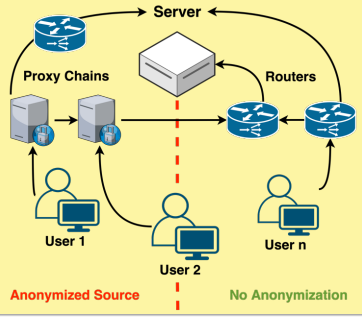
Real-Time Flow Correlation Attacks with P4: A Distributed Approach for Tracking Malicious Users

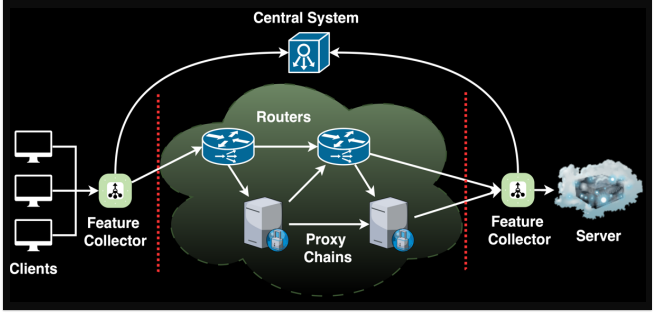
1. Anonymization Networks

Proxy Chains and Anonymity networks (such as Tor) enhance user privacy by routing traffic through multiple nodes, masking the true source of communication.



2. Correlation Attacks

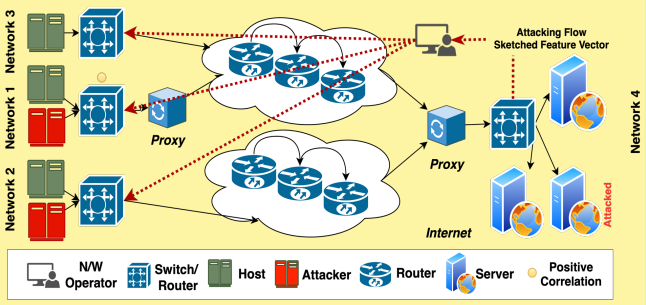
- Correlation attacks observe traffic at multiple network vantage points.
- They match patterns like packet timing, size, and flow direction.
- This allows attackers to link anonymized flows and uncover user identities.
- All flows are correlated on a central system.



3. Challenges in Existing Work

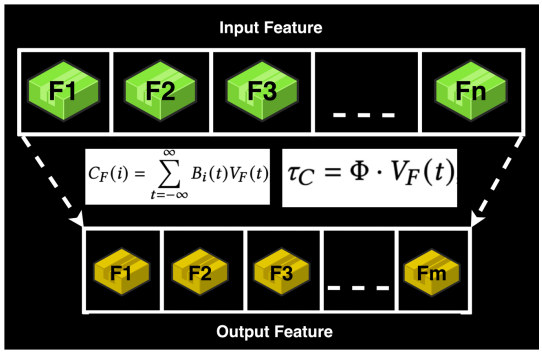
- Centralized systems can perform 1 × *n* correlation, across the network, but they require high memory and computational power to store and analyze all flow data, posing issues in real-time correlation.
- Need: A distributed framework that offloads these computationally intensive tasks across multiple devices.
- **Solution:** Utilize P4 switches as edge devices which allows each switch to handle a portion of the 1 × *n* correlation as 1 × *n/y* tasks (y = total switches).

Proposed Topology



4. Distributed Correlation Attack

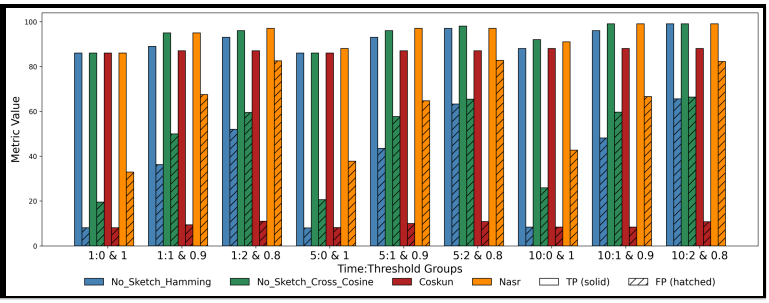
- **Decentralized Correlation:** P4 switches perform real-time correlation without a central processor.
- **Dynamic Flow Tracking:** Each switch extracts the flow's 5-tuple and updates its table in real-time at line rate.
- **Efficient Sketching:** Compress the full packet count vector V=[v1,v2,…,vn], into a smaller vector F=[f1,f2,…,fm] (with m≪n; In this work n=100 & m=5).
- **Local Similarity Computation:** The target's sketched vector is distributed to all switches (by the Controller), which then locally compute similarity metrics to correlate flows.



5. Evaluation

Coskun [1] : Achieves the same TP/FP as no-sketching with lower memory, optimal at time threshold 1 and Hamming threshold 0.

Nasr [2] : Yields high TP rates but with increased false positives.



UNIVERSITY OF WATERLOO

Gurjot Singh
g86singh@uwaterloo.ca

[1] – › Coskun, B. and Memon, N., 2009, December. Online sketching of network flows for real-time stepping-stone detection. In *2009 Annual Computer Security Applications Conference* (pp. 473–483). IEEE.

[2] –› Nasr, M., Houmansadr, A. and Mazumdar, A., 2017, October. Compressive traffic analysis: A new paradigm for scalable traffic analysis. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2053–2069).