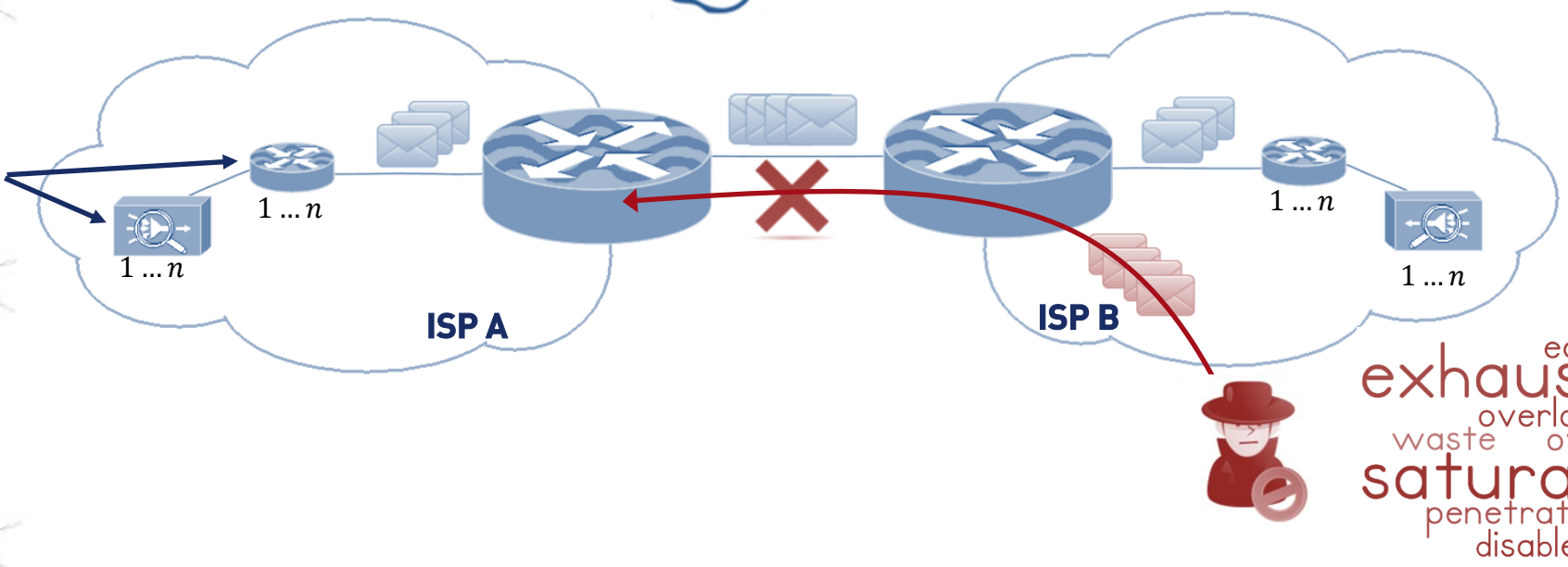
Real-time DDoS Defense

A Collaborative Approach

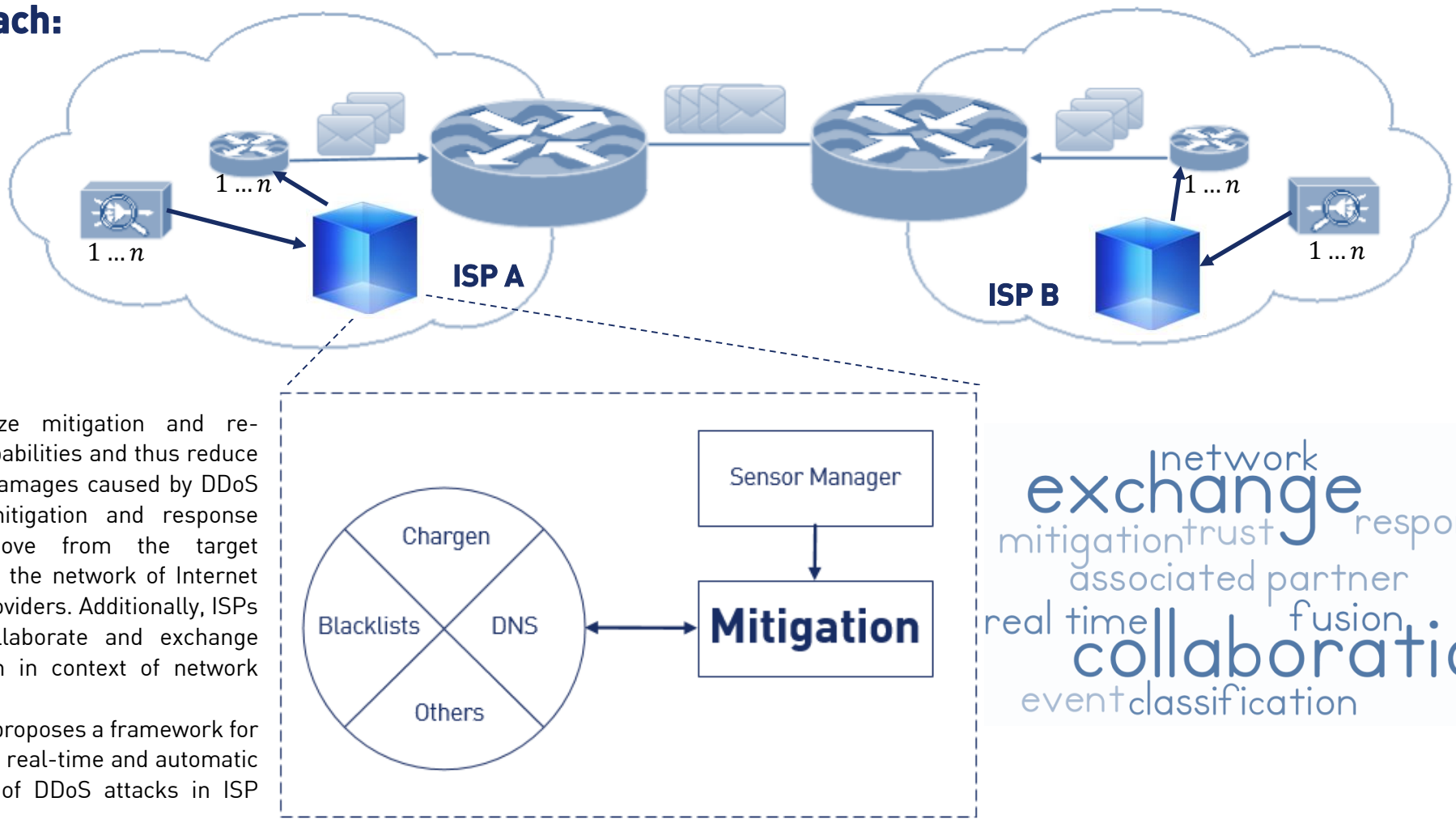
Problem:
What happens, if 400 Gbps are reaching  **network?** [1][2]



Research Questions:

1. Is real-time and automatic mitigation at ISP level performed and if yes, how?
2. How can the effect of DDoS attack be limited?
3. How can the framework for real-time and automatic mitigation be validated?

Approach:



To optimize mitigation and response capabilities and thus reduce potential damages caused by DDoS attacks, mitigation and response should move from the target network to the network of Internet Service Providers. Additionally, ISPs should collaborate and exchange information in context of network security.
This work proposes a framework for flow-based real-time and automatic mitigation of DDoS attacks in ISP networks.

[1] Anstee, D., Bussiere, D., Sockrider, G., Morales, C.: Worldwide Infrastructure Security Report. Technical Report IX, Arbor Networks Inc. (January 2013) http://www.arbornetworks.com/research/infrastructure-security-report.
[2] Prince, M. Technical Details behind a 400 Gbps NTP Amplification DDoS attack (February 2014) http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

The work has been funded by the German Federal Ministry of Education and Research #16BY1201F, CASED and by EU FP7 Flamingo (ICT-318488).

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

UNIVERSITEIT TWENTE. CASED

Contact
Jessica Steinberger[1,2]
Anna Sperotto[2]
Aiko Pras[2]
Harald Baier[1]

[1]da/sec – Biometrics and Internet Security Research Group,
University of Applied Sciences Darmstadt, Darmstadt, Germany
{Jessica.Steinberger, Harald Baier}@h-da.de

[2]Design and Analysis of Communication Systems (DACS)
University of Twente
Enschede, The Netherlands
{J.Steinberger, A.Sperotto, A.Pras}@utwente.nl