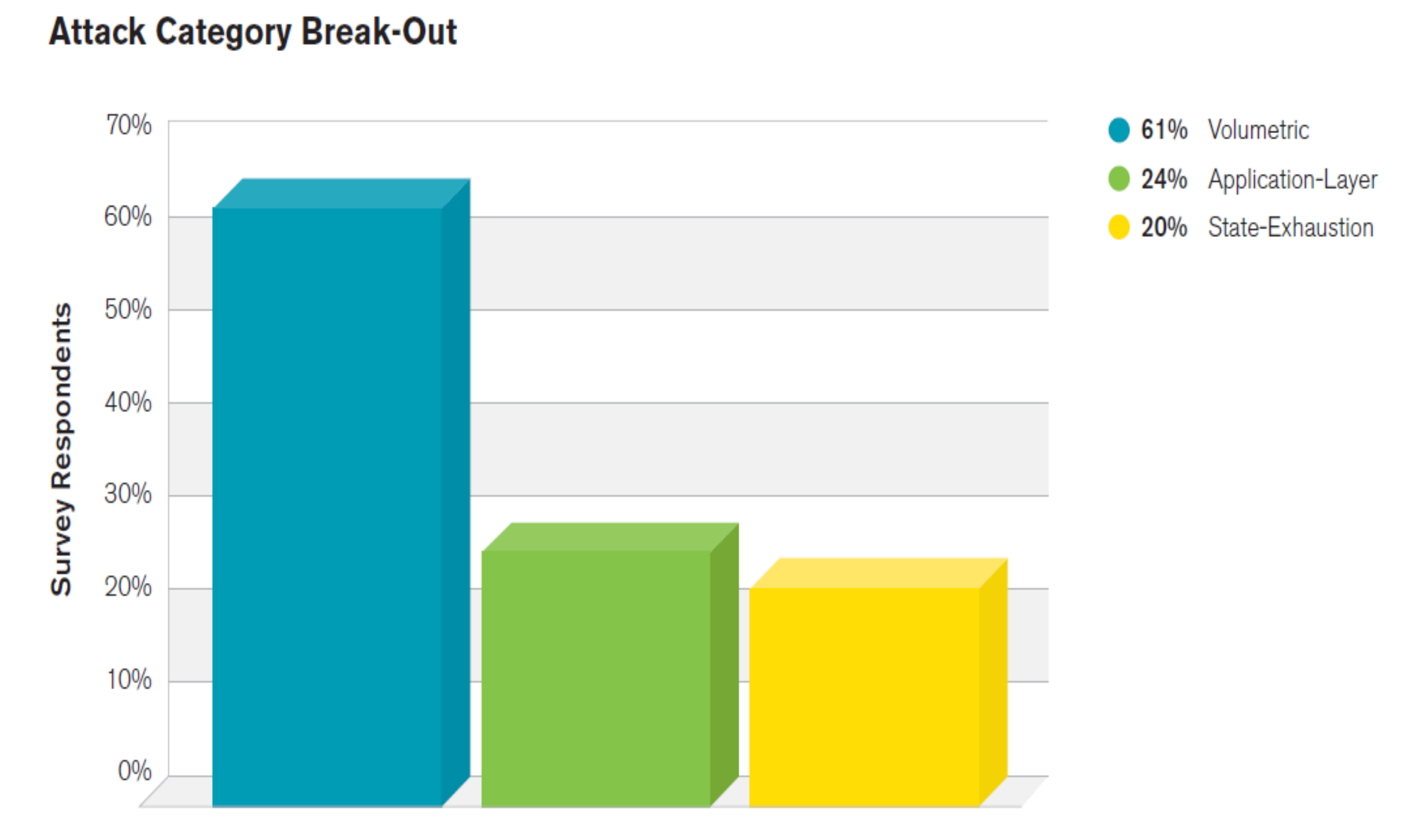
Towards Autonomic DDoS Mitigation using Software-Defined Networking

Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, Hervé Debar

Télécom SudParis, Institut Mines-Télécom

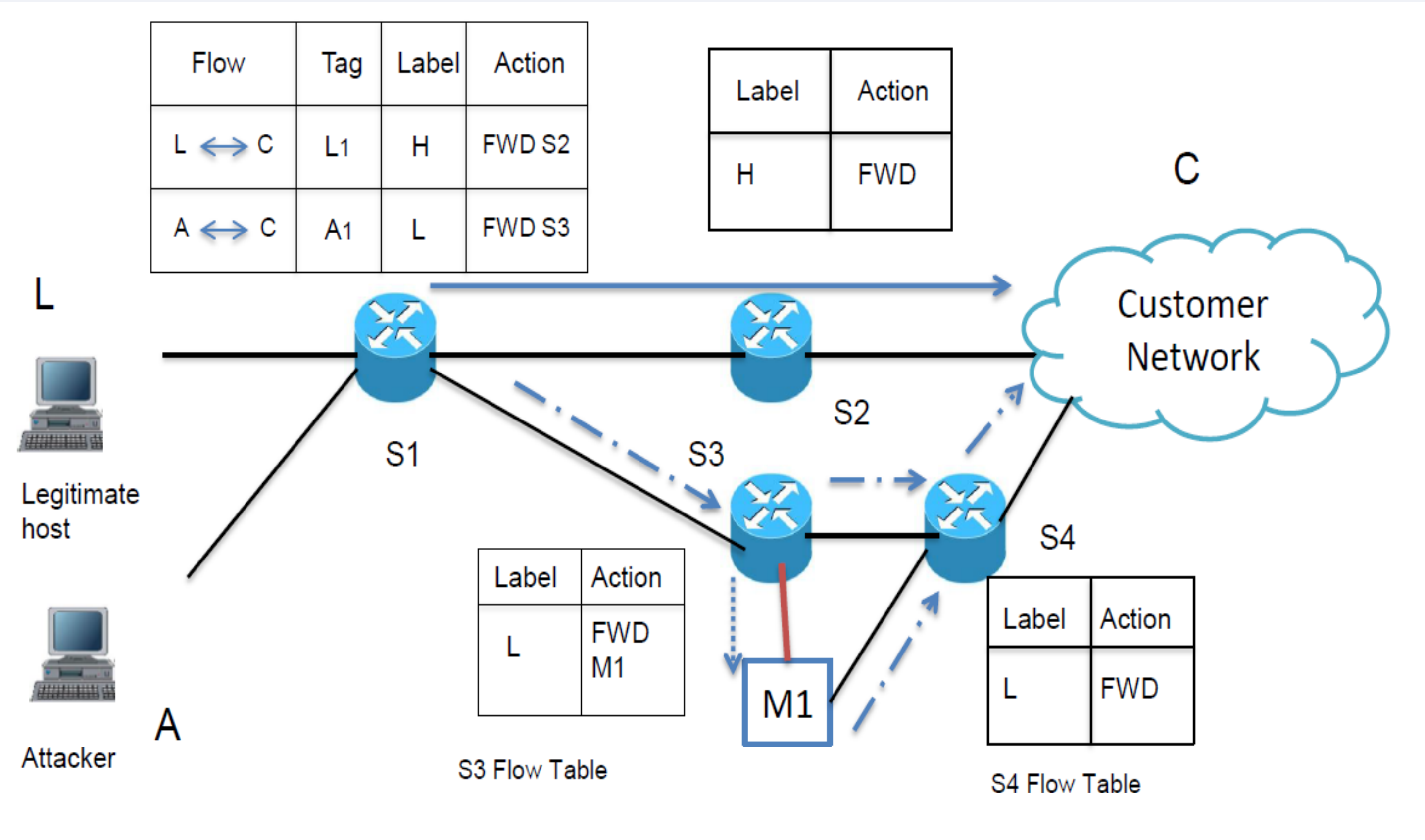
Problem



Motivation

	Self-configuration	Self-optimization	Self-healing	Self-protection
Capability-based DDoS technique	×	√	×	√
Congestion based technique	×	√	×	√
Packet marking	×	√	×	√
Stateful policy technique	×	√	√	√

