From an IP Address to a Street Address: Using Wireless Signals to Locate a Target

Craig A. Shue (WPI), Nathanael Paul (USF)
And **Curtis R. Taylor** (WPI)

WOOT '13
August 12, 2013
Washington, D.C.

Outline

- Motivation and Goals
- Current Approaches
- Our Approach
  - Covert Wireless Signaling
- Experiments
- Countermeasures
- Summary
- Future Development

Motivation

- Online criminals must be apprehended
  - Child predators, online assailants
- Current work is not accurate or fast enough for many law enforcement purposes
  - ISP subpoenas are slow.
- Most US homes use wireless networks (61% - 80% in recent studies [1])

Goals

- Fast localization
  - Under an hour would be excellent
- Precise localization
  - Street address or exact triangulation
- Avoid the need for ISP subpoenas
  - Best to avoid any special law enforcement power
- Universally applicable
  - Works on targeted computers, smartphones, tablets, etc.
- Use only commodity hardware and software
  - Keep approach inexpensive
- Minimally invasive/noticeable
  - Avoid alerts to all but most sophisticated targets

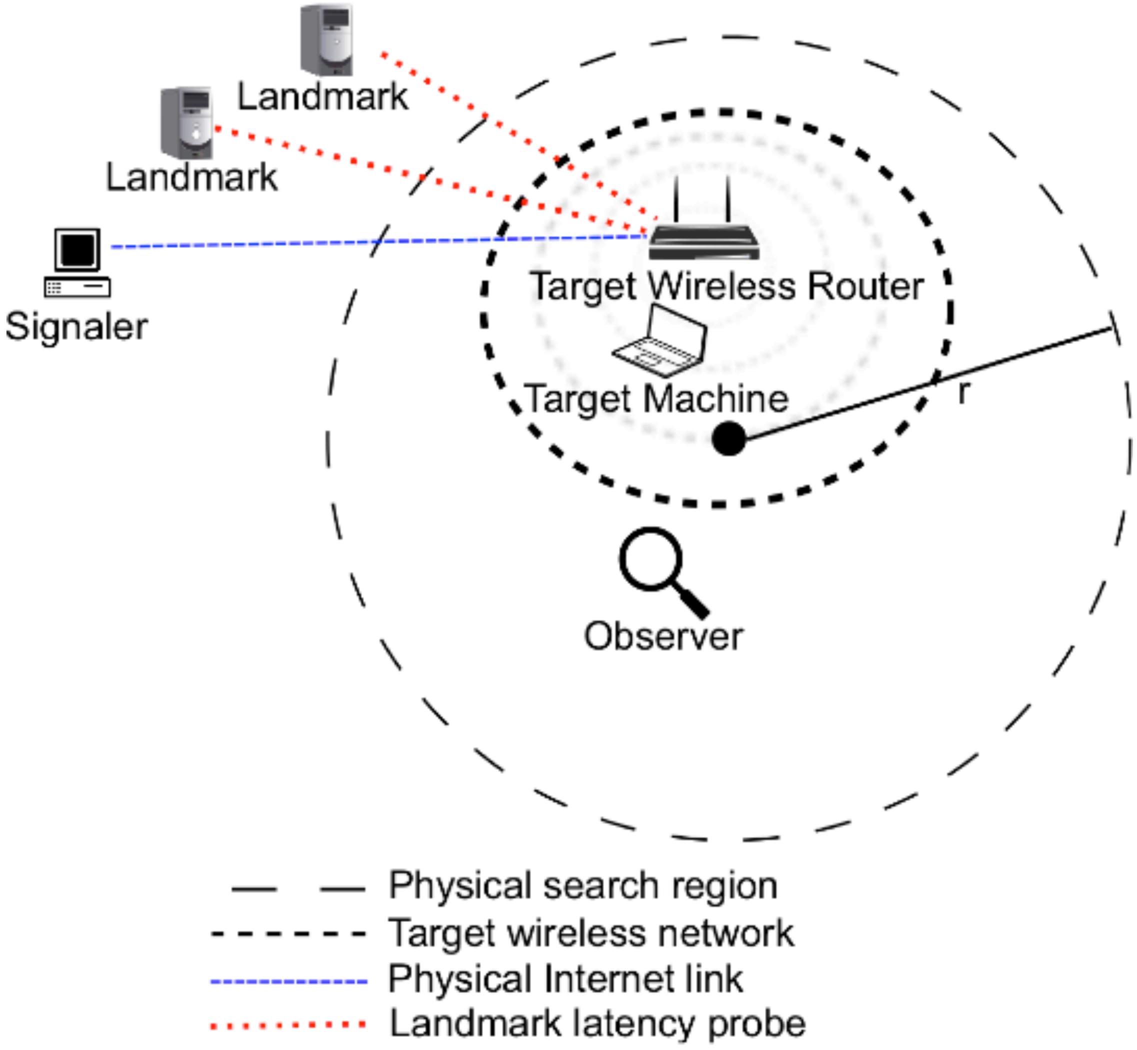
Current Approaches

- Wang *et al.* [2] used latency measurements to get within 690m radius circle.
  - US census: up to 33,000 people near NYC
  - Depends on many servers as landmarks for better accuracy
- Chen *et al.* [3] linked activity behind NATs.
- Area approximation based on IP prefix
  - Not reliable

Our Approach

- Bridges gap between Wang and Chen.
- Assumes Wang’s localization of 690m
- Uses covert wireless signals
- Consists of 3 components: the Observer, Signaler, and Target
  - Signaler sends communication to Target
  - Observer physically searches for signal
- Code name: Marco Polo

Layout of Components



Covert Wireless Signals

- Concerned only with packet sizes
  - Packet length field is not encrypted
