Enriching IDS events using traffic monitoring data

Ralph Koning
Universiteit van Amsterdam

Nick Buraglio (ESnet), Paola Grosso (UvA), Cees de Laat (UvA)

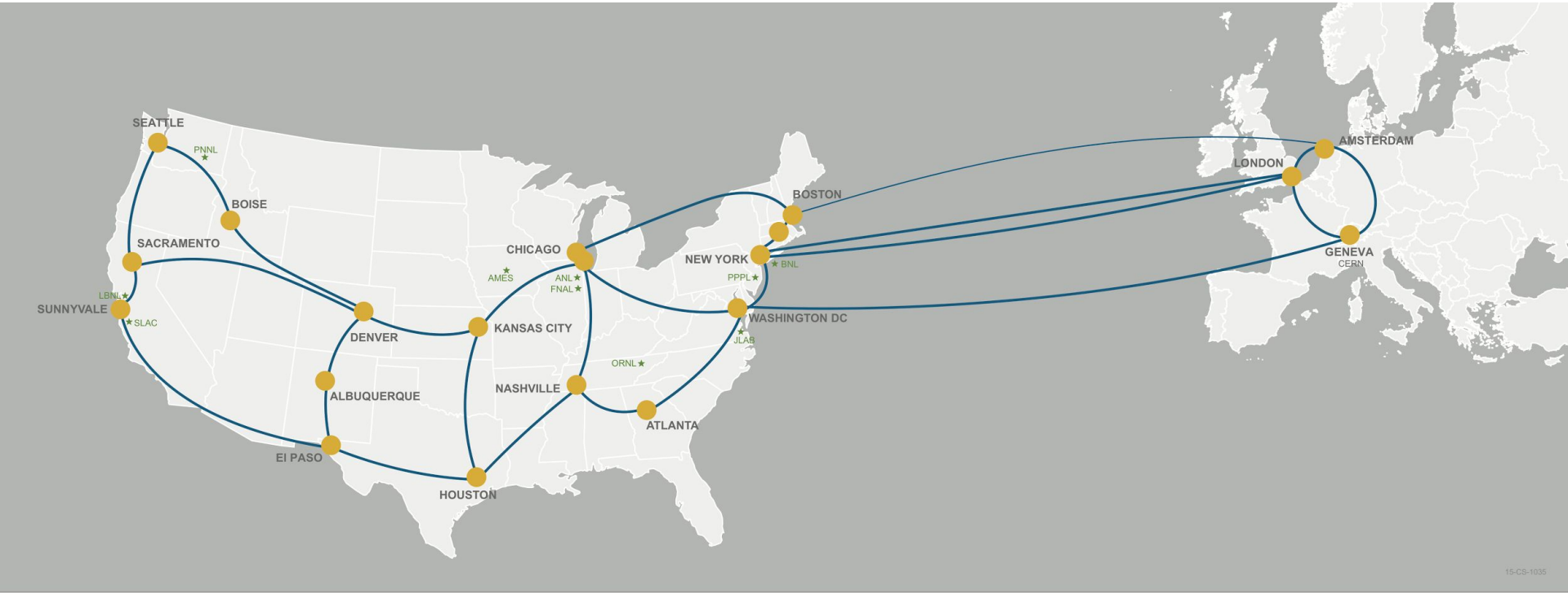
Motivation

To effectively block attacks, the information from an IDS is not always sufficient.

When an event triggers, the security team has to manually collect additional data from different sources to enrich the event to create context and understanding of the event

Only then appropriate action can be taken.

ESnet



ESnet
ENERGY SCIENCES NETWORK

★ Department of Energy Office of Science National Labs

Ames	Ames Laboratory (Ames, IA)
ANL	Argonne National Laboratory (Argonne, IL)
BNL	Brookhaven National Laboratory (Upton, NY)
FNAL	Fermi National Accelerator Laboratory (Batavia, IL)
JLAB	Thomas Jefferson National Accelerator Facility (Newport News, VA)
LBNL	Lawrence Berkeley National Laboratory (Berkeley, CA)
ORNL	Oak Ridge National Laboratory (Oak Ridge, TN)
PNNL	Pacific Northwest National Laboratory (Richland, WA)
PPPL	Princeton Plasma Physics Laboratory (Princeton, NJ)
SLAC	SLAC National Accelerator Laboratory (Menlo Park, CA)

