Using Wireshark to collect some traffic and some analysis of this traffic

(Based on lecture notes for II2202: Quantitative examples, 2010.09.10)

G. Q. Maguire Jr.

2011.03.23

Experiment

Captured packets using Wireshark during a long (2150.12 second) VoIP call

$\Rightarrow$ at least: 107,505 RTP packets in each direction

$\Rightarrow$ 429 RTCP packets in one direction

From network to local user agent

Raw output fom Microsoft Excel 2010 (Beta)

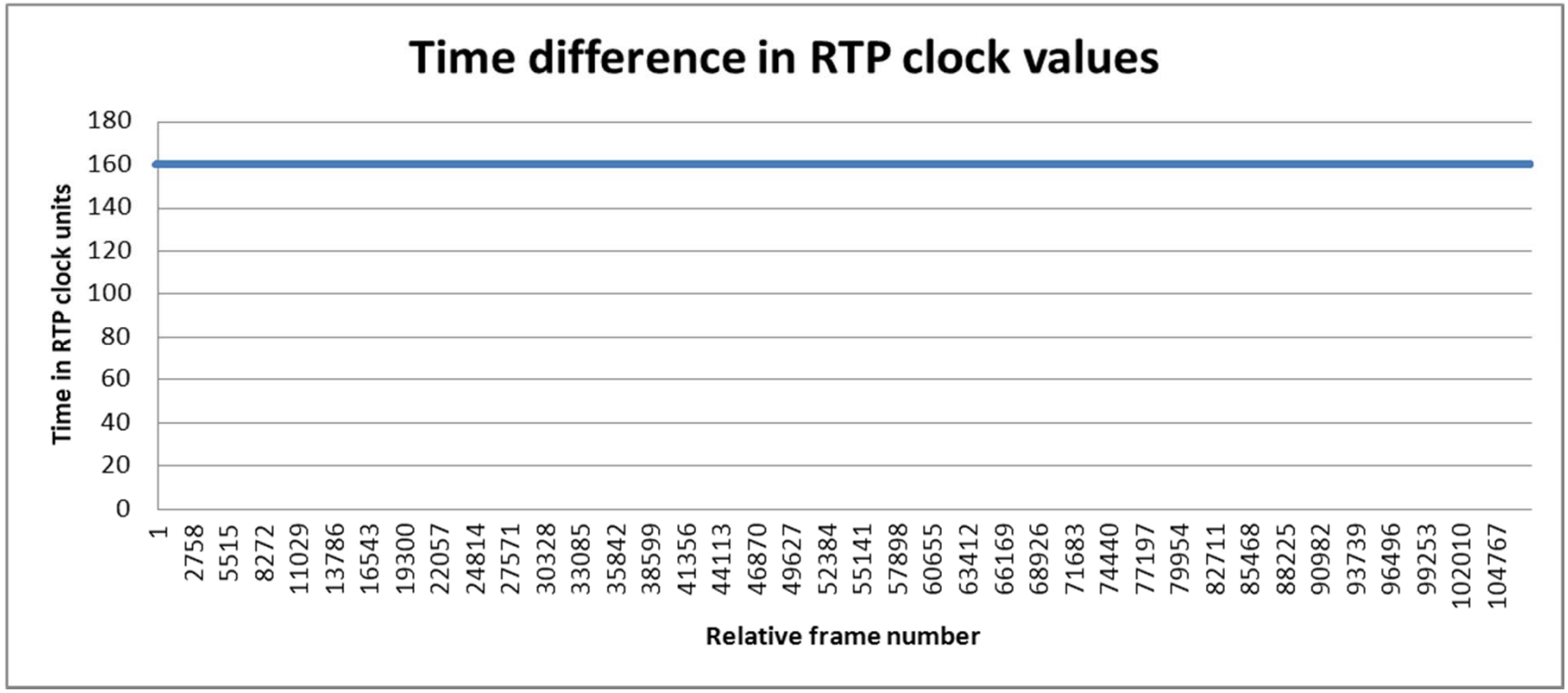
Difference in RTP clock from previous sample

Mean	160
Standard Error	0
Median	160
Mode	160
Standard Deviation	0
Sample Variance	0
Kurtosis	#DIV/0!
Skewness	#DIV/0!
Range	0
Minimum	160
Maximum	160
Sum	17200960
Count	107506
Confidence Level(95.0%)	0

Inter-arrival times in seconds of RTP packets

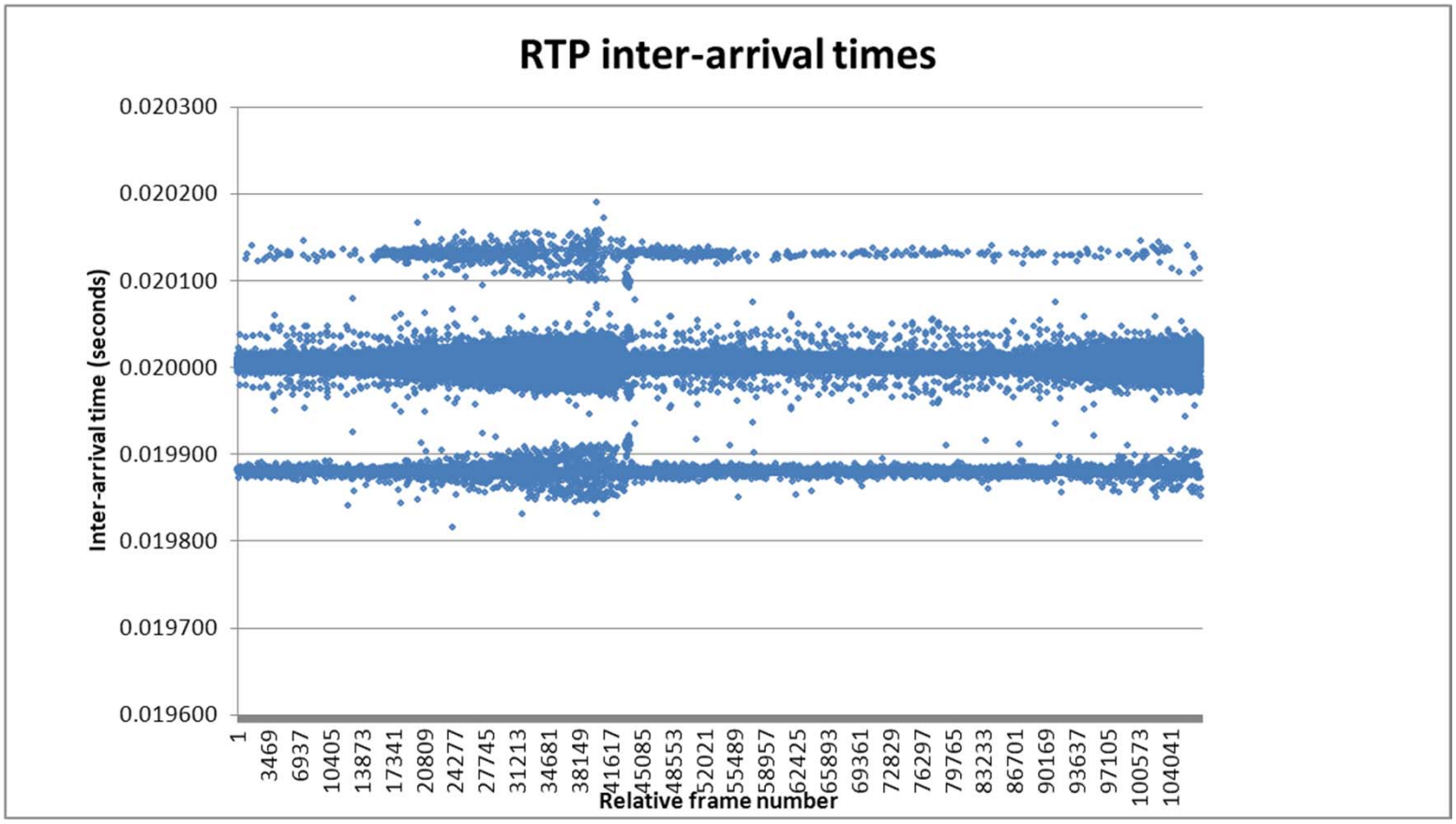
Mean	0.019999999
Standard Error	9.28526E-08
Median	0.020004
Mode	0.020005
Standard Deviation	3.04446E-05
Sample Variance	9.26874E-10
Kurtosis	12.36652501
Skewness	-2.054662184
Range	0.000374
Minimum	0.019815
Maximum	0.020189
Sum	2150.11991
Count	107506
Confidence Level(95.0%)	1.8199E-07

First look at the RTP clock differences

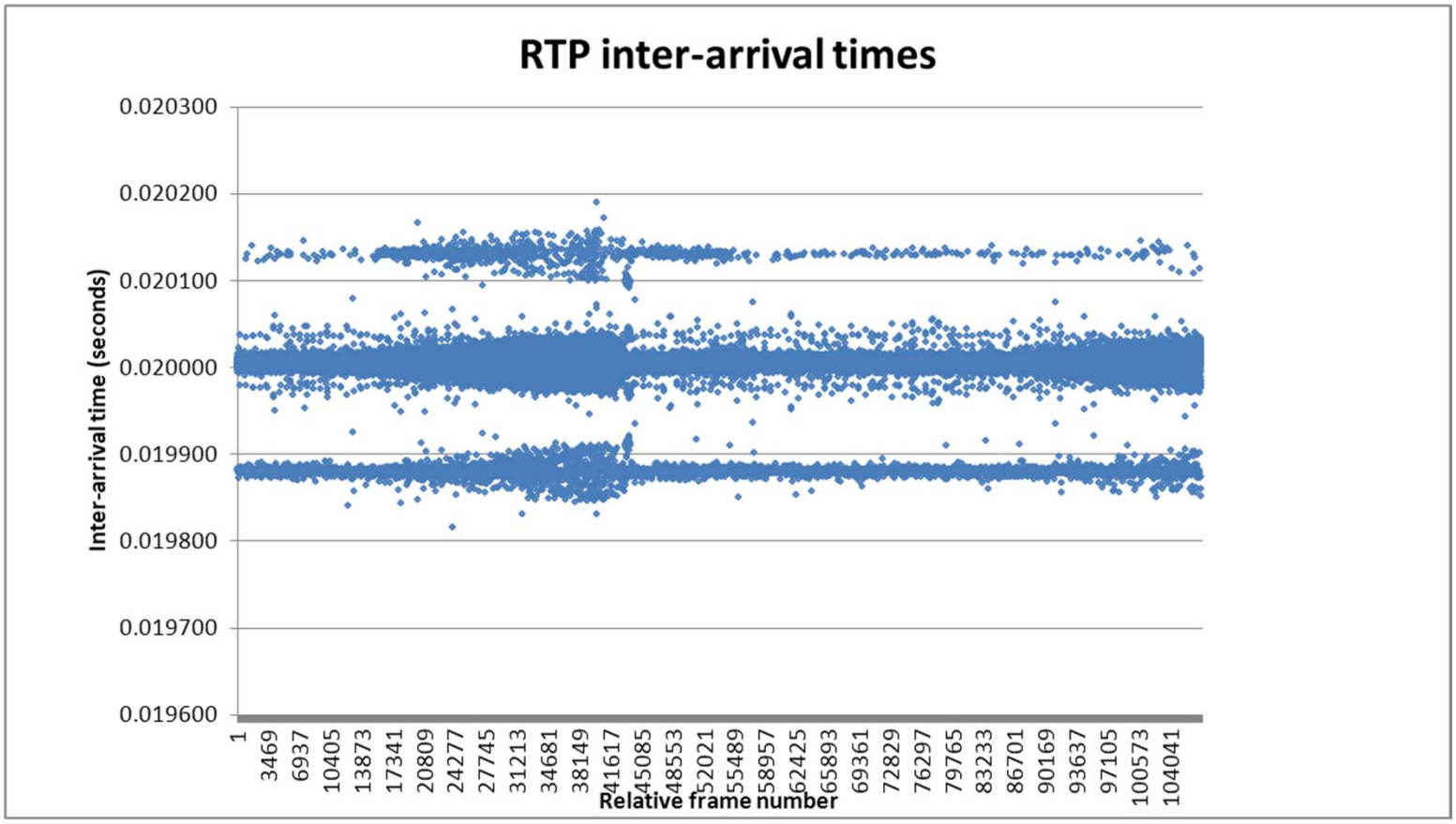


Conclusion: 160 audio samples per frame, with a frame time of 0.20 ms
$\Rightarrow$ 8 K sample/second sampling rate – consistent with ITU-T G.711 PCMA encoding

