PROGRAMMABLE NETWORK SERVICES

Hardware accelerated lightweight authentication

Jeffrey Panneman, Floris Drijver, Piotr Zuraniewski, Niels van Adrichem, Bart Gijsen

RON++, 03-12-2018

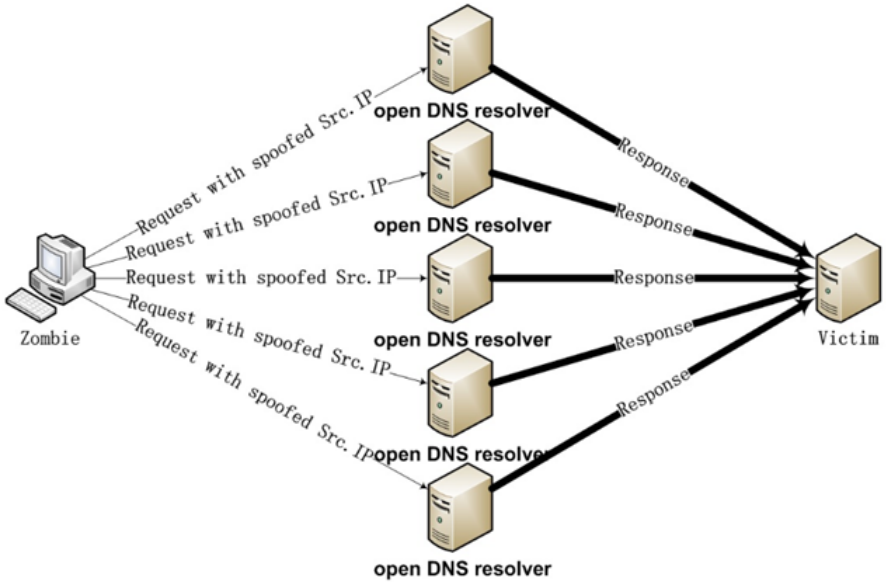
TNO innovation for life

CONTENTS

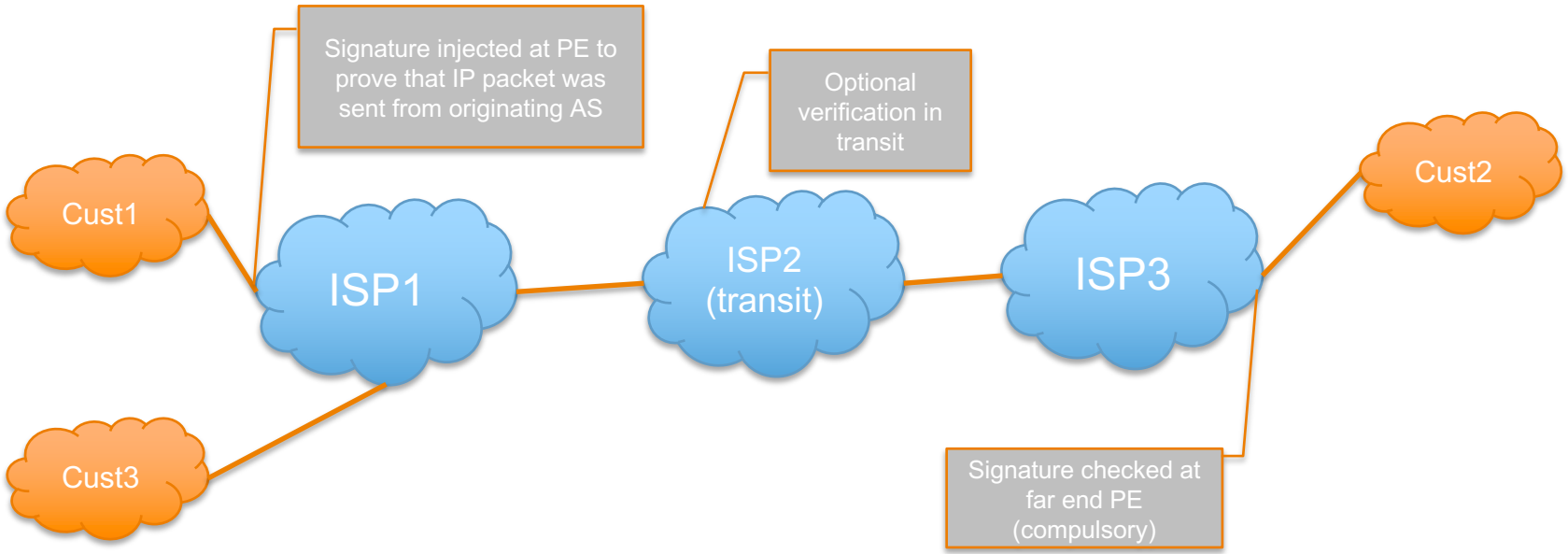
- Introduction + Motivation
- Cryptographic considerations
- Design + Implementation
- Analysis & Results
- Future Work + Conclusions

