

# On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews

Suman Jana      Sneha K. Kasera

School of Computing  
University of Utah

# Introduction

SSID: Mobicom 2008  
MAC: 00:14:BF:7C:71:2F

SSID: Mobicom 2008  
MAC: 00:14:BF:7C:71:2F



Original AP



Fake AP



- fake AP masquerades original AP's identifiers
- also known as "Evil Twin" attack
- wireless nodes automatically connect to known APs
- public programs, e.g., rglueap, rfakeap, available

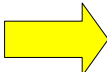
# Fake AP: Serious Problem

- 802.11i supports use of digital certificates to check authenticity of AP
  - distribution across domains problematic
- alternate solution
  - AP fingerprinting
    - ♦ find unique device characteristics that cannot be fabricated

# AP Fingerprint Options

- MAC address
  - easily spoofed
- device driver characteristics (Franklin et al.)
  - difficult to separate multiple devices with same device driver
- clock skew
  - can be used to fingerprint a device (Kohno et al.)
- we explore using clock skew as AP's fingerprint


# Clock Skew: Origin

- a clock consists of
  - oscillator, controlled by crystal
- actual crystal frequency varies with
  - type of crystal
  - crystal cut
- even with same crystal type, cut
  - limited mechanical accuracy  different clock skew

# Kohno's Problem Context

- used TCP/ICMP timestamps to show clock skew of device (PC, laptop)
  - remains constant over time for same device
  - varies significantly across devices
- must deal with
  - millisecond resolution clock
  - variable delays
    - network congestion, different routing paths
    - between timestamp generation, packet transmission

# Our Wireless LAN Scenario

- AP sends beacon packets periodically to advertise itself
- beacon packets
  - contain timestamp, microsecond accuracy
  - timestamped by hardware after winning MAC contention  
 minimal delay variation
  - sent at 10-100 packets/second
- fast, fine granular clock skew determination possible

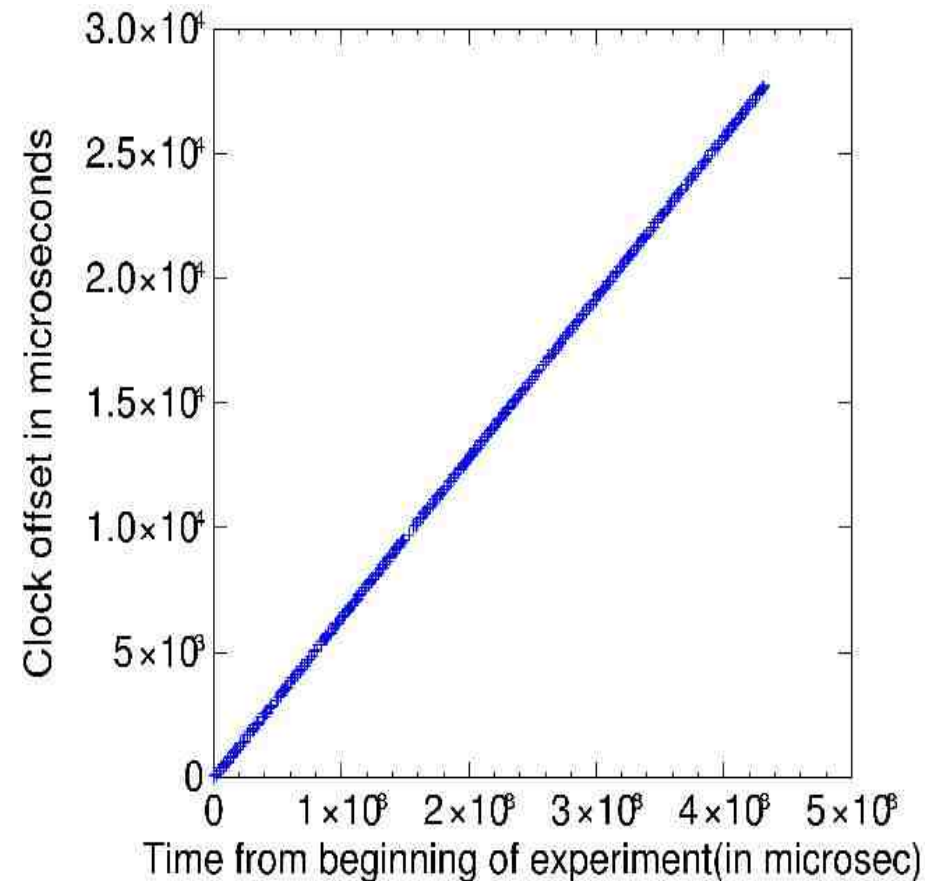
# Our Solution

- use clock skew of AP as it's fingerprint
- maintain record of clock skews of authorized APs
- calculate clock skews of active APs from beacon packet timestamps
- check measured skews with known ones
- if no match declare fake AP
- note: clock skew estimates are relative to fingerprinter's clock



