TAIWAN TECH
NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Measuring clock skews of remote devices via wireless communications

Wei-Chung Teng
Dept. of Computer Science & Information Eng.
National Taiwan University of Science and Technology
(a.k.a. Taiwan Tech)

What is clock skew?

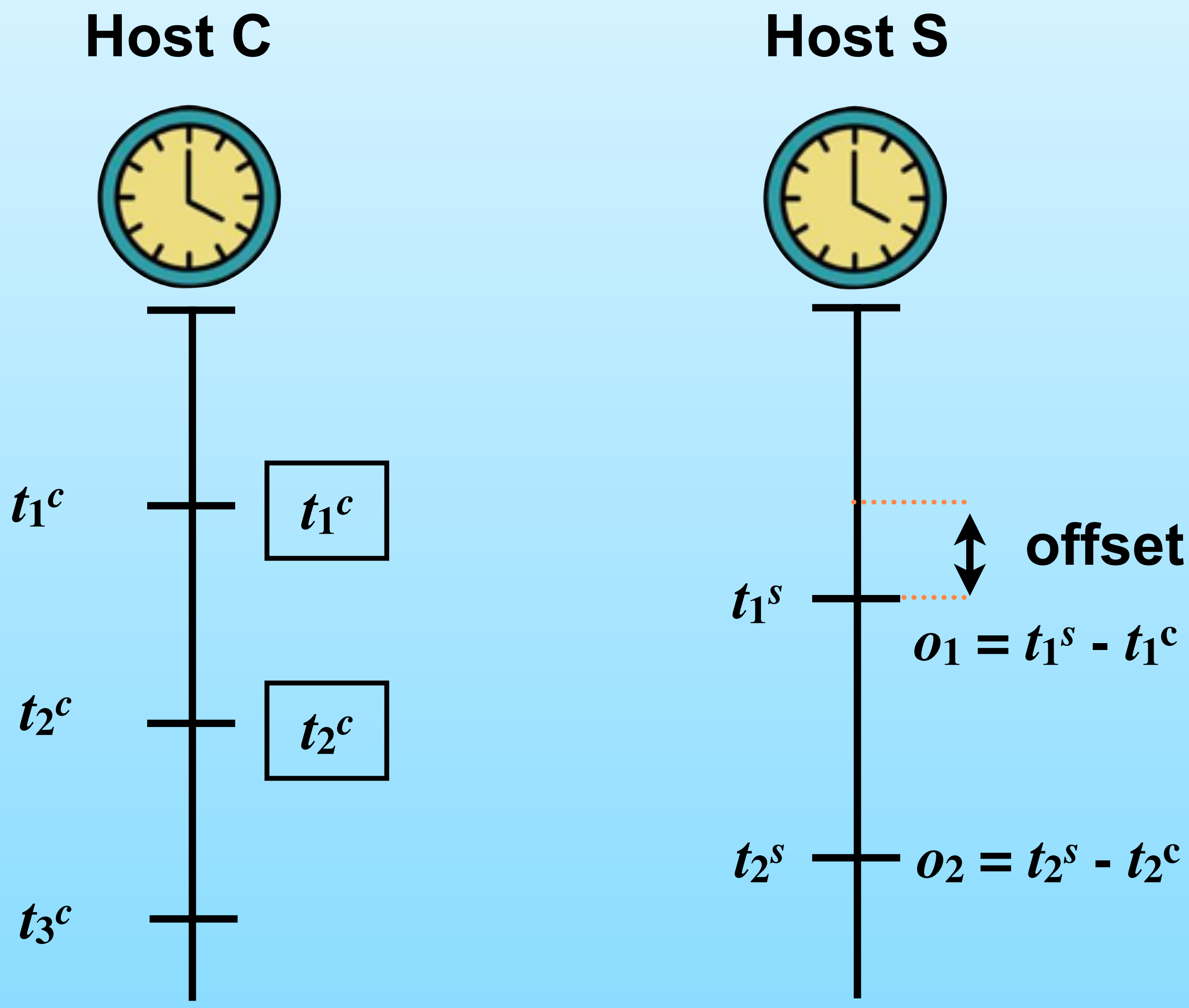
- Almost all digital device has a clock (crystal oscillator), and quartz crystal in every device works in slightly different frequency.
- Thus the speeds (sec/sec) of each two clocks are slightly different
  - we call the difference *relative clock skew*

Why should we care about clock skew?

- Clock skews of the same clock remain the same in normal temperature.
- Past researches (e.g. Kohno, 2005) show that every clock skew measured remotely differs with others at μs precision
- Clock skew is suitable to serve as the physical identity of a digital device

How to measure a (relative) clock skew?

- Let $C_x(t)$ be the time reported by the clock of device x.
- **Offset**: The difference between the time reported by C_c and C_s.
- **Frequency**: The rate at which the clock ticks. The frequency of C_c at time t is $C_c'(t)$.
- **Skew** (δ): The difference in the frequencies of two clocks, e.g., the skew of C_c relative to C_s at time t is $\underline{\delta(t) = C_c'(t) - C_s'(t)}$.