INTRODUCTION + MOTIVATION

- Other Autonomous Systems on the Internet cannot be trusted
  - They allow subscribers to forward packets from unauthentic IP addresses
  - Per-AS Reverse Path Filtering can solve this, unfortunately few ISPs implement it
- Main cause why UDP Reflection Attacks and TCP SYN-flood attacks are so successful



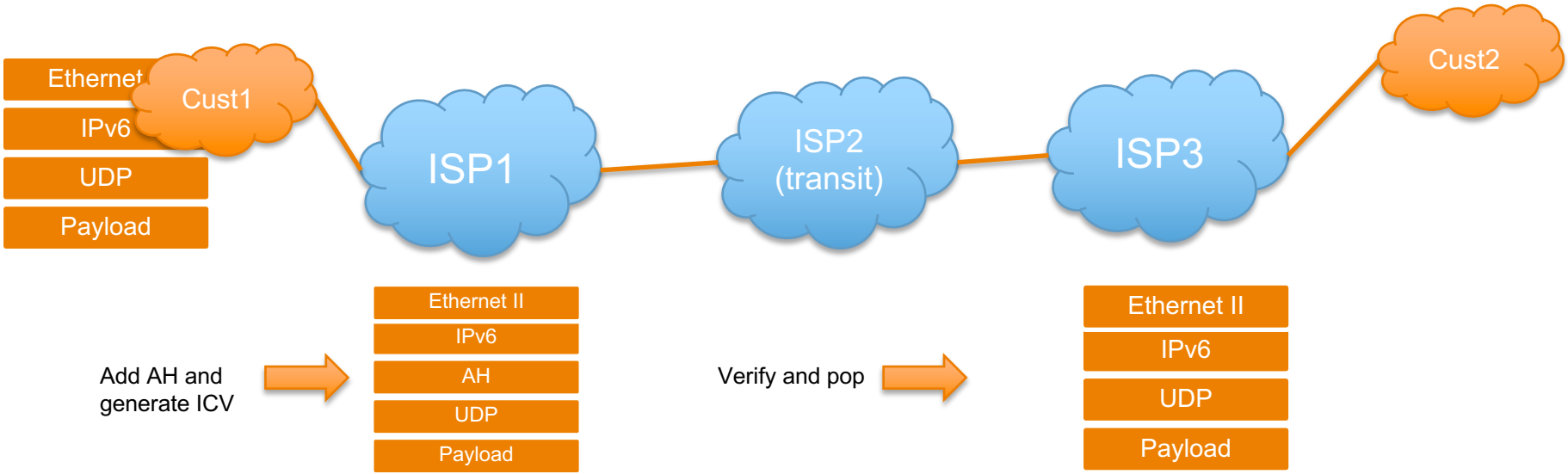
OVERALL IDEA



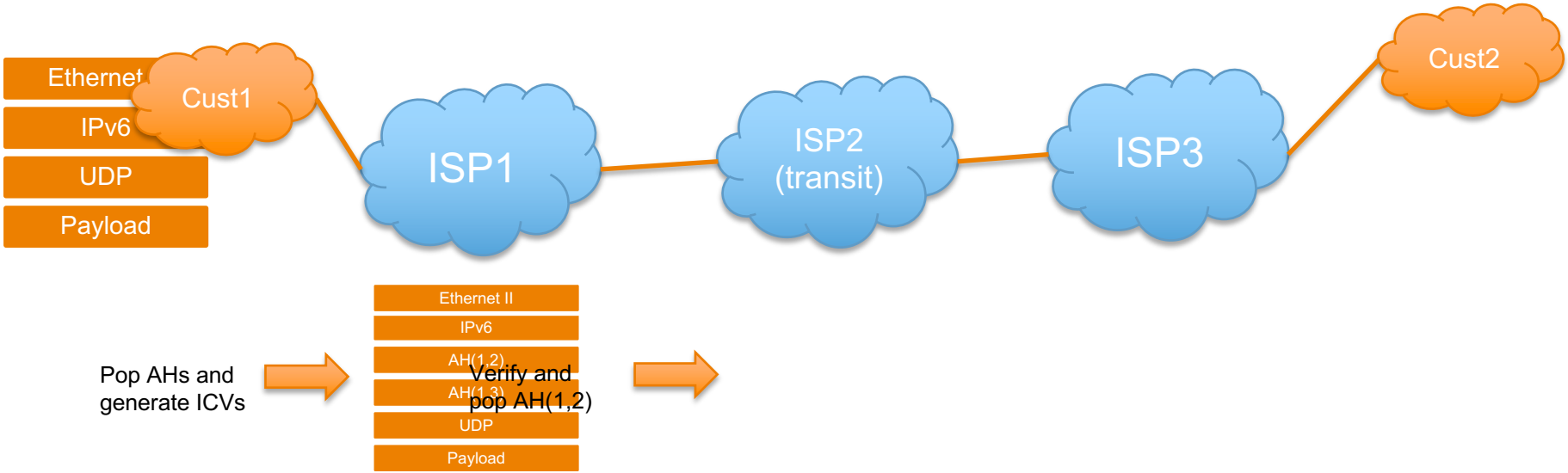
REQUIREMENTS AND CONSIDERED SOLUTIONS

- Flexibility and speed
  - Netronome Agilio LX 2x40GbE SmartNIC (P4/C with hardware accelerated crypto functionality!)
- Any (transit) peer should be able to verify the authenticity of the source of a packet
  - Ideally use asymmetric crypto function – just 1 signature needed – but not supported by LX card
  - Symmetric crypto function also possible (shared secret per AS pair)
- Backward compatibility – non-participating/non-compliant systems should just forward
  - Use IPv6 Authentication header (AH, one of extension headers)
  - Don’t reinvent the wheel, piggyback on earlier IPsec RFC and IP pseudo-header
  - Limit to authentication / (part of) packet integrity, not full encryption – programmability allows it
- Minimal 128-bit security level