# Clock Skew

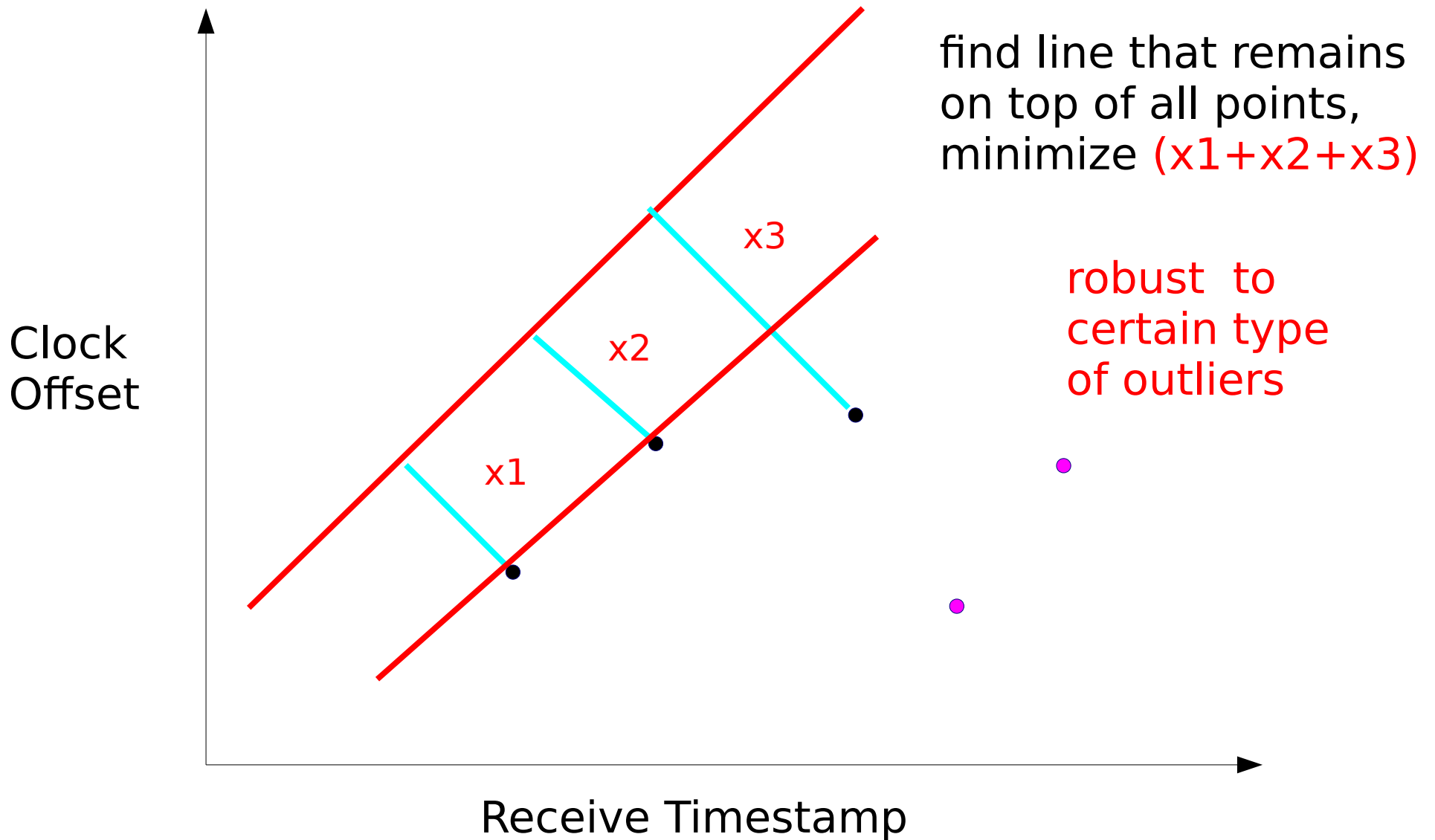
- Clock offsets
  - (beacon transmit time - beacon received time)
- Clock skew
  - rate of change of offset
  - expressed as parts per million (ppm)



