Leveraging Heterogeneous Programmable Data Planes for Security and Privacy of Cellular Networks, 5G & Beyond

JUNO-3 PI Meeting

Aug. 28, 2025

K. K. Ramakrishnan, Shaoyu Tu

University of California, Riverside, CA

&

Timothy Wood, Cuidi Wei

George Washington University, Washington D. C.

Toru Hasegawa

Shimane Univeristy

Yuki Koizumi and Junji Takemasa

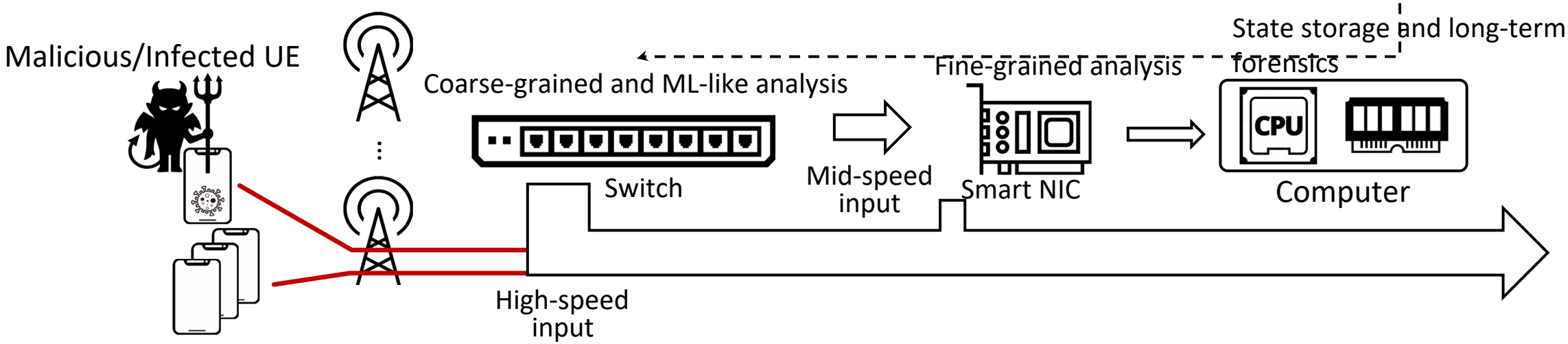
Osaka University

&

Toshiaki Tanaka and Jun Kurihara

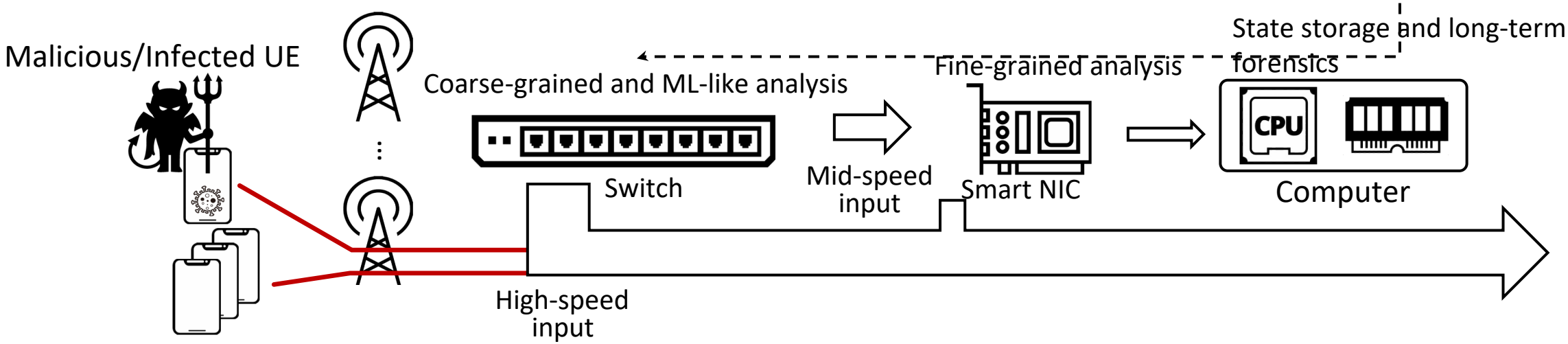
University of Hyogo

Programmable Data Planes for Network Performance Monitoring & Security



- Our project seeks to use high speed programmable switches, SmartNICs and end-host servers supporting network functions to provide security monitoring and privacy protection solutions
  - Develop an efficient, high performance network security solution, including for cellular networks
- Cellular networks support a growing amount of traffic from mobile and Internet of Things (IoT) devices
  - Implementations moving to software-based environments: potential for increased vulnerability to security attacks, including violation of user privacy through eavesdropping
  - More low-volume, slow and stealthy attacks: difficult to detect, need more memory and compute capacity
- Monitoring: we will develop a collaborative filtering system for real-time monitoring of network traffic
  - Most of the traffic processed by high-speed programmable switches to extract coarse-grained metrics
  - Suspicious traffic redirected to programmable SmartNICs or the host for detailed forensics

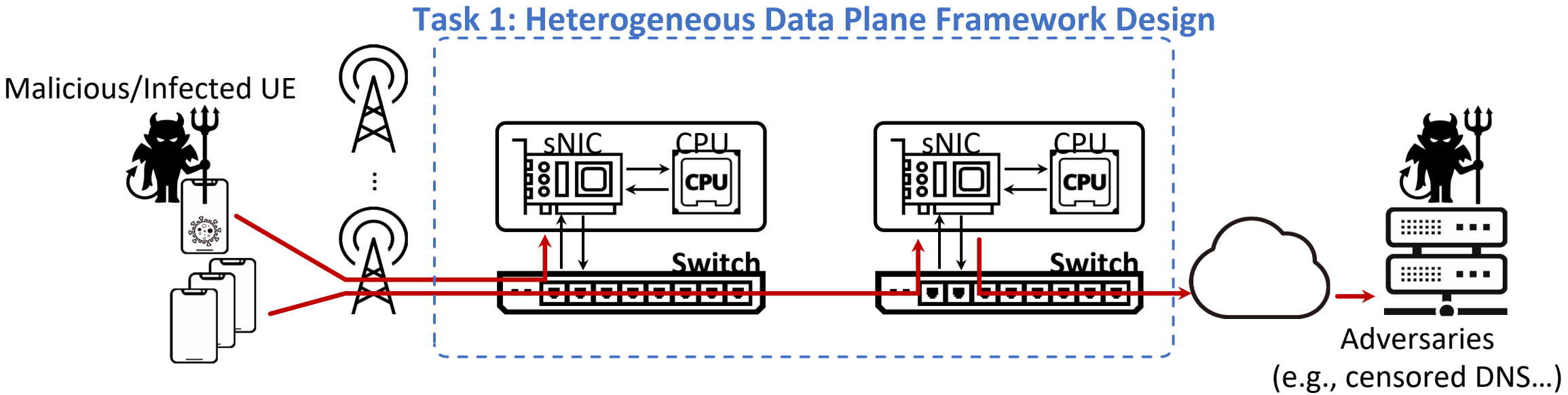
Programmable Data Planes for Network Performance Monitoring & Security



- Privacy Protection: utilize P4 programmable switches for anonymization and privacy protection
  - Lightweight Anonymization at Terabit rates within the network layer with high-speed P4 switches
  - Use traffic morphing to handle fingerprinting attacks
- Project builds on decade-long work on switching, SmartNIC and NFV work by PIs and collaboration between the PIs based in the US and Japan
- Societal Impact: Provide strong threat prevention and privacy preservation of cellular network users

