(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 213716100 U
(45)授权公告日 2021.07.16

(21)申请号 202020965272.6

(22)申请日 2020.05.30

(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号

(72)发明人 林永杰 黄紫林 许伦辉

(74)专利代理机构 广州粤高专利商标代理有限公司 44102
代理人 何淑珍 江裕强

(51)Int.Cl.
G08B 13/00(2006.01)
G08B 3/10(2006.01)
G01S 5/02(2010.01)

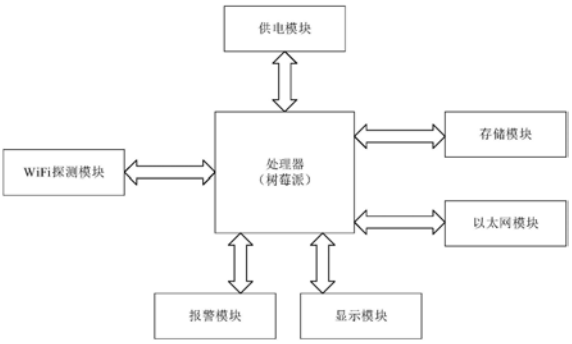
权利要求书1页 说明书3页 附图3页

(54)实用新型名称

一种基于无线通信信号的目标入侵检测装置

(57)摘要

本实用新型公开一种基于无线通信信号的目标入侵检测装置,包括处理器、WiFi探测模块、以太网模块、存储模块、报警模块、显示模块和供电模块。处理器分别与WiFi探测模块、以太网模块、存储模块、报警模块、显示模块和供电模块相连接。WiFi探测模块周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号,将其对应的信号信息传输至处理器。处理器基于阴影衰减模型对WiFi探测模块回传的接收信号强度指示值进行欧式距离换算,并执行入侵判断,当目标与检测装置之间的欧式距离低于预设阈值时,视为监控区域内有目标入侵。供电模块为检测装置提供电源。本实用新型成本低、适应性强、发展前景好。



CN 213716100 U

1.一种基于无线通信信号的目标入侵检测装置,其特征在于,包括WiFi探测模块、处理器、以太网模块、存储模块、显示模块和供电模块,其中:

所述WiFi探测模块用于周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号信息并将所述信号信息传输至处理器,所述信号信息包括设备的物理地址、时间戳和接收信号强度指示;所述WiFi探测模块采用WiFi探针TZ-1002;所述目标携带的无线通信设备为WiFi终端设备,是手机、笔记本电脑、平板电脑中的一种或多种;

所述处理器用于处理WiFi探测模块捕捉的信息,基于阴影衰减模型对WiFi探测模块捕捉的接收信号强度指示值进行欧氏距离估计换算,并执行入侵判断,当WiFi探测模块与被测目标之间的欧式距离低于预设距离阈值时生成报警指令;

所述以太网模块与处理器相连,提供对外通信接口,实现装置与中央服务器或云端数据库的数据互通;

所述存储模块与处理器相连,用于储存处理器计算产生的数据;

所述显示模块与处理器相连,用于显示目标与检测装置之间的欧式距离、物理地址和时间戳;

所述供电模块与处理器相连,用于为检测装置提供电源。

2.根据权利要求1所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:所述监控区域是以目标入侵检测装置为圆心、预设距离阈值为半径的圆形区域。

3.根据权利要求1所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:所述存储模块是以SD卡为内存硬盘的存储单元;所述处理器是以SD卡作为存储模块的树莓派。

4.根据权利要求1所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:所述入侵判断具体包括:当目标与检测装置之间的欧式距离大于预设距离阈值时,认为该目标没有入侵监控区域;当目标与检测装置之间的欧式距离小于预设距离阈值时,认为该目标入侵监控区域。

5.根据权利要求1所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:所述预设距离阈值为20m。

6.根据权利要求1所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:还包括报警模块,所述报警模块与处理器相连,接收并执行处理器生成的所述报警指令。

7.根据权利要求6所述的一种基于无线通信信号的目标入侵检测装置,其特征在于:所述报警模块是扬声器,所述扬声器接收处理器传输的报警指令后发出声音。

一种基于无线通信信号的目标入侵检测装置

技术领域

[0001] 本实用新型涉及目标入侵检测技术及电子产品制造与应用技术领域，具体涉及一种基于无线通信信号的目标入侵检测装置。

背景技术

[0002] 随着社会经济和科技的发展，区域安保和重点区域监控越来越受到人们重视，而目标入侵检测技术也在智慧交通、建筑监控、工业自动化等领域发挥着重要的作用。目标入侵检测是区域安保和监控领域的自动化解决方案，通过传感器等检测手段可以了解到是否有人突然入侵监测区域，一旦监测到入侵目标便立即发出报警。