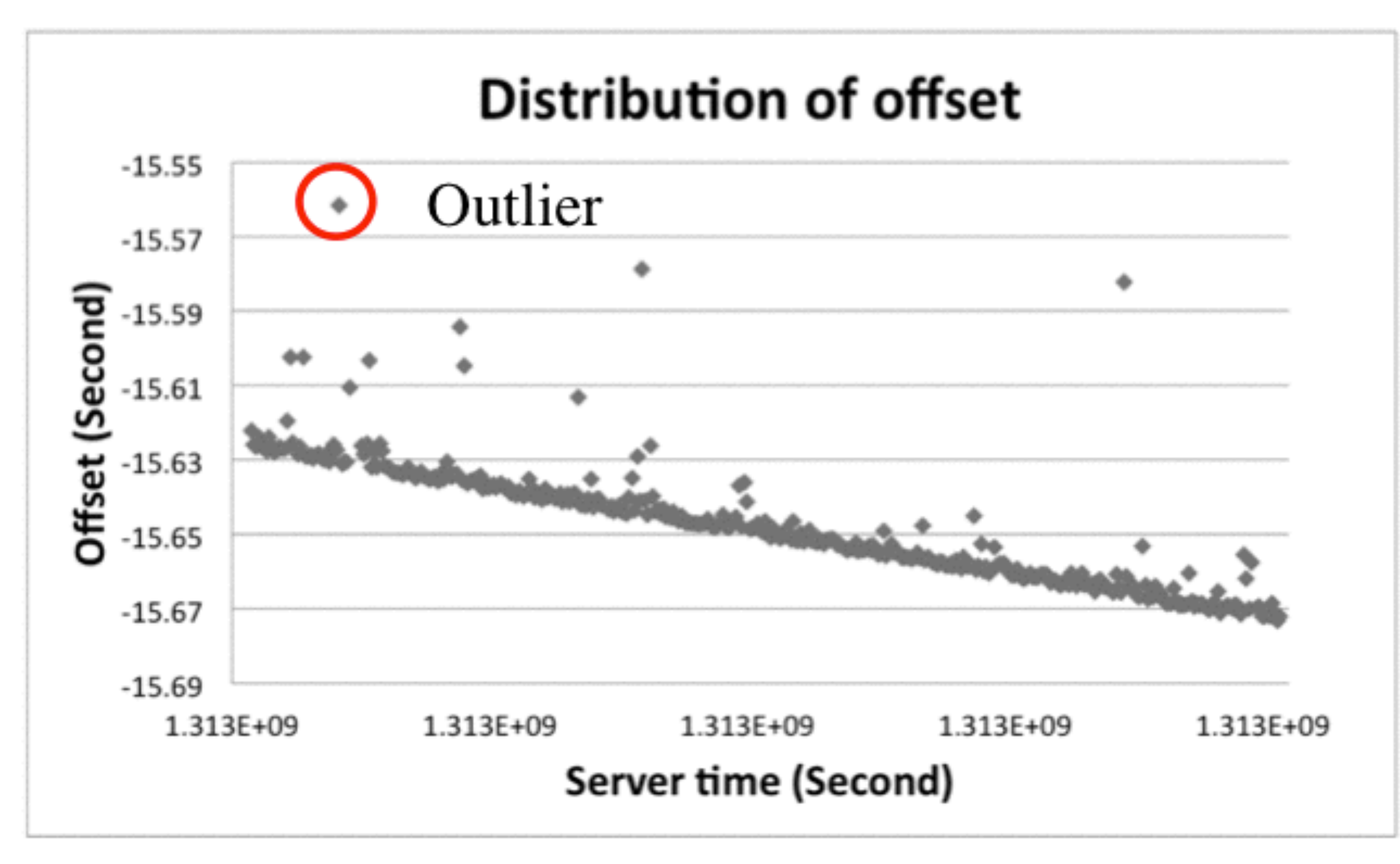


How to measure a (relative) clock skew? cont.

- Since there exists communication delay, we are unable to know the exact offset, but (offset + delay)
  - but the delay is irrelevant to measuring the clock skew *if the delay is a constant*
- We have $\delta(t_2) = \frac{o_2 - o_1}{t_2^s - t_1^s}$

How to measure a (relative) clock skew? cont.

- Since the communication delay is never a constant (there exists jitter), we can not use just two timestamps, we need more samples.



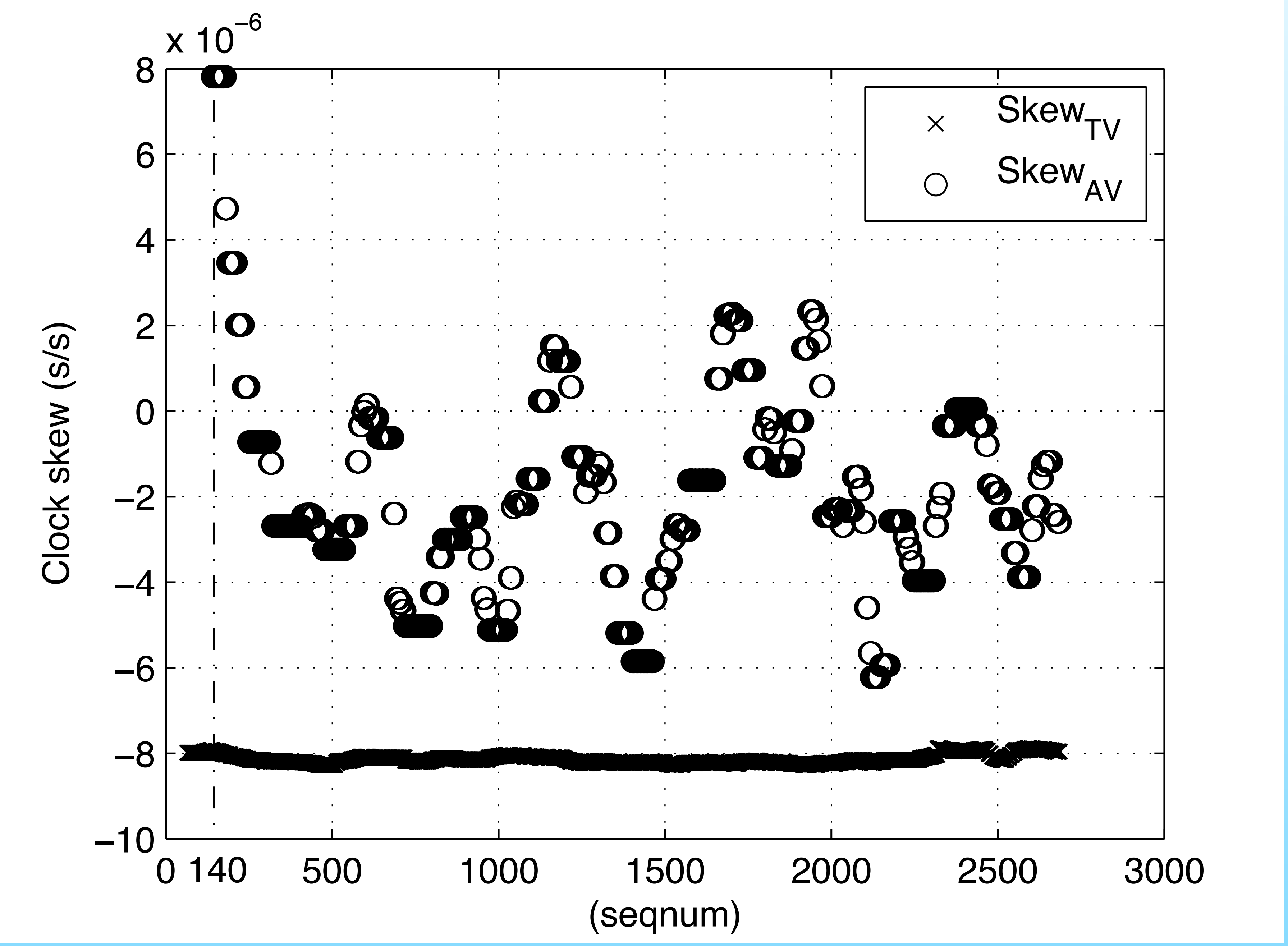
How to measure a (relative) clock skew? cont.