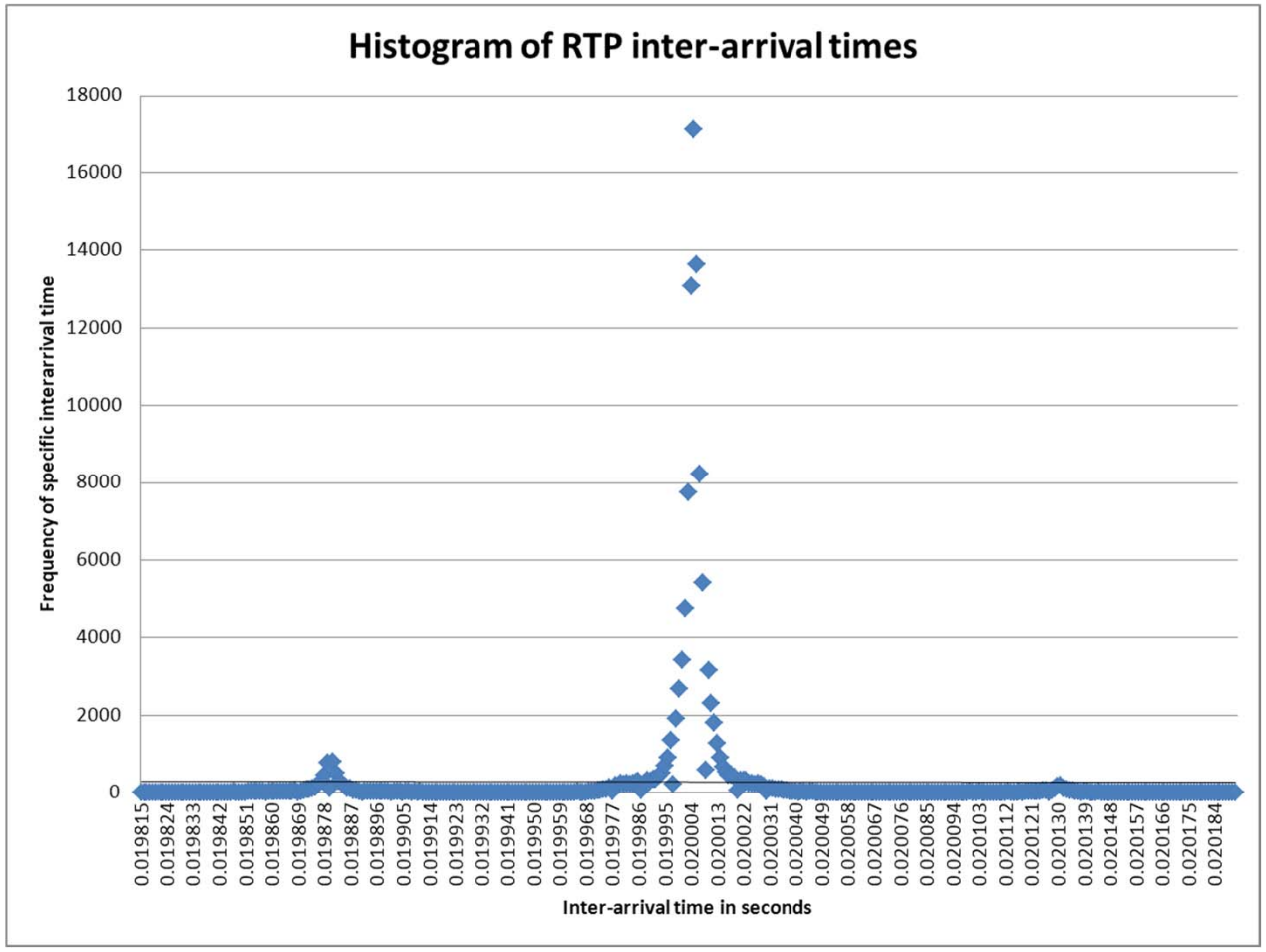
RTP inter-arrival times as measured by Wireshark