[0003] 在传统的目标入侵检测技术中，常用的检测手段一般是被动红外、摄像头、二氧化碳传感器和无线电波。如文献《机场围界入侵目标红外图像检测方法》中程思竹等人实现用被动式红外技术对机场围界的目标入侵检测、文献《基于MFC+OpenCV的视频监控区域入侵检测系统设计与实现》中吴双使用摄像头实现了视频技术的目标入侵检测。然而，这几种检测手段都存在一定的局限性，无法同时满足目标入侵检测技术的成本要求和精度适用性，被动红外传感器的范围较低、检测精度较低、且需要较高的部署成本；摄像头抗干扰能力弱，无法穿透墙壁，在黑暗和烟雾环境中性能较差，同时可能存在隐私问题；而雷达和超宽带等检测方案精度较高，但价格昂贵。

实用新型内容

[0004] 针对上述情况，为克服现有技术之缺陷，弥补传统入侵检测技术中成本和适用性的矛盾，本实用新型旨在提供一种WiFi技术的无线信号目标入侵检测装置。

[0005] 本实用新型通过采用以下技术方案实现。

[0006] 一种基于无线通信信号的目标入侵检测装置，其特征在于包括探测模块、处理器、WiFi以太网模块、存储模块、显示模块和供电模块，其中：

[0007] 所述WiFi探测模块用于周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号信息并将所述信号信息传输至处理器，所述信号信息包括设备的物理地址、时间戳和接收信号强度指示；

[0008] 所述处理器用于处理WiFi探测模块捕捉的信息，基于阴影衰减模型对WiFi探测模块捕捉的接收信号强度指示值进行欧氏距离估计换算，并执行入侵判断，当WiFi探测模块与被测目标之间的欧式距离低于预设阈值时生成报警指令；

[0009] 所述以太网模块与处理器相连，提供对外通信接口，实现装置与中央服务器或云端数据库的数据互通；

[0010] 所述存储模块与处理器相连，用于储存处理器计算产生的数据；

[0011] 所述显示模块与处理器相连，用于显示目标与检测装置之间的欧式距离、物理地址和时间戳；

[0012] 所述供电模块与处理器相连，用于为检测装置提供电源。

[0013] 进一步地,所述WiFi探测模块采用WiFi探针TZ-1002。

[0014] 进一步地,所述监控区域是以目标入侵检测装置为圆心,预设阈值为半径的圆形区域。

[0015] 进一步地,所述目标携带的无线通信设备为WiFi终端设备,是手机、笔记本电脑、平板电脑中的一种或多种。

[0016] 进一步地,所述存储模块是以SD卡为内存硬盘的存储单元;所述处理器是以SD卡作为存储模块的树莓派。

[0017] 进一步地,所述入侵判断具体包括:当目标与检测装置之间的欧式距离大于预设距离阈值时,认为该目标没有入侵监控区域;当目标与检测装置之间的欧式距离小于预设距离阈值时,认为该目标入侵监控区域。

[0018] 进一步地,所述预设距离阈值为20m。

[0019] 进一步地,还包括报警模块,所述报警模块与处理器相连,接收并执行处理器生成的所述报警指令。

[0020] 进一步地,所述报警模块是扬声器,接收处理器传输的报警指令后发出声音。

[0021] 与现有技术相比,本实用新型具有如下有益效果:

[0022] 本实用新型提供的目标入侵检测装置通过WiFi探测模块捕捉入侵目标携带的无线通信设备发出的探测请求帧,提取出RSSI值、MAC地址及时间戳信息,在此基础上估算目标与检测装置之间的欧式距离,进一步判断目标是否入侵至监控区域内,实现了WiFi信号的目标入侵检测,与传统技术相比,本实用新型硬件成本低、适用性强,同时无需其他辅助设备支持,可监测范围广。

附图说明

[0023] 图1是一种基于无线通信信号的目标入侵检测装置的结构示意图。

[0024] 图2是本实用新型实施例提供的目标入侵检测装置的工作流程示意图。

[0025] 图3是本实用新型目标入侵判断工作流程示意图。

具体实施方式

[0026] 下面结合图1-图3,对本实用新型作进一步地详细说明,但本实用新型的实施方式不限于此。

[0027] 请参阅图1,本实施例提供的一种基于无线通信信号的目标入侵检测装置包括WiFi探测模块、处理器、以太网模块、存储模块、报警模块、显示模块和供电模块,其中:

[0028] 所述WiFi探测模块用于周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号信息并将所述信号信息传输至处理器,所述信号信息包括设备的物理地址(Media Access Control Address, MAC)、时间戳和接收信号强度指示(Received Signal Strength Indicator, RSSI);

[0029] 所述处理器用于处理WiFi探测模块捕捉的信息,基于阴影衰减模型对WiFi探测模块捕捉的RSSI值进行估计距离换算(欧氏距离),并执行入侵判断,当目标与检测装置之间的欧式距离大于预设距离阈值时,认为该目标没有入侵监控区域;当目标与检测装置之间的欧式距离小于预设距离阈值时,认为该目标入侵监控区域,此时,处理器生成报警指令并

将所述报警指令发送至报警模块使所述报警模块发出警报；

[0030] 所述以太网模块与处理器相连，提供对外通信接口，实现装置与中央服务器或云端数据库的数据互通；

[0031] 所述存储模块与处理器相连，用于储存处理器计算产生的数据；

[0032] 所述报警模块与处理器相连，接收并执行处理器发出的报警指令；

[0033] 所述显示模块与处理器相连，用于实时显示目标与检测装置之间的欧式距离、物理地址和时间戳；

[0034] 所述供电模块与处理器相连，用于为检测装置提供电源。

[0035] 本实施例的WiFi探测模块，采用WiFi探针TZ-1002，WiFi探针TZ-1002与处理器相连，周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号信息，并将其传输至处理器。

[0036] 本实施例中，监控区域是以目标入侵检测装置为圆心，预设距离阈值为半径的圆形区域。所述目标携带的无线通信设备为WiFi终端设备，是手机、笔记本电脑、平板电脑中的一种或多种。

[0037] 本实施例中，所述存储模块是以SD卡为内存硬盘的存储单元；所述处理器是以SD卡作为存储模块的树莓派；所述报警模块是扬声器，接收处理器传输的报警指令，能够发出“滴滴滴”的声音。

[0038] 请参阅图2，本实施例提供的目标入侵检测装置的工作流程如下：

[0039] S1、装置启动，WiFi探测模块开始探测周围设备信号；

[0040] S2、WiFi探测模块将探测数据传输至处理器，处理器接收数据开始处理，并将记录写入存储模块内；

[0041] S3、处理器筛选到有记录的RSSI值高于预设距离阈值；

[0042] S4、处理器生成报警指令传输至报警模块，报警模块响起；

[0043] S5、处理器将入侵设备信息传输至显示模块，显示模块更新信息，显示出入侵设备的MAC地址、时间戳和欧式距离。

[0044] 本实施例中目标入侵判断的工作流程，如图3所示。首先，开启WiFi探测模块，并进行电路自检。如未成功启动WiFi探测模块，处理器生成“模块异常”的警告指令，并通过以太网模块发送至中央服务器，以形成异常日志便于反馈和查询；如成功启动WiFi探测模块，WiFi探测模块周期性捕捉监控区域内目标携带的无线通信设备发出的探测请求帧信号信息。然后，处理器对采集得到的RSSI转化为欧式距离，并对欧式距离进行判断。最后，依据不同的判断结果，通过报警模块实现目标入侵检测的报警提醒。当无法进行距离判定或距离判定为空值，处理器生成“数据异常”的警告指令，并通过以太网模块发送至中央服务器，形成异常日志便于反馈和查询。当欧式距离低于预设距离阈值时生成报警指令，报警模块即扬声器据此发出警报。在本实施例中，设计目标入侵检测装置的预设距离阈值为20m，在目标携带无线通讯设备距离检测装置小于20m时能发出报警信号。

[0045] 本实施例实现了WiFi信号的目标入侵检测，硬件成本低，适用性强。

[0046] 以上所述仅是对本实用新型的较佳实施例而已，并非对本实用新型作任何形式上的限制，凡是依据本实用新型的技术实质对以上实施例所做的任何简单修改，等同变化与修饰，均属于本实用新型技术方案的范围内。