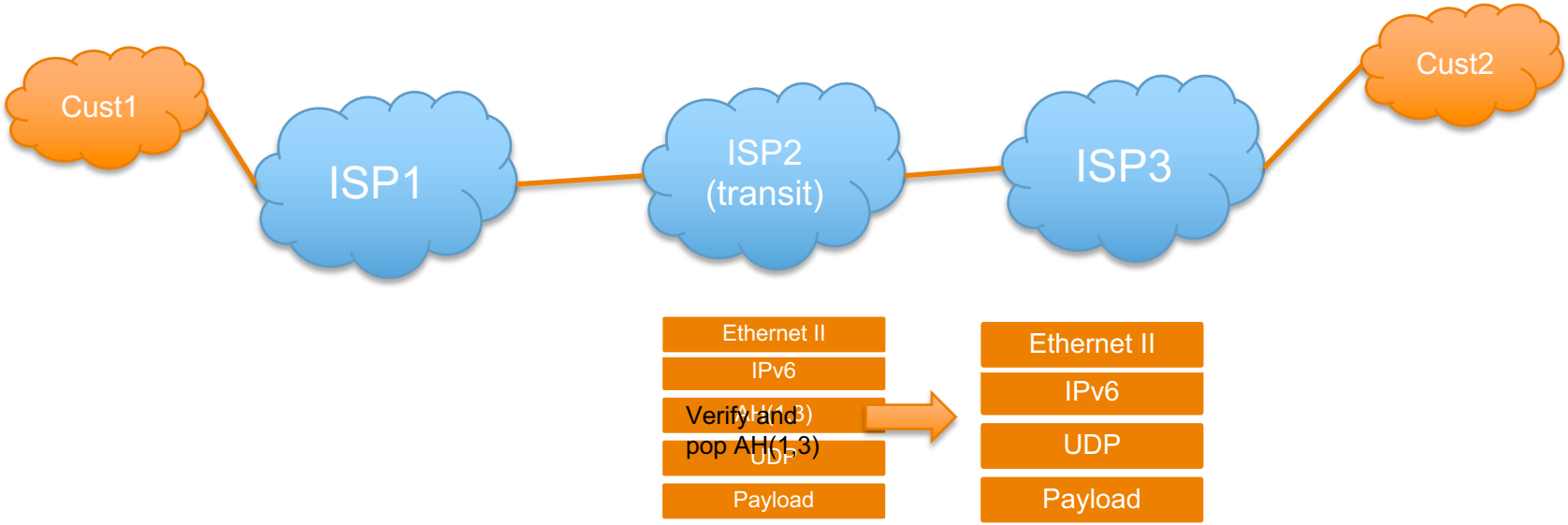
MULTI-AS SETUP – TRANSPARENT TRANSIT



MULTI-AS SETUP – VERIFICATION IN TRANSIT

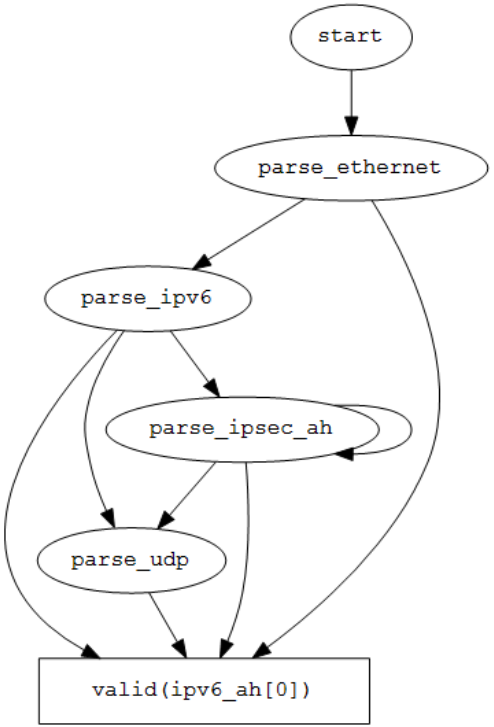


MULTI-AS SETUP – VERIFICATION IN TRANSIT

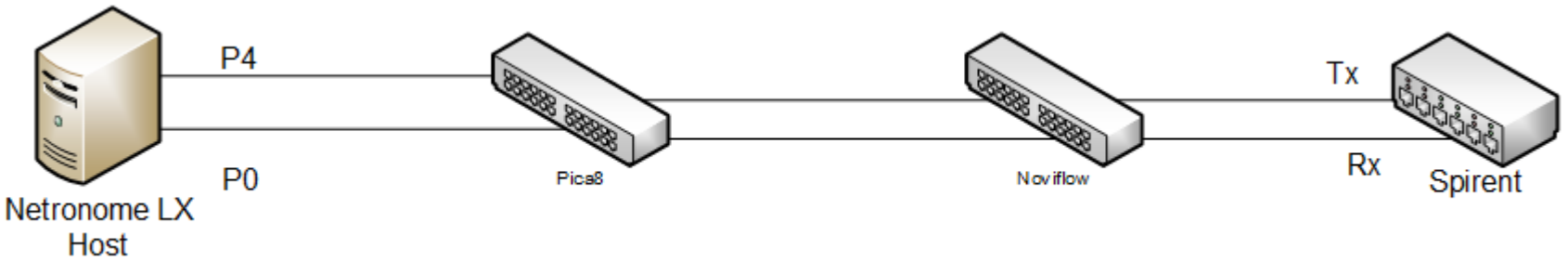


IMPLEMENTATION

- Combination of P4 and Micro-C
  - Micro-C exclusively for crypto library interaction
  - HMAC calculated over IPv6 pseudoheader
- Usage of registers for sequence counters
- Use of recirculation to limit use of Micro-C
  - Internally resend the packet to ingress pipeline
- Header stack needs to have a maximum configured