Overview of Project Accomplishments

Tasks 1-2: Heterogeneous Data Plane Monitoring

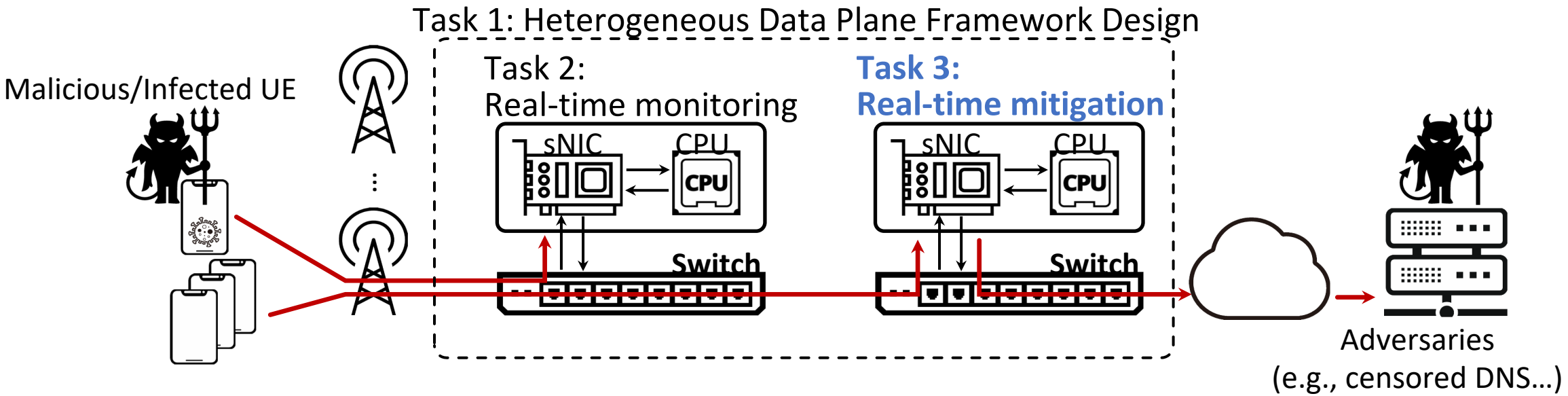


- Design a programmable data plane framework to leverage heterogeneity:
  - P4 Switches: High bandwidth (Tbps), limited memory (MBs)/programmability
  - SmartNICs: Moderate bandwidth (Gbps), moderate memory (GBs); Programmable
  - Host CPUs: Limited bandwidth, large memory (TBs), general purpose CPUs
- Use heterogeneous data plane for real-time monitoring of cellular network
  - 5G core based on multi-tier programmable data and control plane components

Task 1-2: Heterogeneous Data Plane Monitoring

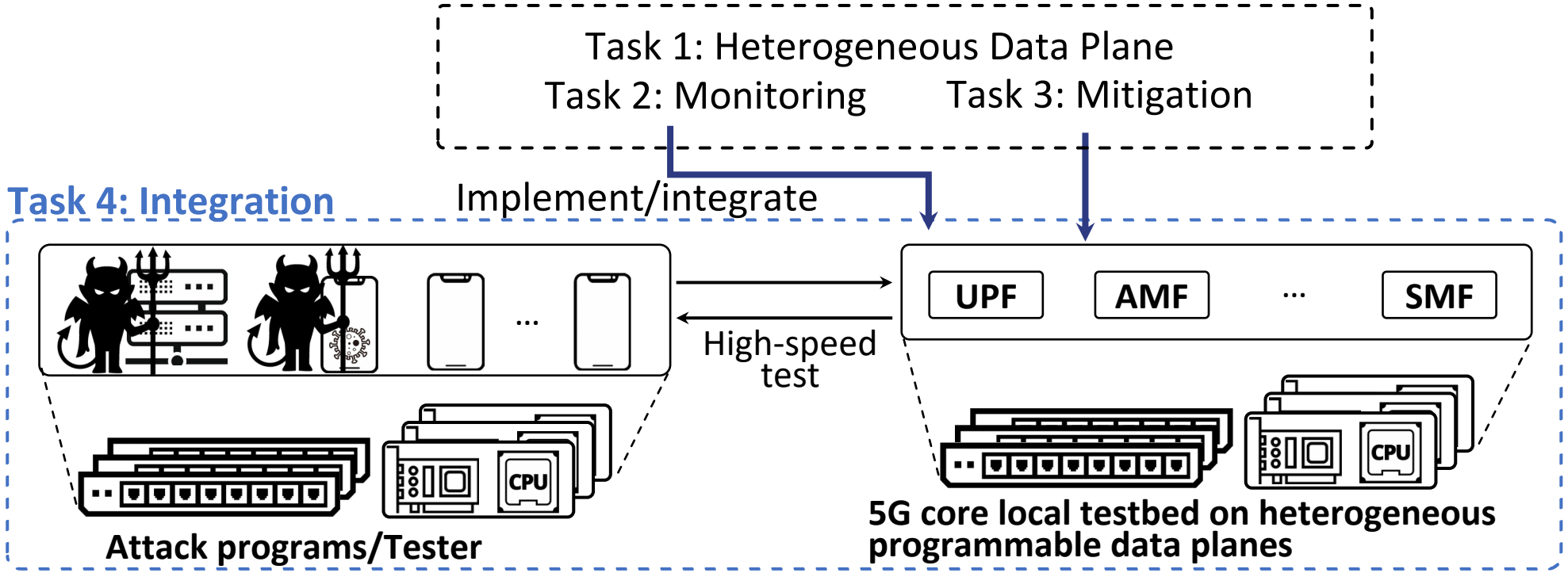
- Goal:
  - Coordinate protocols between various programmable network devices to overcome their limitations while optimizing their strengths, to enable real-time monitoring and security
- Key techniques
  - **Cooperative flow filtering** and state caching across heterogeneous programmable network devices
  - **In-network ML inference:** get high throughput by using the pipelined processing of packets on P4 switches and SmartNICs and slicing of GPUs on hosts
  - **Optimization algorithms** that use models of component capabilities to effectively determine which traffic monitoring modules to place on which types of data plane hardware

Task 3: Real-time Privacy Preservation/Attack Mitigation



- Prevent attacks and preserve privacy for mobile users
  - Lightweight traffic encryption protocols to provide relationship anonymity
  - Traffic obfuscation techniques to prevent fingerprinting attacks

Task 4: Integration



- Deploy a holistic system to study security and performance properties
  - Optimize the combination of hosts, P4 switches, and SmartNICs
  - Evaluate traffic monitoring and privacy preservation techniques on 5G testbed

Task 1/2: Heterogeneous Data Plane for Real-Time Monitoring

Low Volume and Slow Attacks

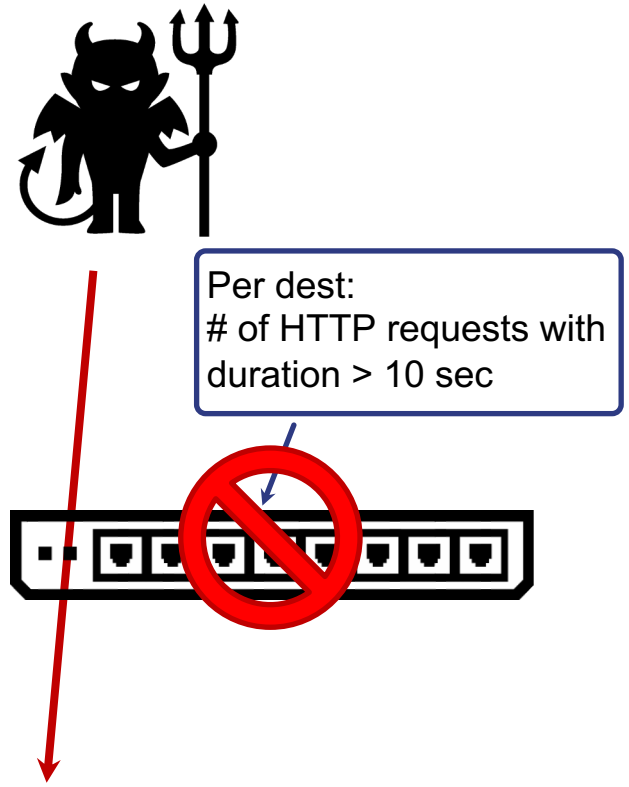
- **SYN Flood Attacks**
  - Sends only a few packets to exhaust a target's kernel socket resources by exploiting the TCP 3-way handshake.
- **Port Scan Attacks**
  - Common method for discovering exploitable open ports of servers on the network.
- **SSH Brute-forcing**
  - An attack where one or more nodes use different username/password combinations to try to log in to a site.

- **Slowloris**
  - Holds open a connection by continuously send partial HTTP GET requests with incomplete headers at a slow rate to keep sockets from closing
- **Slowbody/RUDY**
  - Holds open a connection by continuously sending incomplete HTTP POST requests with large Content-Length value within the HTTP header at a slow rate to keep sockets from closing

Hard to detect and can be extremely damaging to end hosts!

