Inferring the Scene Using Wireless Traffics and World Knowledge

Xiaoyi Han & Binglu Chen

Motivation and Objective

- smart home IoT devices & low-cost wireless sensors
- privacy leakage

↓

- an attack method
- infer human movement within a specific room
  - wireless traffic from camera sensors
  - trained neural network
- demonstrate the serious privacy threats

Goal

- Accurate Classification:

  Achieve high accuracy in classifying static, slight movement, movement, and intense movement.

- Performance Optimization:

  Compare and fine-tune models to select efficient algorithms suitable for analyzing wifi packet data.

- Practical Application:

  Provide a general solution for similar time-series data analysis tasks in different scenarios.

Related Work

- RF-based Localization and Tracking → just infer position
- WiFi received signal strength indicator (RSSI) and Channel State Information(CSI) →
  - an extra device
  - a specific environment
- User Behavior Analysis in IoT Devices →
  - access sensor data like app usage history and movement patterns
  - use a set of simple sensors, whose patterns are identified

Novelty

- Wifi Packets Based
  - Use a computer to capture the wifi packets between camera and router
  - Compared to RSSI- and CSI-based methods, we don’t need a receiver
- H.264 Camera Transmission Rule and Packet Transmission Patterns:
  - H.264 compresses video by encoding I-frames with full images and P/B-frames with differences.
  - This results in larger packets for motion and smaller packets for static scenes.
- Requires No Wifi Access
  - Same as an attacker in real-world scenario, our project use the encrypted data without wifi access.

Technical Method

Self-collected dataset:

I. Simulation of human living environment

Includes:

- 5 distinct backgrounds
- 5 different figures
- 4 movement states

A total of 100 samples.

I. Captured Surveillance camera corresponding Wi-Fi packets, each with 40 seconds.

Static

Slightly move

Move

Intensive move

Technical Method

Wi-Fi Packets Characters:

- **Sequential Nature**

Wi-Fi packets arrive one after another in a specific order.

- **Time Dependencies**

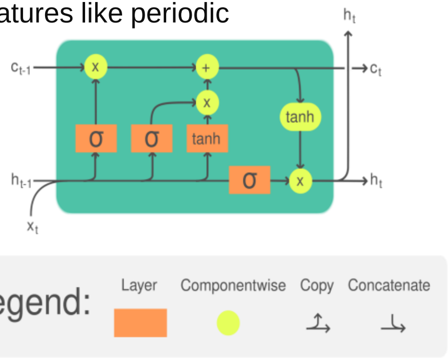
Wi-Fi packets depend on time. For example, the time between packets can show if the transmission is busy.

- **Pattern of transmission**

The pattern of packet transmission includes features like periodic bursts, changes in packet size.

LSTM (Long Short-Term Memory)

- LSTM is designed to process sequences, maintaining an internal memory of past inputs.
- LSTM captures short-term and long-term time dependencies
- LSTM can identify transmission patterns over time by learning from sequential data.



Technical Method

Extracted feature from samples:

- **Packet length**
- **Relative timestamp**
- **Timing difference between packets**
- **Raw data**

Normalized

LSTM

Dimension Reduction with
Principal Component Analysis (PCA)
Dimension=256

Dimension = 2832
includes redundant information and noise

Reduce data and model complexity

Experimental Evaluation

Training Set Metrics:

Accuracy: 0.74

Precision: 0.81

Recall : 0.74

Classification Report:

	precision	recall	f1-score
Static	0.93	0.72	0.81
Slightly Move	1.00	0.60	0.75
Move	0.58	1.00	0.73
Intensely Move	0.75	0.63	0.69
accuracy			0.74
avg	0.81	0.74	0.75

Experimental Evaluation

Validation Set Metrics:

Accuracy: 0.48

Precision : 0.51

Recall : 0.50

Classification Report:

	precision	recall	f1-score
Static	0.44	0.57	0.50
Slightly Move	0.75	0.30	0.43
Move	0.45	0.71	0.56
Intensely Move	0.40	0.40	0.40
accuracy			0.48
avg	0.51	0.50	0.47

Experimental Evaluation

```
Overall Metrics:
Accuracy: 0.67
Precision : 0.72
Recall : 0.67
Classification Report:
                precision       recall  f1-score
        Static          0.74    0.68    0.71
 Slightly Move          0.74    0.48    0.63
        Move        0.55        0.92    0.69
Intensely Move          0.67    0.58    0.62
        accuracy                        0.67
             avg            0.72        0.67    0.66
```

Experimental Evaluation

The model's performance on the validation set is insufficient, while it performs well on the training set, indicating the issue of overfitting.

Static and **Move**:
These two classes show relatively high precision and recall, demonstrating that the model performs well on these categories.

Slightly Move and **Intensely Move**:
These classes have lower recall, suggesting the model struggles to differentiate them effectively. This could be due to imbalanced sample distribution or insufficient feature representation.

Conclusion

Data Processing and Feature Extraction:

- Successfully extracted features from `.pcap` and `.json` files containing network traffic data.
- Standardized input data through alignment, normalization, and dimensionality reduction

Model Development and Comparison:

- Implemented various classification models, including traditional machine learning models (KNN, SVM, Decision Tree, HMM) and deep learning models (MLP, LSTM).
- Achieved good performance on the training set with some models (e.g., LSTM).

Performance Analysis:

- The models demonstrated good capability in identifying static and movement categories.
- For slight movement and intense movement categories, recall rates were relatively low due to insufficient features.

Future Directions

Feature Extraction and Optimization:

The current features may not effectively distinguish between slight movement and intense movement. In the future, more discriminative features could be explored.

Model Generalization:

The performance gap between the training and validation sets indicates that the model suffers from overfitting. Increasing the dataset size to improve the model.

Multi-Modal Data Integration:

Network traffic data and motion information are processed separately. In the future, integrating these two types of data to construct a unified feature space could significantly enhance the model's performance.

Division of Work

Binglu Chen：

1. Collecting wifi packets
2. Process data with LSTM
3. Data dimension reduction with PCA
4. Fine-tuning and testing different models, performance analyzing

Xiaoyi Han:

1. Generating and modifying 4 types of motion
2. Collecting camera videos
3. Resizing 100 samples to 300/800/1000/3600
4. Build different types of models and train it to compare the performance.

Thank you!