  - P4 Design limit
- Instruction limit hit easily
  - Compiled P4 produces quite a lot of instructions
  - (very) Limited available space
  - Forces us to run with only half of the available threads



TEST METHODOLOGY(1/2) – TESTBED



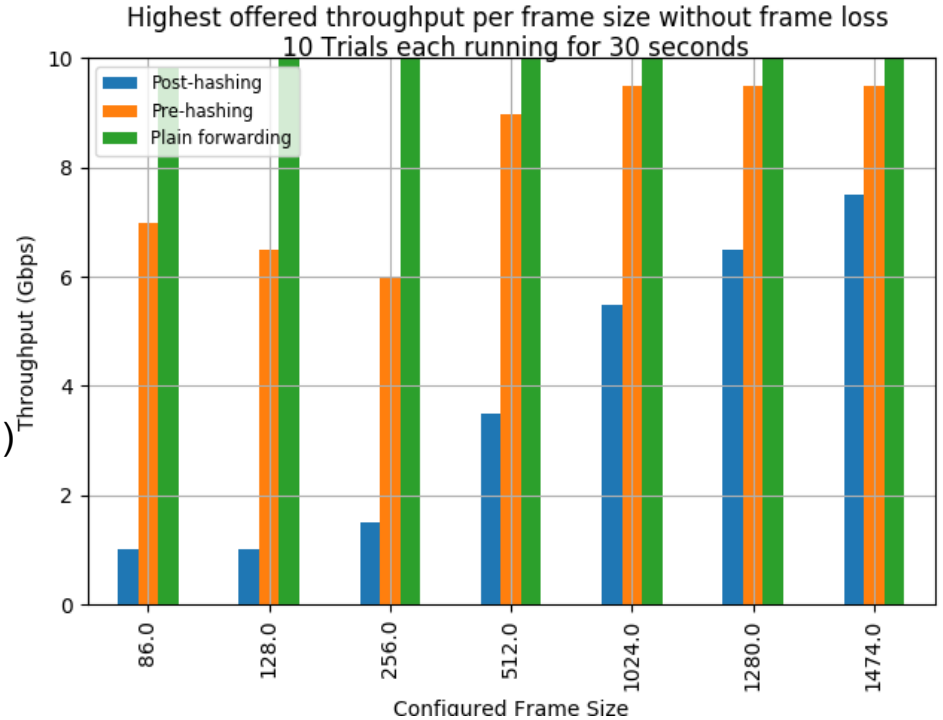
- Spirent – hardware traffic generator, can pump IPv6 traffic @10Gbps (x12)
- NoviFlow – hardware accelerated OF1.5+ SDN switch (16x10Gbps)
- Pica8 – partially hardware accelerated OF1.3 SDN switch
- AgilioLX – gets traffic, runs our code and sends output via its other interface
  - Card is in 40G mode