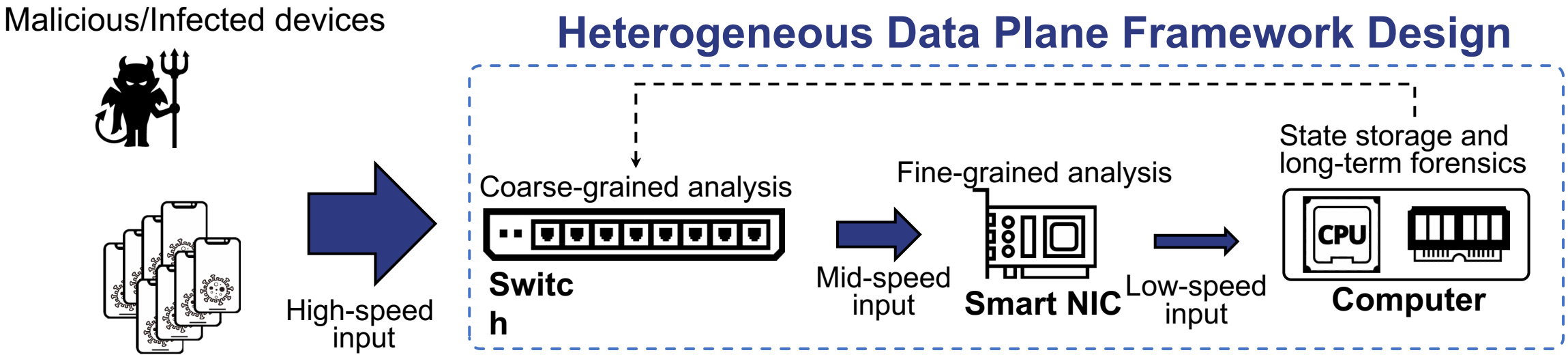
Programmable Switch Constraint Implications

- Slowloris Attack [1]
  - keeps open a very large number of connections to a target web server
  - difficult to serve legitimate web requests
- A constrained programmable switch could conduct coarse-grained analysis [2]
- A host-based IDS can then conduct fine grained analysis [3]
  - SmartNICs/FPGA have been widely used for monitoring [4, 5]
  - SmartNICs
    - Have fewer hardware limits compared to switches
    - Can reduce costly bus and host overheads
    - have acceleration functionality - encryption, hash calculation



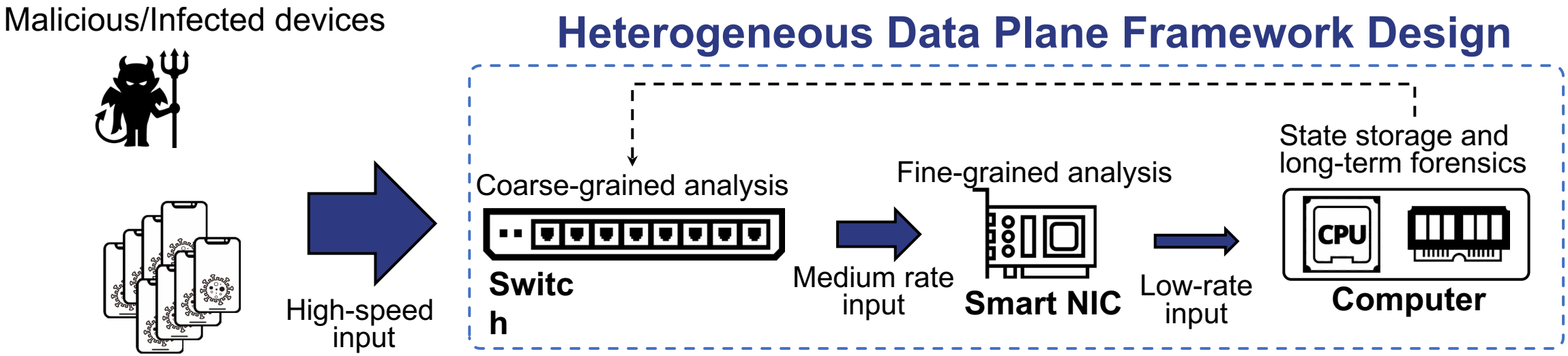
[1] Slowloris DDoS attack (CloudFlare)
[2] Sonata: Query-driven Streaming Network Telemetry (SIGCOMM 2018)
[3] Zeek https://zeek.org
[4] Achieving 100Gbps Intrusion Prevention on a Single Server (OSDI 2020)
[5] Turboflow: information rich flow record generation on commodity switches (EuroSys 2018)

Heterogeneous Data Plane Monitoring



- Objective: Finding “a needle in a haystack”
  - Monitor low-volume and slow attacks in a high-speed network
- Approach:
  - Cooperative flow filtering and state caching across heterogeneous programmable network devices
  - Coordination among heterogeneous devices to overcome their limitations while optimizing their strengths, to enable real-time security monitoring

The Dataplane's Strengths and Weaknesses



	Throughput	Memory	Programmability
Switch (per pipe)	**1.6 Tbps ↑↑**	**10 MB ↓↓↓**	**P4**
SmartNIC (per port)	**40 Gbps**	**4 GB**	**P4 + MicroC**
Host (per core)	**10 Gbps**	**25 GB**	**General purpose**

Harnessing Heterogeneous Data Plane Devices

1. How to perform **stateful** monitoring of Terabit scale traffic to detect **low and slow attacks**?
   - **Differentiate between suspicious and benign flows as quickly as possible**
2. How to overcome the **limited memory** of the switch and the **limited bandwidth** of the NIC/host?
   - **"Flip-the-script": Use specialized switch data structures to track benign flows and use NIC/host to analyze & identify suspicious traffic**
   - **Rather than Sketch-like approaches that focus on finding 'elephant malicious flows'**
3. How to coordinate multiple devices to work together?
   - **Optimize communication via data plane paths to be substantially quicker than control plane updates**

Harnessing Heterogeneous Data Plane Devices

1. How to perform **stateful** monitoring of terabit scale traffic to detect **low and slow attacks**?

   Differentiate between suspicious and benign flows as quickly as possible

2. How to overcome the **limited memory** of the switch and the **limited bandwidth** of the NIC/host?

   "Flip-the-script": Use specialized switch data structures to track benign flows and use NIC/host to analyze & identify suspicious traffic

   Rather than Sketch-like approaches that focus on finding 'elephant malicious flows'

3. How to coordinate multiple devices to work together?

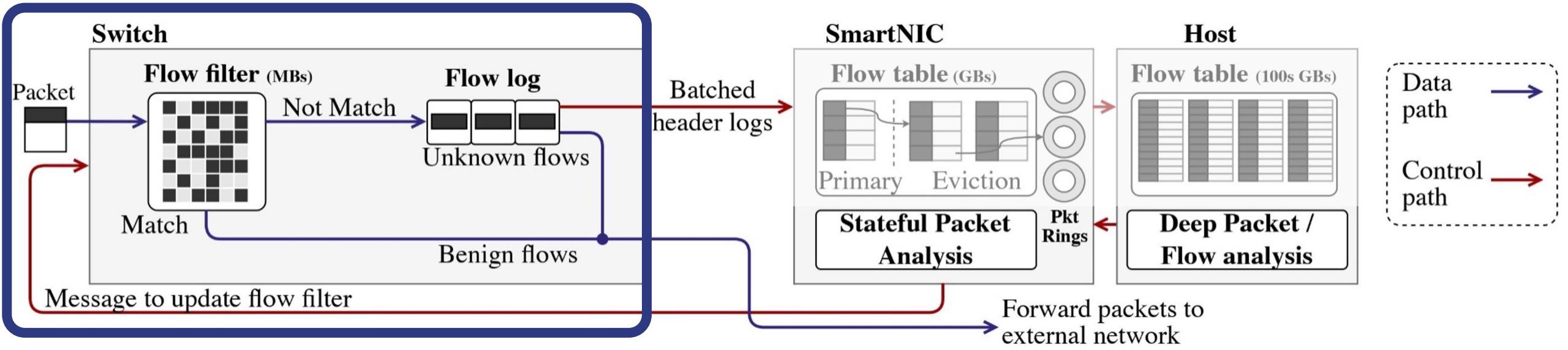
   Optimize communication via data plane paths that are substantially faster than control plane updates

Benign vs. Suspicious Flows

	Benign Flows	Suspicious Flows	Examples
TCP connection establishment	3 packets	1 or 2 packets	Syn Flood, Port Scan
Connection Authentication	often > 20 authentication-related packets within a short time	often < 10 authentication packets within a short time	SSH Brute Forcing, FTP Brute Forcing
HTTP Requests	Full HTTP Requests	Partial Requests	Slowloris, Slowbody/RUDY

