定位。但是这种方法已经有点不太好用了，是因为摄像头的夜视不一定需要红外光来实现，还可以使用高感光度和大光圈来弱光成像，另外在刻意偷拍的场景，摄像头肯定已经做过处理，隐藏了红光或者摄像头不会发出红光。所以这种解决方案不太实用。

基于电磁干扰的方法。首先是这种方法需要专门的磁通量传感器，增加了额外设备，不太方便。其次，场景内肯定会有一些其他的电器设备，同样会产生电磁，如果摄像头的位置和这些电器距离很近，就会产生电磁干扰，误导使用者认为此处没有摄像头。所以这种方法并不可靠。

基于 WiFi 来感知摄像头。这种方法基于摄像头的无线数据包来检测的。调研了三种市场上的三款软件，DT 小听、针孔摄像头探测器和反偷拍。在同一个房间内做了对比实验，实验结果并不准确，出现了误识别和漏检的现象，准确率较低，且并不能进行定位。总之，就是不好用。

2. 类似摄像头定位的相关研究。

首先是基于带有摄像头的小型无人机定位。在 [?] 中提到了一种基于物理闪光刺激来定位室外无人机的方法。这种方法是通过分别建立信噪比（SNR）和距离以及角度的回归关系来进行距离和角度的定位。但是这种方法的平均误差也有 1 米到 1.5 米，在室外的情况下，关系不大，基本可以确定无人机的位置，但是室内就不太好了，而且室内环境复杂，这种方法的误差可能会更大。

其次是专注于室内定位的相关研究。关于室内定位的研究有很多，基于的无线信号有 WiFi、蓝牙、RFID 和 UWB，还有可见光通信（visible light communication）等，基于的技术常见的有基于指纹的，比如我们常见的“画格子”，如图 1。另外一种是方式利用到达角（AOA），然后进行三角定位。当然还有一些其他的方式。但是这些方式都没有关注过发射端，因为他们默认信号发射端和接收端他们都是可以控制的，他们要定位的是二者之间的人或者物。

最后是关于和我们方案有关的一些研究。首先是隐藏摄像头的存在感知**??**。它可以利用 MAC 地址和特殊的流量发送特点判断周围是否存在摄像头。其次是 HomeSpy **??**, 它是利用摄像头画面内图像变化来探测人体的存在性，关于摄像头的画面变动以及流量变化做了清晰的展示。

3 意义

3.1 主要挑战

1. 判断检测到的摄像头是否在你所在的密闭空间内，例如检测到周围有无线摄像头，但要确定是不是在你的房间内。需要改进**??**中的解决方案。

2. 判断摄像头的方向和距离。摄像头所处的空间不确定性很大，指纹定位难度太大且很可能出现不可接受的误差。利用信号到达角的技术，摄像头功率的不稳定以及摄像头本身模式的不同带来的改变，无法预测，需要实验测试，目前并没有相关文献做出详细的阐述。其他一些技术如时间到达角和信号到达角一样，都需要实验测试。

3.2 论文贡献

1. 提出了一种基于信噪比的方法判断摄像头是否在你的视线距离内。2. 本文提出了一种基于摄像头实时流量变化的检测并定位隐藏无线摄像头的方法。3. 在安卓平台上实现了该方法，对 N 种摄像头在 M 个环境下作了测试，平均识别准确率达到了 X%，平均定位准确率达到了 Y%。

4 方案

4.1 安全模型

非法摄像头的安装者可以将摄像头安装在房间的任意隐蔽的位置，摄像头和房间内的路由器连接但是不允许用户登录路由器的管理界面更改路由器的设置信息。为了随时可以拍到房间内的信息，摄像头默认是一直处于工作状态的。

4.2 技术依据

首先关于贡献点一，在**??**中关于信号穿过障碍物例如墙壁，玻璃等，功率会有不同程度的下降，环境噪声基本保持不变，这就会造成信噪比降低，和在同一房间内的摄像头的信噪比会有明显的区别。具体的阈值等需要实验验证确定。

4.3 方案描述

5 评估

5.1 评价标准

5.2 对比方案

5.3 实验设置