Aalto University
School of Electrical
Engineering

Unwanted Traffic Control Using Global Trust Management

Zheng .Yan; Raimo.Kantola; Yue.Shen @aalto.fi
COMNET @AALTO University

Motivation

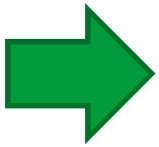
- Firewalls, Virus Protection, Intrusion Detection, Spam Filtering are all *Defensive tools* against Unwanted Traffic
- Senders of (massive amounts of) Unwanted Traffic are professionals who are making money taking advantage of 99,9xx% of the rest of Internet users → there is a whole value chain of grey economy in this area
- We need to *attack* the grey economy and make it unprofitable
- NB:Unwanted = what the receiver says is unwanted → must organise voting on the opinions

Objective: New Incentive Structure

- Tariff of transit, peering and connection = f(Trust value of ISP and Host)
- → ISPs has incentive to invest in protection against unwanted traffic and avoid higher than average tariffs
- → It makes sense for local ISPs to actively sell security service to consumer subscribers, SMEs and larger corporations
- → It makes sense to customers to pay for better security
- → Overall Global Trust Management brings more money into the system: gives additional products for local ISP to sell to willing customers

Related Work

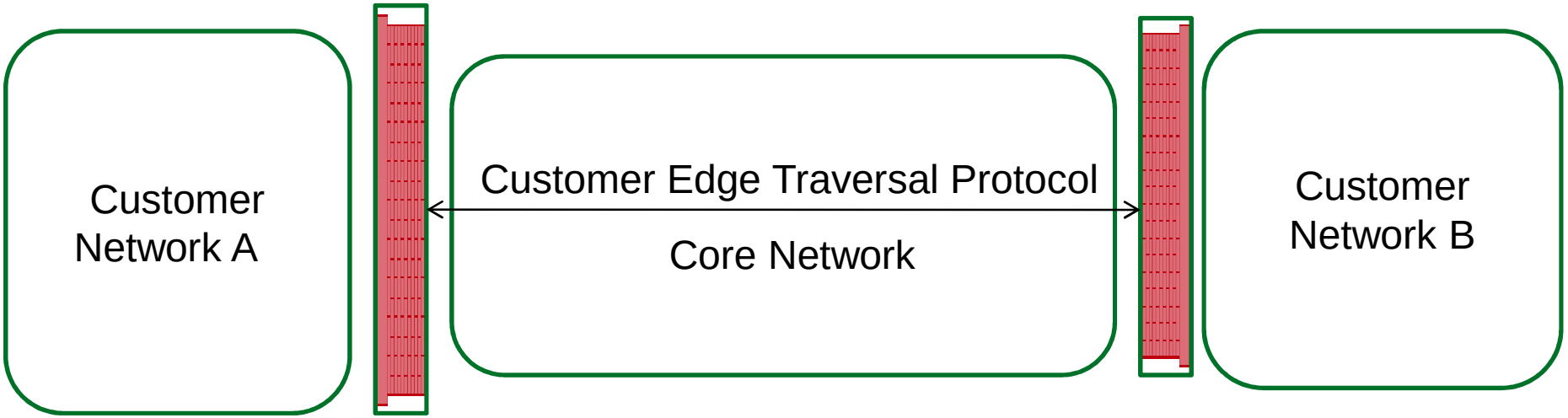
- SPAM filtering
- Whitelisting, blacklisting of sites
- Trust management/distributed reputation system, mainly against Spam
- Defense against SPIT
- Instant messaging: Anti-SPIM based on trust



1. We lack a generic solution against unwanted traffic
2. Incentive structure against unwanted traffic is weak and as a result deployment takes a long time

Edge to Edge Tunneling and Trust Help in Protecting Customer Networks

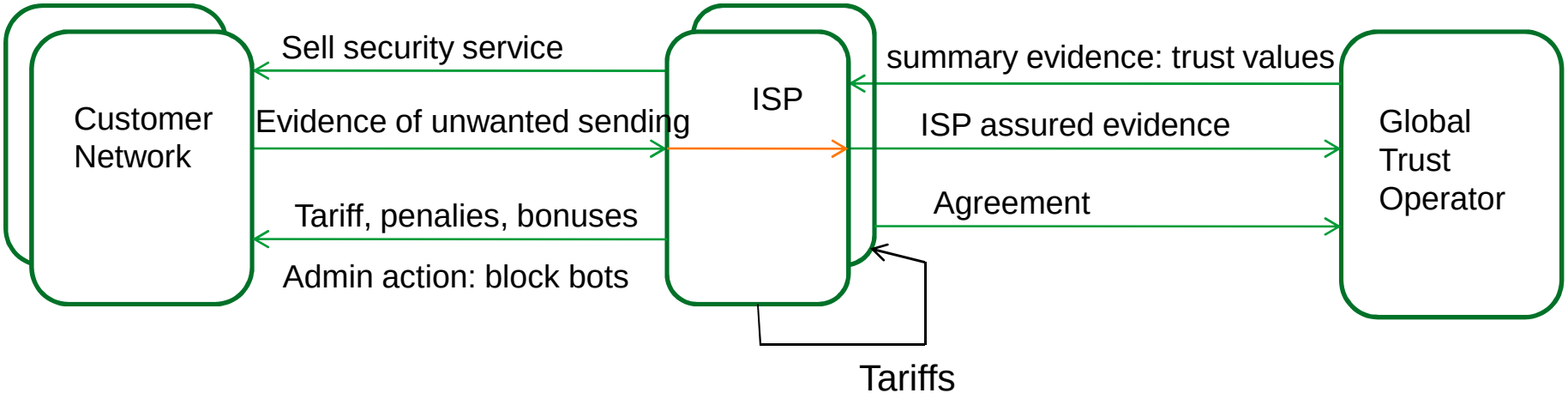
- Build Edge to Edge Trust: design and develop edge to edge trustworthy communications