TEST METHODOLOGY(2/2) – METHOD

- RFC 2544 Frame Loss Test
- Varying frame sizes: 86, 128, 256, 512, 1024, 1280, 1474 (including CRC, IPv6 AH will add 44B)
  - Base input packet is 66 bytes (Eth+IPv6+UDP)
  - Spirent adds 20 byte signature per packet
- Fill the link with varying percentages load
  - Ranges from 5% to 100%
- 10 trials with varying test duration (30 & 60 seconds)
- Different test cases
  - Plain forwarding (forward from one port of LX card to another)
  - Pre-hashing (add AH, don’t call crypto yet)
  - Post-hashing (add AH, call crypto)

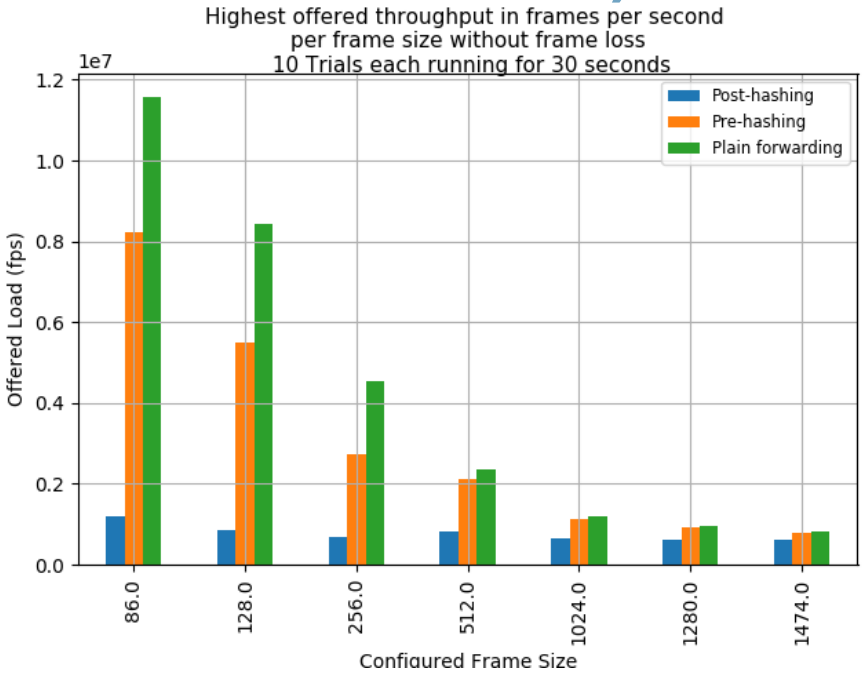
ANALYSIS & RESULTS (GIGABITS PER SECOND)

- Select the highest offered load where there were 0 lost frames
  - No error bars (variability) because of this
- Can easily handle 10G with plain forwarding
- Test of 30 seconds showed unexpected results for pre-hashing test case
  - Drop in performance as frame size increased
  - Many cases with just a few lost frames(<0.01%)
- Test of 30 seconds showed expected results for post-hashing test case
  - Crypto island interaction is very expensive