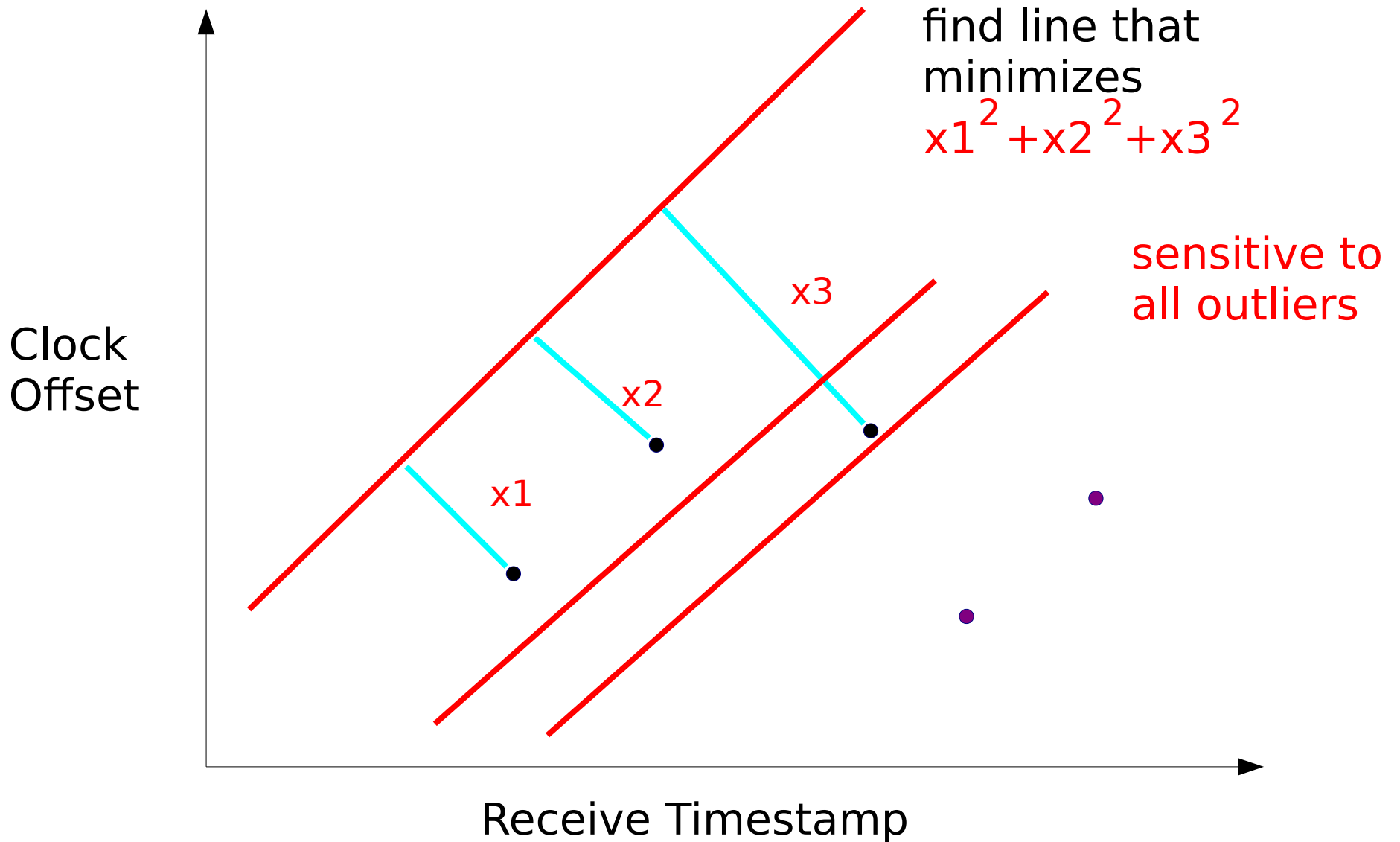
# Estimating Clock Skew from Clock Offset Set

- fit line through clock offset points, determine its slope
- two methods for fitting line
  - linear programming method (LPM)
  - least square fitting (LSF)

# How LPM Works?



# How LSF Works?



# Separating packets from original, fake APs

- original, fake AP(s) can operate at same time
- need to separate packets to determine clock skew(s) of fake AP(s)
  - can help to identify attacker
- algorithm to fit separate lines through data
- LPM may fail to detect fake AP sometimes
  - fake AP packets considered outliers
- LSF always detects fake AP

# Implementation

- capture beacon frames, record timestamps, compute clock skews of APs
- two laptops with Linksys WPC 55AG, Intel 3945ABG wireless cards
  - open source drivers
    - ◊ Madwifi
    - ◊ Intel's driver
  - monitor mode support

# High Precision Receive Timestamp

- **challenge** - how to obtain high precision (microsecond) receive time?
  - use *do\_gettimeofday()* for microsecond resolution
  - timestamp field in Prism monitoring headers in Madwifi, Intel 3945ABG drivers only 4 bytes long
  - use Radiotap header - 8 byte timestamp field

# Experimental Data - 3 Traces

- *ACM Sigcomm 2004 trace*
- *residential trace A, Boulder*
- *residential trace B, Salt Lake City*