Often it is possible to detect “good” flows quickly

Packet Processing Flow

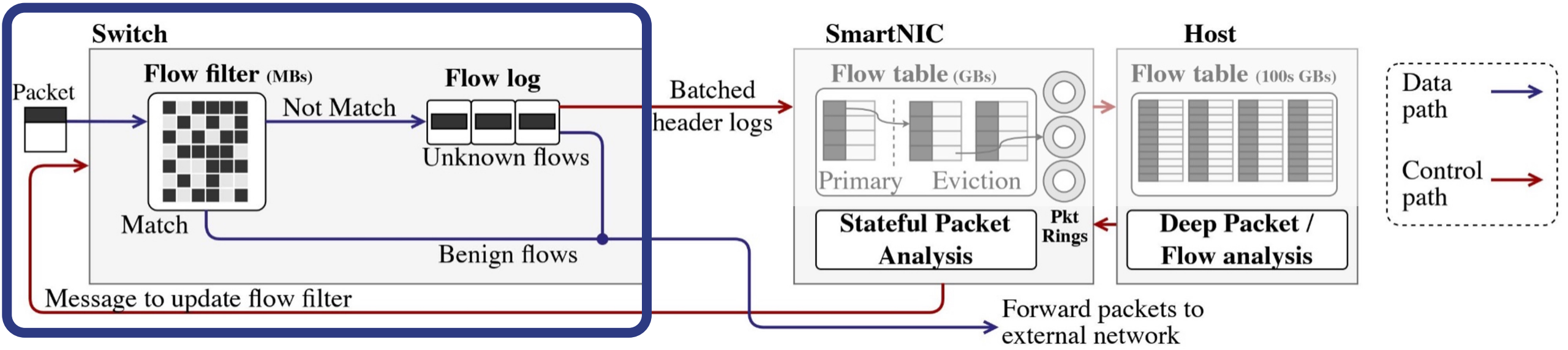


- **SmartNIC/Host Analysis**:
  - Treat first few packets of all flows as "**suspicious**" and send for monitoring
  - Mark flows as "**benign**" if classified safe
- **Switch**
  - ✗ Stateful processing
  - ✓ Filter that reduces the load on and communication to the host.

Harnessing Heterogeneous Data Plane Devices

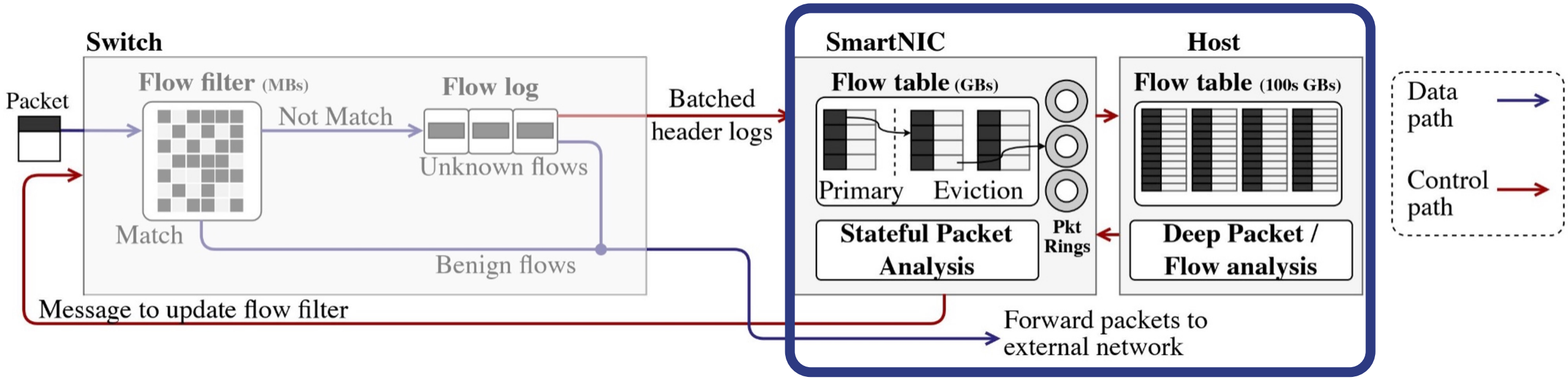
1. How to perform **stateful** monitoring of terabit scale traffic to detect **low and slow attacks**?
   - **Differentiate between suspicious and benign traffic**
2. How to overcome the **limited memory** of the switch and the **limited bandwidth** of the NIC/host?
   - **"Flip-the-script": Use specialized switch data structures to track benign flows and use NIC/host to analyze & identify suspicious traffic**
   - **Rather than Sketch-like approaches that focus on finding 'elephant malicious flows'**
3. How to coordinate multiple devices to work together?
   - **Optimize communication via data plane paths that are substantially faster than control plane updates**

Switch Data Structures



- Tracks **benign flows** to be forwarded directly to network in a space-efficient manner with simple operations
  - Switch flow filter is based on Bloom and Cuckoo filters
- Extended to balance risk (false positives) and overhead (false negatives)
  - False positives caused by the nature of the Bloom filter
    - Identify suspicious flows as benign
  - False negatives because of deletion of old flows
    - Identifies benign flows as suspicious

NIC/Host Data Structures



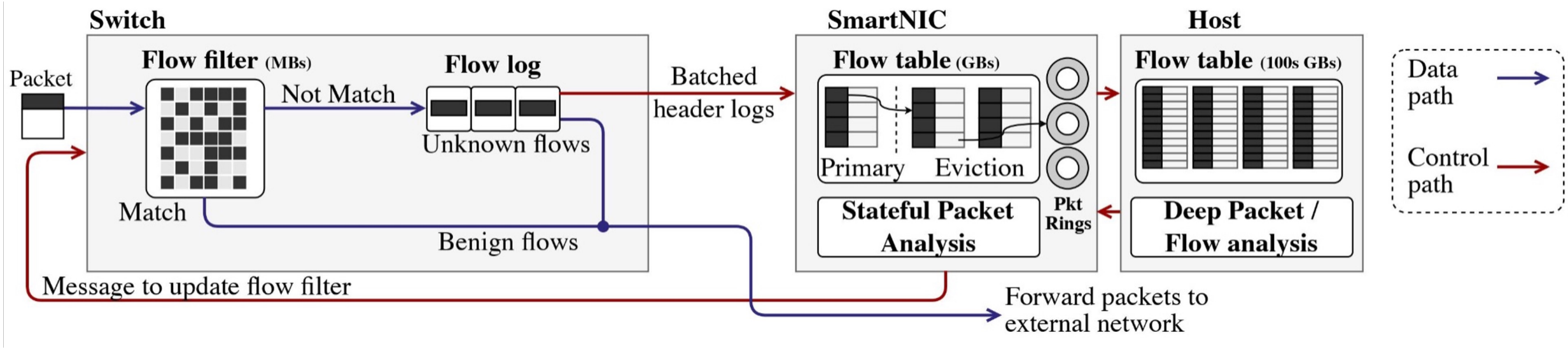
- **SmartNIC/Host Flow Tables [6]**
  - Consists of hash tables and ring buffers
  - Supports 25M to 100M flow entries on the smartNIC
  - Lossless tracking both packet-level and flow-level features at 43 MPPS
  - Host retains information about all flows seen so far

[6] Sourav Panda, Yixiao Feng, Sameer G Kulkarni, K. K. Ramakrishnan, Nick Duffield, and Laxmi N. Bhuyan, "SmartWatch: Accurate Traffic Analysis and Flow-state Tracking for Intrusion Prevention using SmartNICs," CoNEXT, Dec. 2021.

