Marco Polo: Geographically Pinpointing Clients on Wireless Networks

Curtis Taylor and Craig Shue
Worcester Polytechnic Institute
{crtaylor, cshue}@cs.wpi.edu

Introduction

Recent work has demonstrated an approach to locate a targeted Internet user to within 690m (0.43 miles). While this scope gives the searcher a general area of the user, it is not useful in many cases. For example, law enforcement officers often need to quickly locate an individual participating in illegal, online activities. To do this, they would go through a lengthy process of getting a subscriber's information from the Internet Service Provider in order to locate the user. This process is also used by copyright holders trying to locate infringers. However, with more precise geolocation, enforcers could skip the subpoena process and go directly to the suspect's location.

Our Goals

- Fast localization
- Precise localization
- Avoid obtaining subpoenas
- Universally applicable
- Use only commodity hardware

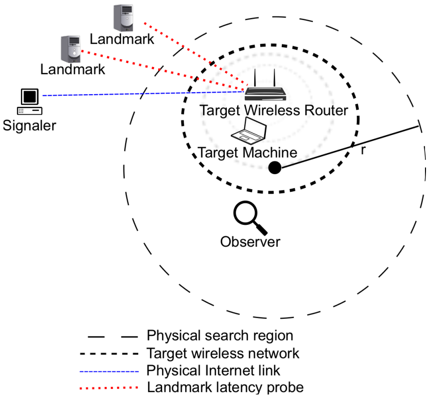
Covert Wireless Signals

To locate a target, one can traverse a physical region looking for specific data being transferred. However, many networks encrypt their network traffic preventing an adversary from simply viewing the contents. To overcome this issue, we use a packet size approach. The packet size approach allows an adversary to monitor the wireless spectrum looking for packet sizes, predetermined by the signaler, that have been shared with the observer. The sizes of the packets need to be uncommon sizes to avoid false positives. We chose our packet sizes to be of random varying sizes between 750-1500 bytes.

Our Implementation

For our implementation and experimentation, we used only commodity hardware and applications. The key pieces to our implementation include:

1. **Signaler** – send beacons to target
2. **Target** – connects and receives signal from signaler
3. **Observer** – monitors wireless spectrum near target looking for beacons



— — Physical search region
- - - - - Target wireless network
.... Physical Internet link
.... Landmark latency probe

Steps in Our Process - Signaler

1. Create a connection to the target
2. Establish search region via landmarks
3. Send signals via connection
4. Dispatch observer to identified search region

Steps in Our Process - Observer

1. Obtain signal pattern from signaler
2. Traverse region looking for wireless embedded signal
3. Identify and pinpoint via triangulation

Experiments

Experiment 1: Apartment Building

The purpose of this experiment was to determine the practicality of finding a target in a multiple level apartment setting. We attempted to locate a target positioned on the second floor of a 3 story apartment building. Figure 1 shows the building and surrounding roadways. Approximately 15 different wireless signals were identified. We not only identified the target from the front sidewalk but also from the roadway in front of the apartment.

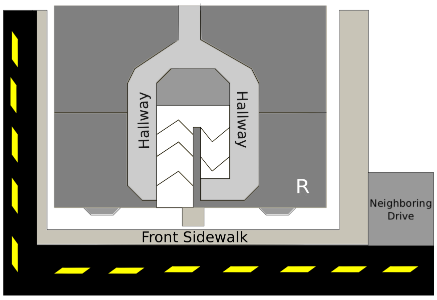


Figure 1 Experiment 1 building layout of the apartment. "R" labels the position of the target's wireless router

Experiment 2: Residential Neighborhood

Our single-blind experiment in a residential area used only public roadways and sidewalks when attempting to locate the target. The adversary was given a search area of approximately 690 meters as shown in Figure 2a. The paths highlighted blue shows the actual path driven. Within 40 minutes, the adversary was able to locate the target within 3 houses. Figure 2b shows the true positive and false positives seen. Throughout this experiment, over 24,000 data-carrying packets were observed and resulted in only a 0.38% false positive rate.

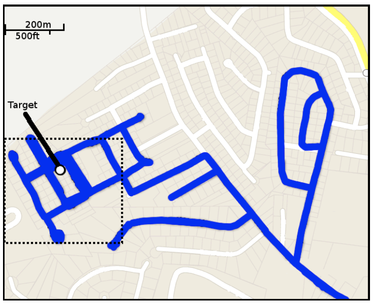


Figure 2a Displays our search region for the residential experiment

	State of the Art	Our Approach
Localization	690m	Roughly 3 houses
Physical Presence Necessary	No	Yes
Specialized equipment	No	Yes
Multiple signalers	Yes	No
Obtains MAC	No	Yes
Can Verify as Correct	No	Yes
Useful for Law Enforcement	No	Yes

Conclusion

We can geographically locate a target transmitting via wireless router. Our approach relies on a signaler sending special sized packets to a target while the observer listens for the packets to be transmitted wirelessly to the client.

- Ability to quickly locate wireless target
- Cost effective
- Uses existing software and hardware
- Works in multiple environments
- Raises privacy concerns

Our approach did not determine the exact target's location, but allowed us to get very close. With specialized equipment, such as directional antenna, and additional metrics, such as wireless signal strength, we may be able to determine the target's exact location.

Acknowledgements

We would like to thank Nathanael Paul for his addition to our research and Matthew Squires for his assistance with initial experiments. We would like to thank Andrew Klein for his advice on wireless protocols and signal analysis. We additionally want to thank Lawrence MacIntyre, Brent Lagesse, Arun Thomas, and Craig Wills for reviewing earlier drafts of our work and providing helpful suggestions for improvements.

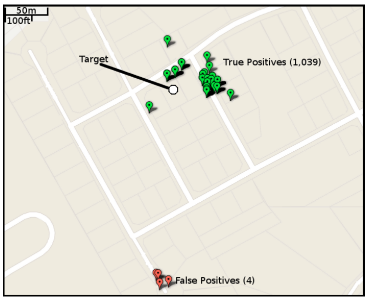


Figure 2b Displays true positives and false positives seen in search region