Software-Defined Adversarial Trajectory Sampling

Kashyap Thimmaraju[1] **Liron Schiff**[2] **Stefan Schmid**[1,3]

kash@fgsect.de schiffli@guardicore.com schmiste@cs.aau.dk

[1] TU Berlin, Germany [2] GuardiCore Labs, Israel [3] Aalborg University, Denmark

Routing Attacks in an Adversarial Network

- **Denial-of-service:** It can drop transit packets.
- **Mirroring:** It can duplicate a packet, and e.g., send one to the correct and one to an incorrect port.
- **Rerouting:** It can forward a packet to the wrong port (e.g., breaking logical isolations).
- **Man-in-the-middle:** It can delete packets, generate new packets, or modify the header or payload of packets (e.g., change VLAN tags to break isolation domains).
- **Injection:** It can inject malformed packets to attack an internal server (an insider attack).

In fact, those attacks can be represented by two primitives: **Drop**, and **Inject**.

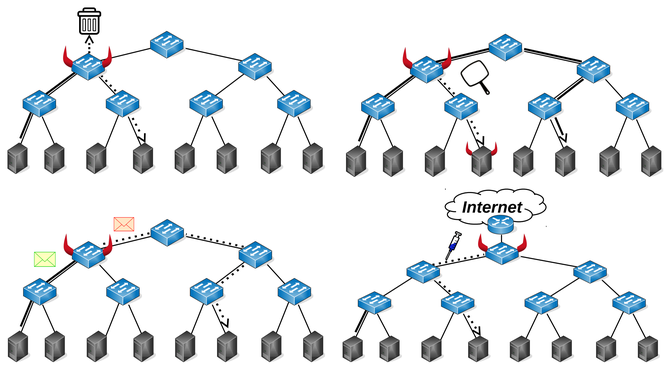

Fig. 1: An overview of possible routing attacks.

Acknowledgement

This research was supported by the Helmholtz Research School on Security Technologies, the Danish Villum foundation project *ReNet*, and in part by the German Federal Office for Information Security.

Adversarial Trajectory Sampling and SDN

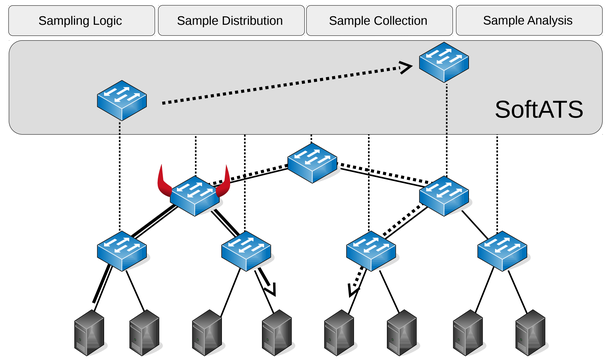

Fig. 2: An overview of SoftATS.

- Sample the same packets across the network, report it to a **centralized** server, and reconstruct the "**trajectory**" [1].
- Sample **different packets**, with **pairs of switches** sampling the same packet [2] (see Fig. 3).
- Sample packets based on their **payload** or **header**, e.g., TCP/UDP checksum, and report **entire** packets.
- **SDN** is an ideal environment to implement **Software-defined Adversarial Trajectory Sampling** (SoftATS).

	B1	B2	A1	A2	X	Y
B1		100	200	300	700	50
B2	100		500	150	400	150
A1	200	500		600	70	400
A2	300	150	600		350	650
X	700	400	70	350		100
Y	50	150	400	650	100	

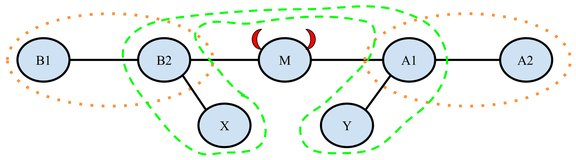

Fig. 3: An example of pair assignments in SoftATS.

∼1000 Packets Suffice To Detect Routing Attacks

- In a **Clos** topology with $k = 4$, *SoftATS* is able to detect drop, and inject attacks, within 1100 packets on average.
- Doubling the **sampling ratio improves** the detection, roughly linearly.
- The **position of the attacker** influences the detection.
- The **attacker's strategy** affects the detection.

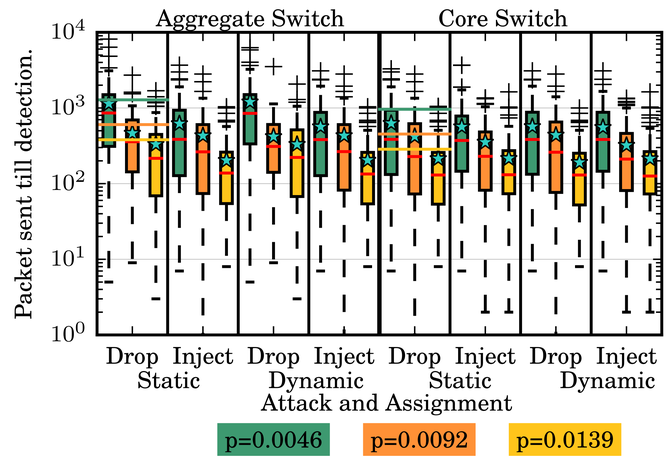

Fig. 4: No. of packets required to detect **drop** and **inject** attacks using SoftATS.

References

[1] N. G. Duffield and M. Grossglauser. Trajectory sampling for direct traffic observation. *IEEE/ACM Trans. Networking (TON)*, 9(3):280–292, June 2001.

[2] S. Lee, T. Wong, and H. S. Kim. Secure split assignment trajectory sampling: A malicious router detection system. In *Proc. IEEE/IFIP Transactions on Dependable and Secure Computing (DSN)*, pages 333–342, 2006.