Harnessing Heterogeneous Data Plane Devices

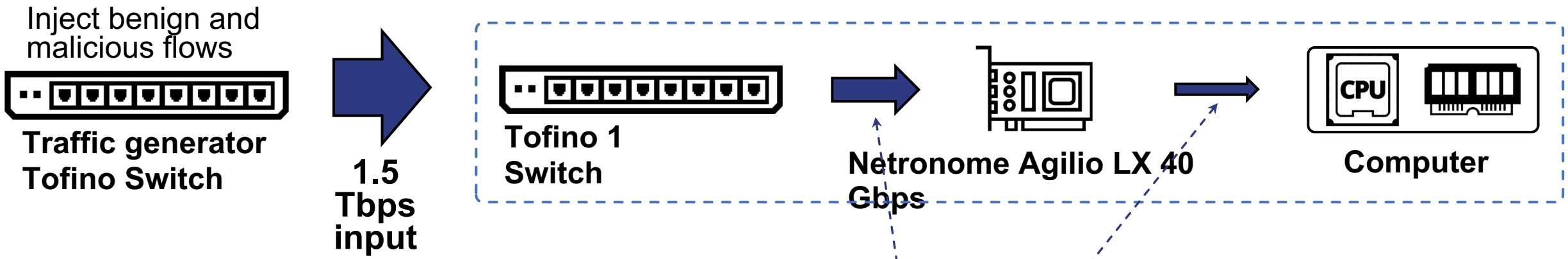
1. How to perform **stateful** monitoring of terabit scale traffic to detect **low and slow attacks**?
   - **Differentiate between suspicious and benign traffic**
2. How to overcome the **limited memory** of the switch and the **limited bandwidth** of the NIC/host?
   - **"Flip-the-script": Use specialized switch data structures to track benign flows and use NIC/host to analyze & identify suspicious traffic**
   - **Rather than Sketch-like approaches that focus on finding 'elephant malicious flows'**
3. How to coordinate multiple devices to work together?
   - **Optimize communication via data plane paths to be substantially quicker than control plane updates**

Data Plane Communication

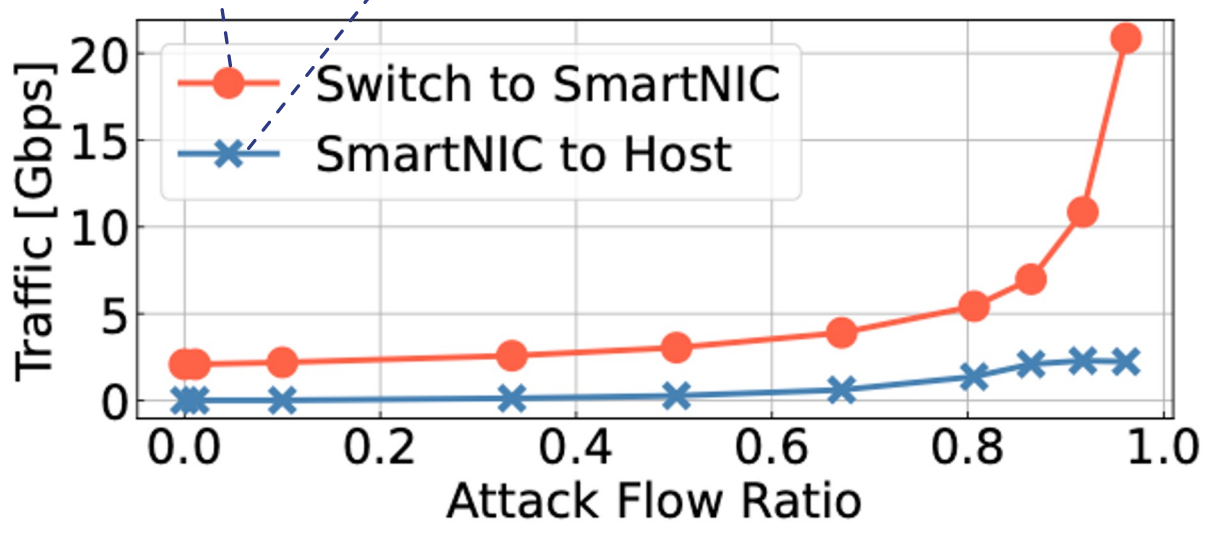


- **Fast communication among the dataplane devices**
  - **Data Plane Messaging:**
    - Avoid slow control plane protocols to update the switch flow filter
- **Efficient communication between the dataplane devices**
  - **Packet Truncation:**
    - Only send key flow information from the packet header
  - **Packet Batching:**
    - Buffers flow information from several packets in a flow log, then transmits them to the SmartNIC/Host when the flow log is full

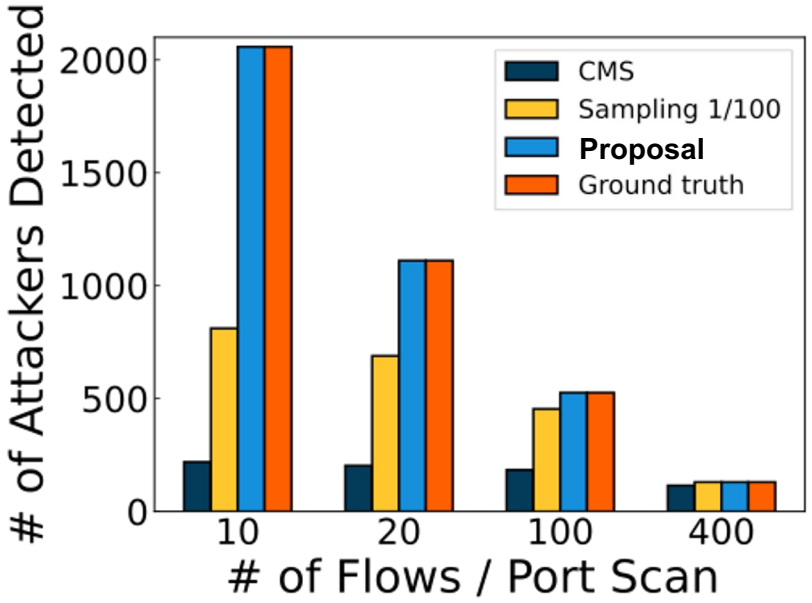
Evaluation: Traffic Load on SmartNIC/Host

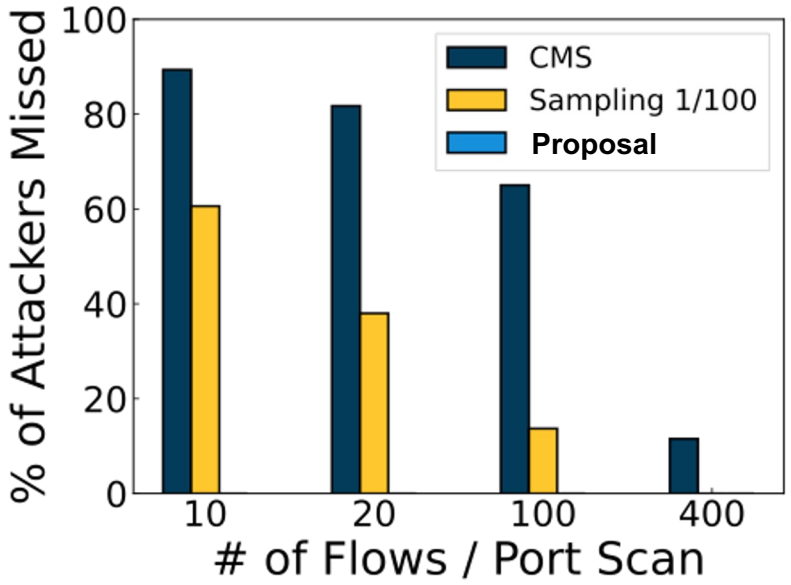


- **1.5 Tbps of traffic incoming to switch**
- Even for large numbers of attack flows, the volume to the SmartNIC remains low, only passing 10 Gbps for α > 0.9.
- 99.3% reduction in traffic that reaches host, could be easily handled by a single core



Evaluation: Detection Performance





- CountMin Sketch can generally detect the heaviest attack flows in high accuracy but does poorly on detecting low-rate attack flows.
- Sampling 1/100 is also good at detecting heavier attack flows but misses a certain portion of low-rate attacks.
- Proposal can detect low-rate attacks quite in high accuracy and also can handle heavy attacks.