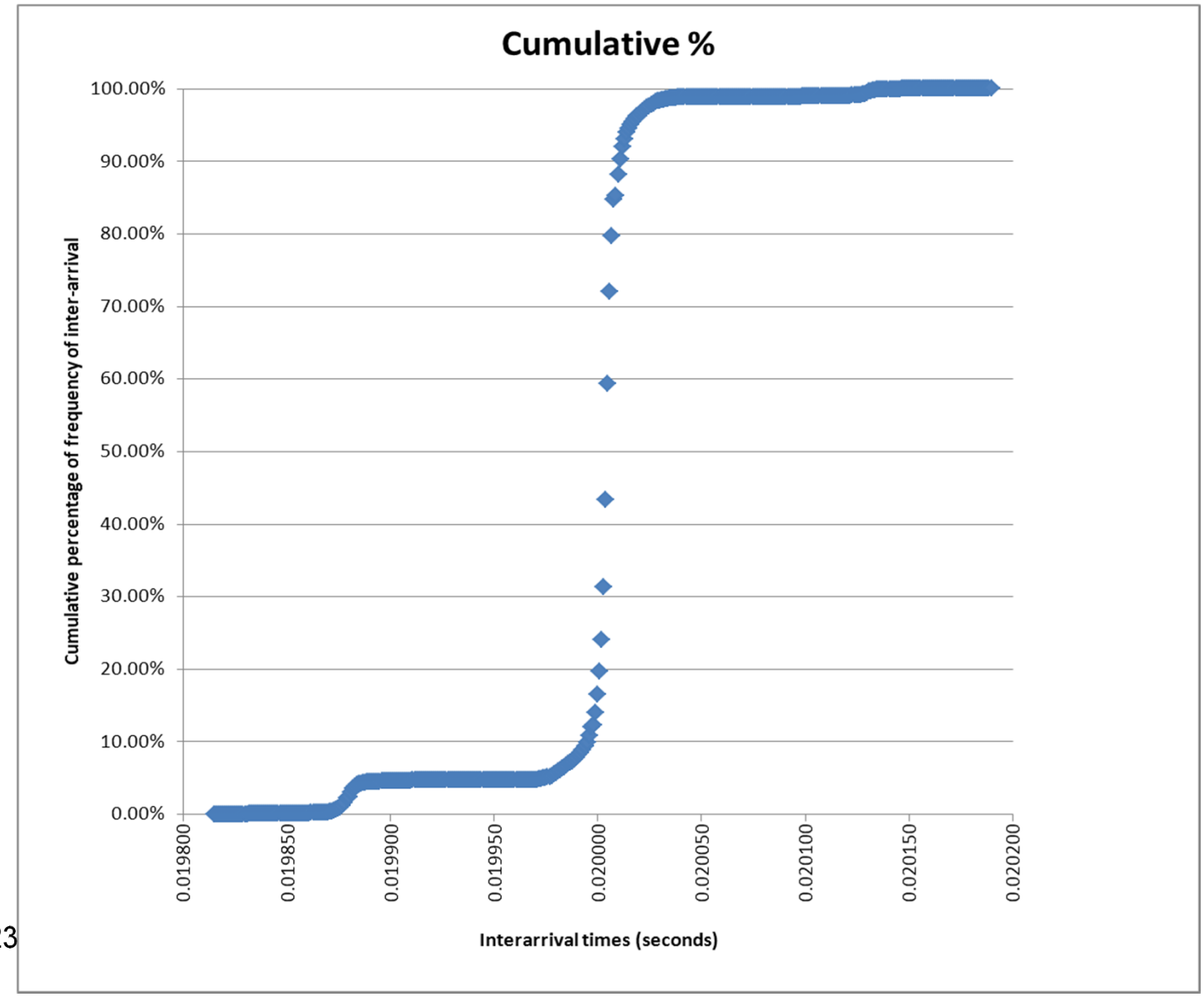
Re-scale vertical axis



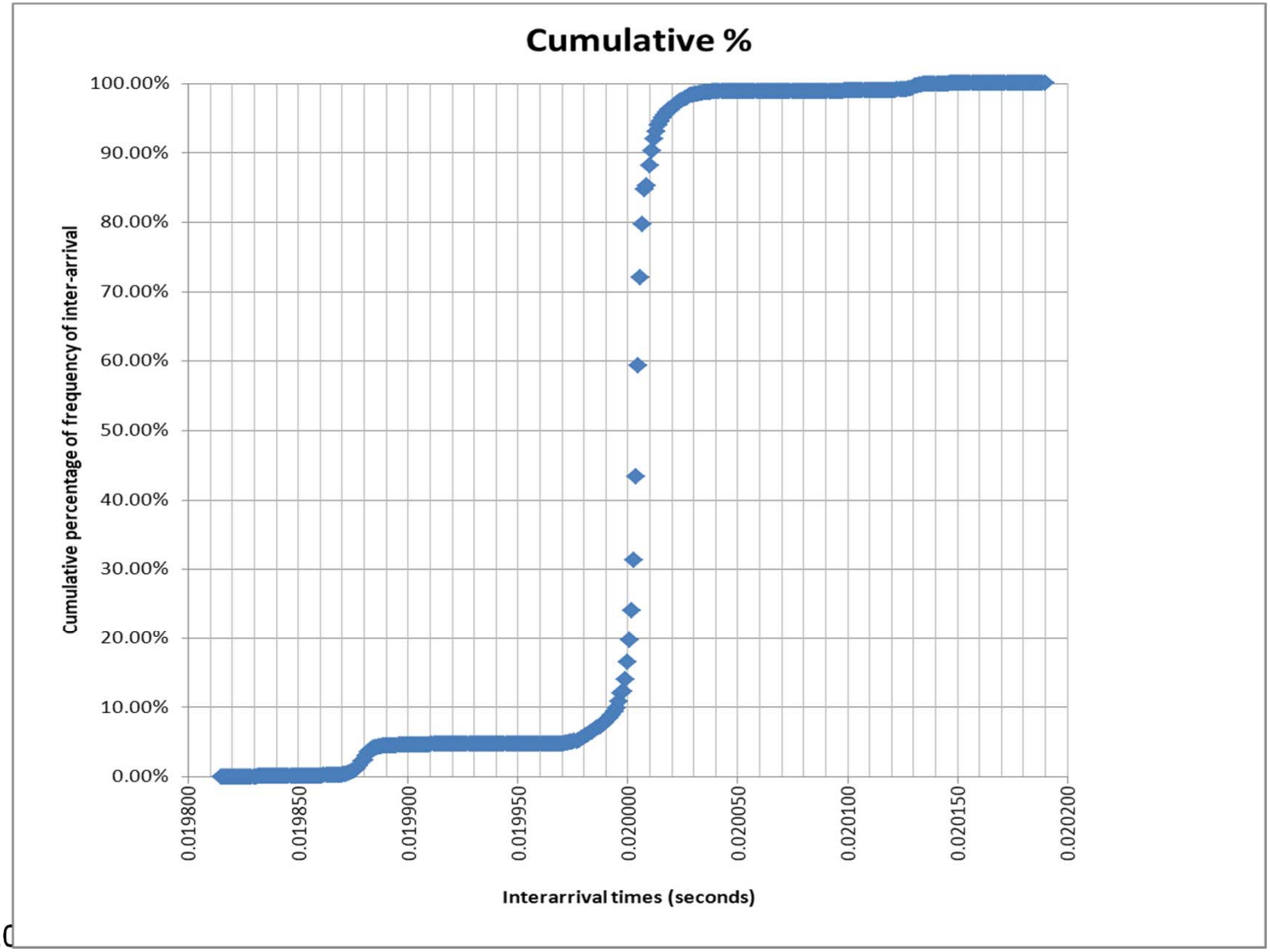
Compute histogram



Plot as a Cumulative Distibution



Add grid lines



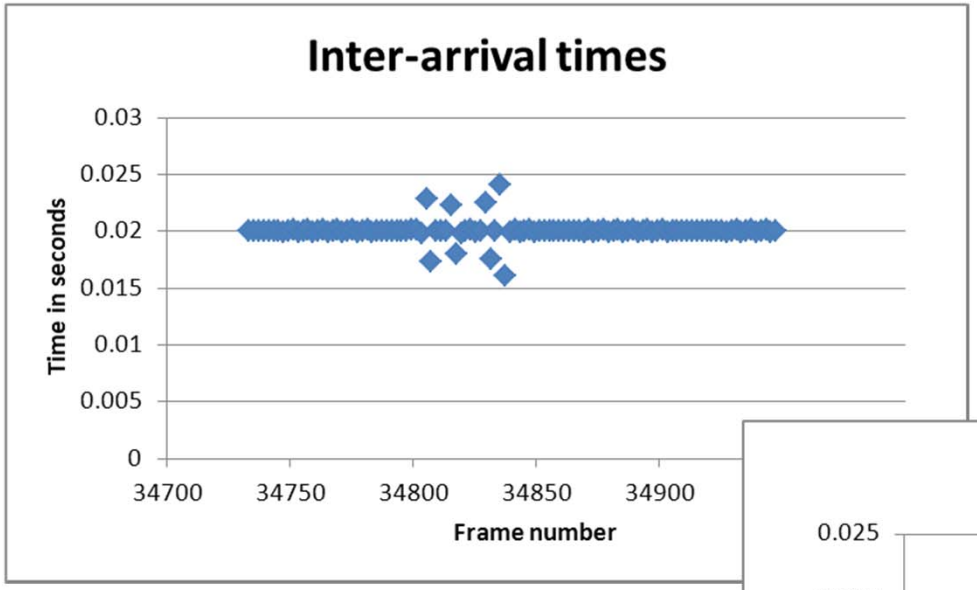
As numbers - near median

	seconds	frequency	Cumulative %
	0.019995	687	9.92%
	0.019996	895	10.75%
	0.019997	1334	11.99%
	0.019998	209	12.18%
	0.019999	1898	13.95%
Mean	0.020000	2671	16.44%
	0.020001	3403	19.60%
	0.020002	4747	24.02%
	0.020003	7742	31.22%
Median	0.020004	13059	43.37%
Mode	0.020005	17121	59.30%
	0.020006	13630	71.98%
	0.020007	8211	79.62%
	0.020008	5404	84.64%
	0.020009	570	85.18%
	0.020010	3158	88.11%
	0.020011	2305	90.26%
	0.020012	1787	91.92%
	0.020013	1262	93.09%
	0.020014	886	93.92%

With varying numbers of samples

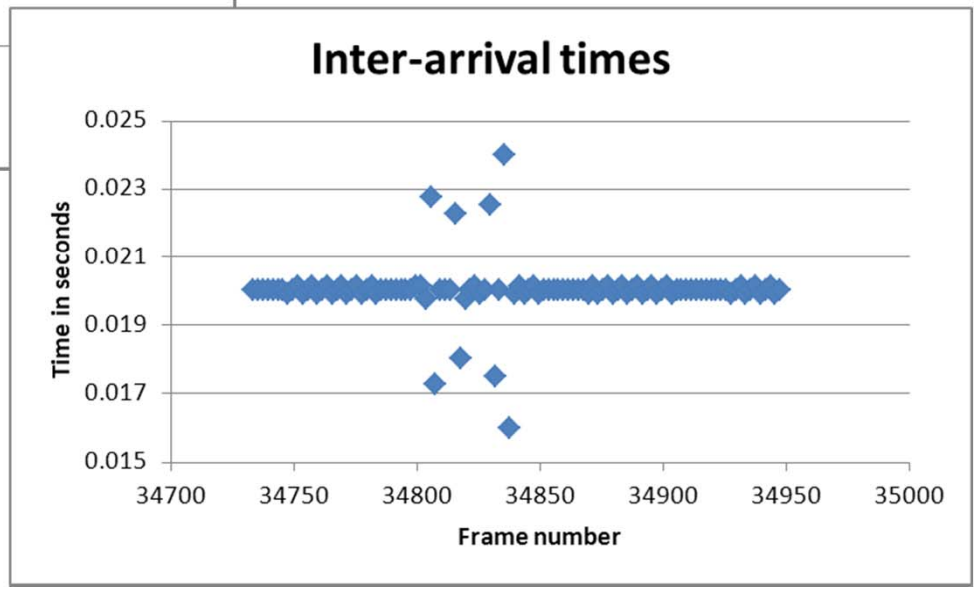
Descriptive Statistics	First 100	First 1K	First 10K	First 100K
Mean	0.02000071	0.020000066	0.020000004	0.02
Standard Error	2.12714E-06	7.53406E-07	2.51164E-07	9.69855E-08
Median	0.020005	0.020004	0.020004	0.020004
Mode	0.020005	0.020005	0.020005	0.020005
Standard Deviation	2.12714E-05	2.38248E-05	2.51164E-05	3.06695E-05
Sample Variance	4.52471E-10	5.67621E-10	6.30831E-10	9.40618E-10
Kurtosis	28.87137928	21.46428225	19.07376827	12.23083198
Skewness	-5.453831468	-4.509853108	-3.831289593	-2.003065575
Range	0.000135	0.000252	0.000277	0.000374
Minimum	0.01988	0.019872	0.019868	0.019815
Maximum	0.020015	0.020124	0.020145	0.020189
Sum	2.000071	20.000066	200.000044	1999.999951
Count	100	1000	10000	100000
Confidence Level(95.0%)	4.2207E-06	1.47844E-06	4.92331E-07	1.9009E-07

Zooming in on behavior

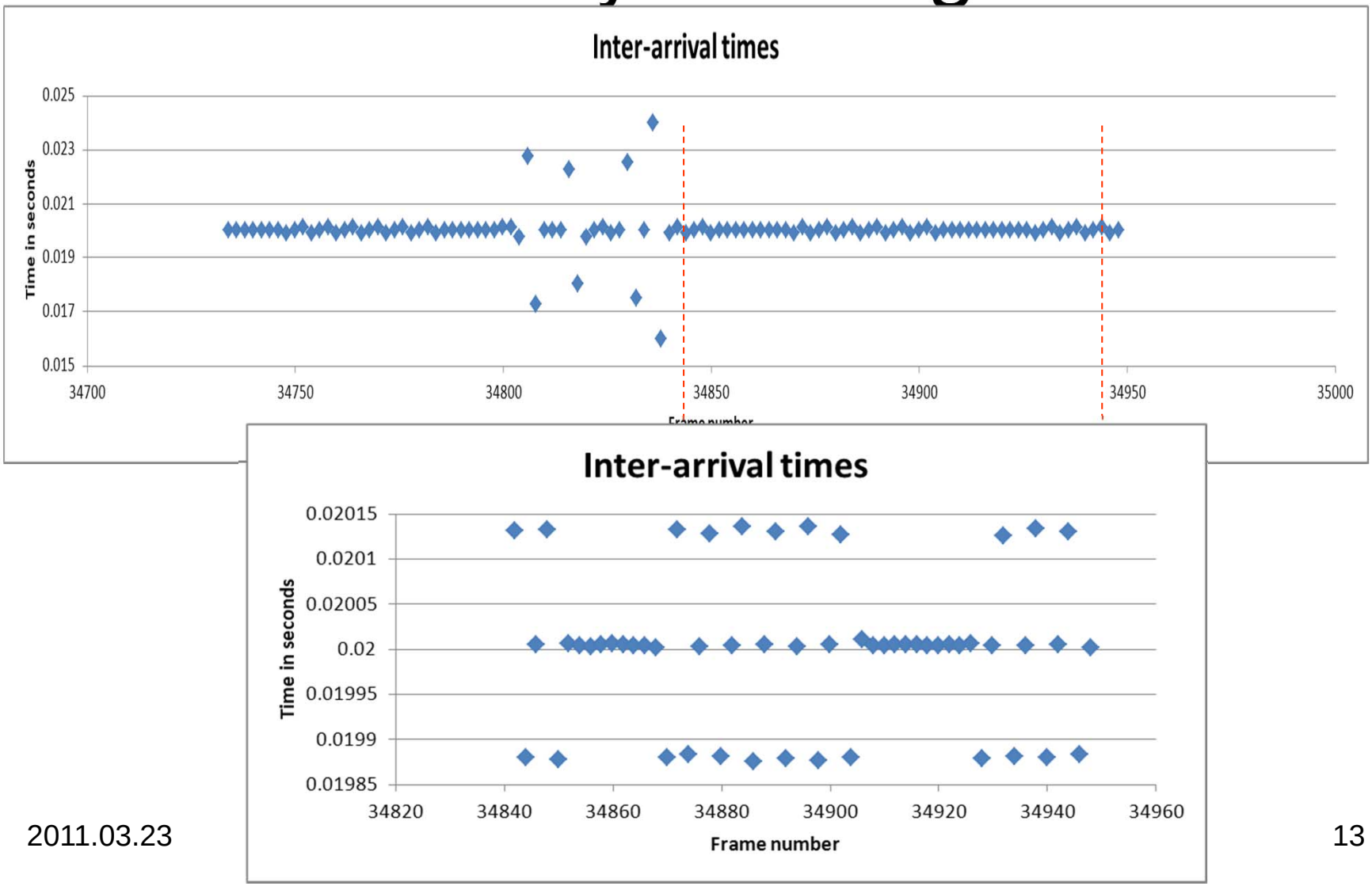


Note that the plot is now a **scatter plot**.

