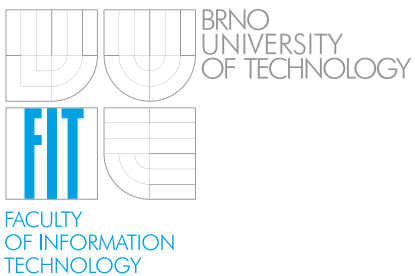
Design and Performance Analysis of Parallel Processing of SRTP Packets

Jan Wozniak

Vysoké učení technické v Brně

Fakulta informační technologií



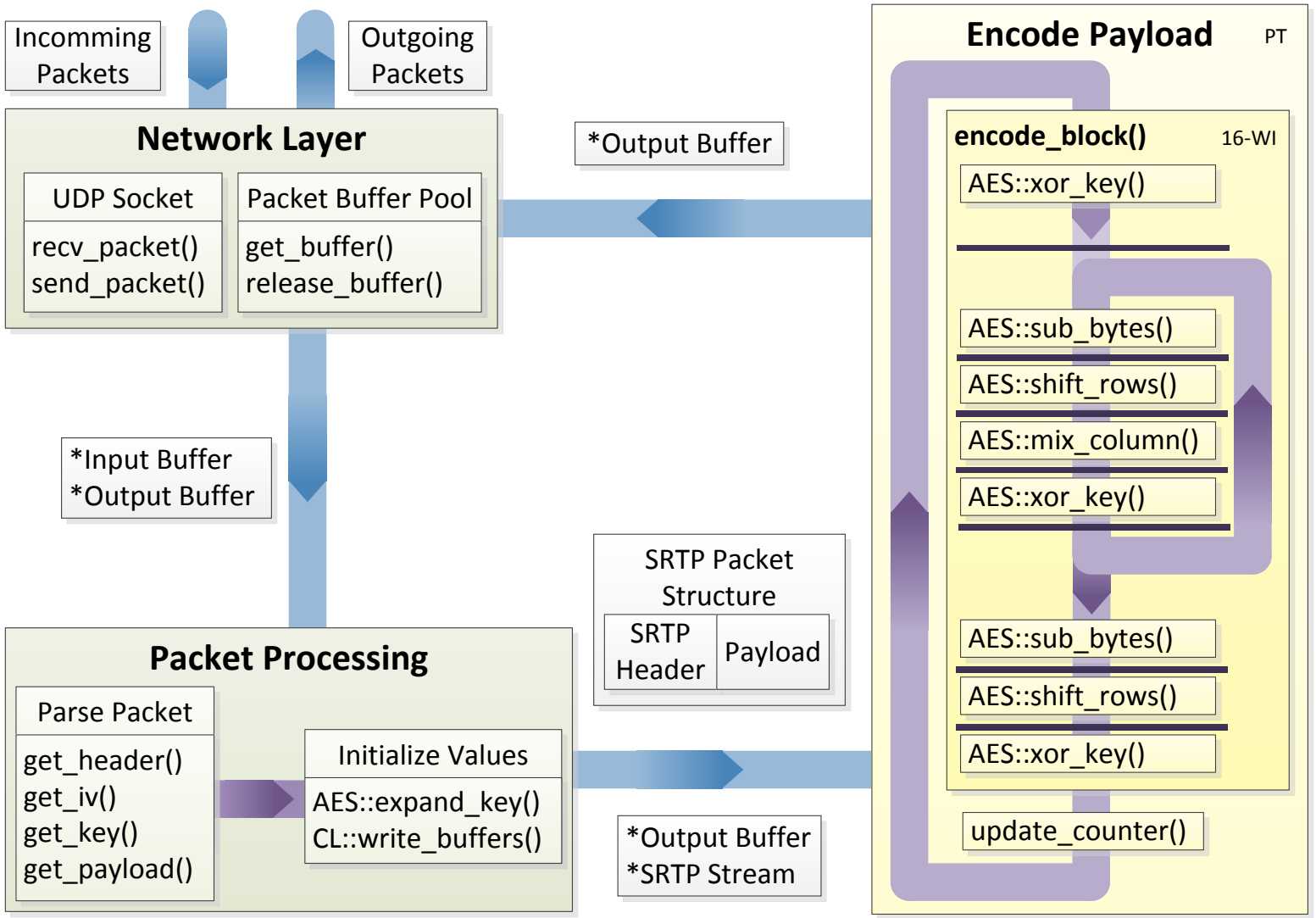
Requirements

- improve concurrent calls on VoIP gateway
- utilize HighPath 4000 softgate's standard hardware
- integrable with current solution