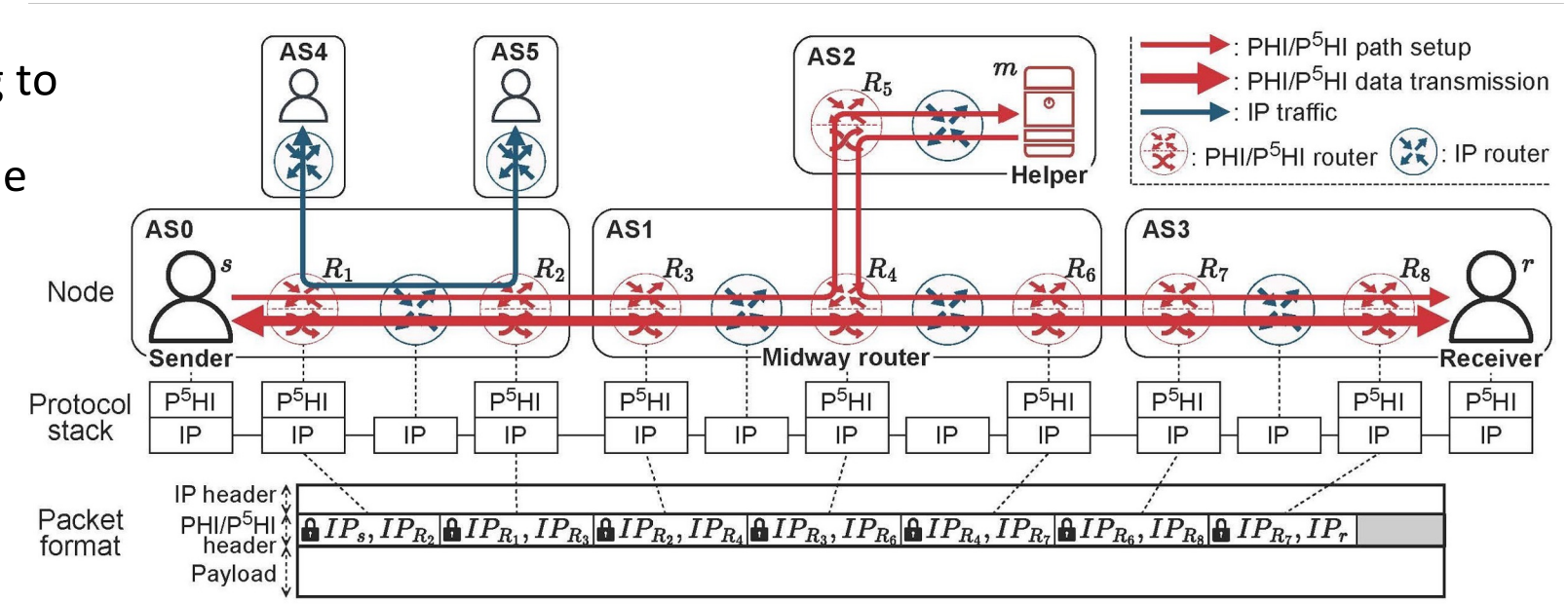
Task 3/4: Real-time Privacy Preservation and Integration

Achievements of Task 3 and 4

- **IP address obfuscation**
  - Implements Lightweight Anonymity Protocol (AP) on a Tofino-based programmable switch
  - Demonstrates high-speed lightweight AP communication between the U.S. and Japan over an intercontinental testbed
- **DNS privacy protection**
  - Designs and implements a multiple-relay-allowed anonymization scheme, µODNS (Mutualized Oblivious DNS), whereas existing schemes use a single relay

Lightweight Anonymity Protocol (AP)

- PHI (Path-hidden lightweight anonymity protocol)
  - Assumption: Local adversary
    - Weak but reasonable adversary who captures packets at a single point of the path
  - Relationship anonymity
    - Routers obscure either source or destination address to prevent a local adversary from correlating source and destination addresses
  - Advantages
    - High-speed forwarding owing to encryption of only headers
    - Short path length owing to the underlying IP routing path
- **P5HI (P4 PHI)**
  - **Hardware-based AP implementation**
  - For both Tofino 1 and 2 switch

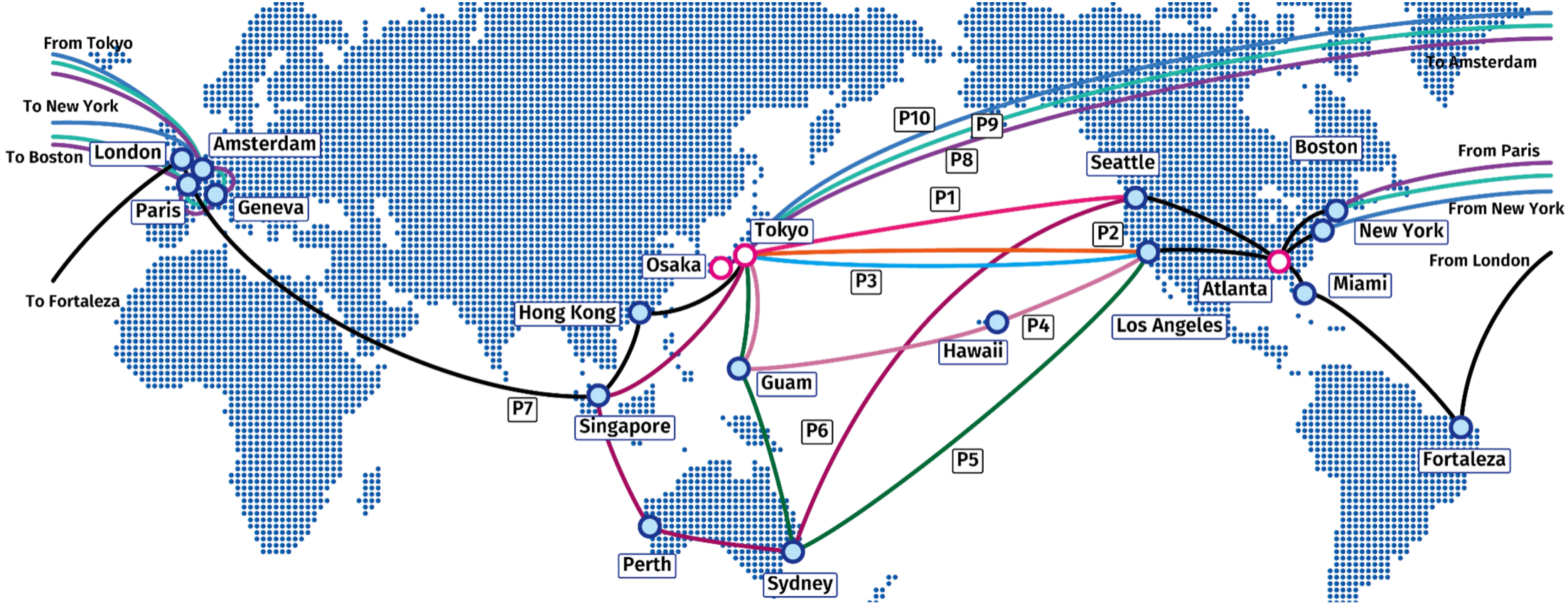


Yutaro Yoshinaka, Junji Takemasa, Yuki Koizumi, Toru Hasegawa, “Design and analysis of lightweight anonymity protocol for host- and AS-level anonymity ,” Computer Networks, Volume 222, 109559-109559, Feb. 2023.

P5HI Experiments over an Intercontinental Testbed

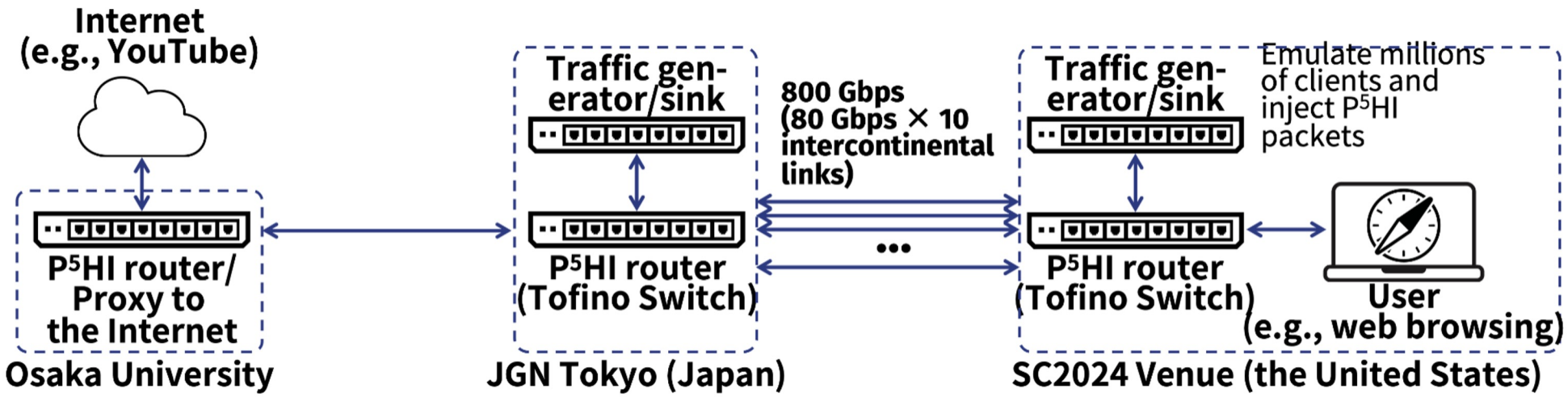
A dedicated **800 Gbps connection** (10 x 80-Gbps links) was established between Tokyo (the NICT's testbed node) and Atlanta (SC24 venue)