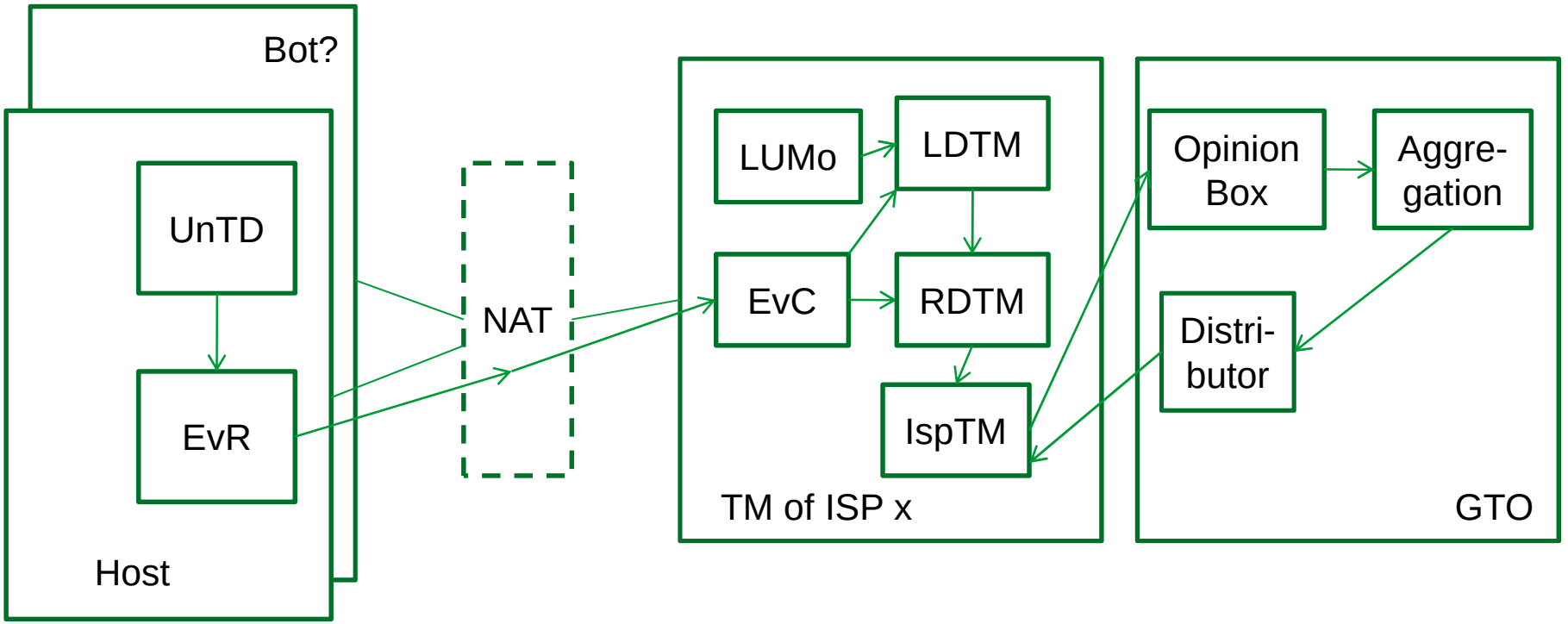
This is defensive also but Customer Edges (FWs) can collaborate before Packet Admission (see www.re2ee.org for more…)
+ Helps in gathering evidence of hostile behavior!