- We can use linear regression to find out the slope which best fits the *trend* of sampled offset
  - might be affected severely by outliners
- We can use linear programming instead
  - not an efficient method if the jitter is large (we need to sample more)
- In a classic sample, most samples are close to (possibly) the minimum delay, so we can pick up points of least delay and run LP with these points.

Question: how to detect a faked clock skew?

- Timestamps are just a series of increasing numbers, sender may alter the speed it increase easily
  - We have found that even for one hop transmission, sender may adjust its skew as it likes
  - However, if we ask the sender to slightly change its sending period from time to time, the fluctuation scale of a faked skew would be more than 10 times of the true skew.

Example: Flooding Time Synchronization Protocol

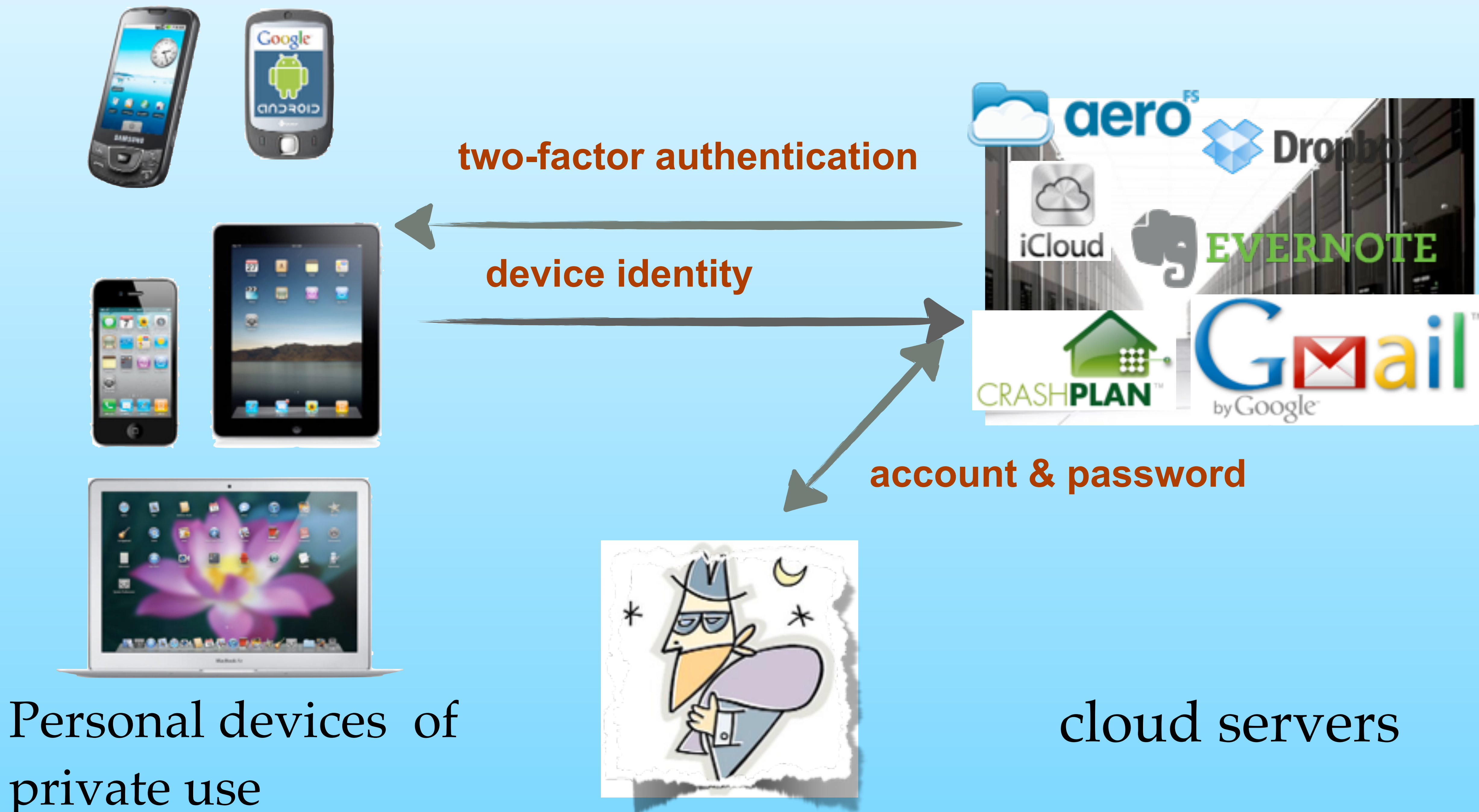


Ding-Jie Huang, Wei-Chung Teng, "A Defense Against Clock Skew Replication Attacks in Wireless Sensor Networks," Elsevier, Vol. 39, pp. 26-37, DOI: 10.1016/j.jnca.2013.04.003, March 2014.*

Question: what is the possible range of clock skew?

