PerCom Pervasive Computing 2025

Elevating Indoor Security with Detection Through the Walls

Guozhen Zhu, Beibei Wang, Weihang Gao, Chenshu Wu*, K. J. Ray Liu

Origin Research

*Department of Computer Science, The University of Hong Kong

guozhen.zhu@originwirelessai.com

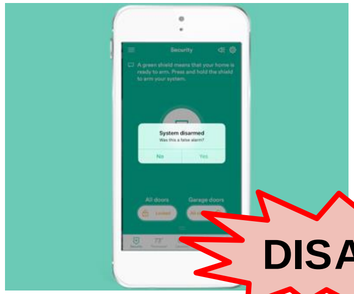
ORIGIN™

Motivation

Indoor intrusion detection systems are crucial for indoor security.

Deterring intruders, protecting people, places, and assets from potential security threats …

However, they struggle with extremely high false alarm rates.



DISARM

Essential needs- reduce false alarms!

Related Works

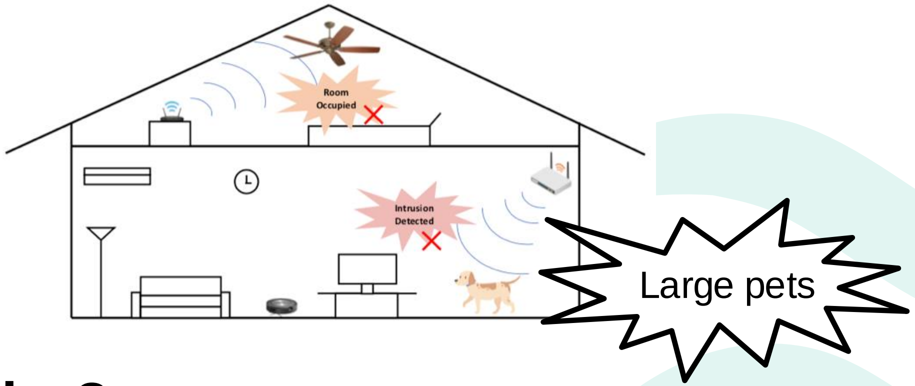
- Non-RF based methods:
  - Camera
  - PIR

Under LOS with limited coverage, …

WiFi

- **Non-intrusive** and privacy-preserving sensing
- **Lower costs** and energy consumption by leveraging existing infrastructure
- The ability to **penetrate walls** and objects for hard-to-reach sensing areas
- **High scalability** due to the **ubiquity** of WiFi
- **Resilience to lighting conditions** for continuous operation

Questions



Q1: Will my WiFi mistake my pets from an intruder?

The sensing systems need to distinguish intentional threats (e.g., intruders) from benign perturbations (e.g., pets or appliances) to eliminate ‘cry wolf’ scenarios

Q2: Can I use the system directly in my home without a

WiFi sensing systems need to achieve accurate performanc
environment without model retraining or parameter tuning, avoiding use

Q3: Can WiFi robustly detect the intruders without spurious alarts?

Intrusion detection system should be reliable and can accurately distinguish the pattern of intruder from others over time.

S_1 S_1 ⋯ S_1 S_1 S_2 S_1 S_1 S_1 → Intrusion?

Q1: Will my WiFi mistake my pets from an intruder?

In many indoor environments, the moving subjects can be:

Human motion

Human

Non-human motion

Pets, robots, electrical appliances…

Non-human

Non-human motion introduce high false alarm rates to WiFi sensing system.

Pets, vacuum machines, and electrical appliances are essential parts of families and extensively exist in various environments.

- About 85 million families in US have pets in 2022 (American Pet Products Association).
- The global robotic cleaners market is $5.59 billion in 2021.
- Electrical appliances such as fans and washing machines are common in households.

--> Distinguishing human and non-human subjects is crucial for practical indoor intelligent applications and systems.

ORIGIN™

Human V.S. Non-human

Different gait patterns:

- Human – bipeds
- Pets – quadrupeds
- Robots - wheeled platforms
- Walk differently --> speed patterns![1]

--> Employ AI models!

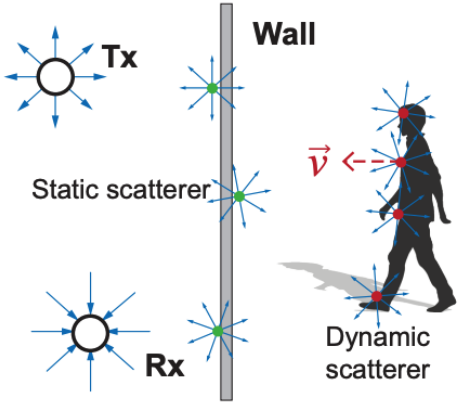
Challenges:

- Features cannot be derived from data:
  - Device limitations:
    - Coverage
    - Noise
  - Motion is complex:
    - Intrusion
    - Multiple people
- Features show overlap:
  - Pet too large

[1] G. Zhu, Y. Hu, B. Wang, C. Wu, X. Zeng and K. J. R. Liu, "Wi-MoID: Human and Nonhuman Motion Discrimination Using WiFi With Edge Computing," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 13900-13912, 15 April15, 2024.