  - We found [750-1500] byte packets to be relatively uncommon.
- Shared packet sizes and timestamps in advance
  - Sharing the database allows signaling and observing to be separated without requiring the parties to communicate.

Signaling Requirements

- Access points (APs) do not require connections.
  - They send directly to the Target.
  - Used in many cases, including universities
- Network Address Translation (NAT) requires a connection
  - Lure Target through honeypots (FBI) purporting to offer contraband
  - Peer-to-Peer NAT traversal
  - Hidden iFrames

Signaling Mechanisms

- Must traverse NAT device, but prevent it from reaching user applications
- Signal can be sent out-of-band.
  - – Use out-of-window TCP packets
    - Traverses NAT using existing mapping
    - Inconspicuously discarded by Target's kernel
- Out-of-band signals allow application-agnostic signaling.

Manipulating NAT Devices

- Connection termination does not necessarily stop the packet flow

Router Model	Forwards Out-of-Window Packets	Forwards After Termination
Belkin F5D8235-4	yes	yes
D-Link DIR-655	yes	yes
Linksys E900	yes	**no**
Linksys WRT54G	yes	yes
Netgear WNDR3700	yes	yes

- In fact, the routers terminating transmissions violate RFCs 2663 and 5382

Experiments

- Conducted two real-world experiments
  - Apartment setting
  - Residential neighborhood

Residential Neighborhood

- Target connected to HTTP server (Signaler) on WPI campus from home wireless network
- Target stayed connected for the duration of the experiment
  - Approximately 40 minutes
- Observer physically traversed search region with laptop and wireless adapter
  - Also had pre-shared packet sizes and timestamps ahead of time.

Residential Neighborhood (continued)

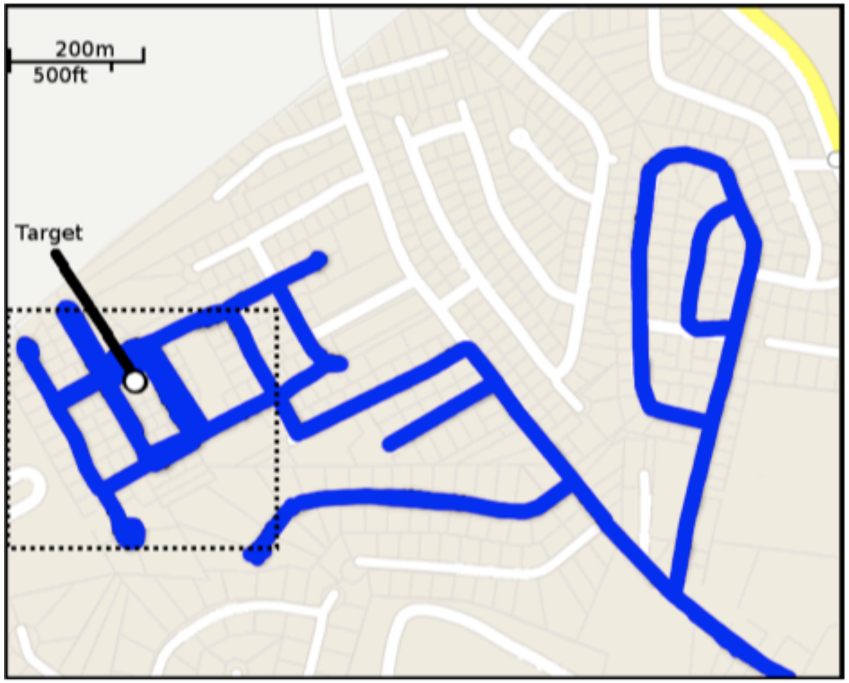


Figure 1: Approximate 690m radius target was located in. Blue depicts path traveled.