Research Title	Min (ppm)	Max (ppm)	Devices
Cristea, M.; Groza, B.,**"Fingerprinting Smartphones Remotely via ICMP Timestamps,"** Communications Letters, IEEE , June 2013	-3.17	87.43	5 devices
Lanze, F.; Panchenko, A.; Braatz, B.; Zinnen, **"Clock skew based remote device fingerprinting demystified,"** 2012 IEEE Global Communications Conference (GLOBECOM)	-30.0	30.0	200 APs
Ding-Jie Huang, et al, **"Clock Skew Based Client Device Identification in Cloud Environments,"** 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA)	-499	67	200 devices
S. Sharma; A. Hussain; H. Saran, **"Experience with heterogenous clock-skew based device fingerprinting,"** the 2012 ACM Workshop on Learning from Authoritative Security Experiment Results (LASER '12)	-150	750	52 devices
Md. B. Uddin, C. Castelluccia,**"Towards clock skew based services in wireless sensor networks," International Journal of Sensor Network, 2011**	-21.11	126.80	8 wireless sensor nodes
Jana, S.; Kasera, S.K.,**"On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews,"** IEEE Transactions on Mobile Computing, March 2010	-1105.69	42.33	24 devices
Ding-Jie Huang; et al,**"Clock Skew Based Node Identification in Wireless Sensor Networks,"** Global Telecommunications Conference, 2008.	-25	62	27 devices

An example application: client device identification for cloud services



TAIWAN TECH
NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

The estimated skews for the same device under different environments

- The estimated skews vary from -21.08 ppm to -23.71 ppm. However, skews of the same network type differ no more than 1.31 ppm.
- Notice that skew of a virtual machine might change every time it reboots.

Network type	Skew estimation	Packets	IP amount
LAN	-21.91 ppm	1001	1
	-23.24 ppm	207	1
	-22.74 ppm	13322	1
ADSL	-21.48 ppm	5837	1
	-21.08 ppm	1400	1
3G	-23.24 ppm	951	1
	-23.71 ppm	1027	1
Wi-Fi	-21.79 ppm	9810	1
	-23.06 ppm	1470	1
Tor	-22.53 ppm	15007	55
	-23.22 ppm	12922	57
	-22.88 ppm	24120	108
VM	-113.19 ppm	868	1
	-114.22 ppm	1001	1
	-6.40 ppm	1001	1
	-6.83 ppm	890	1

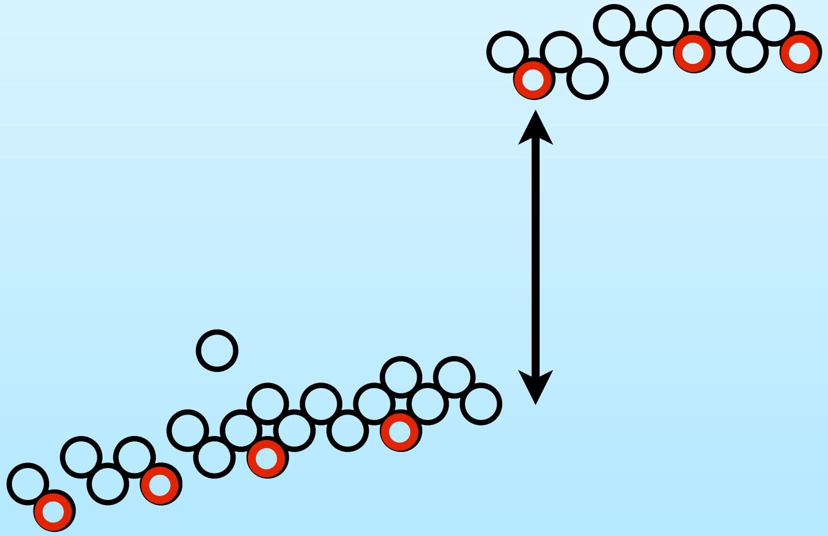
Some new issues on clock skew measurement for WiFi/mobile communications

1. Jump points
2. (varying) Minimum sampling time period
3. Outliners below the crowd

Jump Points

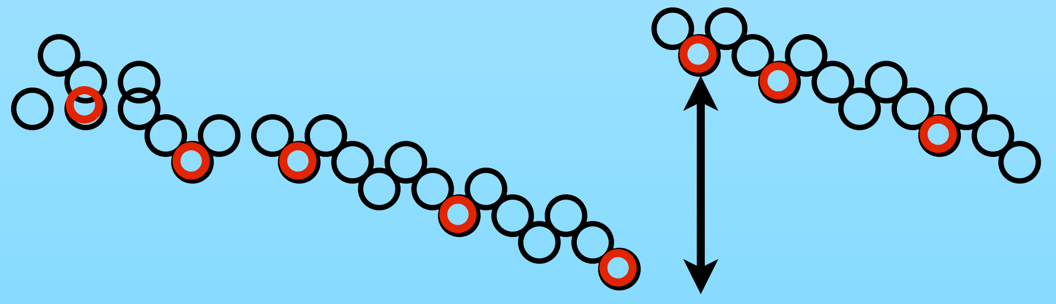
- Caused by a sudden change of offset or delay

