

引用格式:于怡然,常俊,吴柳繁,等. 基于 Wi-Fi 信道状态信息的免训练入侵检测系统[J]. 微电子学与计算机, 2020, 37(5): 18-22. [YU Y R, CHANG J, WU L F, et al. Training-free intrusion detection using channel state information of Wi-Fi signals [J]. Microelectronics & Computer, 2020, 37(5): 18-22.]

基于 Wi-Fi 信道状态信息的免训练入侵检测系统

于怡然,常俊,吴柳繁,彭予

(云南大学 信息学院, 云南 昆明 650091)

摘 要: 随着无线通信技术的飞速发展, Wi-Fi 已经广泛应用于公共和私人领域, 基于无线技术的无设备被动入侵检测技术在智能家居领域有着广阔的应用前景. 针对现有的解决方案难以解释不同场景下性能存在巨大差异, 本文设计了一种基于 Wi-Fi 信道状态信息的免训练入侵检测系统, 利用 Wi-Fi 设备上细粒度的信道状态信息(CSI)捕捉由人体移动引起的细微变化. 为了放大这种变化, 使用多重信号分类算法(MUSIC)对 CSI 时间序列的协方差矩阵进行特征分解, 利用信号速度向量与噪声子空间的正交性来提取路径变化速度, 并通过计算对应路径的相位差变化进行入侵检测的判断. 在两个典型的室内环境(会议室和卧室)中进行评估, 结果显示平均假阳性(FP)为 1.07%, 平均假阴性(FN)为 1.87%. 结果表明该方法能够有效消除环境变化对于检测精度的影响, 提高系统的鲁棒性.

关键词: 入侵检测; 免训练; 信道状态信息; 多重信号分类算法; 鲁棒性

中图分类号: TN99

文献标识码: A

文章编号: 1000-7180(2020)05-0018-05

Training-free intrusion detection using channel state information of Wi-Fi signals

YU Yi-ran, CHANG Jun, WU Liu-fan, PENG Yu

(Department of Information, Yunnan University, Kunming 650500, China)

Abstract: With the rapid development of wireless communication technology, Wi-Fi has been widely used in public and private fields. The wireless device-free passive human detection technology has broad application prospects in the field of home automation. Considering that the existing solutions are difficult to explain the huge performance differences in different scenarios, this paper introduces a training-free intrusion detection using channel state information of Wi-Fi signals, Which exploits the fine-grained channel state information (CSI) on Wi-Fi devices to capture the minor variations caused by human movement. To amplify such variations, the multiple signal classification algorithm (MUSIC) is used to decompose the covariance matrix of the CSI time series, and the orthogonality of the signal angular velocity vector and the noise subspace is used to extract the path change speed. and by calculating the phase difference of the corresponding path judges the intrusion detection We implemented our human detection method in two typical indoor environments (i. e. , a meeting room and a laboratory) and the results demonstrate an average false positive (FP) of 1.07% and an average false negative (FN) of 1.87%. The experimental results show that the proposed method can effectively eliminate the influence of environmental changes on detection accuracy and improves the robustness of the system.

Key words: intrusion detection; training-free; channel state information; MUSIC; robust

收稿日期: 2019-08-07; 修回日期: 2019-09-10

基金项目: 国家自然科学基金(61162406); 云南省高校频谱传感与边疆无线电安全重点实验室开放课题(C6165903); 云南省教育厅科学研究基金(2019J0007)

1 引言

近年来,无设备的被动人体检测引起了人们的极大兴趣.与传统的基于传感器^[1]的方法相比,无需额外设备也不存在感知覆盖范围的问题,能更好地用于入侵检测系统,成为智能家居的一个重要安全组件.目前基于摄像^[2]或者雷达^[3]的方法都可以提供良好的检测精度,然而各自的限制却阻碍了它们的广泛部署.而基于 Wi-Fi 信号的入侵系统利用接收信号强度(RSSI)^[4-5]作为信号特征,但 RSSI 即使在一个固定的链路上也会有很大的波动,检测结果并不可靠的^[6-9].

针对上述问题,本文设计了一种基于 Wi-Fi 信道状态信息的免训练入侵检测系统,利用从普通 Wi-Fi 设备获得的 CSI 值来捕获由人体移动导致的细微变化.