Carrier networks are different

Aspect	Enterprise/Campus	Carrier/Transit
network capacity	small: one organization	huge: accommodates many institutions
external connectivity	limited (single or redundant uplink)	many connected networks
application security	security can be tailored to application	need to allow everything
restrictions and policies	can be applied anywhere	subject net neutrality laws
impact of countermeasure	may affect users of a host or system accommodates	can affect many users and other networks

Input sources

Bro

NetFlow

PACKET DESIGN™

Route Explorer

splunk>

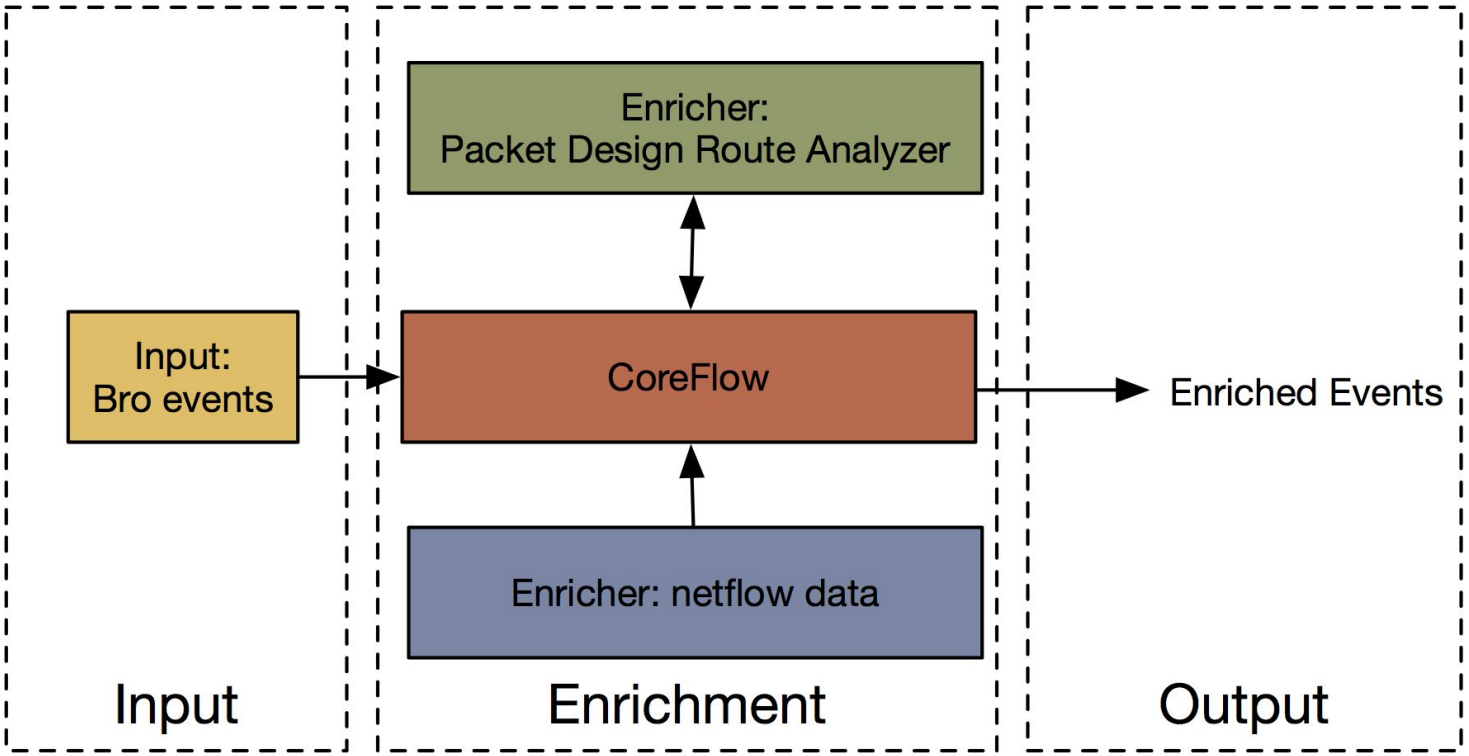
Research questions

Can we correlate data from these different sources?