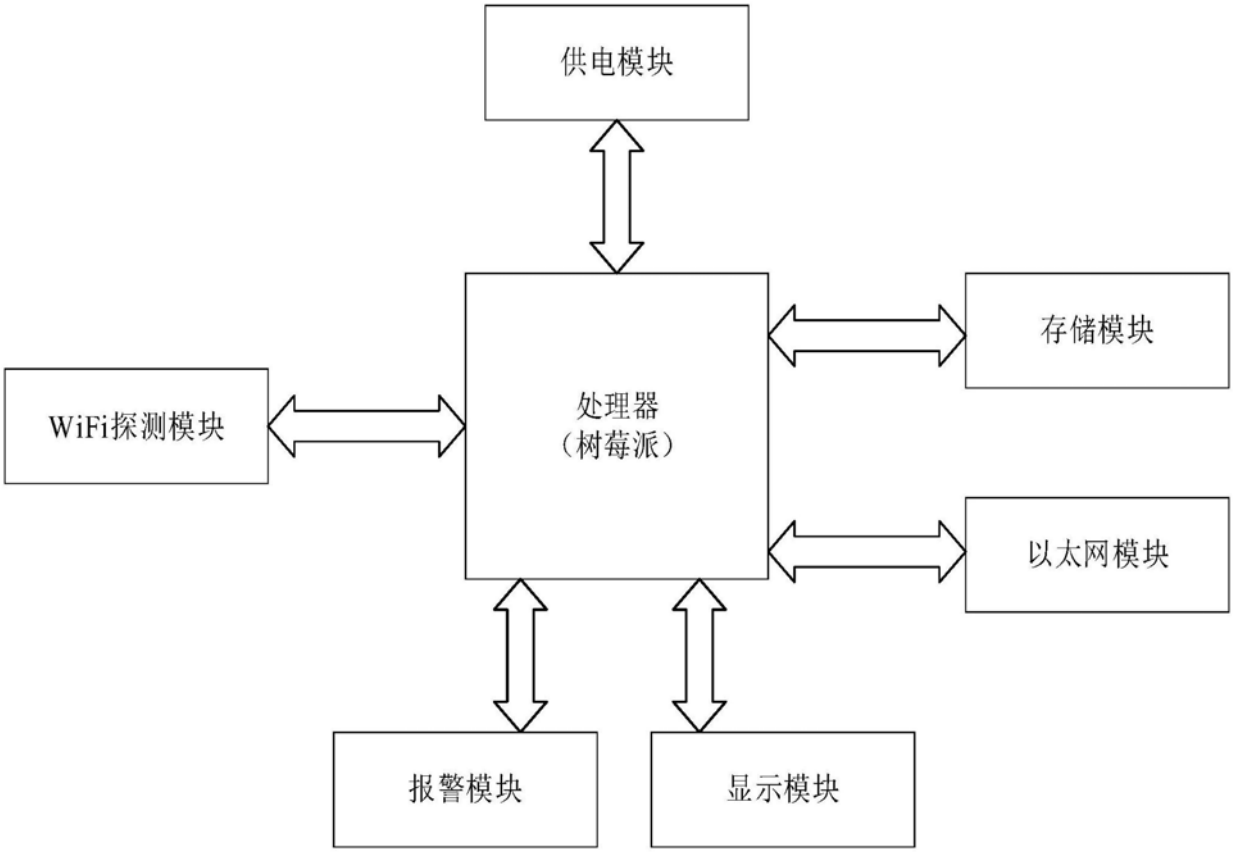


图1

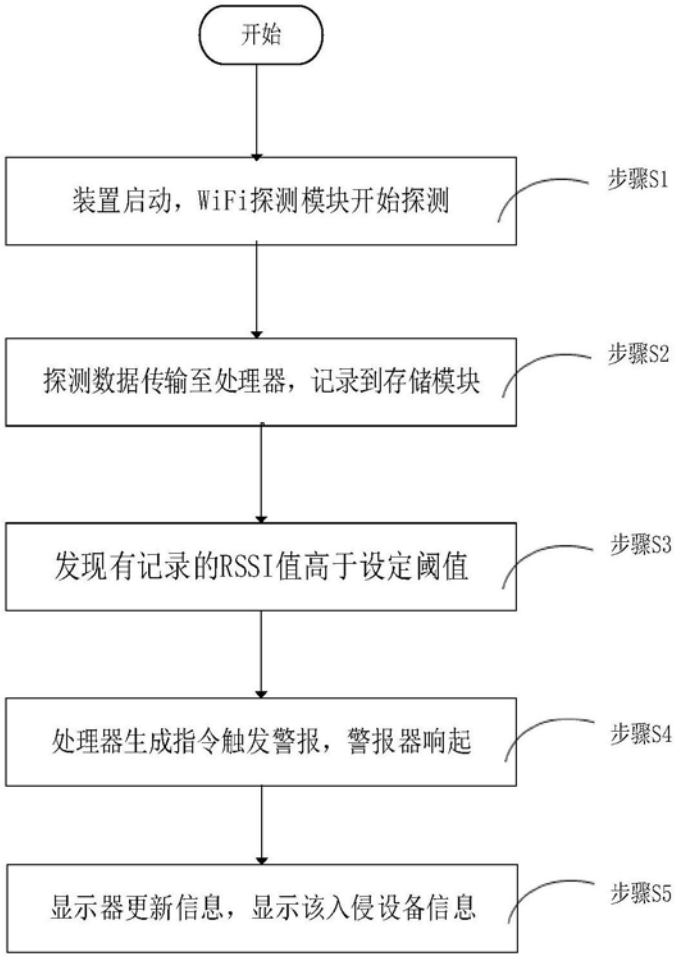

开始
装置启动，WiFi探测模块开始探测
步骤S1
探测数据传输至处理器，记录到存储模块
步骤S2
发现有记录的RSSI值高于设定阈值
步骤S3
处理器生成指令触发警报，警报器响起