2 理论基础

随着无线技术的飞速发展,Wi-Fi 射频信号的作用已经从单一的通信介质扩展到非侵入性的环境传感工具.在这里引入 CSI 信号模型来解释无线通信信道由于人体移动导致的相位变化.

2.1 CSI 模型

在典型的室内环境中,信号不仅沿直线传播,还会被物体反射,比如墙壁,家具以及人等等.因此,CSI 是所有路径信号叠加的结果,第 n 个子载波在 t 时刻的 CSI 值 $H_n(t)$ 为:

$$H_n(t) = \sum_{k=1}^L \gamma_{k,n} + e_n(t) \quad (1)$$

式中, $n \in N$, N 表示可用子载波集, L 是室内环境中的路径总数, $e_n(t)$ 是第 n 个子载波在 t 时刻的白噪声. $\gamma_{k,n}$ 代表第 n 个子载波从发射天线到接收机沿第 k 条路径在 t 时刻接收到的信号,可以表示为:

$$\gamma_{k,n} = \zeta_k e^{-j2\pi \frac{d_k}{\lambda_n}} \quad (2)$$

ζ_k 是第 k 条路径的衰减, d_k 是 t 时刻第 k 条路径的长度. λ_n 表示第 n 个子载波的载波频率:

$$\lambda_n = \frac{c}{f_c + n/N_{\text{DFT}} T_s} \quad (3)$$

式中, f_c 是载波中心频率, c 为光速, T_s 为采样间隔, 值为 $T_s = 1/B$, B 为 Wi-Fi 信号的基带带宽, N_{DFT} 是离散傅里叶变换(DFT)的大小.在静态环境下,路径的增益和延迟是时不变的.

2.2 人体移动对 CSI 的影响

在所有接收到的路径信号中,来自静态物体(如

家具、墙壁)反射的信号被定义为静态路径信号,其他被非静止目标反射的信号被定义为动态路径信号.注意,静态路径信号既包括直接路径信号,也包括在人类活动过程中不发生变化的墙壁和家具反射的信号.当人体目标在环境中进行活动时,包括行走和摆手等原地活动时,一个或多个路径的增益和相位将随时间发生变化.如图 1 所示,动态路径长度变化为 $\Delta d_{\text{path}} = v_{\text{path}} t$.通过文献^[10]可知,第 k 条路径随时间变化的衰减 $\zeta_k(t)$ 可表示为:

$$\begin{aligned} \zeta_k(t) &= \zeta_k \times (1 + \frac{\Delta d_k}{d_k})^{-\psi} \\ &= \zeta_k \times (1 + \frac{v_k t}{d_k})^{-\psi} \end{aligned} \quad (4)$$

式中, Δd_k 是由人体移动引起额外附加位置位移, ψ 是路径损耗指数, v_k 为路径变化速度.在短时间 t 内,由于 $\Delta d_k \ll d_k$,因此可以近似的认为 $\zeta_k(t) = \zeta_k$.

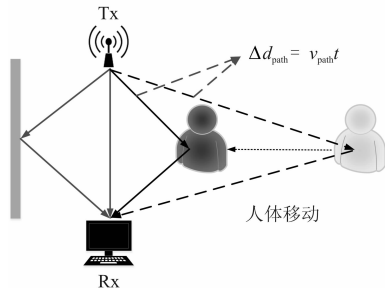


图1 人体移动导致的反射路径长度变化

另一方面,人体的移动会改变路径长度从而影响信号的相位变化,第 k 条路径的路径长度 $d_k(t)$ 可以表示为:

$$d_k(t) = d_k + \Delta d_k = d_k + v_k t \quad (5)$$

因此, $H_n(t)$ 可以重新表示为:

$$\begin{aligned} H_n(t) &= \sum_{k=1}^L \zeta_k e^{-j2\pi \frac{d_k(t)}{\lambda_n}} + e_n(t) \\ &= \sum_{k=1}^L e^{-j2\pi \frac{v_k t}{\lambda_n}} \zeta_k e^{-j2\pi \frac{d_k}{\lambda_n}} + e_n(t) \\ &= \sum_{k=1}^L e^{-j2\pi \frac{v_k t}{\lambda_n}} \gamma_{k,n} + e_n(t) \end{aligned} \quad (6)$$

