Using IPFIX to inspect network security draft-fu-ipfix-network-security-00

Tianfu Fu	futianfu@huawei.com
Dacheng Zhang	dacheng.zdc@alibaba-inc.com
Danping He	ana.hedanping@huawei.com

Background

New Challenges of DDoS Attacks

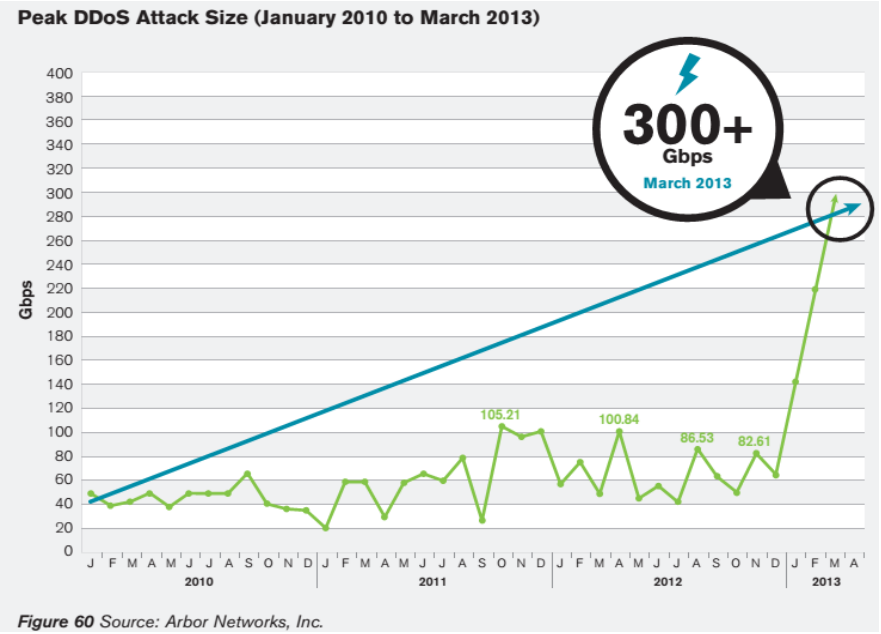
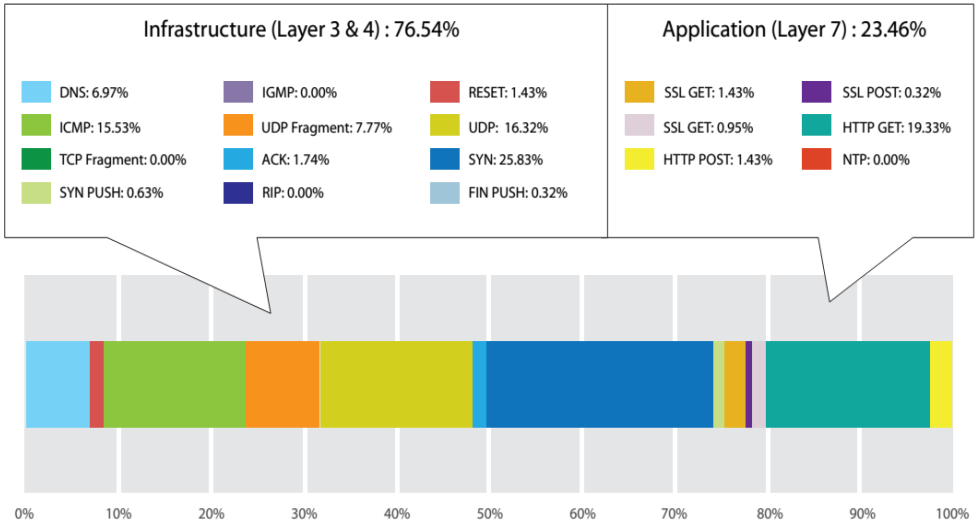


Figure 60 Source: Arbor Networks, Inc.

Figure E: Q1 2013 Reported DDoS Attack Types.[10]



The traditional volumetric flood attack continues to grow rapidly in size of dozens or even hundreds of Gbps.