Q2: Can I use the system directly in my home without any calibration?

Raw CSI reflects multipath propagation from both **static** and **dynamic** subjects. Deep learning models also learn the contextual information.



As a result, data-driven methods based on deep learning models are highly sensitive to environmental changes.

--> Use environment-agnostic statistic to force models to learn pattern from dynamic subjects.

Q3: Can WiFi robustly detect the intruders without spurious alerts?

The motion classification is based on a small segment of WiFi data, which ignores the **long-term temporal pattern** of motion.

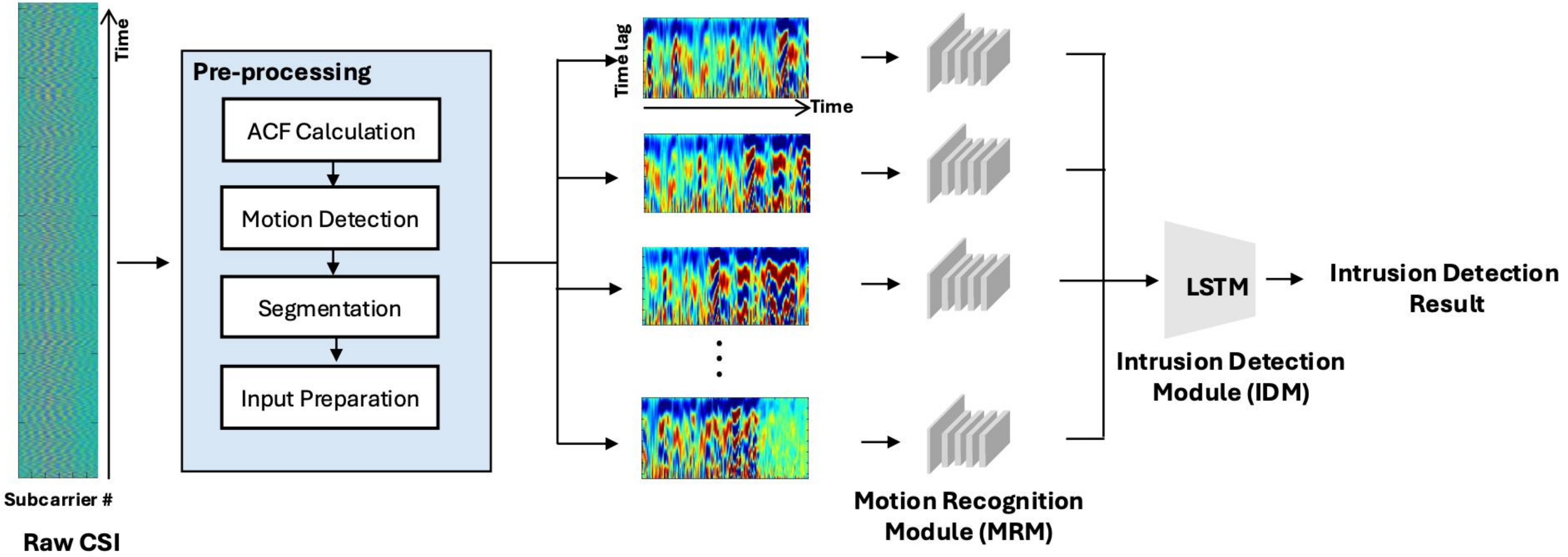
A single misclassification can cause a spiky false alarm, eroding user's trust.

$S_1\ S_1 \cdots S_1\ S_1\ S_2\ S_1\ S_1\ S_1 \longrightarrow$ **Intrusion?**

--> Insight: sequential movements are likely from the same subject.