- Happen when a device run SNTP/NTP with time servers



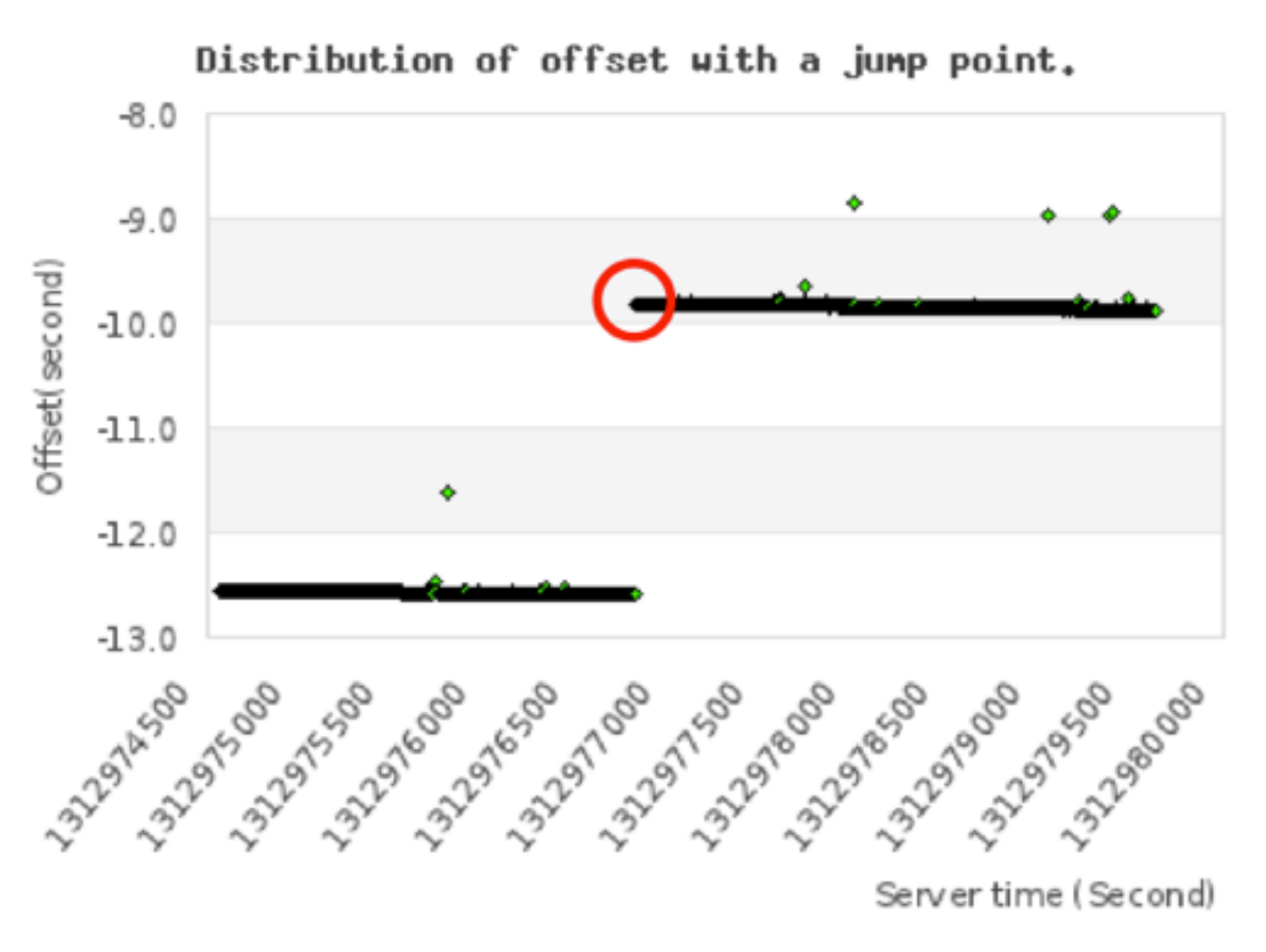
- Happen when a mobile device changes base station during a mobile communication sessions