SRTP parsing

- usual size 2 to 10 AES blocks
- careful allocation of resources vs. massive parallelization
- minimize average delay caused by packet processing on gateway

Application Design



Persistent Thread

- kernel uses at most as many blocks as can be concurrently scheduled
- schedules work through queues, not hardware
- provides ”global synchronization”
- work-item’s lifetime through the entire execution of kernel

SRTP header															
Payload															
dc	de	c4	c5	dc	d0	d5	51	53	5d	5f	5b	46	46	46	5b	AES block 1
46	46	46	5b	44	41	42	4f	42	47	42	43	59	58	59	5f	AES block 2
5f	52	59	44	44	5f	51	54	55	55	51	56	50	52	5e	58	AES block 3
5d	52	52	50	57	54	d4	d6	d5	51	53	57	d6	d6	d0	d7	AES block 4
57	56	57	d0	d3	d6	d5	55	51	50	d6	df	d2	d1	d4	d6	AES block 5
dc	db	da	dd	d6	55	dc	d0	d4	5d	44	5c	56	d6	d5	d4	AES block 6
d5	d7	50	d4	51	d0	61	6f	76	fe	ef	f7	77	66	50	ff	AES block 7
e5	d7	74	4a	c9	f9	f7	5c	76	5f	f5	f3	dd	4e	42	d8	AES block 8
f7	c9	50	44	50	cd	c9	d4	4d	41	57	d1	51	58	44	52	AES block 9
d3	d1	50	58	5b	55	d4	53	59	43	47	5f	51	5d	56	d2	AES block 10
MKI & Authentication tag															

Results

Following graph visualizes distribution of packet delays in *ms* over *number of concurrent calls* using G.711 with sampling period 20ms during test.