ORIGIN™

System Design



System Design

Environment-agnostic Dynamic Statistic Extraction

1. Take channel power response of CSI

$$\begin{aligned} G(t,f) &\triangleq |\tilde{H}(t,f)|^2 \\ &= |H(t,f)|^2 + 2\,\mathrm{Re}\{n^*(t,f)H(t,f) \\ &\quad \exp(-j(\alpha(t)+\beta(t)f))\} + |n(t,f)|^2 \\ &\triangleq |H(t,f)|^2 + \varepsilon(t,f), \end{aligned}$$

2. ACF of channel power response

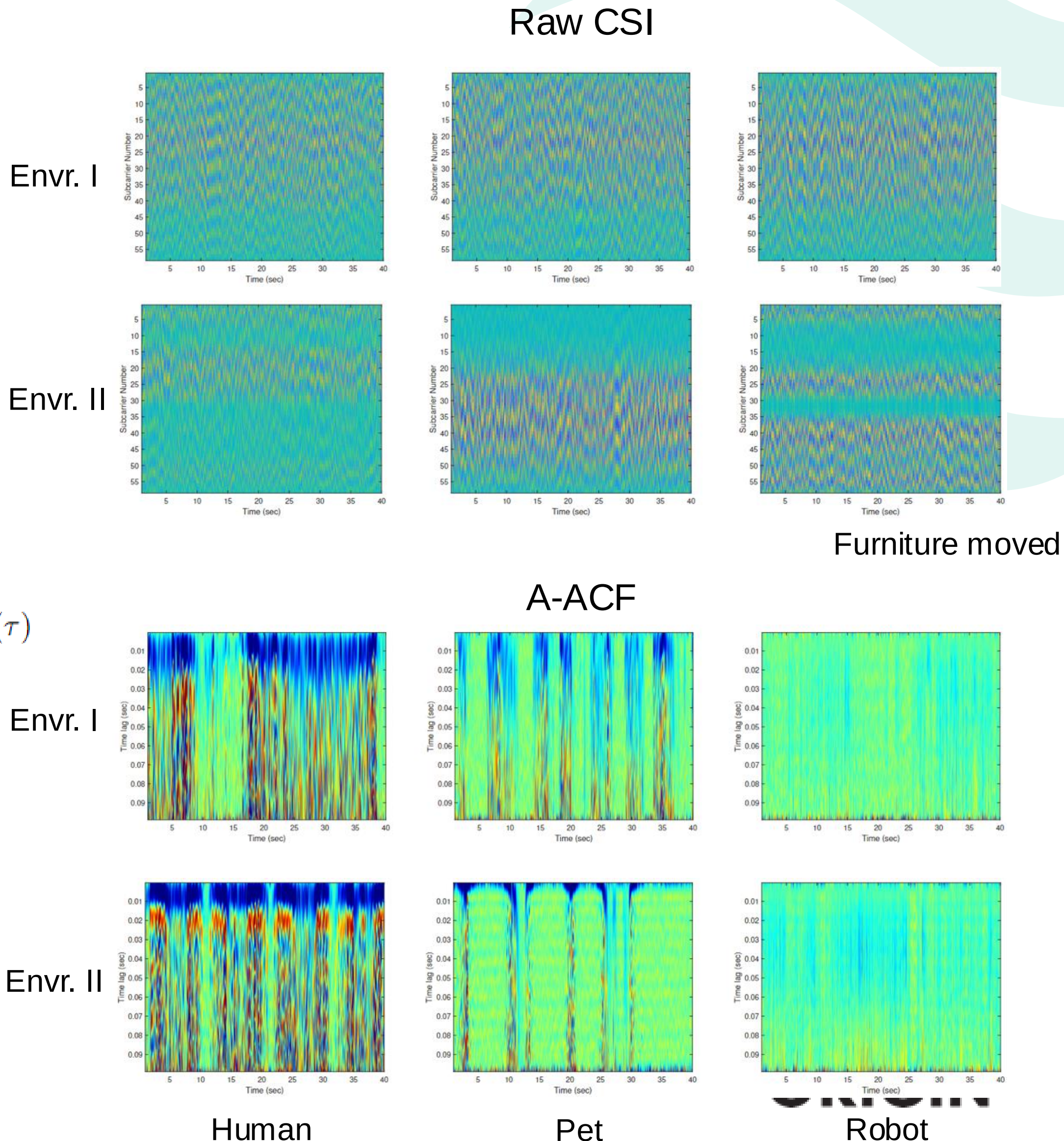
$$\begin{aligned} \rho_G(\tau,f) &= \frac{\mathrm{cov}[G(t,f),G(t+\tau,f)]}{\mathrm{cov}[G(t,f),G(t,f)]} \\ &= \frac{\sigma_s^2(f)}{\sigma_s^2(f)+\sigma_n^2(f)}\rho_s(\tau,f) + \frac{\sigma_n^2(f)}{\sigma_s^2(f)+\sigma_n^2(f)}\delta(\tau) \end{aligned}$$

3. Apply Maximum Ratio Combine (MRC)

$$\hat{\rho}_s(\tau) = \sum_{i=1}^{N_s} \rho_G(\tau = \frac{1}{F_s}, f_i)\rho_G(\tau, f_i)$$