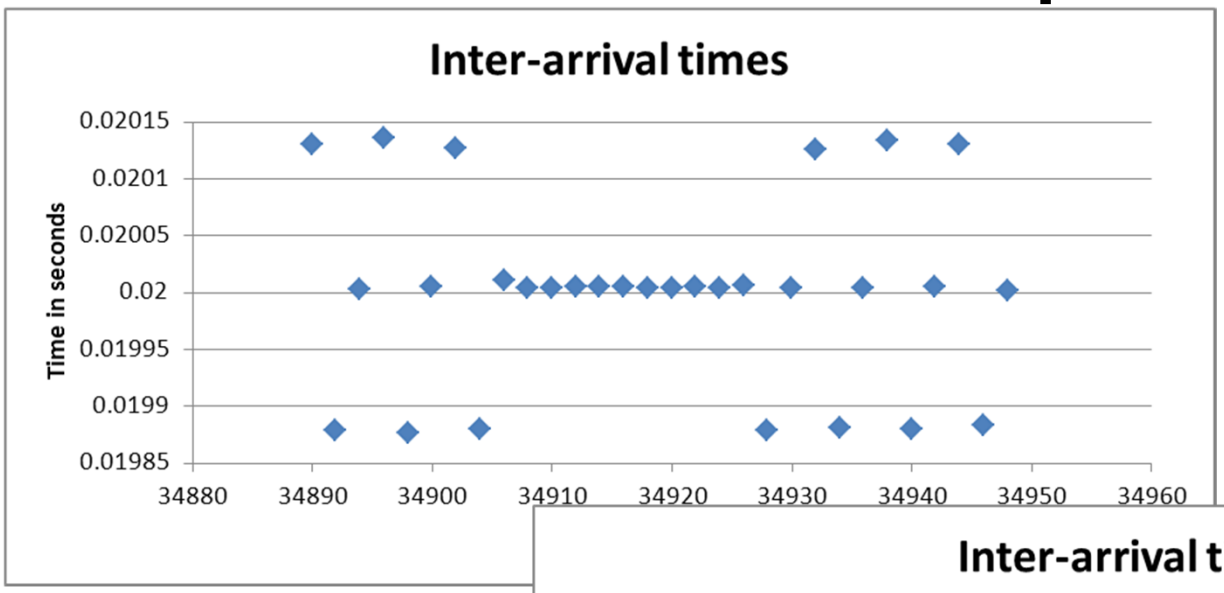
Re-scale

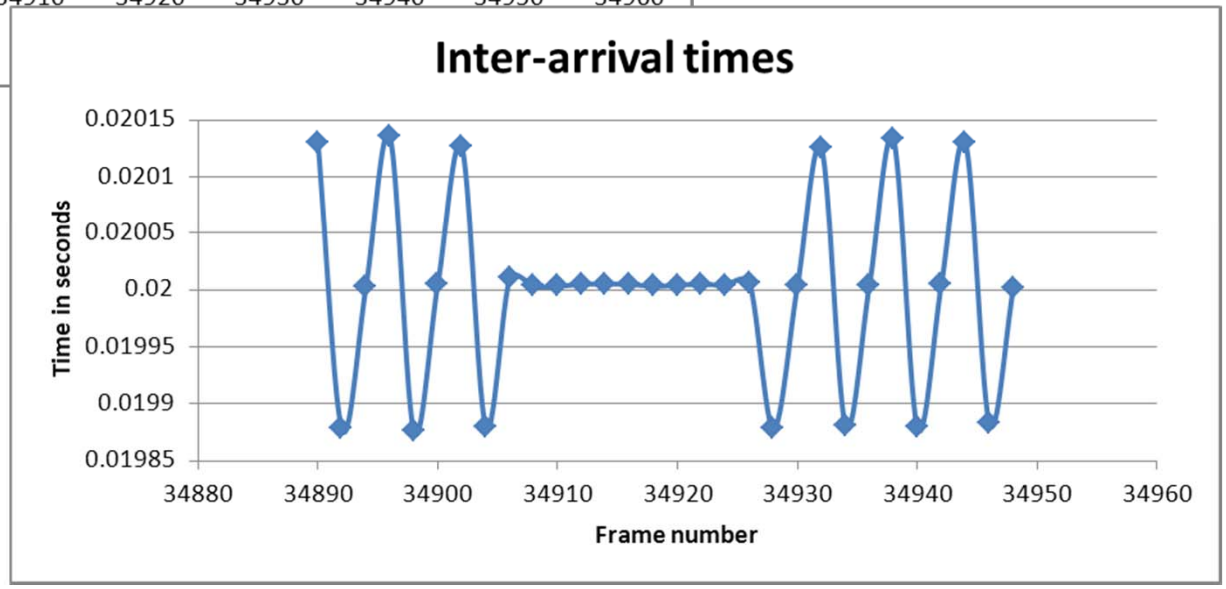


Looking in more detail at a relatively “flat” region



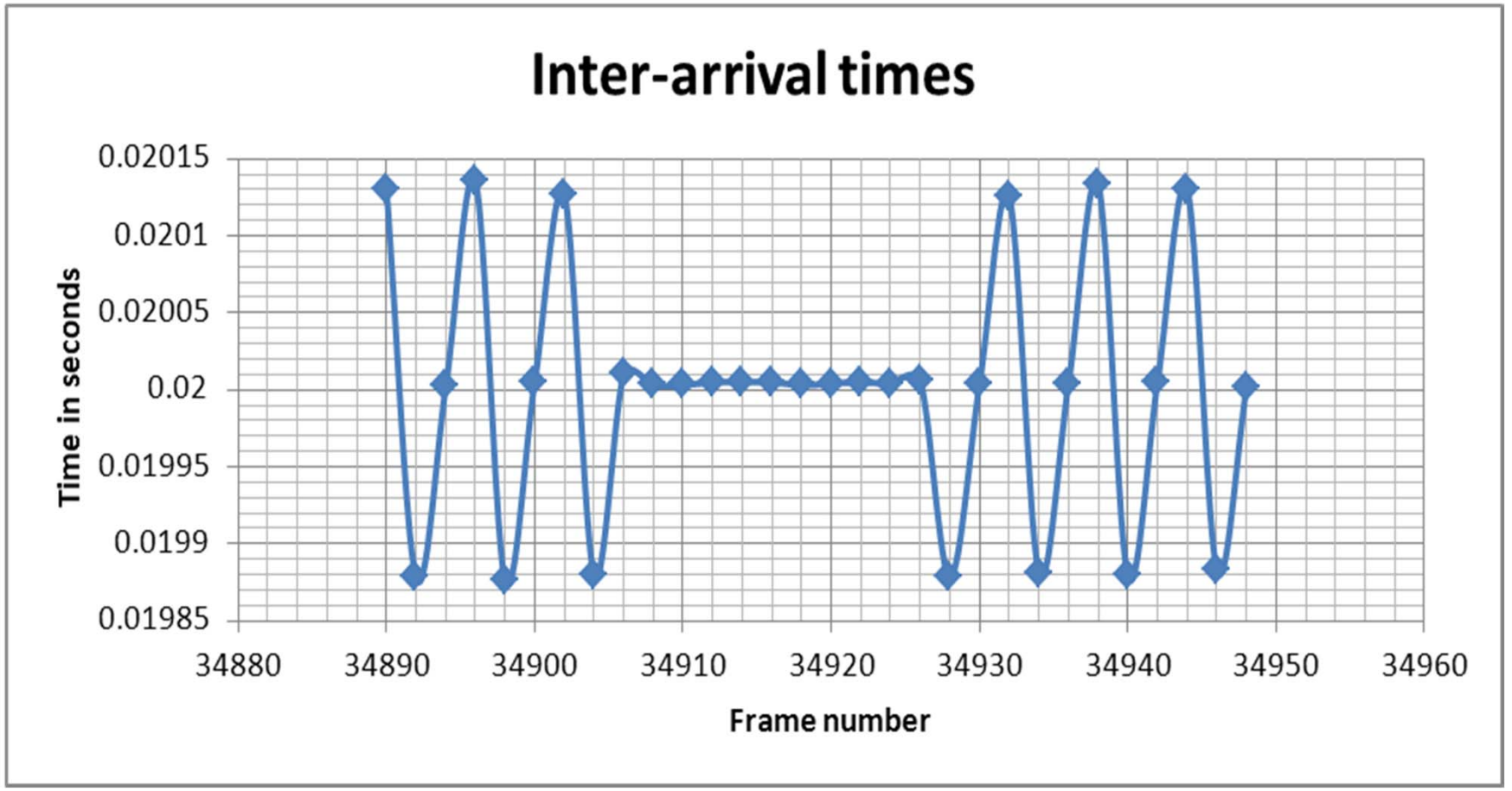
Is there some pattern?