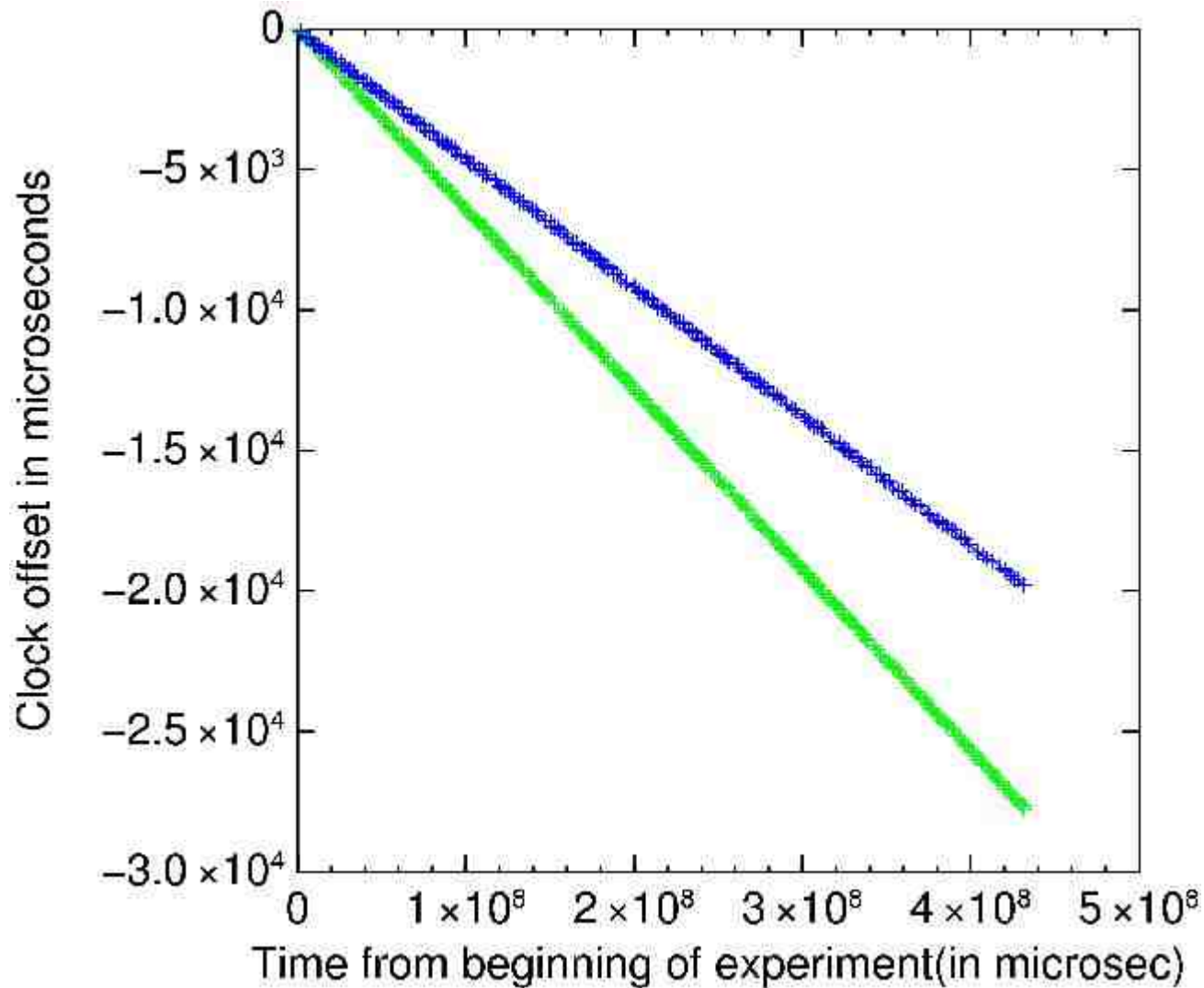
# Results from Sigcomm 2004 Trace

- 5 APs
- low resolution receive timestamps (in milliseconds)
- clock skew estimate required ~300 packets using LPM, ~900 packets using LSF
- each AP had different clock skew (minimum difference 2 ppm)
- clock skew computed from different parts of data resulted in consistent values