- Happen when a mobile device switches from WiFi to 4G or vice versa

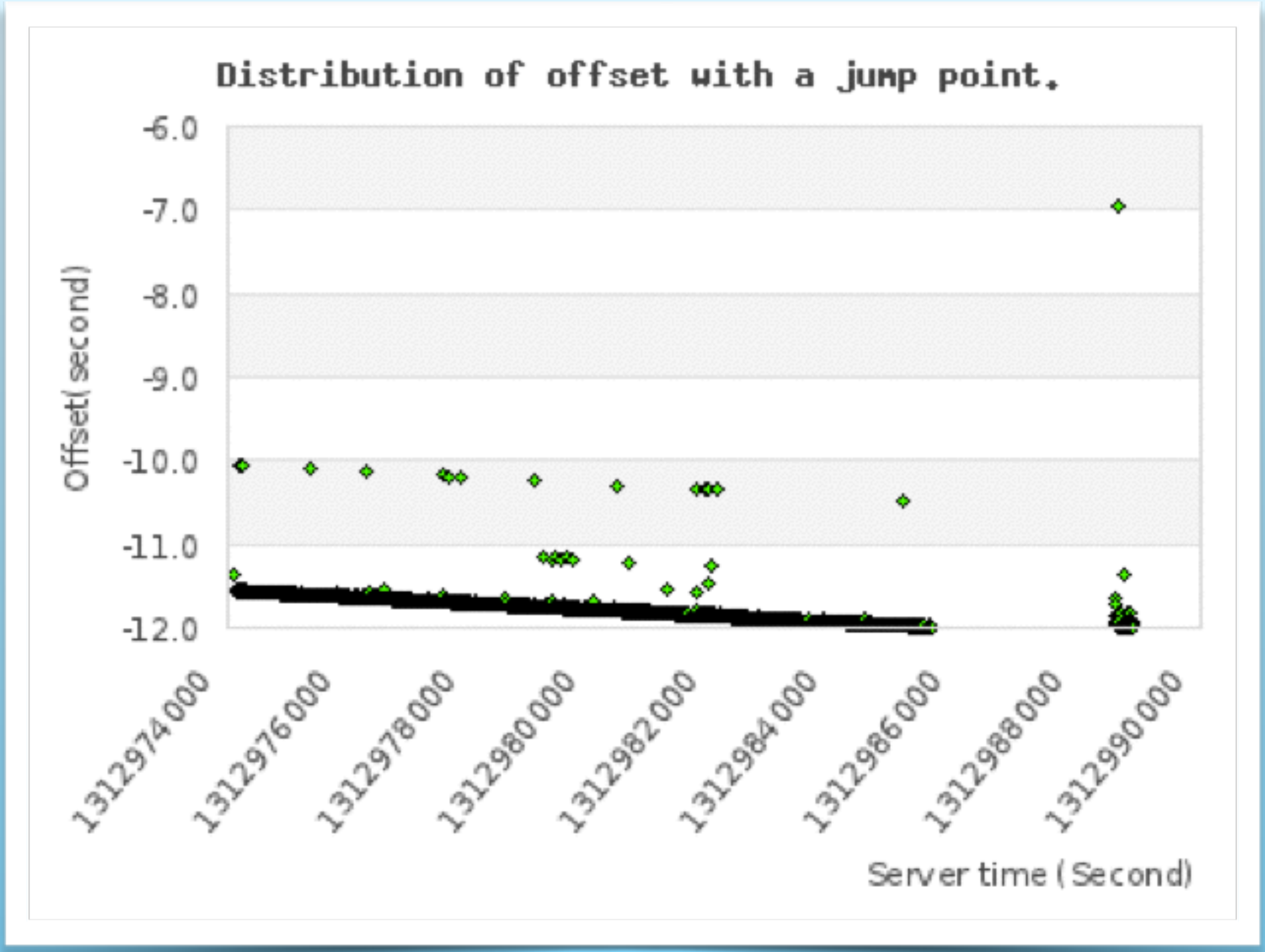


A jump point example

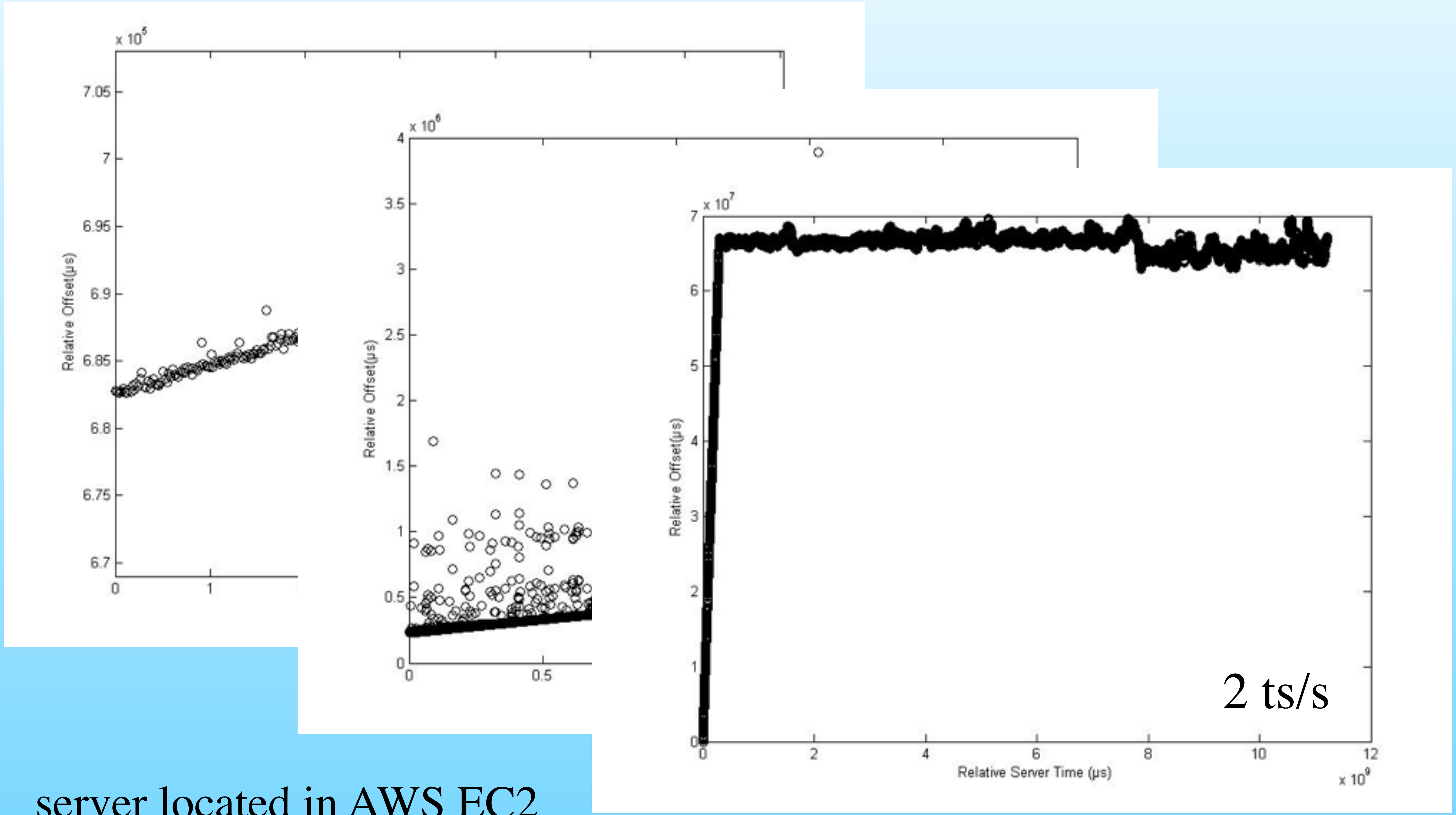
- A jump point of offset occurs if the client is performing time synchronization with a time server or roaming between different network providers.