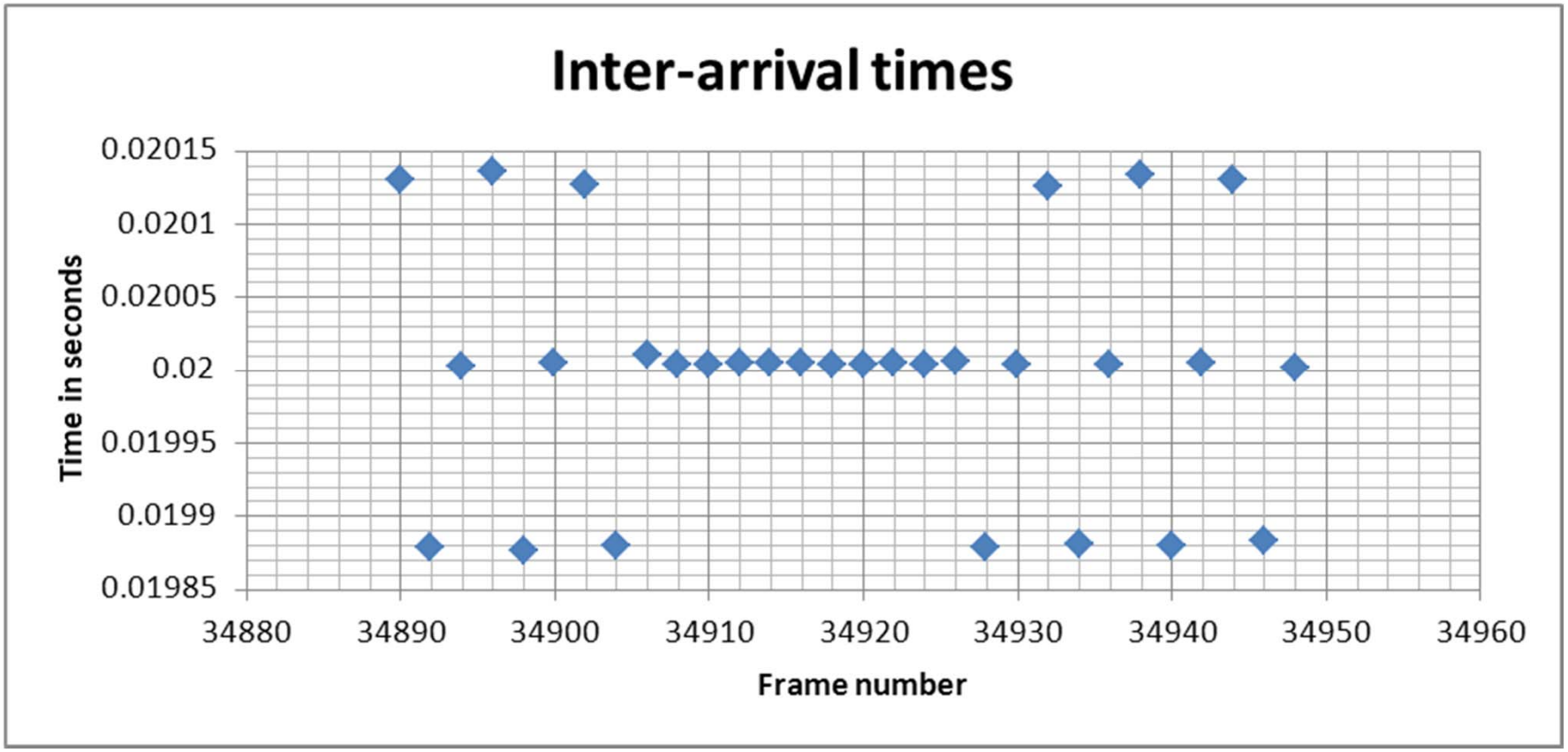


Not continuous data, but connecting with lines shows the values oscillate

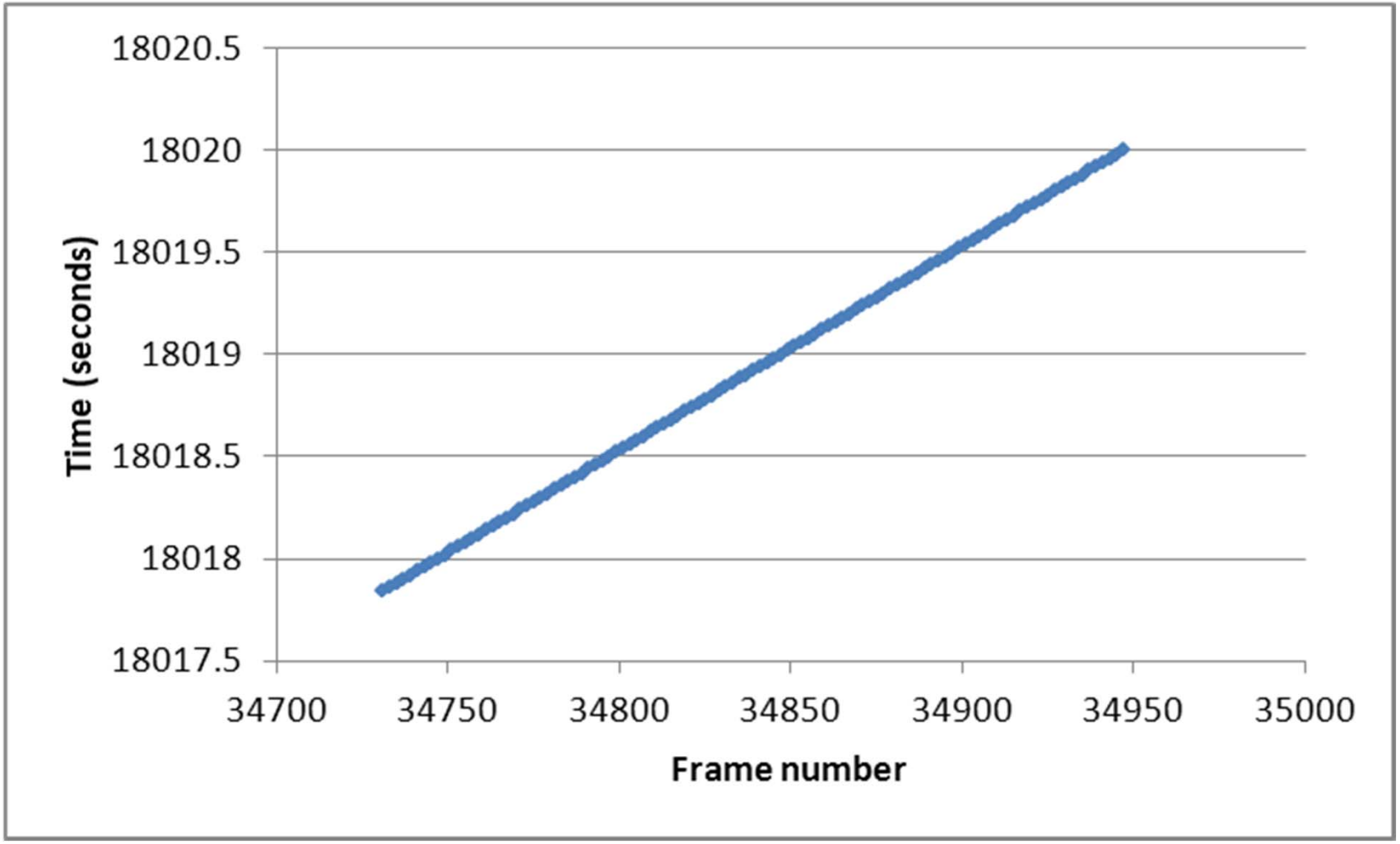
Adding grid lines



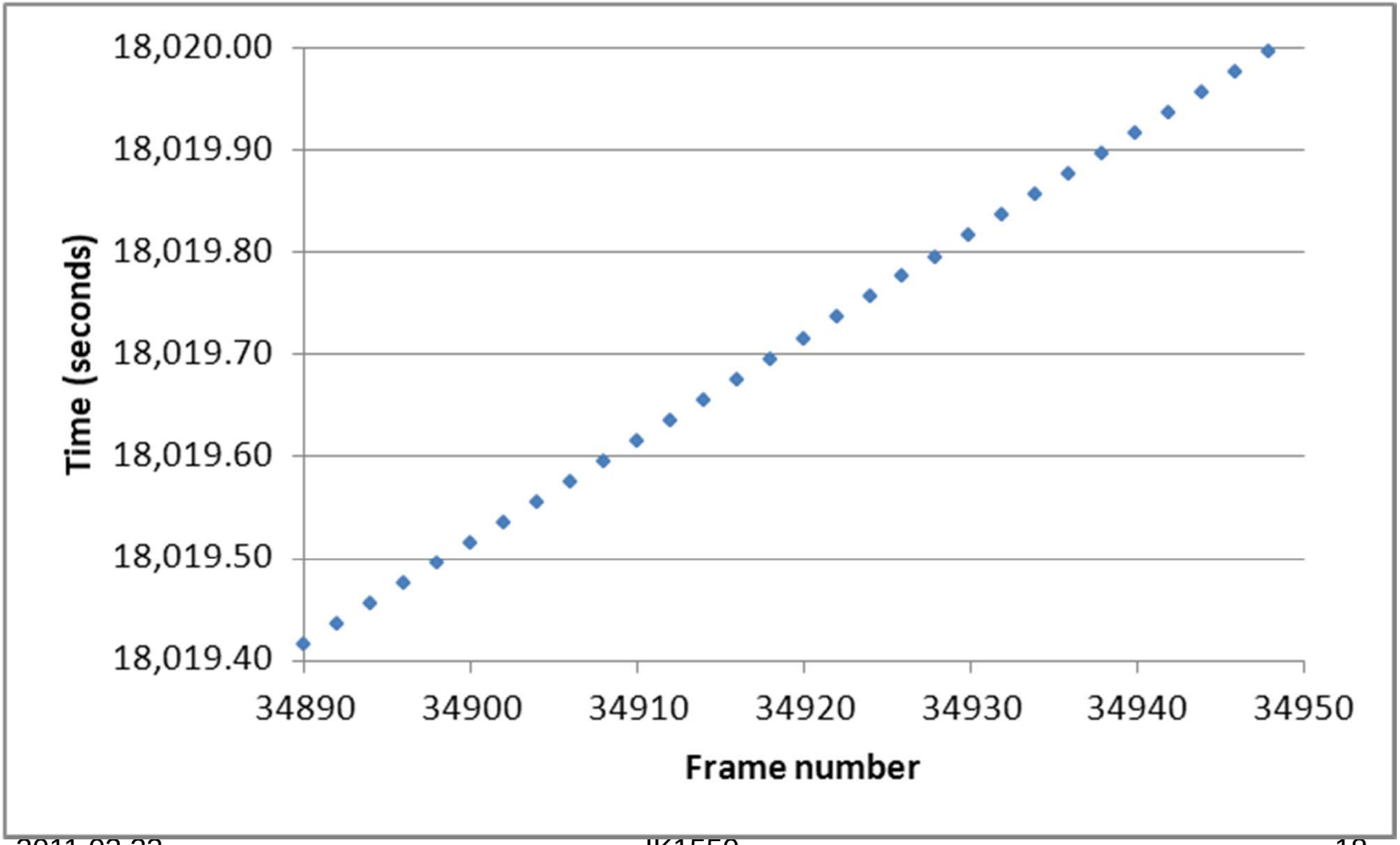
Are grid lines alone sufficient?