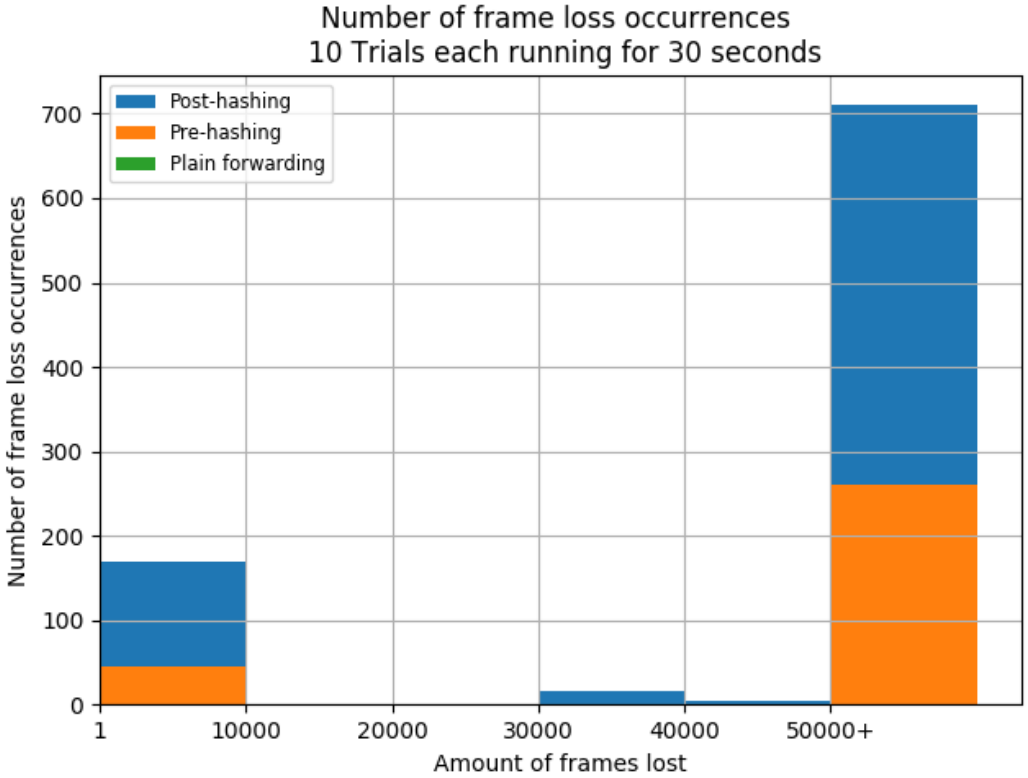
ANALYSIS & RESULTS (FRAMES PER SECOND)

- Select the highest offered load where there were 0 lost frames
  - No error bars (variability) because of this
- Can easily handle 10G with plain forwarding
- Test of 30 seconds showed unexpected results for pre-hashing test case
  - Drop in performance as frame size increased
  - Many cases with just a few lost frames(<0.01%)
- Test of 30 seconds showed expected results for post-hashing test case
  - Crypto island interaction is very expensive



ANALYSIS & RESULTS (FRAME LOSS DISTRIBUTION)

- Bulk of losses are significant(>50k frames)
- However, large amount of frame loss is under 10k frames
  - e.g 100 frames lost with 100mil sent



FUTURE WORK

- Key distribution – public keys
- Key exchange – negotiate symmetric keys per AS pair
- Use of asymmetric signatures
  - Not yet available in Netronome hardware
- Dynamic security associations – cipher suite selection
- Optimize performance
  - Usage of other half of threads (currently not used to increase instruction limits)
  - Remove recirculation step
  - Forced to disable FlowCache due to massive frame loss when enabled, needs investigation
- Implement crypto as part of service function chain using e.g., segment routing

CONCLUSIONS

- Proved that customized crypto operations at multigigabit speed are possible
- Found the limits of operations w.r.t.
  - Crypto island interaction
  - Headers manipulations
    - Pushing extension headers and deparsing header stack
    - SDK cannot parse more than 16 headers
    - 16/Large stack takes up a lot of memory and leads to exhaustion
  - Instruction count limit
- Lightweight authentication is feasible using (current) programmable hardware
  - More performance can be squeezed out of the hardware with optimization

RON2017 REVISIT

- Last year we dove into complex, nested TLV packet (NDN) processing
  - Used the same hardware
  - Crypto library was not available
  - Barely any P4 code, mostly Micro-C
- Update last years project, goal is to integrate crypto library and grow familiarity for this years project
- Optimized Micro-C code with assistance from Netronome engineers
- Card becomes unresponsive and in bad state with (too) high packet influx
  - Only fix is re-flashing firmware
  - Debugged with Netronome, solution not yet found
- (stable) Performance went from ~10 Mbps to ~60 Mbps
  - Needs further investigation and support from Netronome


THANK YOU FOR YOUR ATTENTION
Take a look:
TIME.TNO.NL
TNO innovation for life