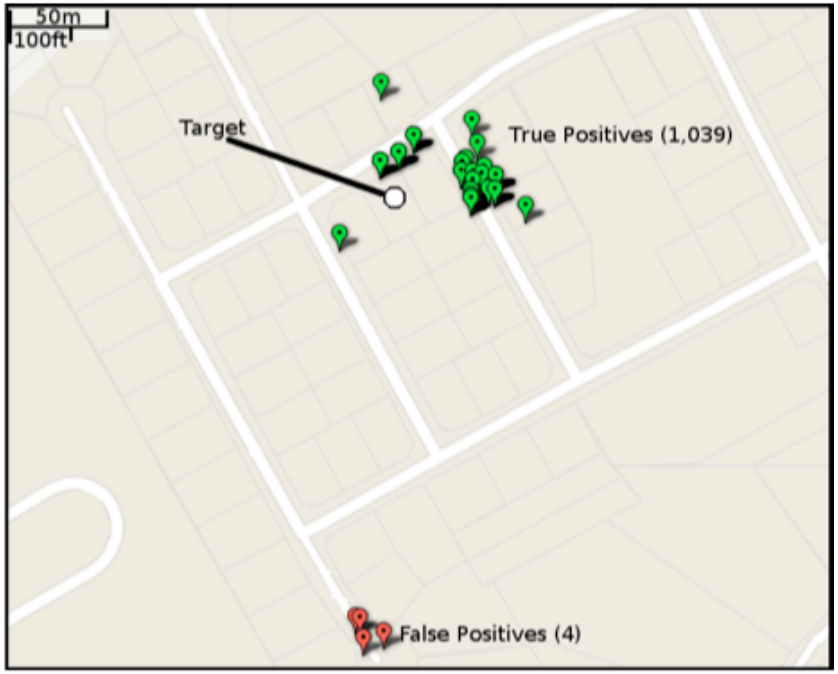


Figure 2: True positives and false positives seen in outlined region.

Residential Study

- Narrowed to three houses
- Target signals blocked by obstacles
  - Wireless router between fireplace and TV
  - Target didn’t want to “bias the experiment” by moving the router
- Experiment did not use enhancements
  - Directional antennas
  - Use of RSSI to determine signal power
- Potential for better results

Countermeasures

- Hardwire
- Proxy server
- Router packet size obfuscation
  - However, doesn’t protect burst patterns
- Anomaly detection
  - E.g., out-of-window packets

Implications

- Internet users are clearly not anonymous
- Anyone can do such tracking
- Legality
  - US federal judge ruled unencrypted data as being, "readily available to the general public", and thus is legal to record under an exception of the Wiretap Act [4].

Summary

- Ability to quickly locate wireless target
- Approach uses three components
  - Signaler, observer, and target
- Uses existing software and hardware
  - Cost effective
- Works on encrypted networks
- Uses covert wireless signals
- Works in different environments
- Raises privacy concerns

Future Directions

- More experiments
- Specialized equipment
  - Directional antenna
- Transition to practical setting

Questions?

- Citations

1) Business Wire, “Strategy analytics: A quarter of households worldwide now have wireless home networks,” http://www.businesswire.com/portal/site/home/ permalink/?ndmViewId=newsview&newsLang=en&newsId=20120404006331&div=-1063439563, April 2012.
2) Y. Wang, D. Burgener, M. Flores, A. Kuzmanovic, and C. Huang, “Towards Street-Level Client-Independent IP Geolocation,” in USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2011.
3) Y.Chen ,Z.Liu, B.Liu ,X.Fu ,and W.Zhao, “Identifying mobiles hiding behind wireless routers,” in IEEE INFOCOM, 2011, pp. 2651–2659.
4) Dist. Court, ND Illinois, “In re Innovatio IP ventures, LLC patent litigation,” MDL Docket No. 2303, Aug. 2012.

WiFi Police