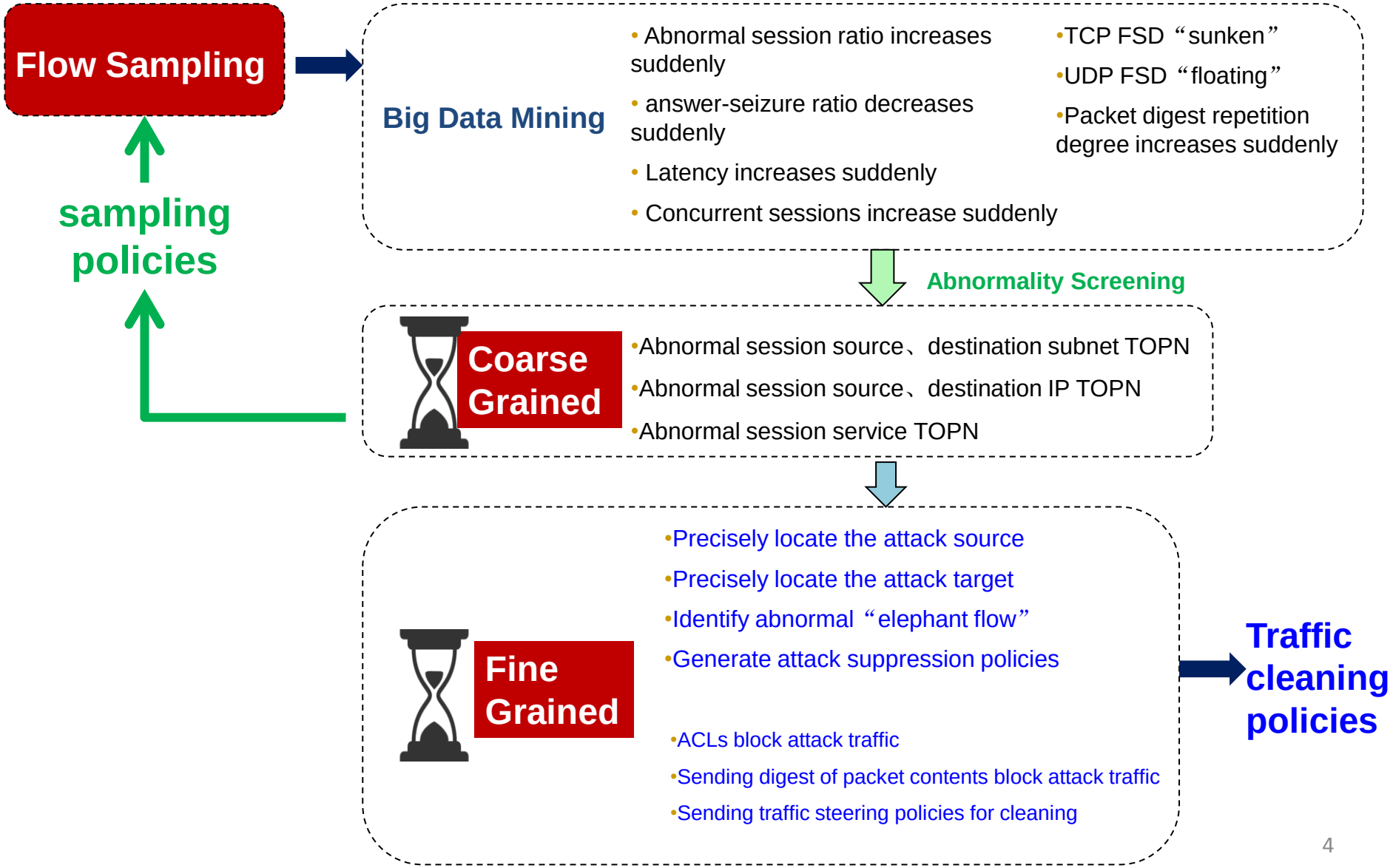
The DDoS attacks are becoming more and more sophisticated. In addition to the existing wide variety of DDoS attacks in Layer 3-7, new attacks emerge very quickly.