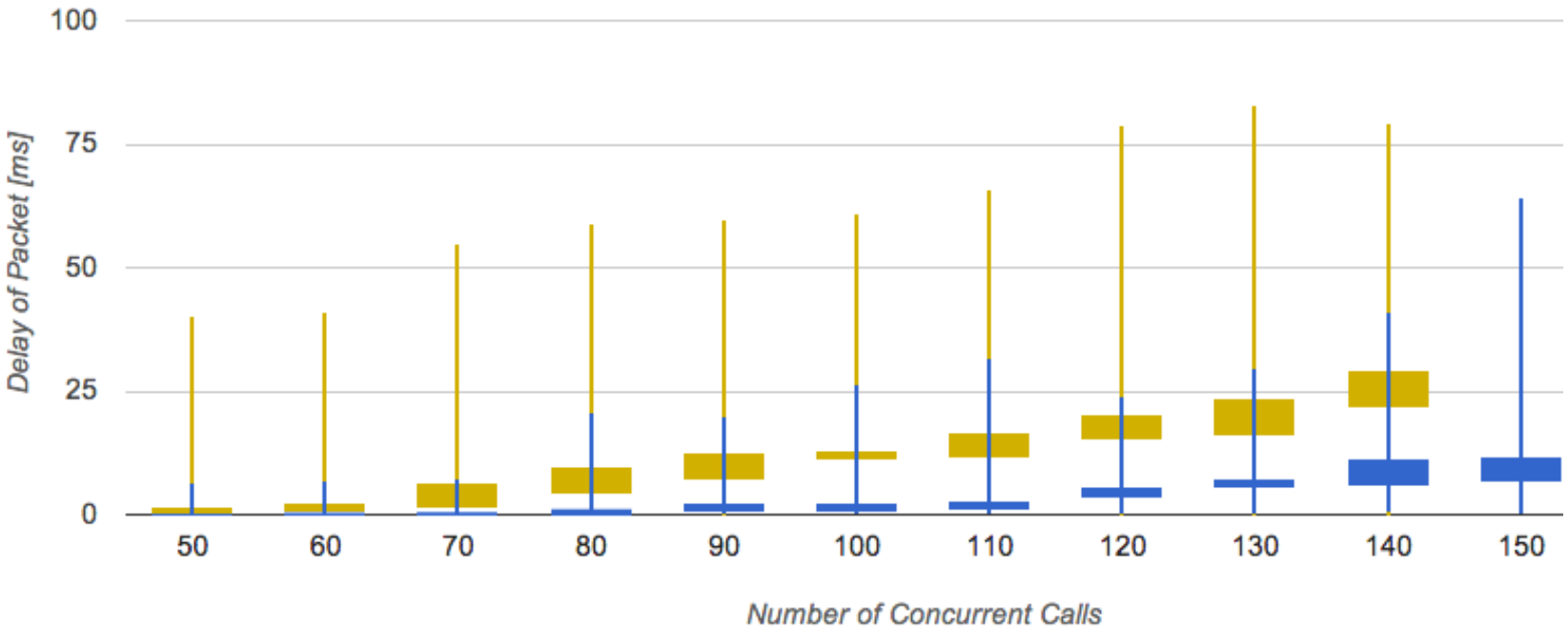


Figure: Comparison of parallel and serial implementation.

Average packet delay caused by SRTP encryption

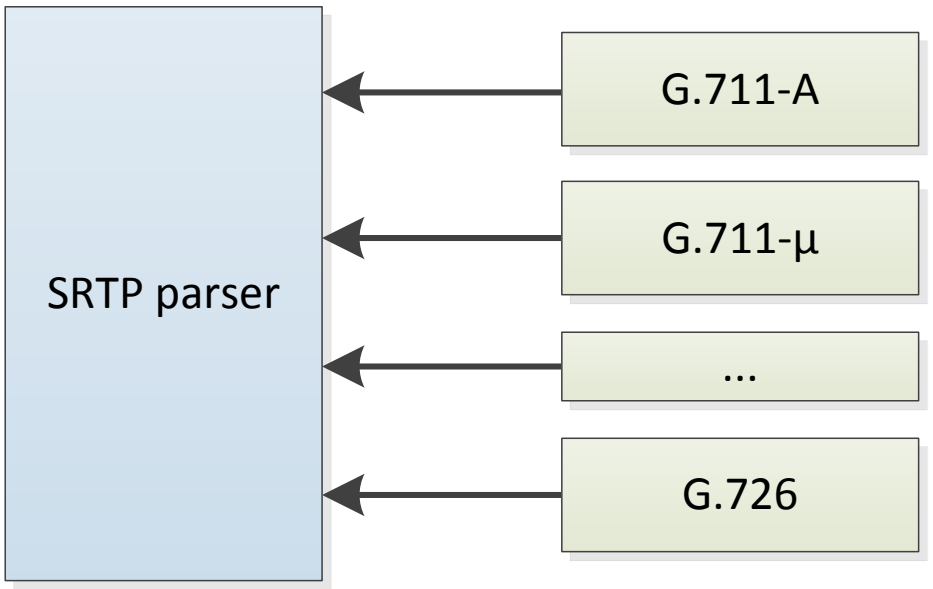
- dropped to one third during 140 concurrent calls
- at least to half during smaller amount of concurrent calls

Thank You

Transcoding

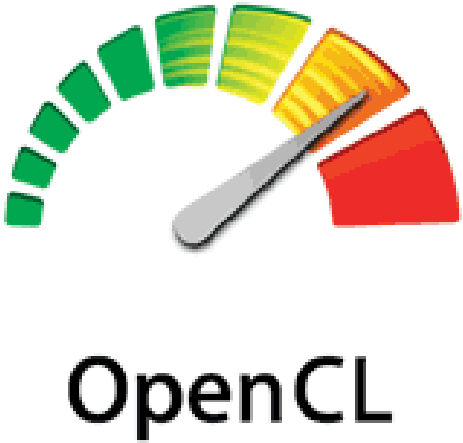
- dynamically linked plugins
- common interface

```
const char* encoding_name
const int PT
transcode(src, dst, len_src, len_dst, pt);
to_pcm(src, raw, len_src, len_dst);
from_raw(raw, dst, len_src, len_dst);
```



Open Computing Language

- standard for parallel computations
- wide support of HW and SW
- active contributions
- many important vendors (including Apple, AMD, intel)



Compiled and tested using:

- processor – intel core i5 2500k
- operating system – OpenSUSE 12.2
- used languages, frameworks and libraries
  - C/C++ std=c++11 (compiled with gcc 4.7)
  - OpenCL 1.2
  - Boost 1.53.0