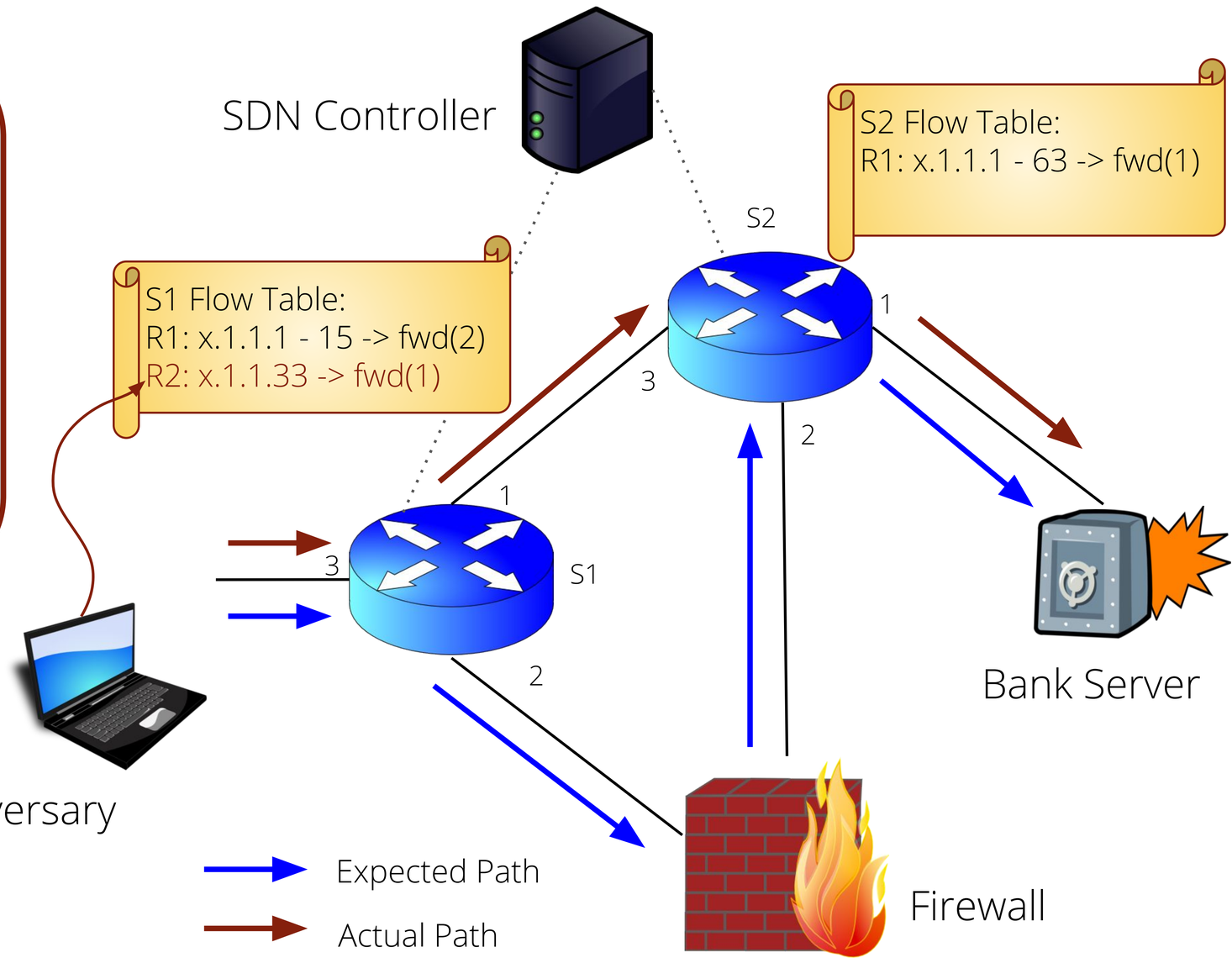
Towards Meticulous Data Plane Monitoring

Apoorv Shukla, Said Jawad Saidi, Stefan Schmid, Marco Canini and Anja Feldmann

Problem: In SDN, a controller may not have a consistent view of the data plane leading to:

- Unexpected or wrong paths taken on data plane
- Unexpected or wrong rules matched on data plane



Causes: Hardware failures
Hardware/software bugs
Attacks
Misconfigurations

Consequences: Security compromise as malicious traffic can attack the network
Critical traffic can be diverted from the expected path

The above figure depicts a SDN scenario where data plane is inconsistent with control plane. An adversary through the switch interface (e.g., ovs-ofctl) inserts a flow rule R2 and thus, not in the knowledge of controller. The flow rule R2 diverts the malicious traffic pertaining to x.1.1.33 on the data plane to bypass the firewall. It is important to note that this rule insertion could be an unintentional misconfiguration from the network administrator.

Current Tools: In SDN, control plane tools are insufficient as control plane is not in sync with the data plane
The data plane tools which rely on tagging do a path-level verification and active probe-generation do a rule-level generation

Limitations: Insufficient or unavailable space in the packet
Active probes or test packets are not representative of production traffic

Solution Space: Dedicated header space for tagging
Tags encoding rule-level and path-level information
Analysis by comparison of control and data plane related information

Literature: [1] Narayana, Srinivas, et al. "Compiling path queries." *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX Association, 2016.
[2] Zhang, Peng, et al. "Mind the Gap: Monitoring the Control-Data Plane Consistency in Software Defined Networks." *Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies*. ACM, 2016.
[3] Perešíni, Peter, et al. "Monocle: Dynamic, fine-grained data plane monitoring." *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*. ACM, 2015.

Contact: Apoorv Shukla (apoorv@inet.tu-berlin.de)

Acknowledgements: This work was supported by Leibniz Prize project funds of DFG - German Research Foundation: Gottfried Wilhelm Leibniz-Preis 2011 (FKZFE 570/4-1) and Danish Villum project ReNet.