通过统计所有子载波集的 CSI,即可得到无线信道矩阵 $\mathbf{H}$:

$$\mathbf{H} = [H_1(t), H_2(t), \dots, H_N(t)] \quad (7)$$

3 系统设计

展示入侵检测系统的总体架构如图 2 所示.人体活动对 Wi-Fi 信号的影响可以体现为 CSI 在时域的相位变化,以及如何从原始 CSI 读数中检索这种

相位变化以用于人体入侵检测。

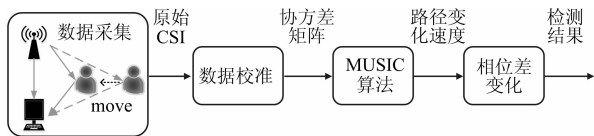


图2 入侵检测系统架构

3.1 入侵检测

首先考虑只有一个人的反射路径信号的情况。当目标非静止时,路径变化速度 v_{path} 在较短的时间内可以看作是一个常数,CSI 的相位变化也是恒定的。其他未被人体目标反射的路径信号不随时间变化,则不会引起 CSI 相位变化。因此,如果能够检测到这样一个恒定的 CSI 相位变化,就可以知道存在一个动态的人的反射路径信号,并进一步检测到人的活动。

利用这一洞察力,将来自路径变化速度 v_{path} 变化不大的 M 个 CSI 样本连接起来。那么对于不同路径的接收信号来说,第 i 个 CSI 样本与第一个样本的相位差为 $e^{-j2\pi v_k t_i / \lambda_n}$,其中 t_i 表示两个样本之间的采样时间间隔。对于这些包中的任何一个,CSI 都是相同 v_k 的线性组合。因此速度向量 $\vec{a}(v_k)$ 可以表示为:

$$\vec{a}(v_k) = [1, e^{-j2\pi \frac{v_k t_2}{\lambda_n}}, e^{-j2\pi \frac{v_k t_3}{\lambda_n}}, \dots, e^{-j2\pi \frac{v_k t_M}{\lambda_n}}] \quad (8)$$

式中,如果路径变化速度 v_k 不为零,那么路径信号为动态路径信号,速度向量 $\vec{a}(v_k)$ 为对应的随时间恒定变化的相位差。如果路径为静态路径,则 v_k 为零,CSI 相位将不会发生变化。通过公式(6)可知,第 n 个子载波下的 M 个 CSI 样本可以表示为:

$$\begin{aligned} X(n) &= [H_n(t_1), H_n(t_2), \dots, H_n(t_M)] \\ &= \sum_{k=1}^L \vec{a}(v_k) \gamma_{k,n} + N(n) \\ &= \mathbf{A}\mathbf{S}(n) + \mathbf{N}(n) \end{aligned} \quad (9)$$

式中, $\mathbf{N}(n)$ 为 M 个样本的噪声矩阵, $\mathbf{A} = [\vec{a}(v_1), \vec{a}(v_2), \dots, \vec{a}(v_L)]$ 为速度矩阵,内部元素为不同路径下的速度向量 $\vec{a}(v_k)$, $\mathbf{S}(n) = [\gamma_{1,n}, \gamma_{2,n}, \dots, \gamma_{k,n}]^T$ 是第 n 个子载波下的信号矩阵,内部元素为不同路径下的接收信号 $\gamma_{k,n}$ 。对于这 M 个 CSI 样本,如果能够计算出每个路径信号的速度向量 $\vec{a}(v_k)$,并检测到一个非零的路径变化速度,就可以知道人体目标是非静止的(要么在移动,要么在执行一些活动)。

因此为了估计每个路径信号的速度向量 $\vec{a}(v_k)$,将使用 MUSIC 算法进行估计。其基本思想

是对接收到 M 个 CSI 样本的 $M \times M$ 阶协方差矩阵 $\mathbf{R}_X$ 进行特征值分解,通过公式(9)可以得到 $\mathbf{R}_X$:

$$\begin{aligned} \mathbf{R}_X &= E[\mathbf{X}\mathbf{X}^H] \\ &= \mathbf{A}E[\mathbf{S}\mathbf{S}^H]\mathbf{A}^H + E[\mathbf{N}\mathbf{N}^H] \\ &= \mathbf{A}\mathbf{R}_S\mathbf{A}^H + \sigma^2\mathbf{I} \end{aligned} \quad (10)$$