(It made possible through the extensive support of the NICT testbed team, the KDDI network operations team, and 21 collaborating institutes)



Demonstrations of P5HI at SC24

1. Demonstration of high-speed anonymous communication
   - **588.4 Gbps anonymous communication between Japan and the U.S.**
     - Performance limited by packet filtering on two links and rate control on one link
2. Demonstration of real applications over anonymous communication
   - **4K YouTube video streaming** from the Internet traversing a proxy server at Osaka University, passing through the JGN Tokyo node, and reaching the SC venue

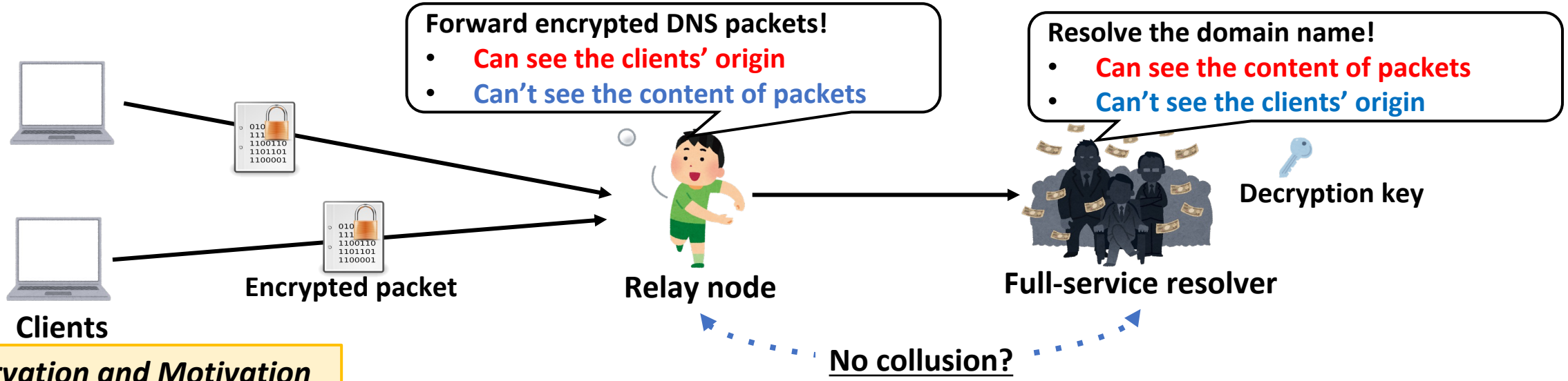


DNS Anonymization against Colluded Network Nodes

Background

Recent increase and exposure of Internet censorship
➜ Strong demands of DNS privacy against **DNS resolvers**
➜ Novel **DNS-dedicated anonymization schemes** have been proposed (e.g., Oblivious DNS over HTTPS (ODoH, RFC9230), a.k.a. Apple Private Relay)

Such schemes are based on the single-relay approach to hide the clients' origin from the censoring resolver



Observation and Motivation

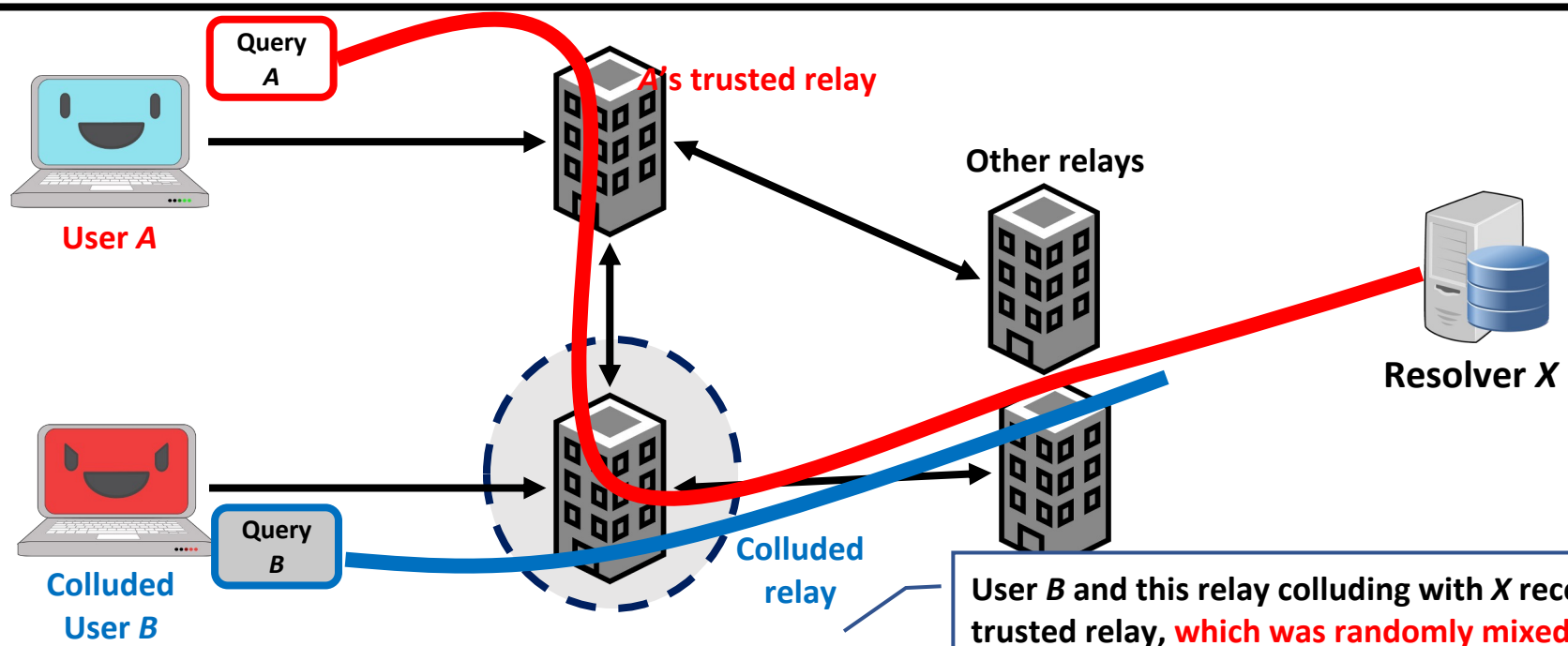
The DNS-dedicated single-relay approach *works fast and maintains UX*, but is easily corrupted when the relay colludes with the target resolver. (In fact, relay nodes and resolvers typically run by just few big techs.)
➜ Our aims are to **design a novel collusion-resistant DNS anonymization scheme**, and to **prove the scheme still maintains UX** in terms of its response speed.

Approach: The Mix-Net

To those ends, we have proposed **multiple-relay-allowed anonymization scheme, µODNS (Mutualized Oblivious DNS), taking an approach of *Mix-Net*** :

- Each relay node ***mixes*** incoming query packets to hide their origins, where origins = **not only clients *but also other relays***
- **Each Client randomly chose the path and # of relays (> 0)**, but the first hop is supposed to be always trusted for the client.