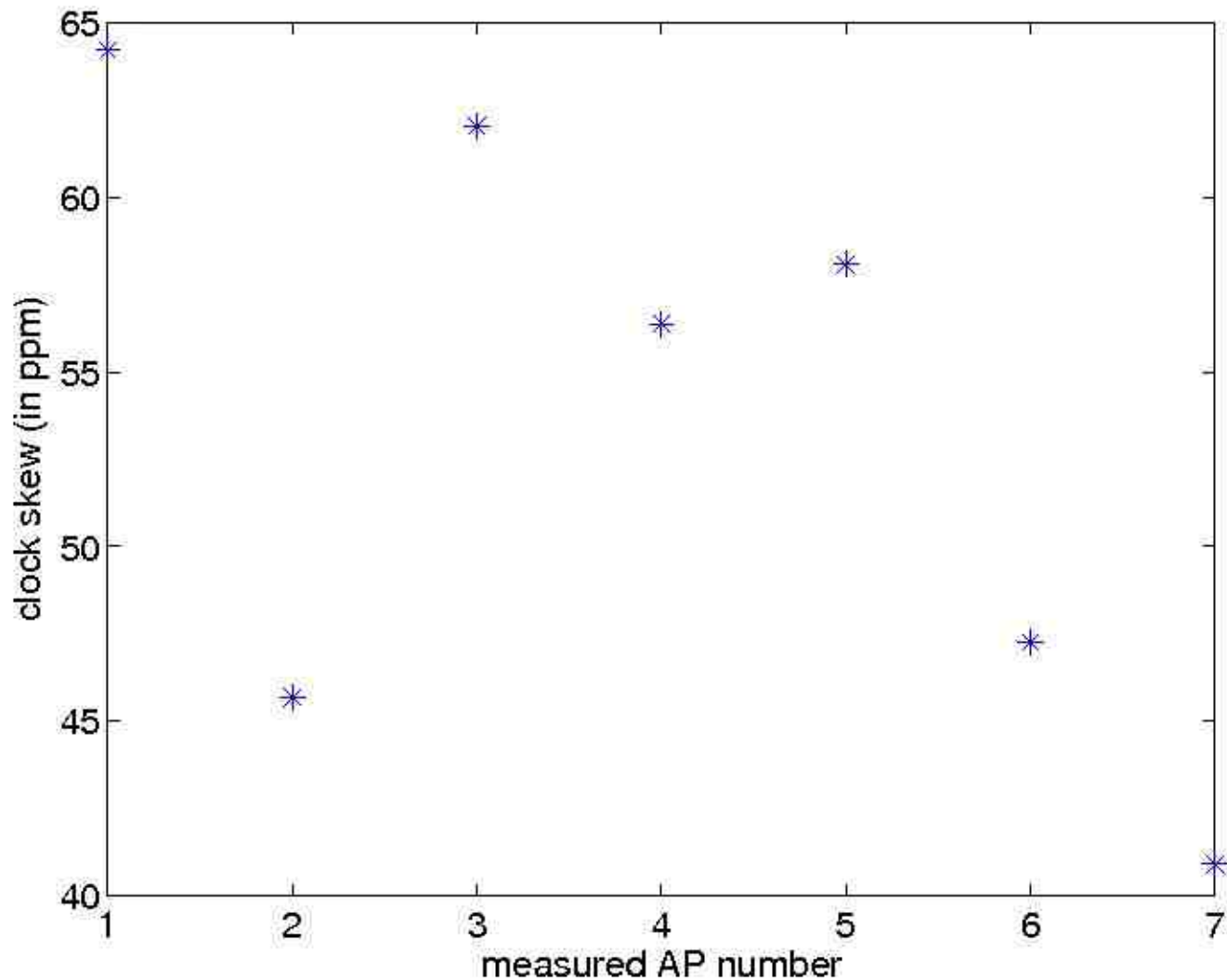
# Results from Residential Traces

- trace A: 8 APs (Boulder, CO)
- trace B: 21 APs (Salt Lake City, UT)
- **only 50-100 packets to estimate clock skew**
- takes only 2-3 minutes
- Kohno's measurements: 1000-2000 packets, 30 min - 1 hour to converge
- significant reduction in skew estimation time