式中, $\mathbf{R}_S$ 是信号矩阵 $\mathbf{S}$ 的相关矩阵, $\mathbf{I}$ 为单位矩阵, σ^2 为噪声的方差。协方差矩阵 $\mathbf{R}_X$ 共有 M 个特征值,其中最小的 $M-L$ 个特征值对应的特征向量构成噪声向量子空间 $E_N = [\vec{e}_1, \vec{e}_2, \dots, \vec{e}_{ML}]$,其他 L 个特征向量构成信号子空间 $E_S = [\vec{e}_{M-L+1}, \vec{e}_{M-L+2}, \dots, \vec{e}_M]$ 。由于信号和噪声子空间是正交的,如果存在路径信号,则对应的速度向量与噪声子空间正交。因此,速度功率谱函数表示为:

$$P(\omega)_{\text{MUSIC}} = \frac{1}{\vec{a}^H(v) E_N E_N^H \vec{a}(v)} \quad (11)$$

该式中分母为速度向量和噪声向量子空间的内积,当 $\vec{a}(v_k)$ 和 E_N 的各列正交时,该分母为零,但由于噪声的存在,实际上为一最小值,因此 $P(\omega)_{\text{MUSIC}}$ 有一尖峰。峰值对应于不同的路径变化速度,通过公式(8)即可得出对应路径的不同时刻的相位差变化。

3.2 数据校准

在实际应用中,还要考虑 WiFi 设备固有噪声对 CSI 模型的影响。在这里主要考虑两个因素:

(1)随机相位失真:由 WiFi 发射机和接收机的局部振荡器的差异引起,由初始相位畸变和线性相位畸变组成。

(2)随机振幅变化:由于射频前端的自动增益控制(AGC)将输入电压调整到模数转换器(ADC)的动态范围。

因此实际测得的 CSI 值 $\hat{H}_n(t)$ 与理想情况下的 CSI 值 $H_n(t)$ 的关系为:

$$\hat{H}_n(t) = \Gamma(t) H_n(t) e^{j(\varphi(t) + \kappa(t)n)} \quad (12)$$

式中, $\Gamma(t)$ 为 t 时刻的 AGC 随机增益, $\varphi(t)$ 为 t 时刻的初始相位畸变, $\kappa(t)$ 为 t 时刻的线性相位畸变。由公式(10)可知,应用 MUSIC 算法计算协方差矩阵时便引入了随机相位失真以及随机振幅变化,导致静态路径的增益和相位也随着时间发生变化。因此在这里需要对协方差矩阵进行修改:

$$\mathbf{R}_X(i, j) = \frac{\sum_{n \in N} H_n(i) H_n^*(j) e^{-j(\varphi^* + \kappa_n^*)}}{\|\mathbf{H}(i)\|_2 \|\mathbf{H}(j)\|_2} \quad (13)$$

式中, $\mathbf{R}_X(i, j)$ 表示协方差矩阵 $\mathbf{R}_X$ 的第 i 行第 j 列的

元素, $\|X\|_2$ 表示向量 X 的 l_2 范数, 在这里公式 (13) 的分母部分对协方差矩阵的每个元素进行标准化, 使得 $\mathbf{R}_x(i, j) \in [0, 1]$, 换句话说也就是分母部分消除了随机增益 $\Gamma(i)$ 和 $\Gamma(j)$ 的影响. φ^* 和 κ^* 是用于消除初始和线性相位畸变, 计算公式如下:

$$K^* = \operatorname{argmax}_k \left| \sum_{n \in N} H_n(i) H_n^*(j) e^{-jkn} \right| \quad (14)$$

$$\varphi^* = \left(\sum_{n \in N} H_n(i) H_n^*(j) e^{-jkn^*} \right) \quad (15)$$

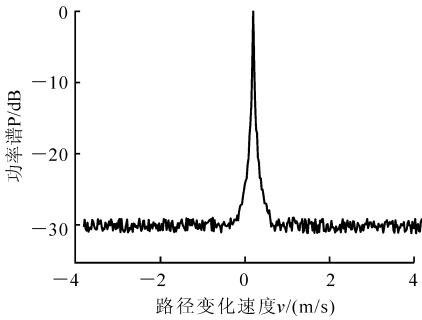
式中, (x) 表示从复数 x 中提取相位的运算符.