➜ Attacker nodes cannot deterministically distinguish origins of query packets since **observed queries are mixed ones that traveled through random path of random length.**



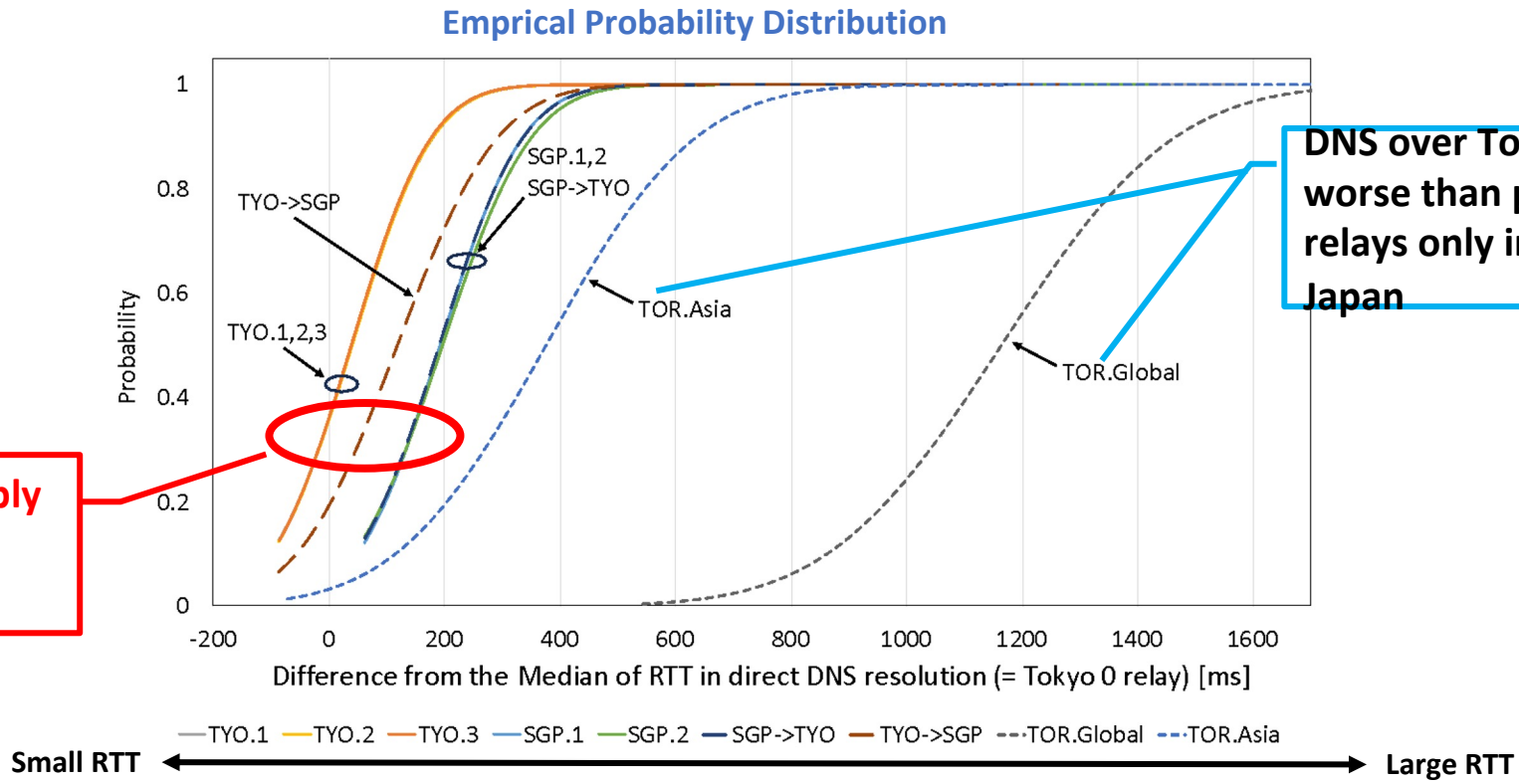
User *B* and this relay colluding with *X* receive encrypted queries from A's trusted relay, which was randomly mixed with ones from User *A* and other users. (Moreover, those may NOT include queries generated by User *A*)

Contribution: Design and Implementation

- **Designed the µODNS over HTTPS (µODoH)** by extending the spec of Oblivious DNS over HTTPS (ODoH) with Mix-Net approach, and **showed its probabilistic anonymity in the presence of colluded nodes.**
- **Released µODoH open source software**, and currently **running a testbed** by connecting several organizations.

Contribution: Performance Evaluation on the Testbed

Over the testbed, we have evaluated the performance of µODNS over HTTPS (µODoH) in terms of the round-trip time (RTT) for DNS query-response, compared with the single-relay ODoH and DNS over Tor ➜ UX still maintains!



µODNS performs comparably with the single-relay ODoH with any relay location.

DNS over Tor performs much worse than µODNS even with relays only in nearby or inside Japan

- J. Kurihara, T. Tanaka and T. Kubo, "µODNS: A Distributed Approach to DNS Anonymization with Collusion Resistance," Computer Networks, Elsevier, vol. 237, p. 110078, Dec. 2023.

Future and On-Going Works for Faster Anonymized DNS

- Design and implementation of a new anonymized protocol with no relay
- New DNS message compression and aggregation technique µODoH's on the encryption layer

- K. Nakano, J. Kurihara and T. Tanaka, "Extensive Study on the Security of Private Information Delivery from Coded Storage," to appear in IEICE Trans. Fundamentals, Mar. 2026.
- R. Aoshima, J. Kurihara and T. Tanaka, "Aggregable Generalized Deduplication," in Proc. ISITA 2024, Nov. 2024.

Close Collaboration Between US and Japan

Yearly project meetings hosted at UC Riverside (Aug 2025, March 2024, Jan 2023)

Weekly online meetings with PIs and students

Valuable exchanges of technical knowledge, close collaboration on posters, conference and journal papers

Dissemination of Project Achievements: Summary

- Publications so far:
  1. Toru Hasegawa, Yuki Koizumi, Junji Takemasa, Jun Kurihara, Timothy Wood, and K. K. Ramakrishnan. “Leveraging Heterogeneous Programmable Data Planes for Security and Privacy of Cellular Networks, 5G & Beyond” IEICE Transactions, 2025.
  2. Cuidi Wei, Shaoyu Tu, Toru Hasegawa, Yuki Koizumi, K. K. Ramakrishnan, Junji Takemasa, and Timothy Wood. “Envisioning a Unified Programmable Dataplane to Monitor Slow Attacks.” IEEE ICNP Workshop Intelligent Classification of High-Speed Network Traffic, 2024.
  3. Yutaro Yoshinaka, Mio Kochiyama, Yuki Koizumi, Junji Takemasa, Toru Hasegawa, “A lightweight anonymity protocol at terabit speeds on programmable switches,” Elsevier Computer Networks, 2024.
  4. Yutaro Yoshinaka, Kanta Tamura, Mio Kochiyama, Yuki Koizumi, Junji Takemasa, Toru Hasegawa, “Toward Terabit-Scale Anonymous Communication Leveraging Programmable Switches,” SC2024 Network Research Exhibition, Nov. 2024.
  5. Kanta Tamura, Yuki Koizumi, Junji Takemasa, and Toru Hasegawa, “Poster: Toward an Optimal Implementation of ChaCha20-Poly1305 for SmartNICs,” IEEE ICNP Poster, Oct. 2024.
  6. Cuidi Wei, Shaoyu Tu, Toru Hasegawa, Yuki Koizumi, K. K. Ramakrishnan, Junji Takemasa, and Timothy Wood. “Poster: A Fast Monitor for Slow Network Attacks.” In 2024 IEEE Cloud Summit, 153–56. Washington, DC, USA: IEEE, 2024. https://doi.org/10.1109/Cloud-Summit61220.2024.00032.
  7. Jun Kurihara, Toshiaki Tanaka and Takeshi Kubo, “µODNS: A Distributed Approach to DNS Anonymization with Collusion Resistance,” Computer Networks, Elsevier, vol. 237, p. 110078, Dec. 2023.
  8. Kentaro Kita, Junji Takemasa, Yuki Koizumi, Toru Hasegawa, “Secure Middlebox Channel over TLS and its Resiliency against Middlebox Compromise,” in Proceedings of IEEE INFOCOM 2023, May 2023.
  9. Cuidi Wei, Ahan Kak, Nakjung Choi, and Timothy Wood, “Towards a Scalable 5G RAN Central Unit,” in Proceedings IEEE INFOCOM 2023 Workshop on Next-generation Open and Programmable Radio Access Networks (NG-OPERA), May 2023
  10. Ryu Watanabe, Ayumu Kubota, and Jun Kurihara, "Application of Generalized Deduplication Techniques in Edge Computing Environments," to Appear in Proceedings of AINA 2023 (M2EC-2023), Juiz de Fora, Brazil, Mar. 2023.
  11. Yutaro Yoshinaka, Junji Takemasa, Yuki Koizumi, Toru Hasegawa, “Design and analysis of lightweight anonymity protocol for host- and AS-level anonymity ,” Computer Networks, Volume 222, 109559-109559, Feb. 2023.
  12. S. Panda, K. K. Ramakrishnan and L. N. Bhuyan, "Synergy: A SmartNIC Accelerated 5G Dataplane and Monitor for Mobility Prediction," 2022 IEEE 30th International Conference on Network Protocols (ICNP), Lexington, KY, USA, 2022.