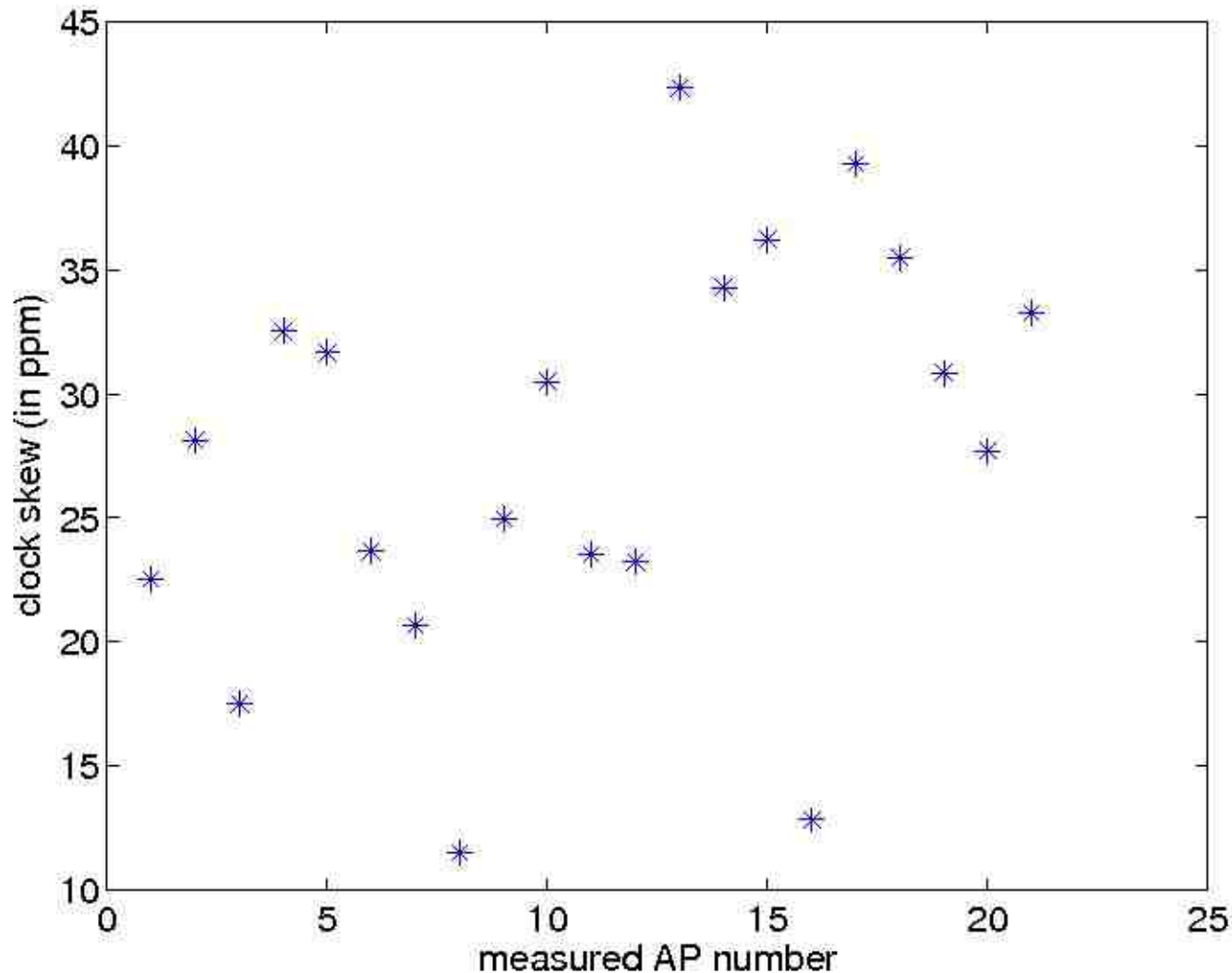
# Clock Offset Sets of Two Different Linksys APs



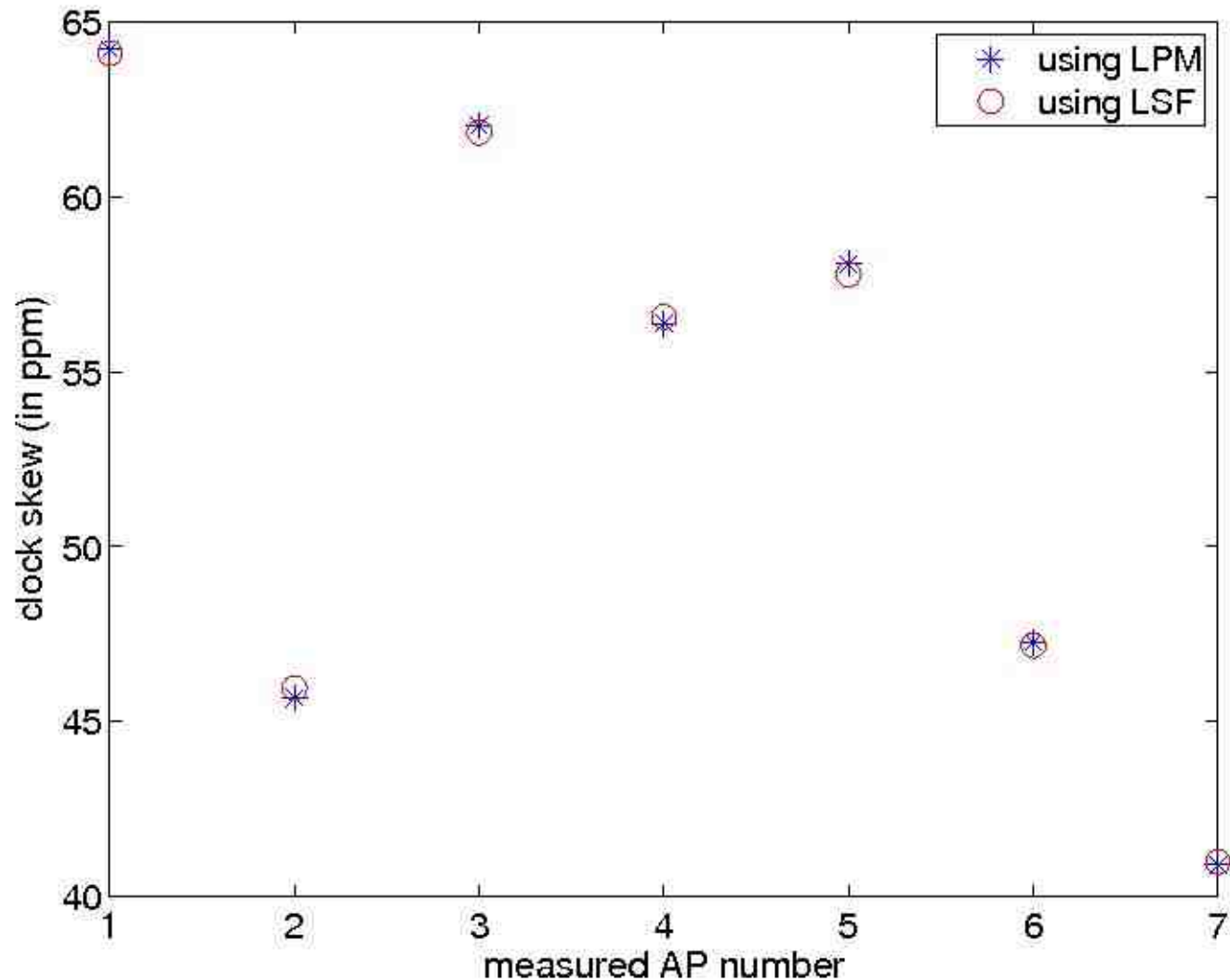
# Clock Skew Estimates for Different APs (Res. Setting A)