步骤S4
显示器更新信息，显示该入侵设备信息
步骤S5

图2

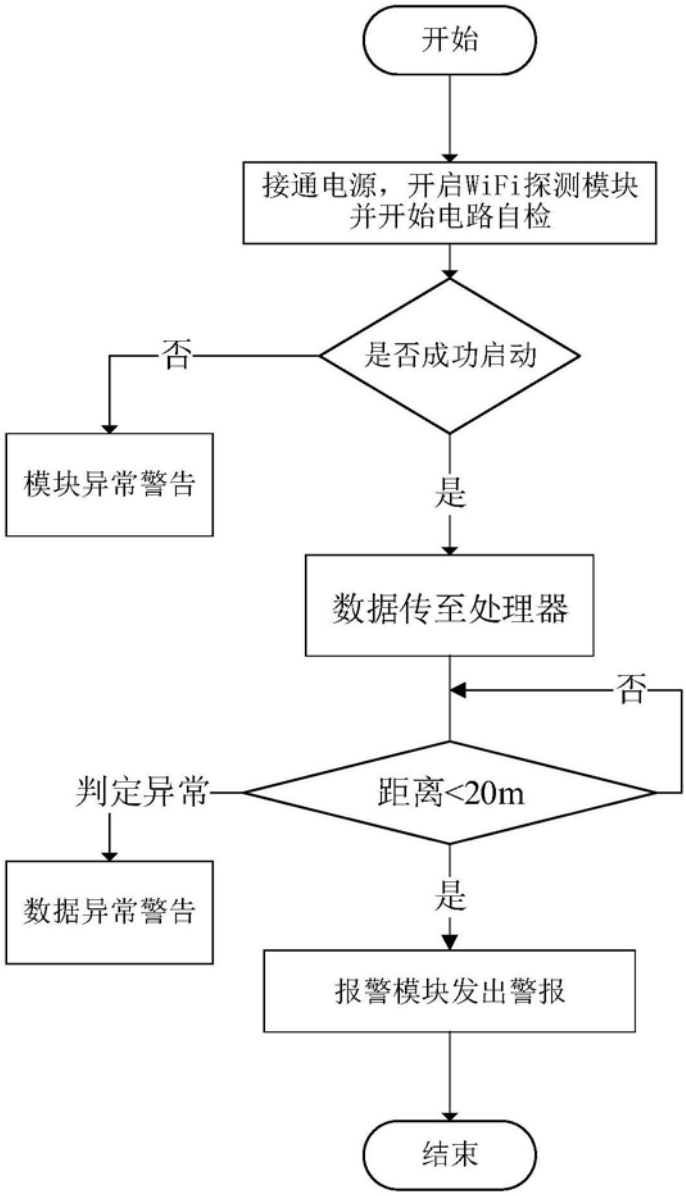

开始
接通电源，开启WiFi探测模块
并开始电路自检
是否成功启动
否
模块异常警告
是
数据传至处理器
否
距离<20m
判定异常
数据异常警告
是
报警模块发出警报
结束

图3