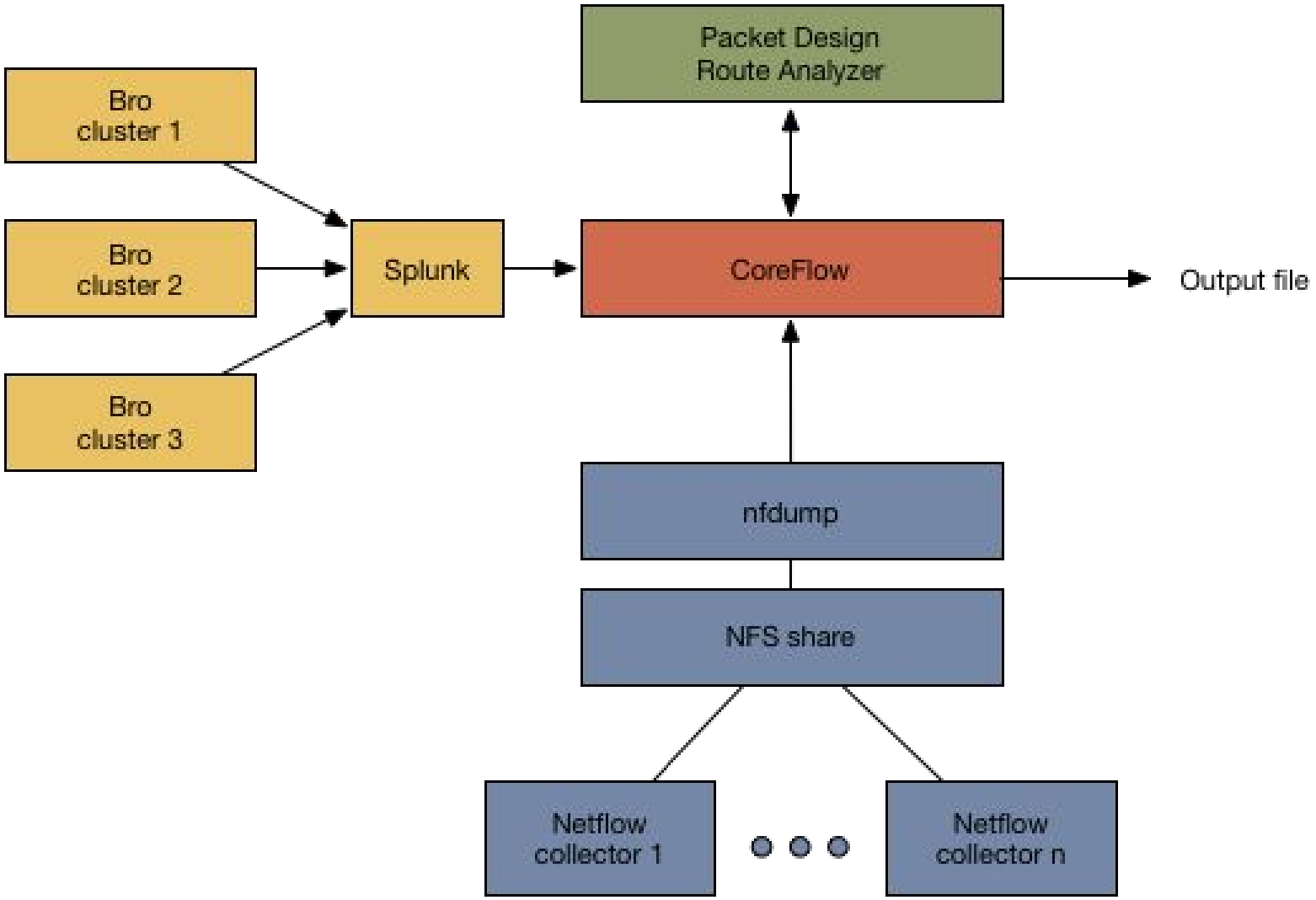
Can we build a poc system that does live correlation of the events on a carrier network?

Do we gain new options and information from enriching the information?