# Clock Skew Estimates for Different APs (Res. Setting B)



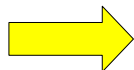
# Clock Skew Estimates Using LPM and LSF (Res. Setting A)



# Effect of Temperature on AP's Clock Skew

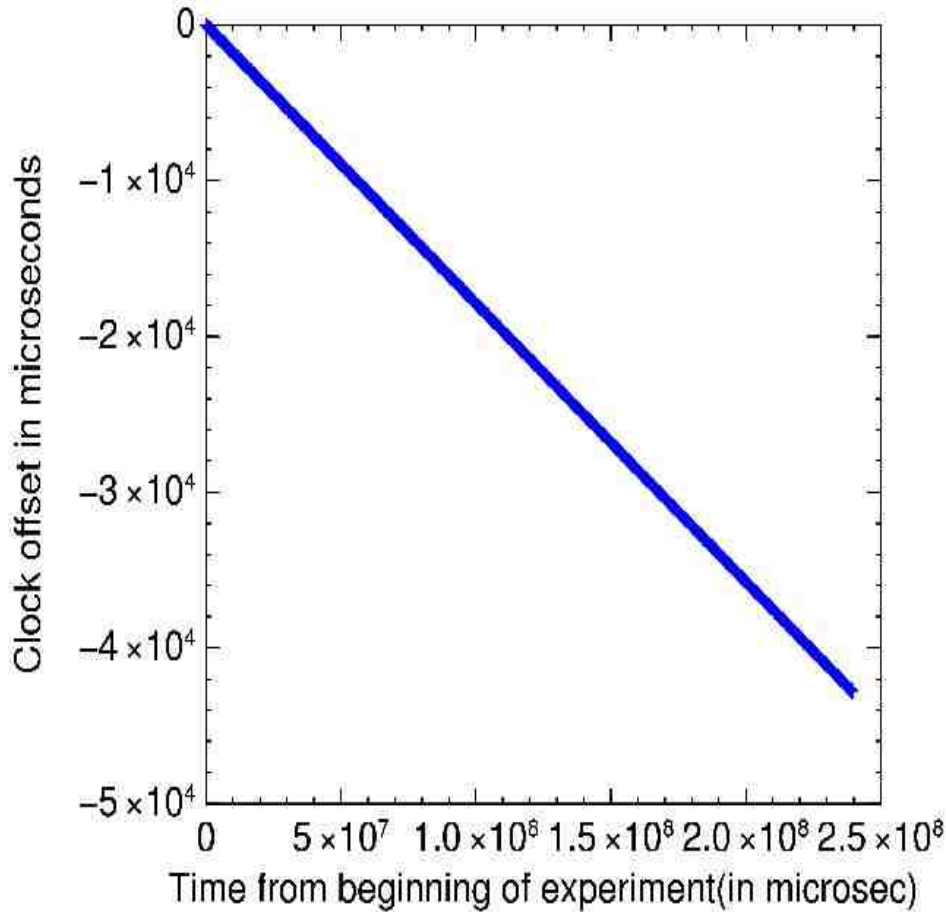
- Pasztor et al: for small time periods (<1000s),  $\text{abs}(\text{clock skew variance}) < 0.1 \text{ ppm}$
- compute clock skew frequently
- if  $(\text{newskew} - \text{currentskew}) \leq \text{max}$  then  $\text{currentskew} = \text{newskew}$ ; else raise fake AP alarm
- $\text{max} = 0.2 \text{ ppm}$