4 实验结果与分析

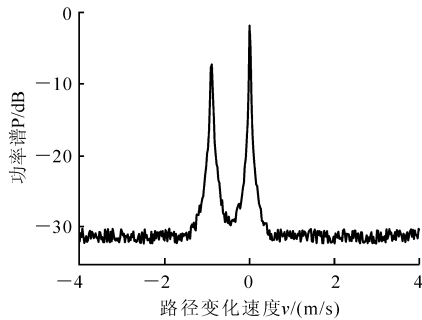
实验通过 Linux 802.11n CSI Tool 从 Intel 5300 网卡获取 CSI 值, CSI 采样率为 200 Hz. 工作频率为 2.4 GHz, 带宽设置为 40 MHz. 发射端是 TL-WR742N 无线路由器, 接收端为配有 3 根天线的迷你台式机. 对于每一个路径变化速度估计, 我们使用了在 0.3 秒内收集的 CSI 样本, 利用接收到的 CSI 样本计算路径变化速度谱.

4.1 结果分析

人的移动会使得动态路径的相位差发生变化, 经过处理, 可以得到基于公式 (11) 的速度功率谱, 如图 3 所示. 由于静态路径不会导致 CSI 相位发生变化, 因此无人的情况下, 只能得到一个速度为 0 左右



(a) 无人移动时



(b) 有人移动时

图3 两种情况下的速度功率谱估计

的谱峰. 一旦有人在检测范围内移动时, 将得到另一个频谱峰值, 它的变化反映出人体的移动情况.

谱峰峰值对应这不同的路径变化速度, 通过速度向量 $\vec{a}(v_k)$ 即可求出对应路径的相位差变化情况. 图 4 为有无人入侵两种不同状态下的相位差变化情况, 可以看出无人入侵情况下, 相位差基本不发生变化, 能够有效消除噪声对检测结果的影响. 而当有人入侵时, 相位差会随着人体的移动产生变化. 因此可以通过相位差变化来实现高鲁棒性的入侵检测, 下面对本文方法在不同场景下进行了评估.

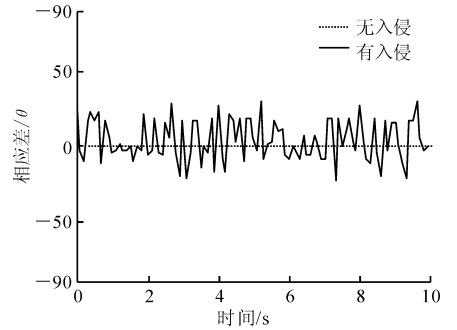


图4 两种状态下的相位差变化

4.2 性能测试

本文在两个典型的环境中(卧室和会议室)评估了本文的方法, 前者配有床、书桌、沙发等, 后者相对空旷. 共招募了 3 名志愿者, 要求他们在房间里自由走动. 观察志愿者的动作, 并记录识别结果. 主要关注以下两个指标来评估检测性能:

(1) 假阳性 (FP): 系统在无人移动时宣布“检测到”的事件的比例.

(2) 假阴性 (FN): 系统无法检测到入侵者的情况.

由于一旦监测环境发生变化, 基于指纹的方法的准确性会下降, 所以只是将本文的方法与基于阈值的检测方法进行了比较.

不同场景下的检测结果如图 5 所示. 在两种情况下, 基于阈值的检测方法性能较差, 平均 FP 和 FN 分别为 6.65% 和 5.35%. 而本文的方法均能达到较好的检测精度, 平均 FP 和 FN 分别为 1.07% 和 1.87%. 此外还看出本文方法可以达到一个非常低的 FP, 这意味着受噪声的影响非常小. 此外, 基于阈值的检测方法在会议室的检测效果明显好于在卧室的检测. 前者相对空旷, 后者堆满了各式各样的家具, 营造出相当复杂的无线传播环境. 而本文方法在两种情况下的性能都是稳定的, 能够有效消除多径对于检测结果的影响.