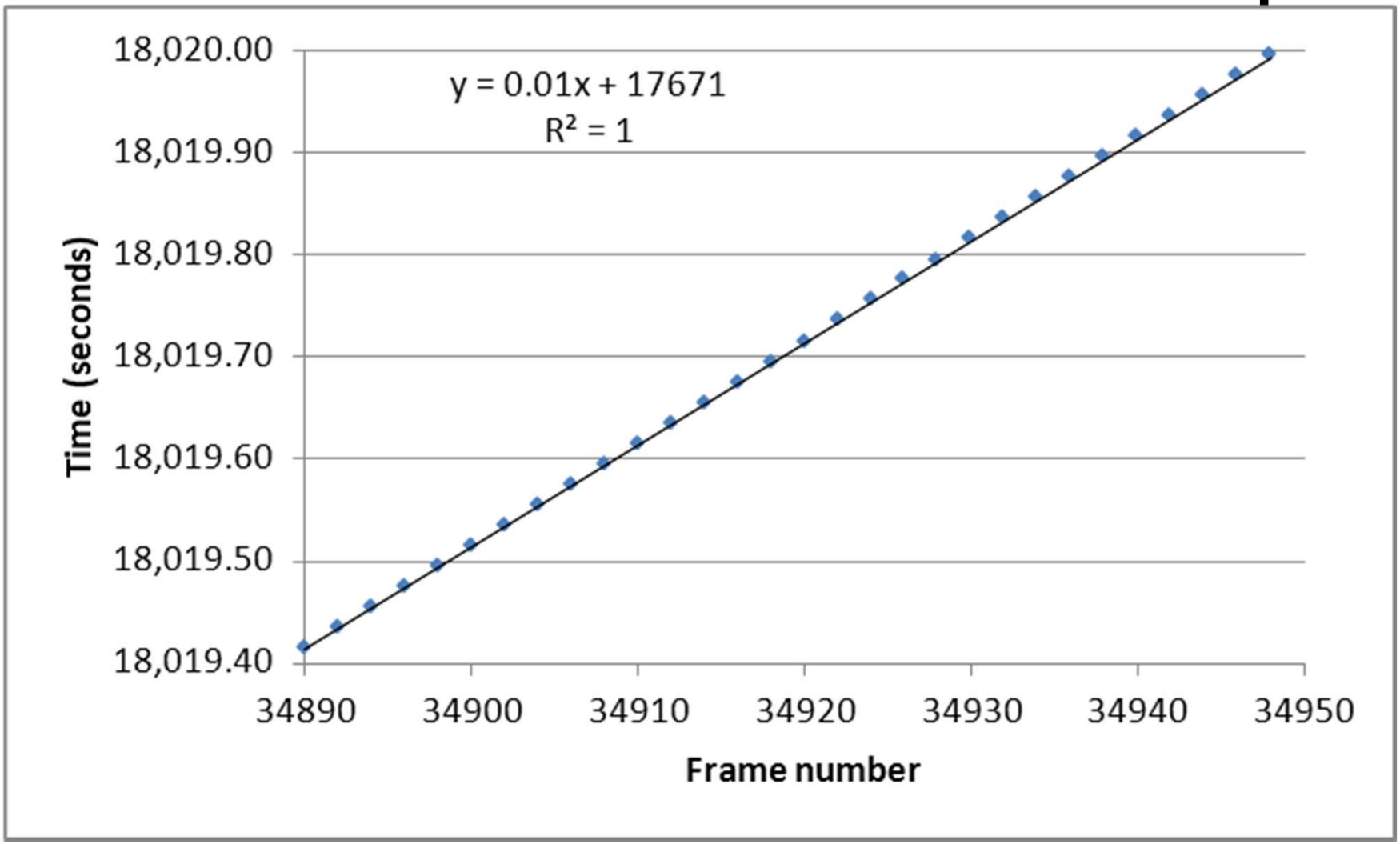
Scatter plots of frame # versus time



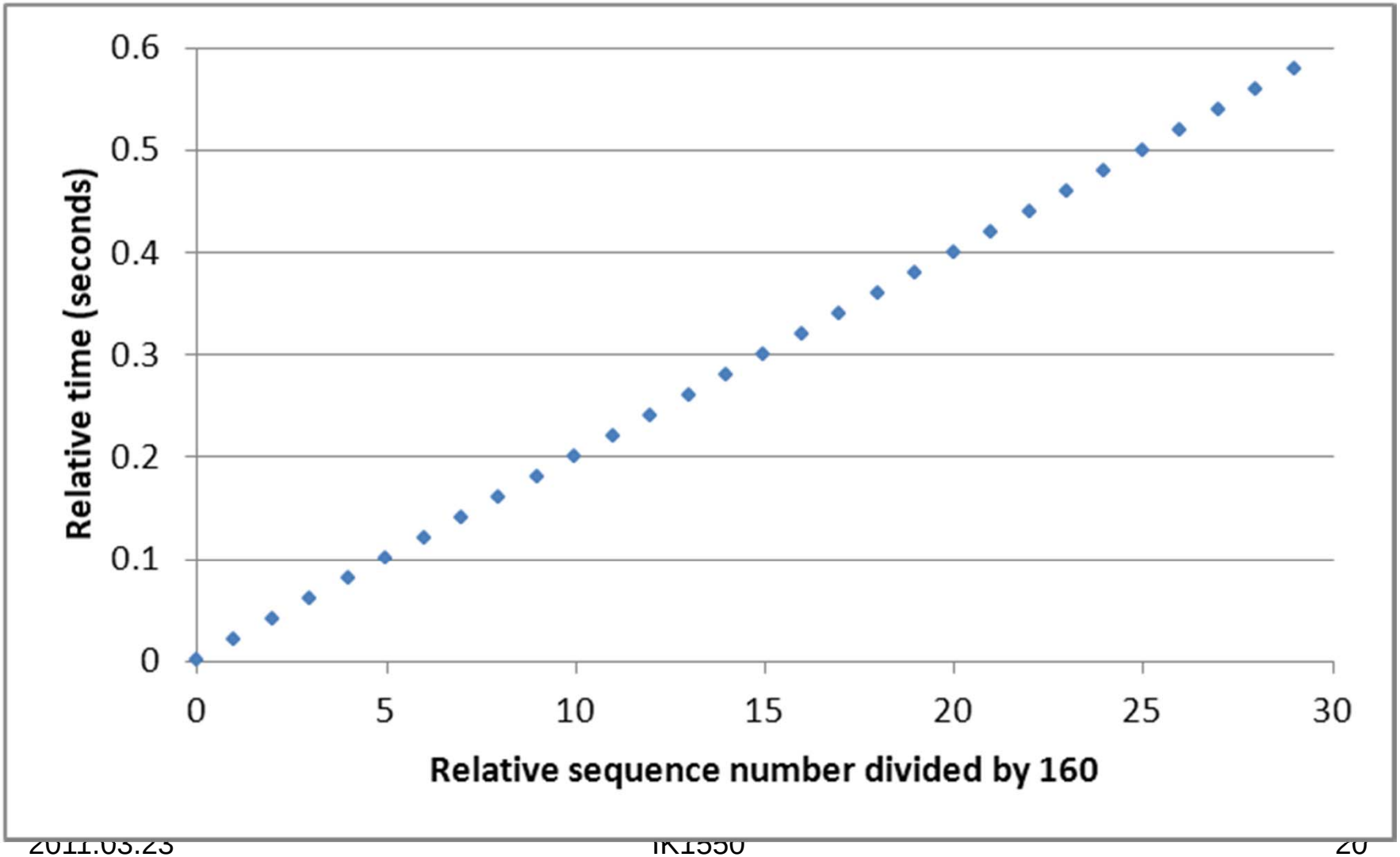
Zoom in on last few samples



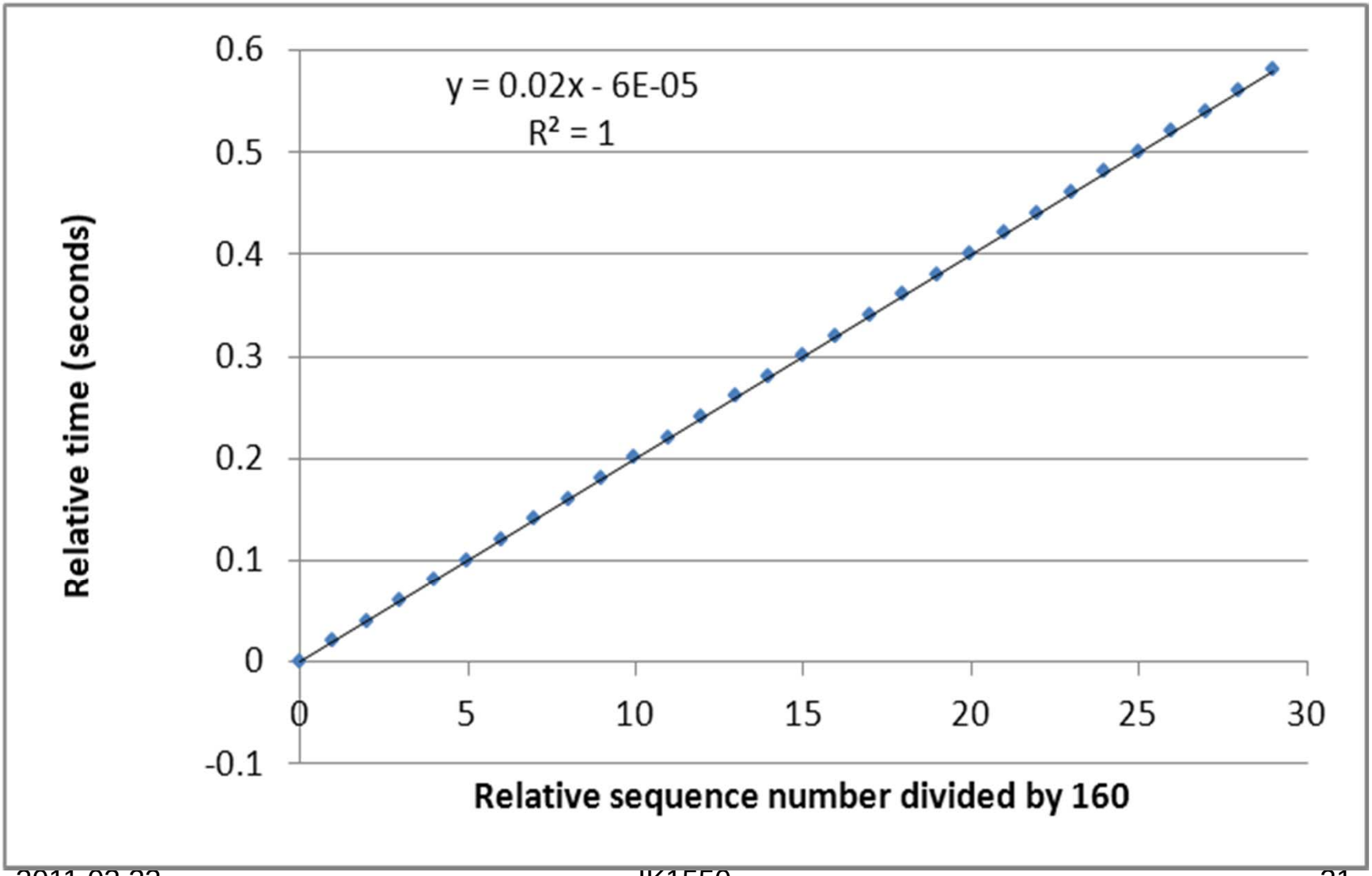
Add a trendline and show eqn.