Global Trust Management Makes use of Evidence from FWs, IDS, Host based tools

- Evaluate Trust on ISP/mISP and host, base tariffs on trust value.
- Objective: Turn current unwanted traffic business unprofitable by introducing a new payoff model



System Model - Study of Trust Dynamics



UnTD – Unwanted Traffic Detector
EvR – Evidence Reporting
EvC – Evicence Collector
LDTM – Local Destination Trust Manager
RDTM – Remote Destination Trust Manager
LUMo – Local User Monitor
IspTM – ISP Trust Manager

Because of NATs, hosts and also bots can not always directly be identified by source address.
IP address prefix can be mapped to an ISP
Roaming users visit foreign networks, a bot can also roam while using an address obtained from the visited network

Constraints of Global Trust Management

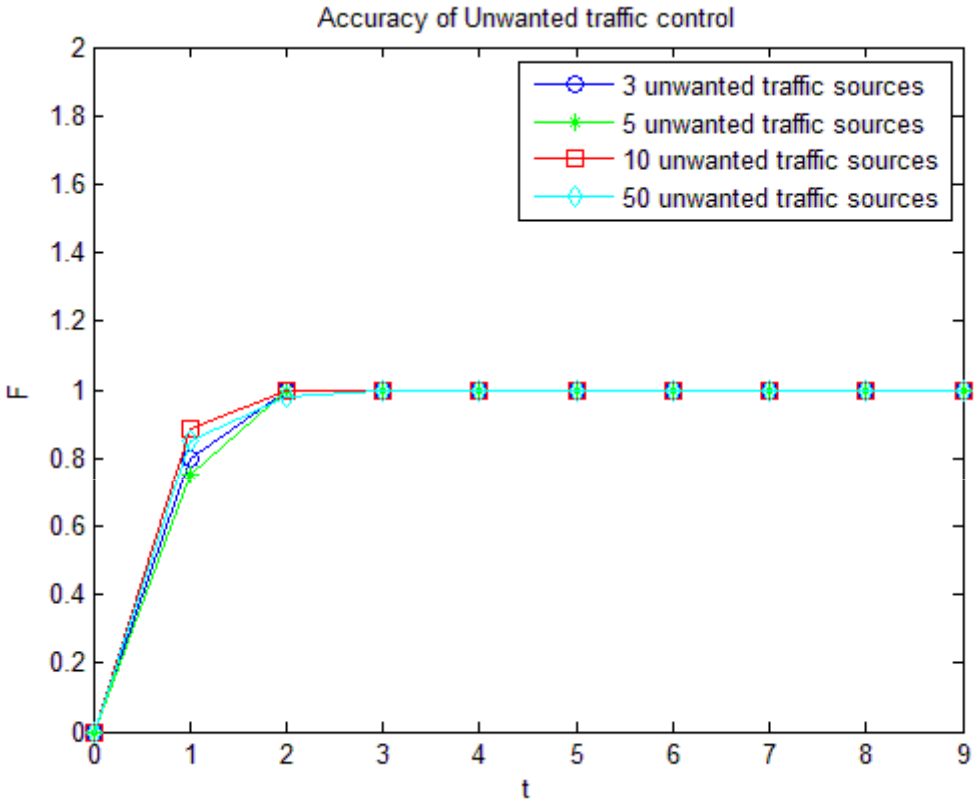
- In this paper we assume that source of attack can be identified, but
  - DDoS attack type traffic → source address can be spoofed
  - Other types of Unwanted traffic: source address is genuine → we are interested in locating front line bot machines that are under the command of the real attacker
  - In Reflector attack, Front line of the attack is just following a protocol but has not been compromised: query comes with a spoofed address of the victim
- ISP based monitoring tools may be used to trace the attack from front line bots back to the command bot
  - (out of scope in this paper)

Role of the Local ISP

- Final decision how to act on the source host (make it pay/block its traffic until the problem is fixed etc) lies with the serving/local ISP
- Only the local ISP sees all the traffic to/from a host that is taking part in generating Unwanted Traffic → local monitoring makes best sense (it is also possible to validate evidence coming from local subscriber using ISP monitoring devices)
- We assume: Local ISP is willing to send evidence of bad behavior of other ISP's customers → lowers its own relative tariffs
- Local ISP may choose to hide compromising evidence of its own customers → GTO must increase ISPs trust when the ISP reveals bots from its own network

Simulation experiments

- Accuracy in case of different share of independent unwanted traffic sources
- Efficiency in case of different infection rates of the victims
- Robustness against attacks on trust management
  - Hide evidence attack
  - Bad mouthing attack
  - (have also done on/off hide evidence but not in the paper)



$$F = \frac{2 \times P \times R}{P + R}$$

P = Precision
R= Recall

Conclusion: Does it work?

- Accuracy: No false positives, No false negatives
- Efficiency: How quickly bots are detected
- Robustness against attacks
  - Hide evidence attack
  - On/off sending of evidence (not in the paper but we have done it)
  - Bad mouthing evidence (we model credibility of evidence)
- Accuracy, Efficiency, Robustness show promising results
- Robustness: Challenge is: a botnet is used to attack the credibility of the Global Trust Management system itself → protection against such attack may mean lower efficiency → this aspect needs FS

Further Study

- Run more simulations with the current System Model, improve model based on results
  - Better integration with existing methods of UnW Traffic detection
  - Study the system under real like traffic from the Internet
- Study and define attack models on all Entities: hosts, ISPs and GTO under the assumption of Global Trust Management
  - Hacker and Unwanted traffic sender behavior will change if GTM is introduced
  - Fine tune trust processing algorithms and system model accordingly