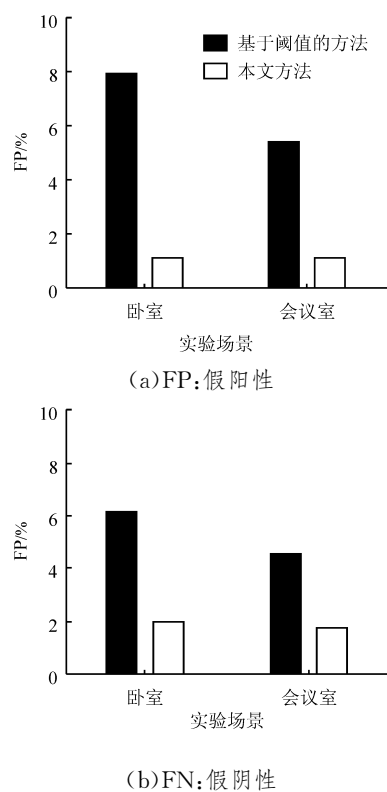


图 5 不同场景下的入侵检测性能比较

5 结束语

本文设计了一种基于 Wi-Fi 信道状态信息的高鲁棒性室内人体入侵检测方案,通过 MUSIC 算法提取由人体移动导致 CSI 相位发生的微小变化,获取不同的路径变化速度.除了具有非侵入性和隐私保护等优点,还能够有效消除多径对于检测结果的影响.本文在两个典型的场景(会议室和卧室)进行了评估,实验结果表明本方案在不同的室内场景下均具有较高的检测性能.随着 Wi-Fi 设备的普及,基于公众通信的无线信号可以广泛的应用在未来智能家居系统中,提供实时、在家和非侵入性的入侵检测.

参考文献:

[1] CHEN L, HOEY J, NUGENT C D, et al. Sensor-based activity recognition[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2012, 42(6): 790-808.

[2] DU H, YU Z, YI F, et al. Recognition of group mobility level and group structure with mobile devices[J]. IEEE Transactions on Mobile Computing, 2017, 17

(4): 884-897.

[3] JOSHI K, BHARADIA D, KOTARU M, et al. WiDeo: Fine-grained Device-free Motion Tracing using RF Backscatter [C]//12th USENIX Symposium on Networked Systems Design and Implementation NSDI 15. Berkeley, CA, USA, 2015: 189-204.

[4] KOSBA A E, SAEED A, YOUSSEF M. Rasid: A robust wlan device-free passive motion detection system[C]//2012 IEEE International Conference on Pervasive Computing and Communications, Lugano, Switzerland. IEEE, 2012: 180-189.

[5] TIAN Z, SHAO L, ZHOU M, et al. A highly-accurate device-free passive motion detection system using cellular network[C]//2016 IEEE Wireless Communications and Networking Conference. Chennai, India , IEEE, 2016: 1-6.

[6] LIU W, GAO X, WANG L, et al. BFP: Behavior-free passive motion detection using PHY information [J]. Wireless Personal Communications, 2015, 83 (2): 1035-1055.

[7] LIU G, LI Y, LI D, et al. Romd: Robust device-free motion detection usin phy layer information [C]//2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Il-san, Korea, IEEE, 2015: 154-156.

[8] LV J, MAN D, YANG W, et al. Robust Device-Free Intrusion Detection Using Physical Layer Information of WiFi Signals [J]. Applied Sciences, 2019, 9 (1): 175.

[9] BAO Y, DONG L, ZHENG Y, et al. WiSafe: a real-time system for intrusion detection based on wifi signals[C]//Proceedings of the ACM Turing Celebration Conference. Chengdu, China. ACM, 2019: 26.

[10] CHEN C, HAN Y, CHEN Y, et al. TR-BREATH: Time-reversal breathing rate estimation and detection [J]. IEEE Transactions on Biomedical Engineering, 2017, 65(3): 489-501.

作者简介:

于怡然 男,(1995-),硕士研究生.研究方向为无线感知.

常俊(通讯作者) 男,(1970-),硕士研究生,副教授.研究方向无线通信与网络.E-mail: changjun@ynu.edu.cn.

吴柳繁 女,(1997-).研究方向为无线传输网络.

彭予 女,(1998-).研究方向为通信与信息系统.