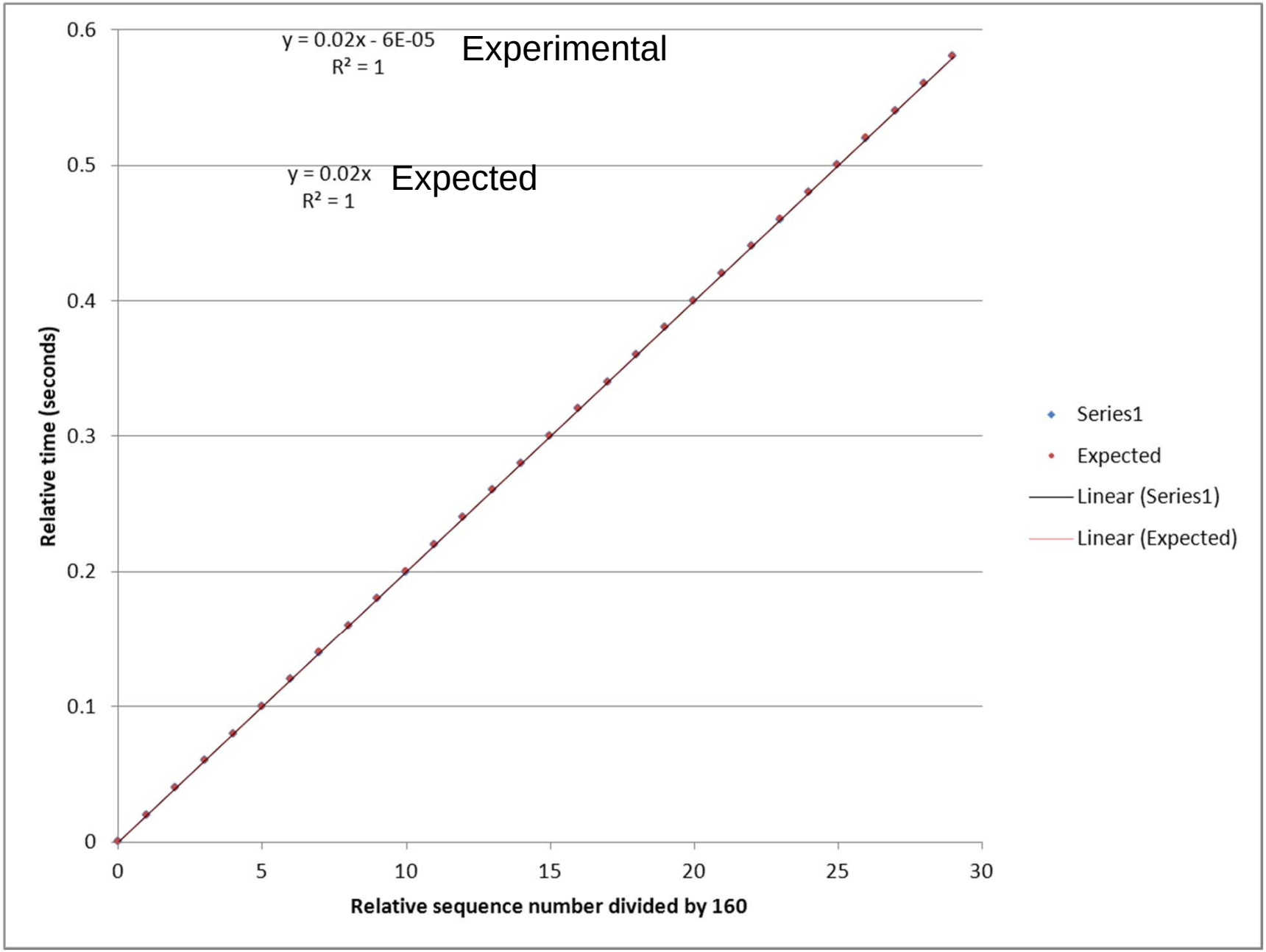


Computing new axis

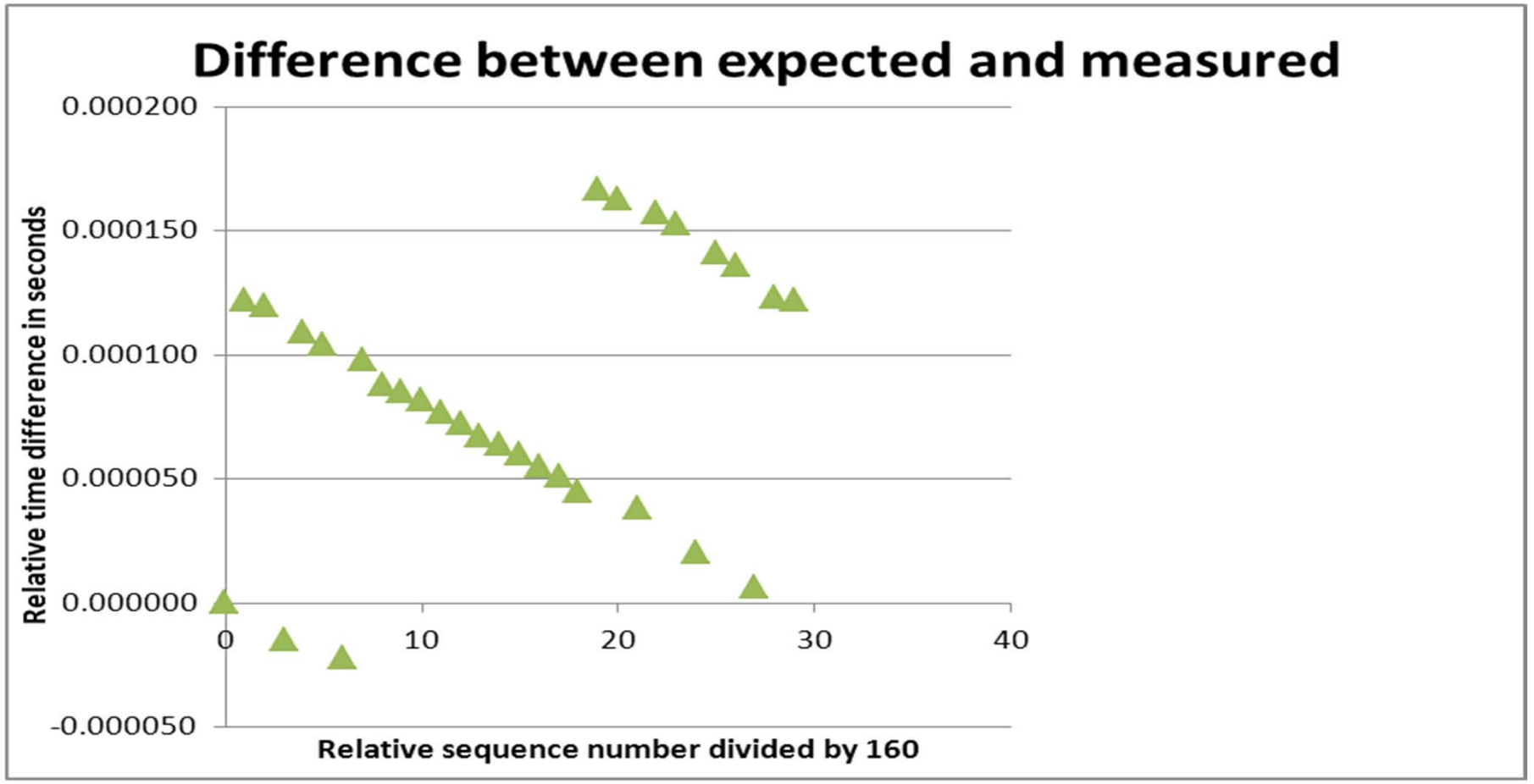


Now add the trendline

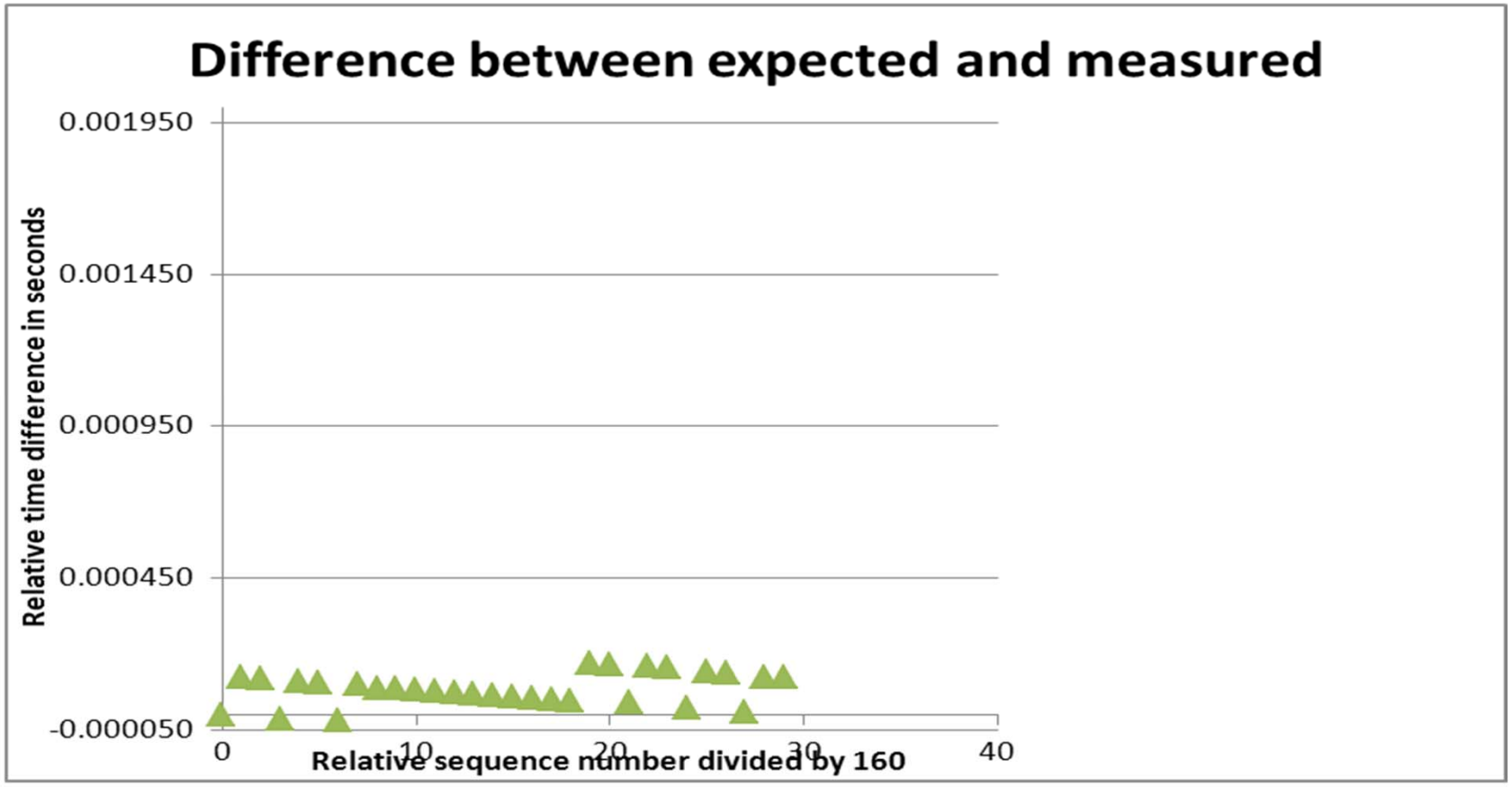



y = 0.02x - 6E-05
R² = 1
Experimental
y = 0.02x
R² = 1
Expected
0.6
0.5
0.4
0.3
0.2
0.1
0
Relative time (seconds)
0
5
10
15
20
25
30
Relative sequence number divided by 160
Series1
Expected
Linear (Series1)
Linear (Expected)

How does the measured data differ from the expected data?



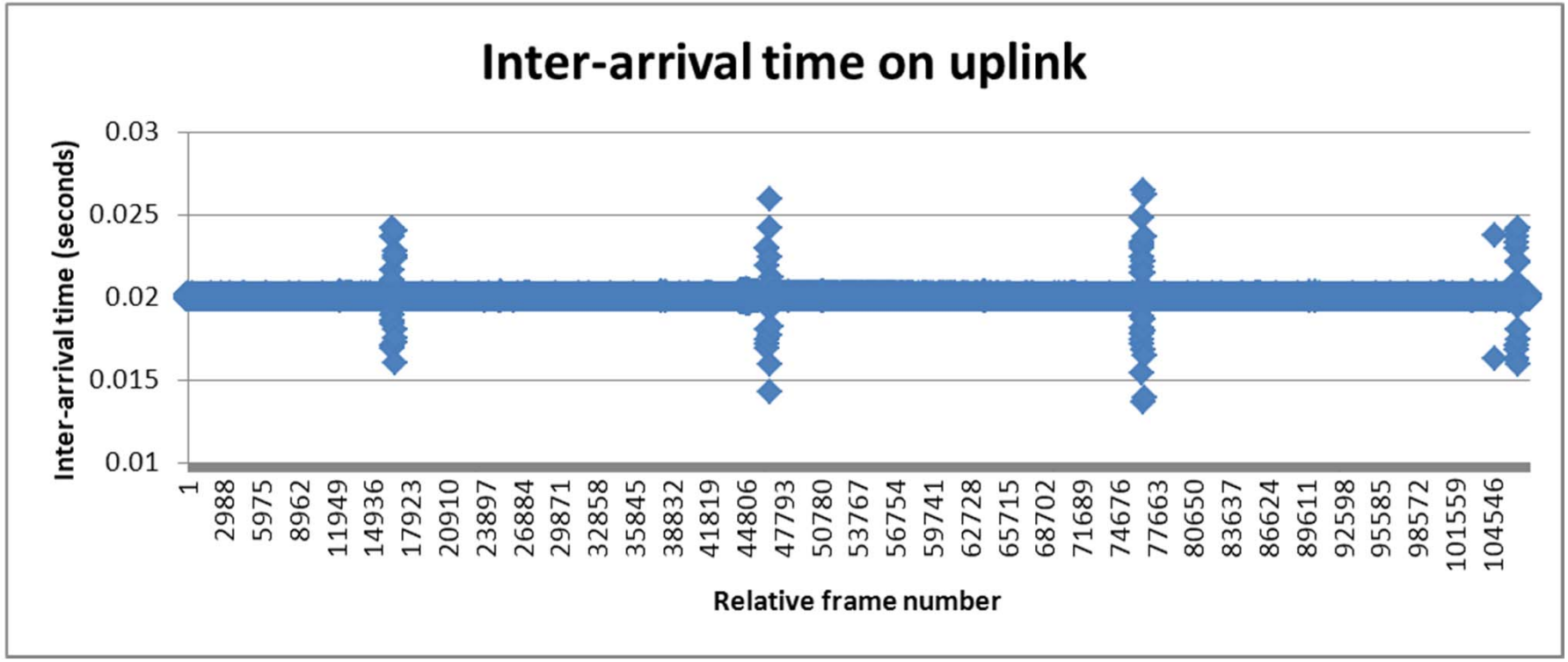
Does the difference matter? Plot scaled to 1/10 of the inter-arrival time period



For traffic in the opposite direction

Mean	0.020000275
Standard Error	3.6743E-07
Median	0.020004
Mode	0.020005
Standard Deviation	0.000120472
Sample Variance	1.45135E-08
Kurtosis	670.0855429
Skewness	0.482218958
Range	0.012759
Minimum	0.013625
Maximum	0.026384
Sum	2150.109545
Count	107504
Confidence Level(95.0%)	7.20157E-07

Uplink inter-arrival times



What is going on?