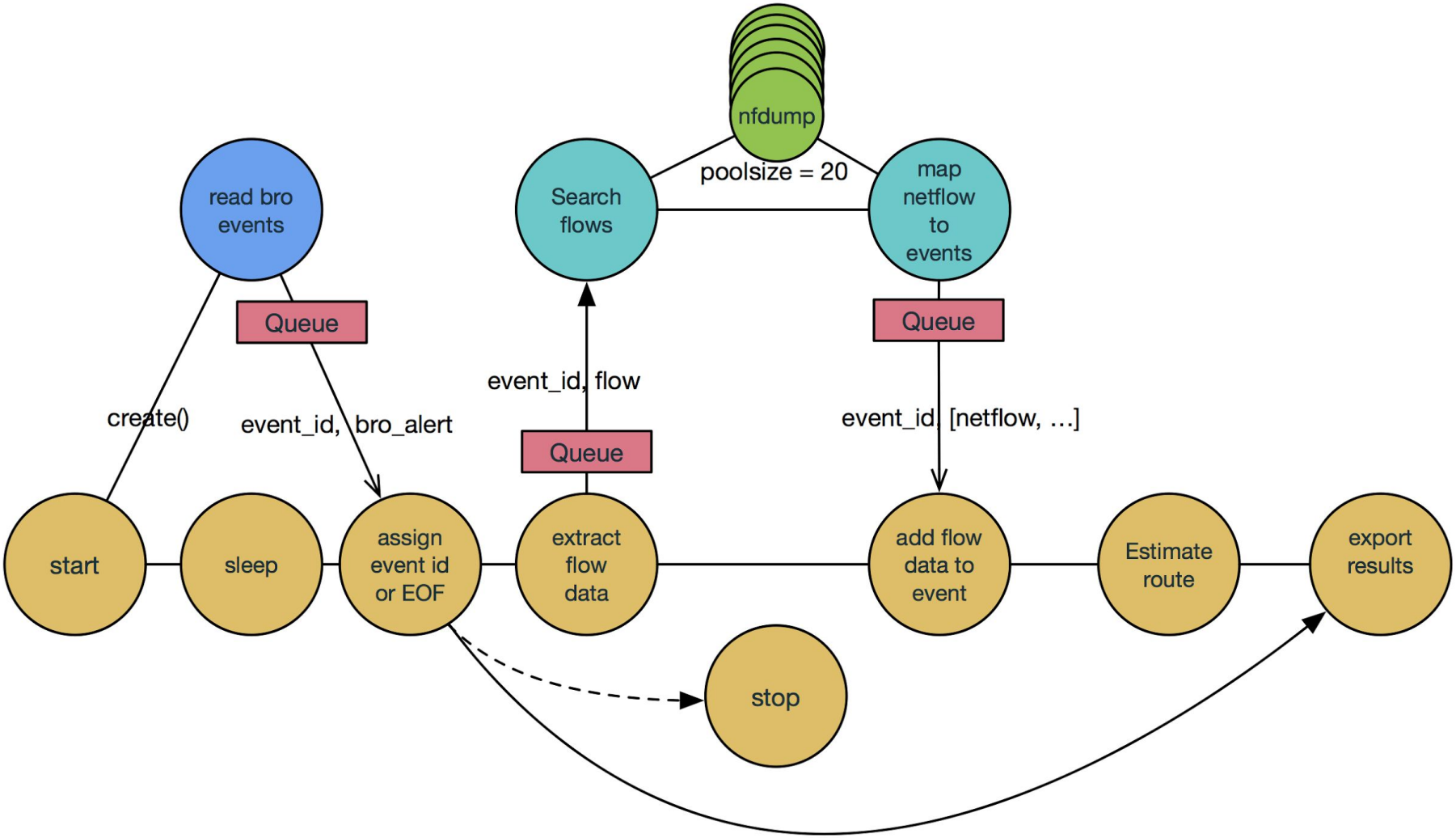
CoreFlow


Enricher:
Packet Design Route Analyzer
Input:
Bro events
CoreFlow
Enriched Events
Enricher: netflow data
Input
Enrichment
Output