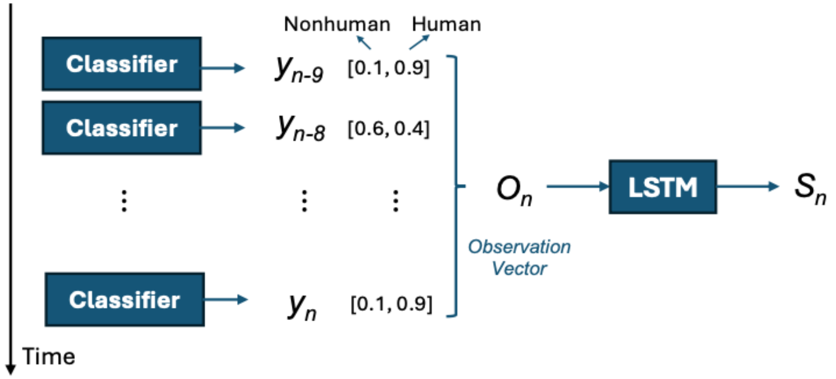
4. Take the differential

$$\Delta\hat{\rho}_s(\tau)$$



System Design

- Motion Recognition Module(MRM)
  - Recognize the non-human motion and filter it out
  - Select ResNet-18 to balance the computation complexity and accuracy
- Intrusion Detection Module (IDM)
  - Learns the relationship between the current and past probability outputs of MRM



Layer name	MRM	IDM
1	Conv, 7×7, 64, Stride 2	LSTM 200 cells
2	Max Pool, 3×3, Stride 2	
	Res-block $\begin{bmatrix} \text{Conv}, 3 \times 3, 64 \\ \text{Conv}, 3 \times 3, 64 \end{bmatrix} \times 2$	–
3	Res-block $\begin{bmatrix} \text{Conv}, 3 \times 3, 128 \\ \text{Conv}, 3 \times 3, 128 \end{bmatrix} \times 2$	–
4	Res-block $\begin{bmatrix} \text{Conv}, 3 \times 3, 256 \\ \text{Conv}, 3 \times 3, 256 \end{bmatrix} \times 2$	–
5	Res-block $\begin{bmatrix} 3 \times 3, 512 \\ 3 \times 3, 512 \end{bmatrix} \times 2$	–
6	Average Pool, 7×7	–
7	Fully Connections, 512×1000	–
8	Softmax	–

-> Enables a more robust assessment of whether an intrusion is present

Evaluation

Environments

(a) (b)

Floor plan of (a) Scenario I, an office building an apartment, and (b) Scenario II, a single family house. Tx and Rx are marked in orange and blue, respectively. The intrusion route is marked in green.

Dataset Information

Scenario	Human	Pet	Cleaning robot	Fan
I	3 Females and 7 Males	8 Dogs	iRobot V3	Rotation
II	1 Female and 3 Males	3 Dogs	iRobot V3	Rotation, Ceiling

Device

Rx in Scenario II

ORIGIN™

Evaluation

Recognition Performance

Method	Validation	Testing
MLP	91.59%	86.14%
LeNet	93.60%	88.83%
ResNet-18	**95.84%**	**91.71%**
ResNet-50	96.02%	90.67%
ResNet-101	96.38%	91.66%
RNN	86.64%	88.82%
GRUNet	89.77%	85.25%
LSTM	85.79%	83.90%
ViT	92.40%	87.77%

- Recognition performance is evaluated by averaging classification accuracy.
- Select ResNet18 for MRM

Detection Performance

	Intrusion Detection Rate	False Alarm Rate	Average Detection Time
Scenario I	100%	0.90%	2.50s
Scenario II	93.33%	2.94%	2.50s

- Our system achieves an average intrusion detection rate of 96.67% and an average false alarm rate of 1.92%.
- These results demonstrate the system's high reliability, precision, and efficiency in promptly detecting intrusions across different environments.

Discussion

Effectiveness of the IDM

	Intrusion Detection Rate	False Alarm Rate
Without IDM	96.67%	9.28%
With IDM	96.67%	1.92%

Computation Complexity and Memory Requirement

Module	MRM	IDM
FLOPS(G)	1.37	$1.85e^{-4}$
Parameters(M)	11.17	$1.82e^{-2}$
CPU inference time(ms)	16.95	0.76
Peak memory usage (MB)	0.65	0.06
Model size (MB)	42.7	0.06

Latency

For a 5 s motion segment:

- Preprocessing time: 2.51 seconds
- Total Training time
  - MRM: 160.39 seconds
  - IDM: 44.56 seconds

Device:

- Intel Core i7 processor
- NVIDIA GTX 2080 GPU
- 16GB of RAM

Its training can be conducted offline, rendering the training time practically negligible.

Thank You