Another type of jump point

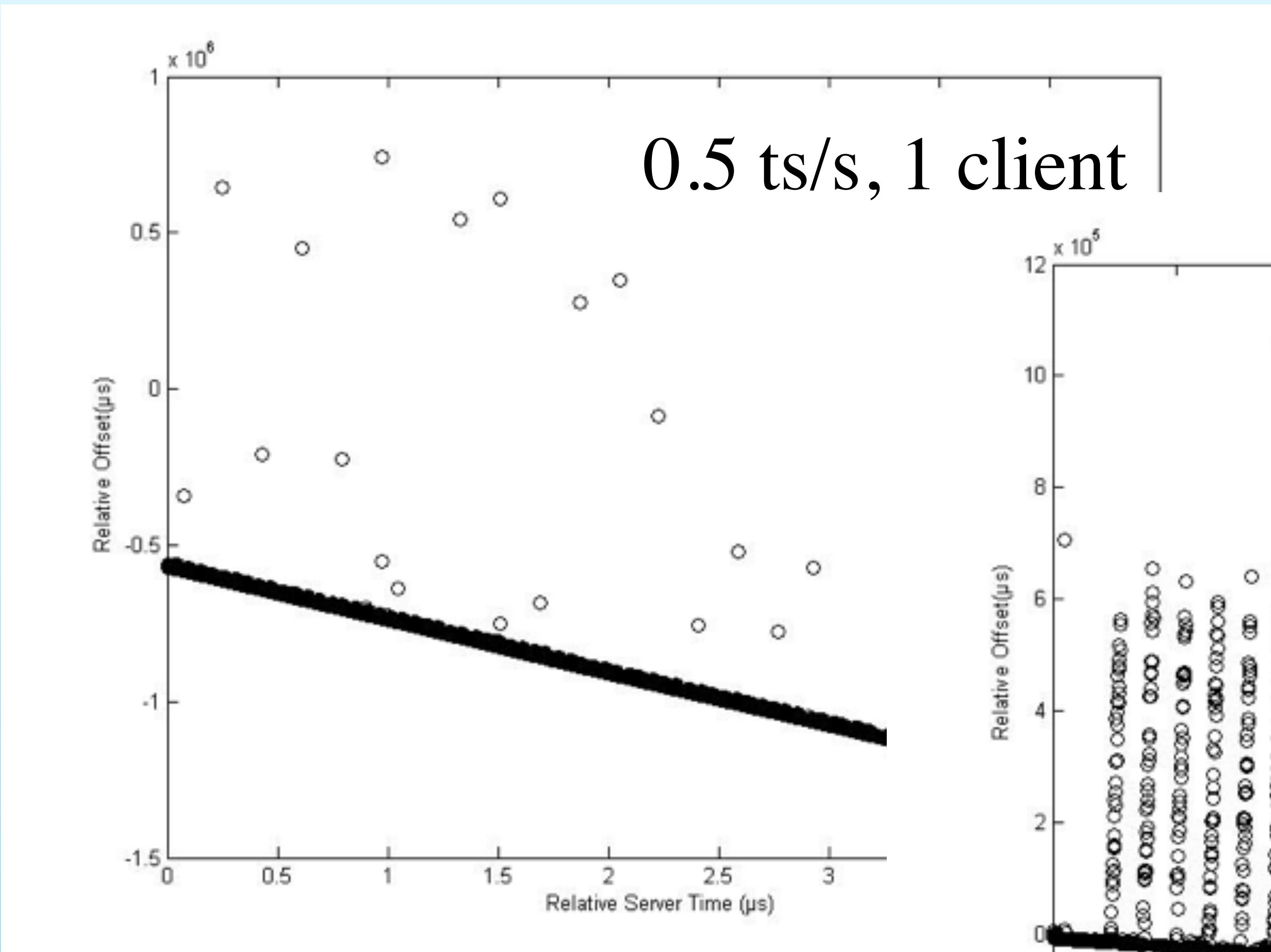


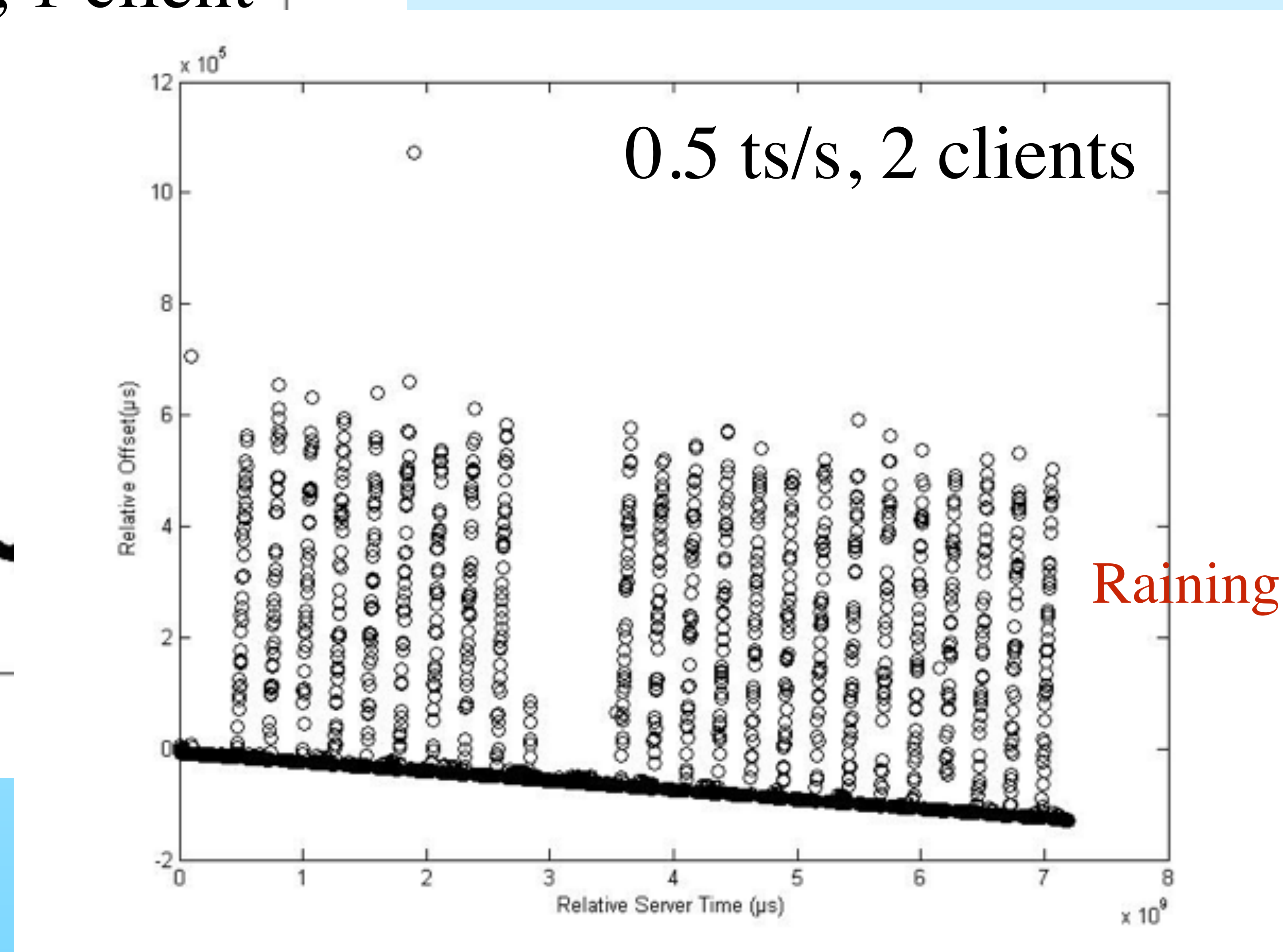
Minimum sampling time period



server located in AWS EC2

Minimum sampling time period cont.



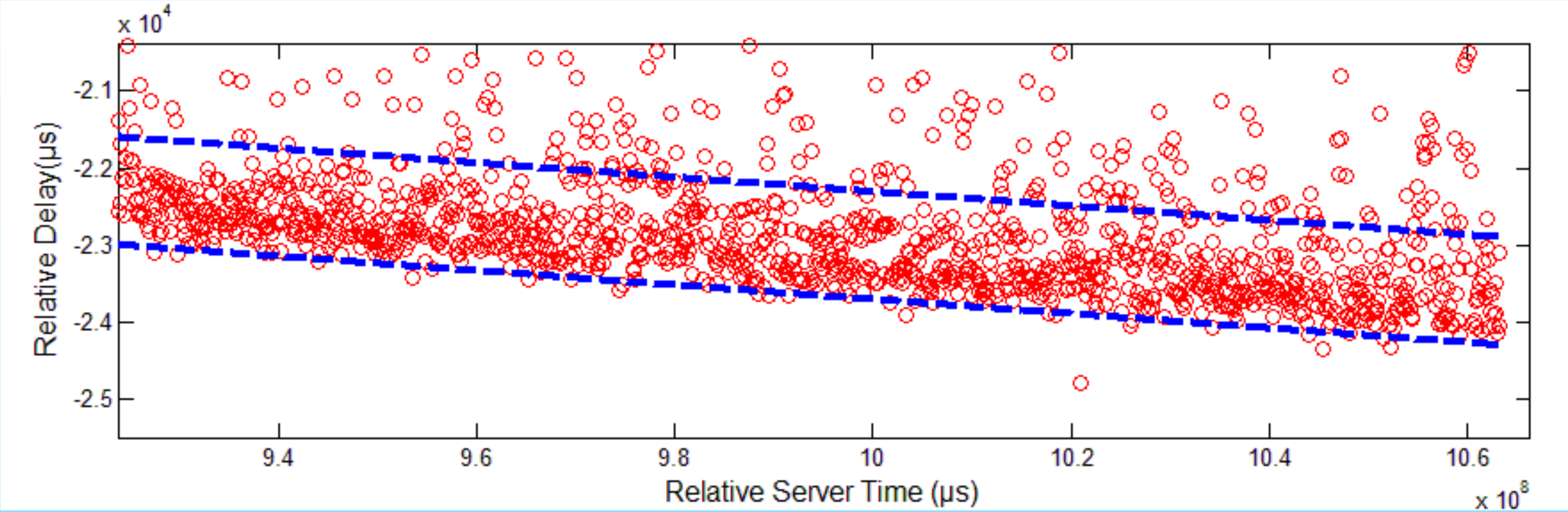


The raining phenomenon

- Always the same slope per receiver (e.g. ~ -1600 ppm)
- Multiple (2~4) lines at the same moment
- Possibly caused by the queuing scheme of network adapter drivers and OSes

Outliners below the crowd

- Only observed in wireless communication till now



Conclusions

- Continuous check for jump points and raining are necessary.
- Adaptive algorithm necessary to adjust the sending period of timestamps
- Hough line transform is effective to eliminate the error caused by "lower" outliers.
- Finally, if the sample is *clean*, we need no more than 2,000 offset values to reach ppm level precision.

תודה