# Clock Skew Fabrication

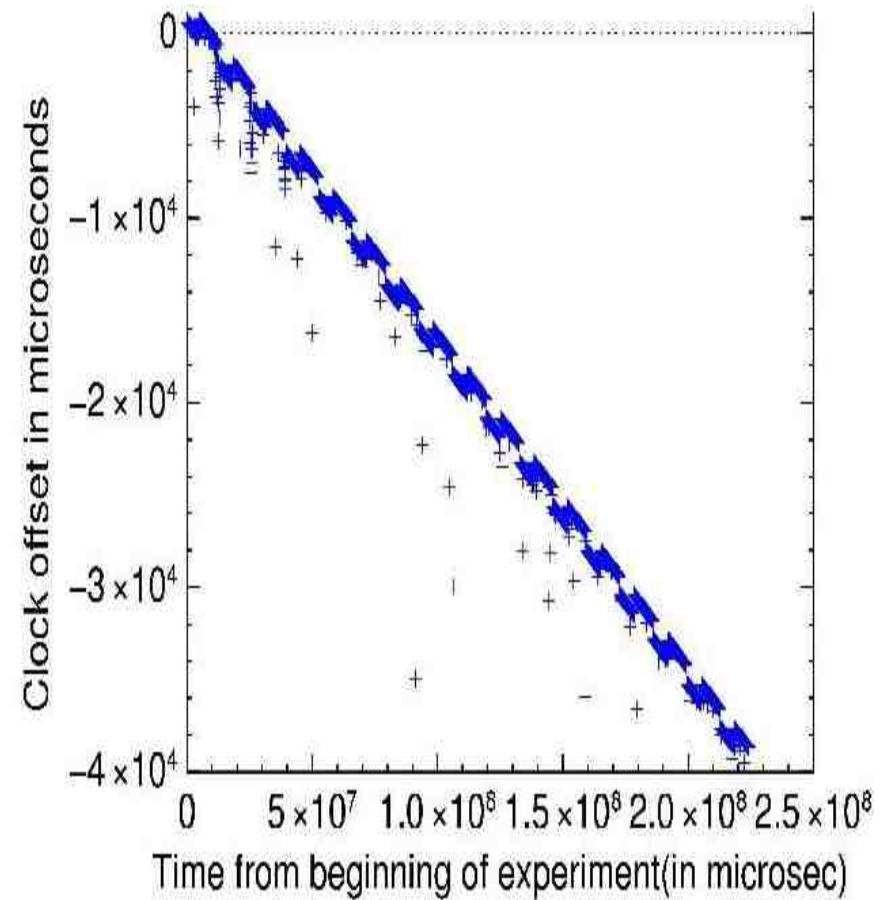
- attacker measures clock skew  $S$
- needs to set its beacon time to
$$TF_i = T_i + S * T_i,$$
where  $T_i$  = actual beacon time at attacker
- in existing WNICs, hardware sets beacon timestamp just before transmitting
  - not possible to change timestamp without modifying hardware
- can use raw packet injection
  - actual transmission times are unpredictable   
fabrication extremely difficult



# Clock Skews of Original AP and Fake AP Using Packet Injection



Original AP: Clock Skew 178.83 ppm



Fake AP: Clock Skew 35 ppm

# Deployment

- should be implemented in Wireless Intrusion Detection System (WIDS) nodes
- in a large network each WIDS node should monitor fixed set of APs

# Summary

- explored use of clock skew to detect fake APs
- clock skew
  - appears to be a good AP fingerprint
  - difficult to fabricate without special hardware
- order of magnitude improvement in estimation time of clock skew (15-20 times)

# Future Work

- collect more data, clock measurements with laptops running on battery power ?
- attacks using programmable devices (e.g., USRP)

Questions ??

<http://www.cs.utah.edu/~suman>

Thank You!!

# Clock skew estimate of virtual APs

AP	Virtual AP1	Virtual AP2
1	23.66	23.66
2	17.53	17.54
3	28.55	28.56
4	32.45	32.46
5	21.24	21.28

- virtual APs
  - multiple identifiers using same hardware
  - have similar clock skew
  - seem to read from the same physical clock
- clock skew can be used to differentiate real and virtual APs