IPFIX Overviews

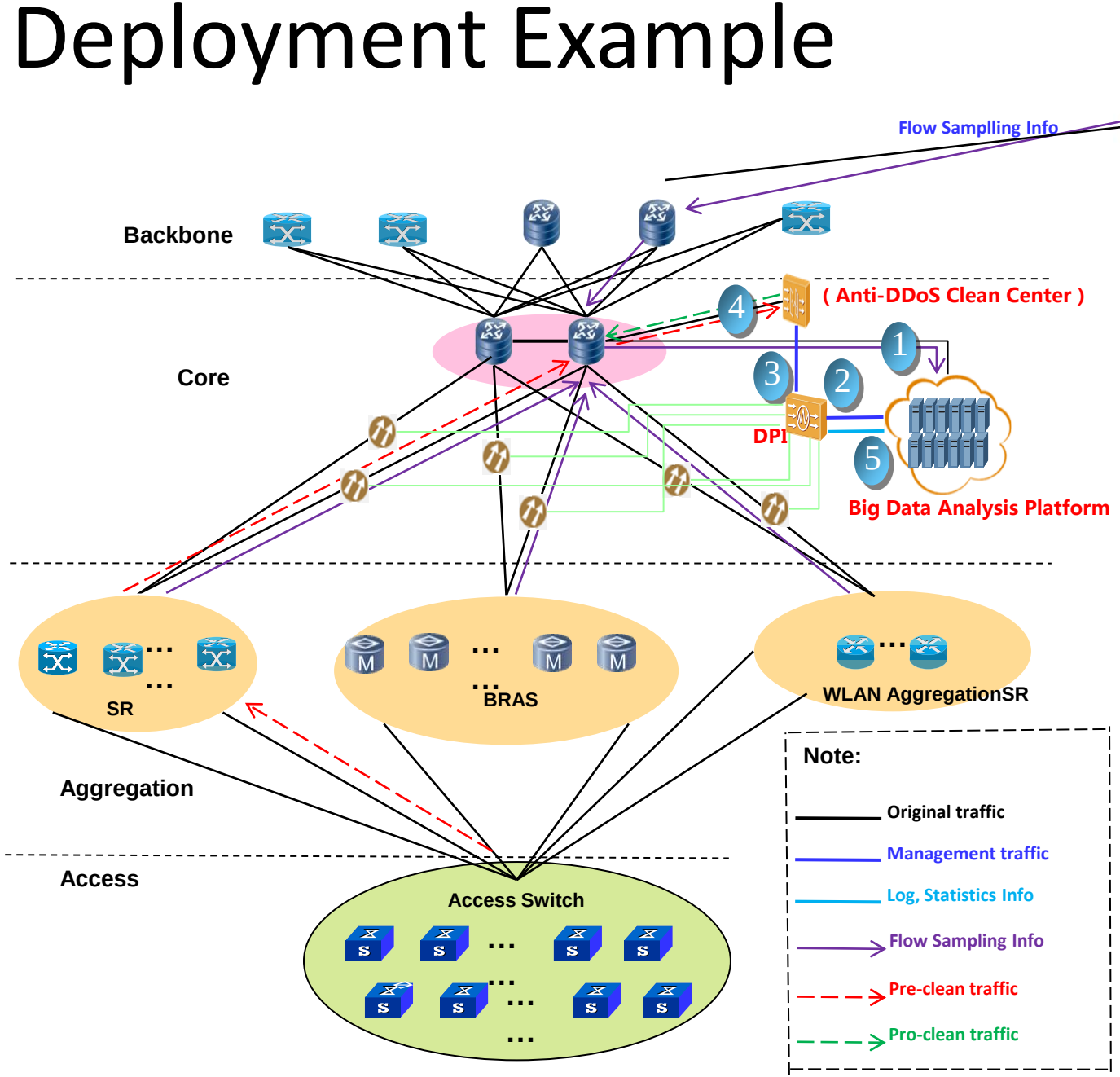
- **Internet Protocol Flow Information Export** (IPFIX): an IETF protocol which defines how IP flow information is to be formatted and transferred from an exporter to a collector.
  - Requirements: RFC3917;
  - Protocol: RFC7011;
  - Information Model: RFC7012;
  - Bidirectional Flow: RFC5103;
  - …

- Using IPFIX to inspect network attacks (Requirements [RFC3917]): **“One of the target applications of IPFIX is attack and intrusion detection.”**

IPFIX Application in Anti-DDoS



Deployment Example



1、Big Data analysis to the suspicious traffic;

2、Apply DPI to the suspicious traffic;

3、SDN controller or NM send traffic blocking or steering policies to SR, BRAS or clean center;

4、Anti-DDoS clean center finishes the traffic cleaning and send to normal traffic back to network;

5、 DPI sends back its detection and clean logs to big data platform for its learning;

6、Remote area network can also use this big data analysis platform

Challenges of Using IPFIX for Security

- **Low sampling probability for small flow:** the smaller sampling probability leads to big difficulty to detect small flow based attacks (SYN-Flood, ACK-Flood, etc)**;**
- **Lack of support for correlated bidirectional sampling:** today's packet sampling is independently applied in each direction and leads to the difficulty to correlate the statistic of both sides. Example: SNMP/DNS Reflected Amplification;
- **Current information is not sufficient:** without detailed information, it's impossible to distinguish some attacks, such as IP fragment attack and Slowloris HTTP attack, from the ordinary ones

Solution: Security Extension of IPFIX

- **Complete Correlated Bidirectional Sampling (CCBS) method:**

  CCBS records all bidirectional packets (e.g. TCP packets from connection setup to close if has) between two peers once that bidirectional flow is selected to be sampled.

- **New IEs to observe different attacks**.

Extended IE Examples

- **Upstream/downstream counters for packets and octets**
  - pktUpstreamCount
  - pktDownstreamCount
- **Fragment statistic**
  - fragmentIncompleteCount
  - fragmentFirstTooShortCount
  - fragmentOffestErrorCount
  - fragmentFlagErrorCount
- **Counter for packets with application error code**
  - applicationErrorCodeCount
- **Extended value of FlowEndReason**
  - A new values is added to FlowEndReason: 0x06 protocol exception timeout

Relations with DOTS

- Same goal: collect and exchange attack related information between different NEs (routers, security devices, cloud-based anti-ddos systems);

- Works in scope?

Thanks!