Use Case



Flow	Tag	Label	Action
L ↔ C	L1	H	FWD S2
A ↔ C	A1	L	FWD S3

Label	Action
H	FWD

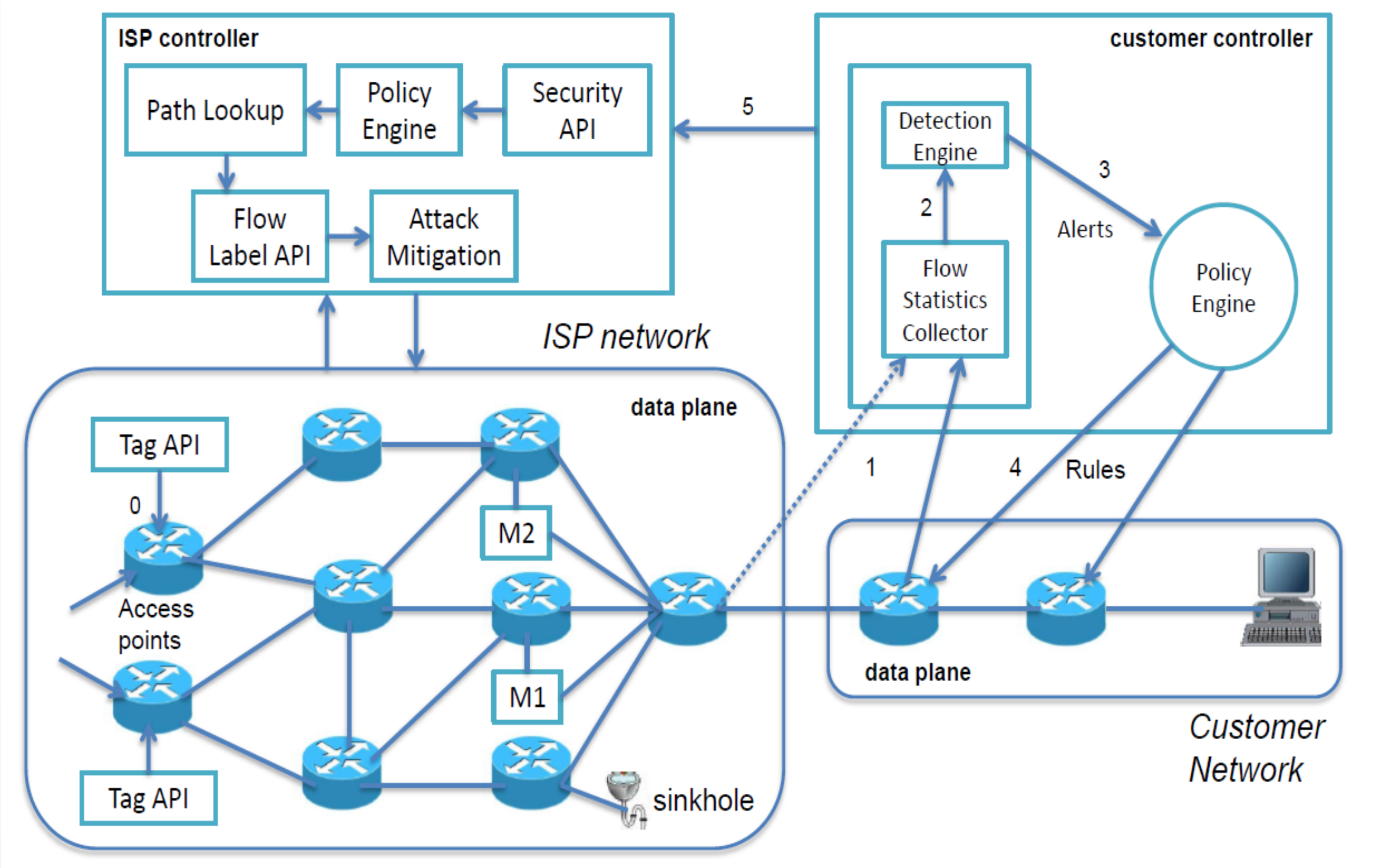
S3 Flow Table

Label	Action
L	FWD M1

S4 Flow Table

Label	Action
L	FWD

Proposal



Framework is built on the following assumptions:

- ➢ Security API is provided by the ISP
- ➢ DDoS detection module is running in the customer network

Conclusion

Self management properties make it possible to achieve autonomic DDoS mitigation:

- ➢ SDN controller's end-to-end visibility allows to optimize the deployment of middleboxes
- ➢ Tags and labels allow for achieving fast, flexible and consistent packet switching
- ➢ Migrating the tagging function to the access switches can reduce the processing overhead of the SDN controller

References

- *Worldwide Infrastructure Security Report*, Arbor Special Report, 2014.
- R. Sahay, G. Blanc, Z. Zhang, H. Debar: *Towards Autonomic DDoS Mitigation using Software Defined-Networking*, accepted at the NDSS Workshop on Security of Emerging Networking Technologies, 2015.
- J.Li: *DrawBridge: Software-defined DDoS-resistant Traffic Engineering*, 2014 ACM Conference on SIGCOMM. ACM, 2014.
- R. Braga, E. Mota, A. Passito: *Lightweight DDoS flooding attack detection using NOX/OpenFlow*, 35th IEEE Conference on Local Computer Networks (LCN), Oct 2010.

Rishikesh Sahay
rishikesh.sahay@telecom-sudparis.eu

NECOMA