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[3]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[2]。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 [1],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[2]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[4]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。关于贡献点二的实现，基于实时的流量变化通过位置走动来判断定位摄像头的位置，主要是受这两篇文章[2][1]的启发，摄像头独特的流量模式，可以让我们通过改变人体位置来改变人体在摄像头内像素的大小，从而引起流量的变化，把这种变化和方向以及距离建立一种映射关系来判断和定位摄像头的位置。备选方案是利用CSI 信息，基于到达角的技术来进行数学三角定位来定量定位摄像头的位置，这个需要进一步的实验来判断哪种方案更加有效。

4.3 方案描述

摄像头侦测。应用平台为安卓智能手机nexus 5，通过监控模式来嗅探当前空间中的无线数据流量的基础信息，例如MAC地址，也可以通过收集一定时间内的指定设备发出的流量来分析流量模式来确定当前空间内的设备中是否存在无线摄像头。如果存在，则进一步通过对SNR 的判断来确定当前房间内是否有摄像头。

流量数据收集。基于github上的项目Nexmon，修改手机nexus 5的WiFi硬件，使手机可以在monitor模式下工作，并通过UDP数据包收集指定MAC地址的数据包并保存为pcap文件。

数据处理及其定位。使用Nexmon中解析工具对pcap文件进行解析，获取每一个报文的MAC地址、时间戳和数据长度等信息。把这些数据进一步在时间域上进行绘图监测跳变点和异常点。在训练阶段对这些跳变点和异常点进行预定义，在屏幕上给与提醒。通过用户的走位，以及异常点的追踪，指引用户向隐藏摄像头的可以点靠近，从而找到隐蔽摄像头。

5 评估

5.1 评价标准

摄像头检测准确率：系统认定为摄像头的设备确实是摄像头的概率。

摄像头检测速度：从启动系统侦测摄像头到给出检测结果的时间。

误差距离：实际摄像头的位置和预测摄像头所在方向的同一平面距离。

5.2 实验设置

实验设备包括一台nexus 5的智能手机，和三台无线摄像头，摄像头的品牌分别是360，小蚁和萤石。相邻的两个房间A和B。实验一是判断摄像头的存在以及是否在同一个房间。分别在房间A和B放置一个摄像头，使摄像头正常工作。在房间A使用CamSpot探测摄像头的存在，并判断那个摄像头在房间A内。实验二是判断摄像头的位置。在一个房间内人体通过走动以及手机界面的提示来逐渐靠近摄像头。主要是测试测试的时间和准确率，以及算法对于边界等跳变点的灵敏度。

备选实验判断摄像头的位置。利用到达角差异和三角定位对摄像头的位置来定位。和实验二的准确率进行对比来确定用那一个方案。

参考文献

[1] Y. Cheng, X. Ji, X. Zhou, and W. Xu. HomeSpy: Inferring User Presence via Encrypted Traffic of Home Surveillance Camera. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, pages 779–782, December 2017.

[2] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. DeWiCam: Detecting Hidden Wireless Cameras via Smartphones. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, pages 1–13, New York, NY, USA, 2018. ACM.

[3] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici. Drones' cryptanalysis - smashing cryptography with a flicker. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1397–1414, 2019.

[4] X. Wu, Z. Chu, P. Yang, C. Xiang, X. Zheng, and W. Huang. Tw-see: Human activity recognition through the wall with commodity wi-fi devices. *IEEE Transactions on Vehicular Technology*, 68(1):306–319, 2019.