Note the spikes near:		time in seconds	difference in time in seconds
16453		329.06	
46682		933.64	604.58
76657		1533.14	599.5
106512		2130.24	597.1

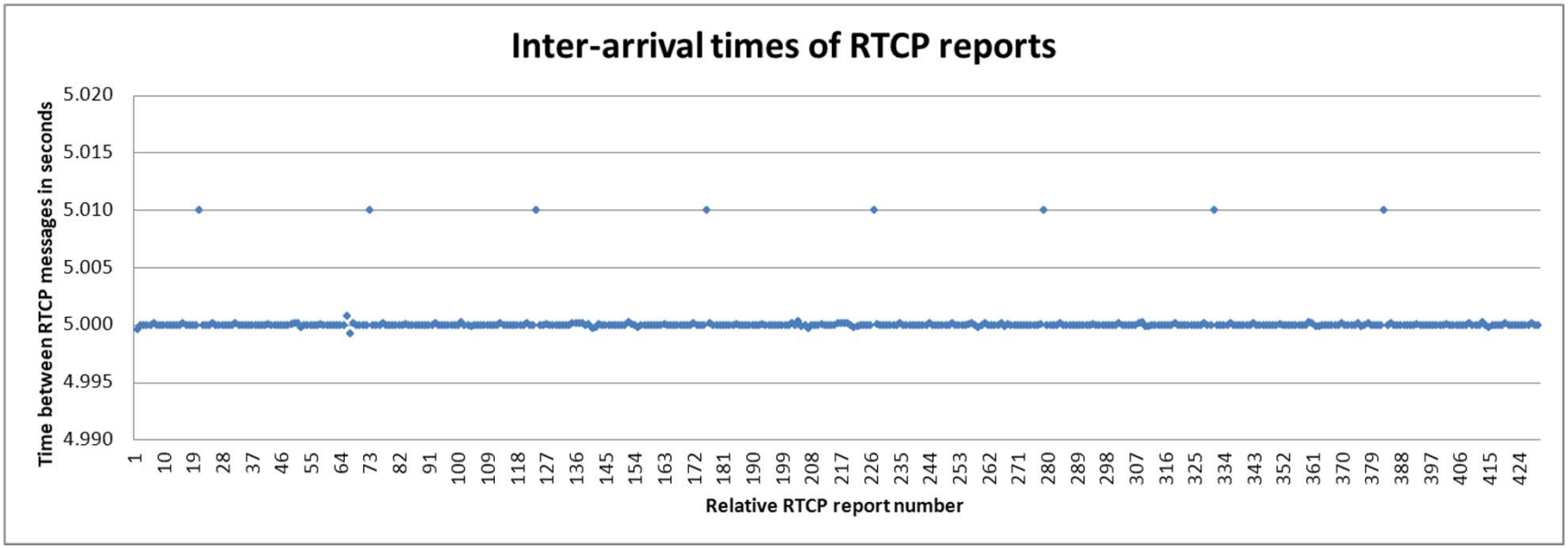
Q: What happens roughly every 600 seconds?

A: DHCP requests

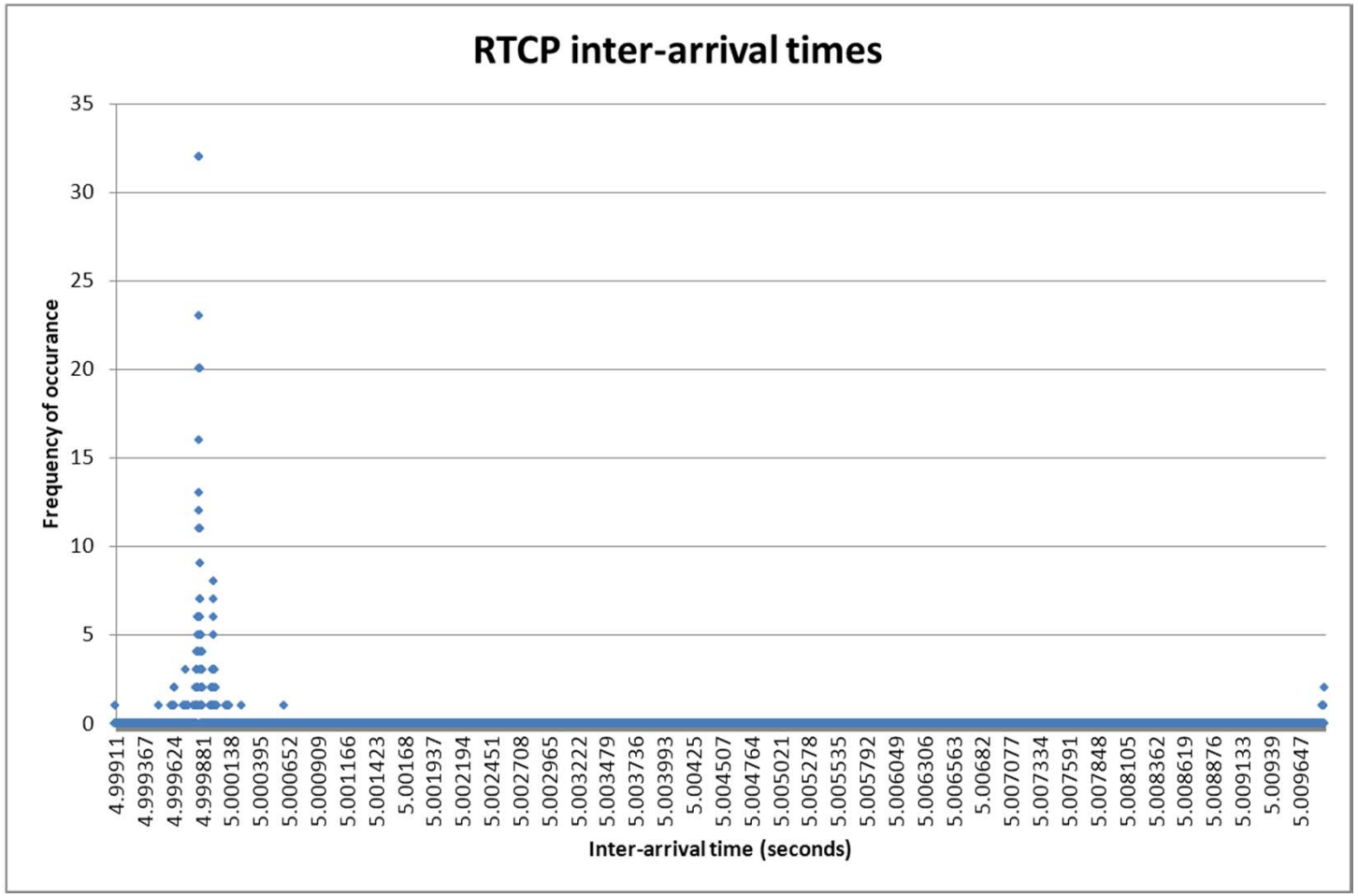
RTCP descriptive statistics

Mean	5.00006104
Standard Error	6.54393E-05
Median	4.999861
Mode	4.99986
Standard Deviation	0.001355399
Sample Variance	1.83711E-06
Kurtosis	48.80806181
Skewness	7.096344028
Range	0.010758
Minimum	4.99911
Maximum	5.009868
Sum	2145.026186
Count	429
Confidence Level(95.0%)	0.000128622

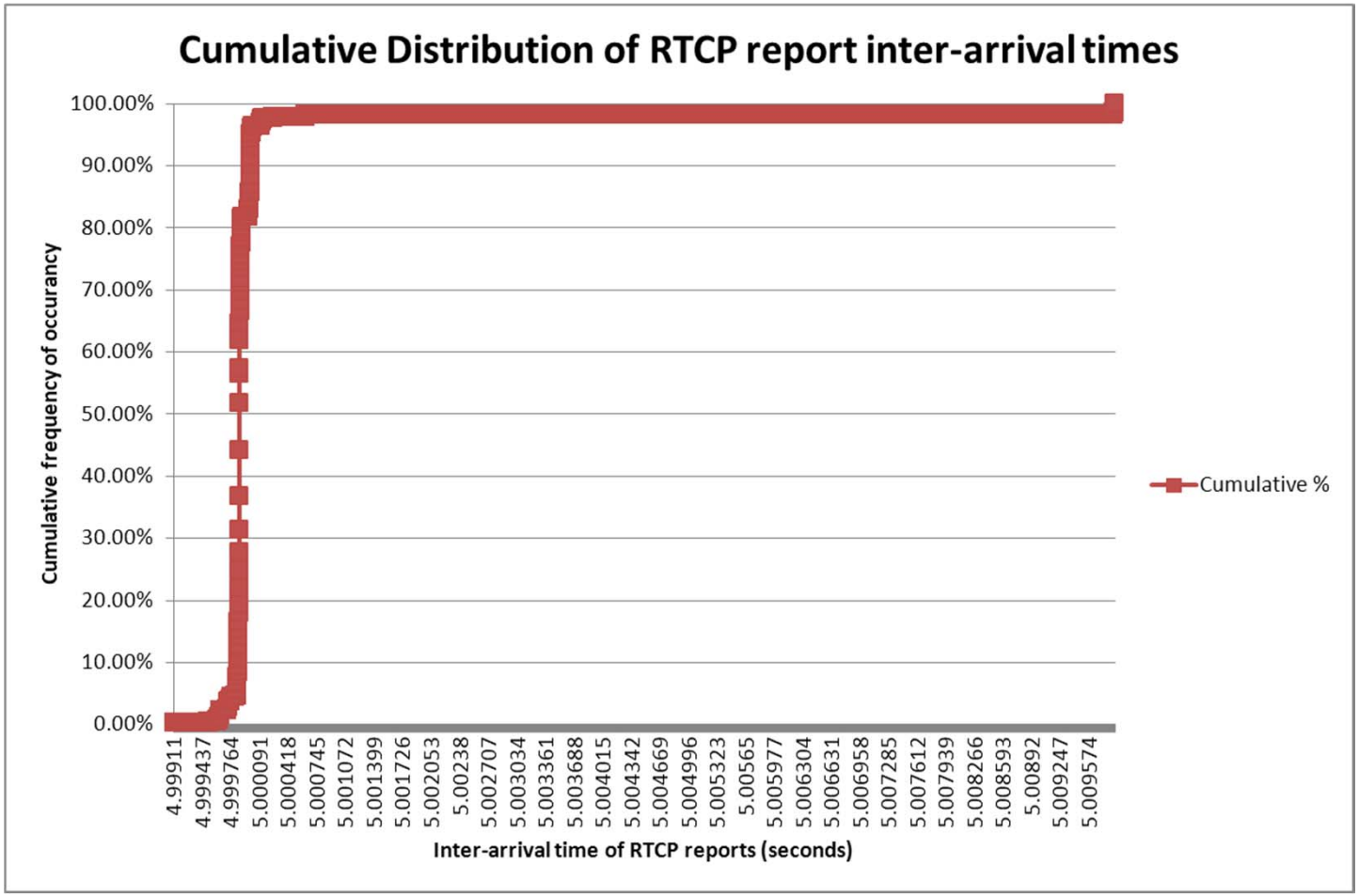
Plot of inter-arrival times of RTCP reports



Histogram of RTCP inter-arrivals



RTCP CDF


Cumulative Distribution of RTCP report inter-arrival times
Cumulative frequency of occurancy
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
4.99911
4.999437
4.999764
5.000091
5.000418
5.000745
5.001072
5.001399
5.001726
5.002053
5.00238
5.002707
5.003034
5.003361
5.003688
5.004015
5.004342
5.004669
5.004996
5.005323
5.00565
5.005977
5.006304
5.006631
5.006958
5.007285
5.007612
5.007939
5.008266
5.008593
5.00892
5.009247
5.009574
Inter-arrival time of RTCP reports (seconds)
Cumulative %