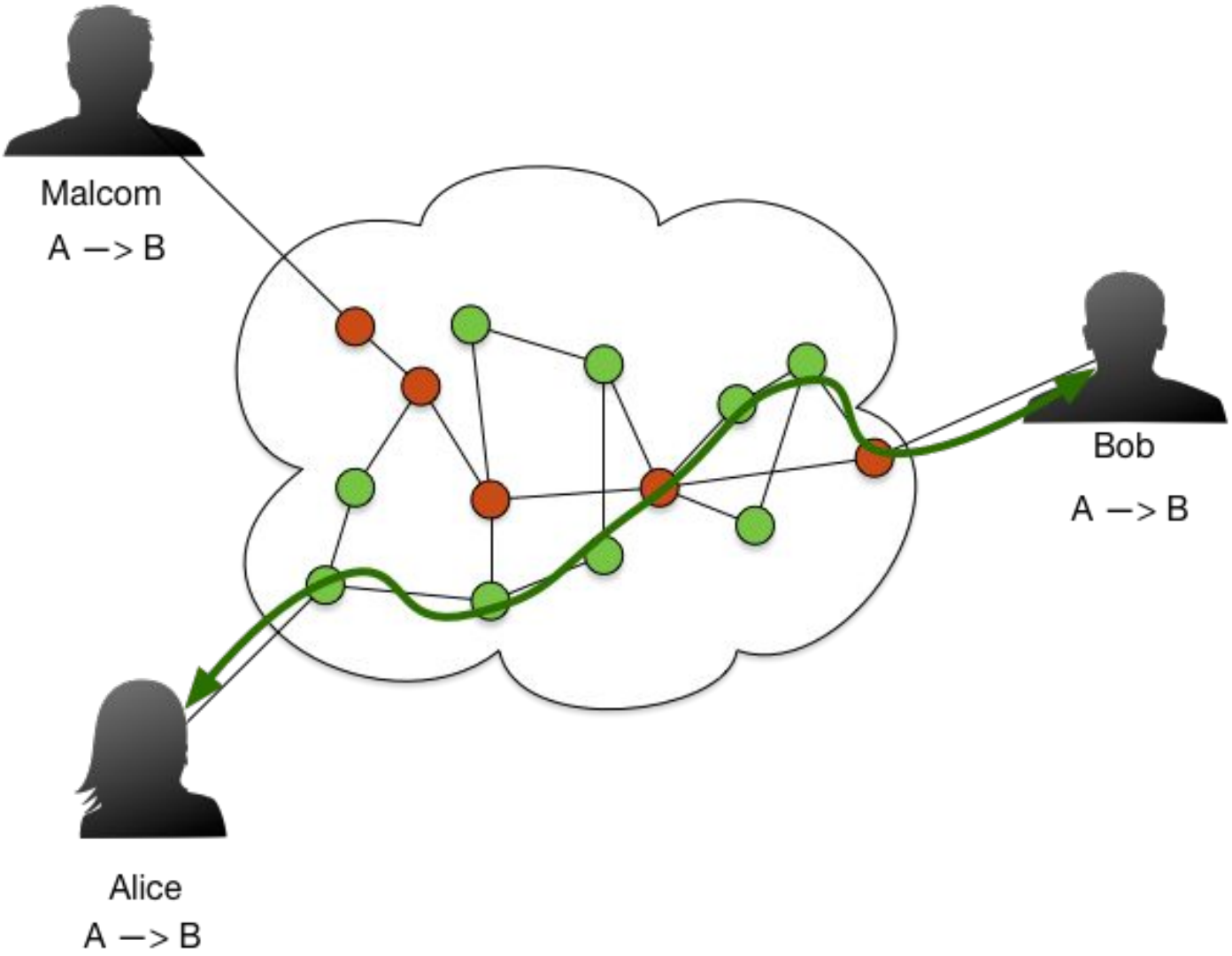
ESnet implementation



CoreFlow execution



Application: traffic spoofing

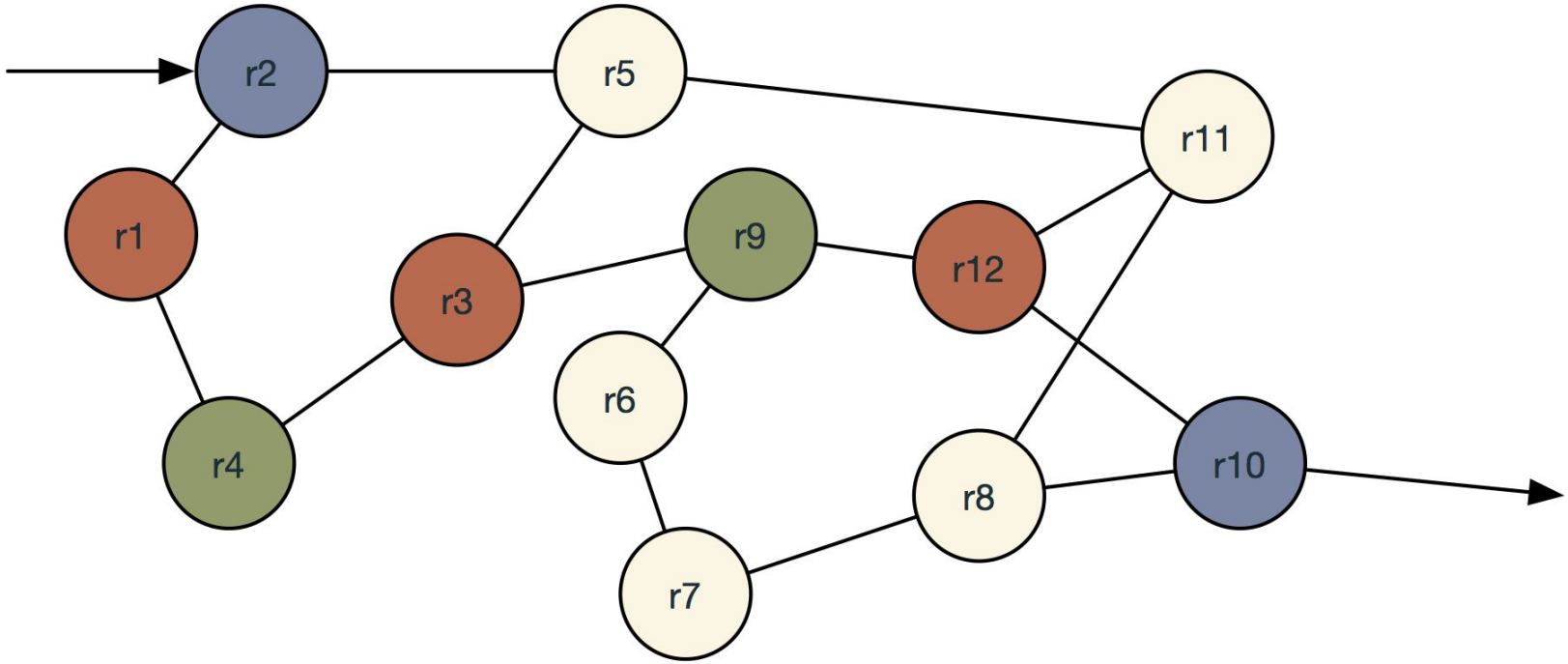


Route Estimation

Algorithm 1 route estimation algorithm

```
1:  topology ← topology graph of the network
2:  depth ← max search depth
3:  D ← detected routers in the path
4:  procedure ESTIMATE_PATH(D)
5:      start ← D[0]
6:      P ← all paths up to depth from start in topology
7:      for each p ∈ P do
8:          R ← add reverse(path)
9:      end for
10:     for each p ∈ P do
11:         for each r ∈ R do
12:             A ← add r + p[1 :])
13:         end for
14:     end for
15:     for each p ∈ A do
16:         if D ⊆ p then
17:             F ← add p
18:         end if
19:     end for
20:     for each p ∈ F do
21:         O ← min(lenght(p))
22:     end for
23:     return O
24: end procedure
```

Route Estimation: Example



Conclusion

Enriching IDS data with NetFlow information gives a better view of an attack.

The enriched information can be used to set up and automate more advanced countermeasures.

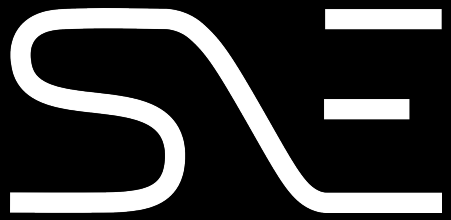
Future work

Aspect	Enterprise/Campus	Carrier/Transit
external connectivity	limited (single or redundant uplink) security can be	many connected networks
application security	tailored to application	need to allow everything
restrictions and policies	can be applied anywhere	subject net neutrality laws
impact of countermeasure	may affect users of a host or system accommodates	can affect many users and other networks
network capacity	one organization	accommodates many institutions

EOF

Contact:

Ralph Koning (UvA / ESnet)
r.koning _at_ uva.nl
https://staff.fnwi.uva.nl/r.koning/



ESnet
ENERGY SCIENCES NETWORK

UNIVERSITY OF AMSTERDAM

ciena

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

COMMIT/

TNO innovation for life

AIR FRANCE KLM