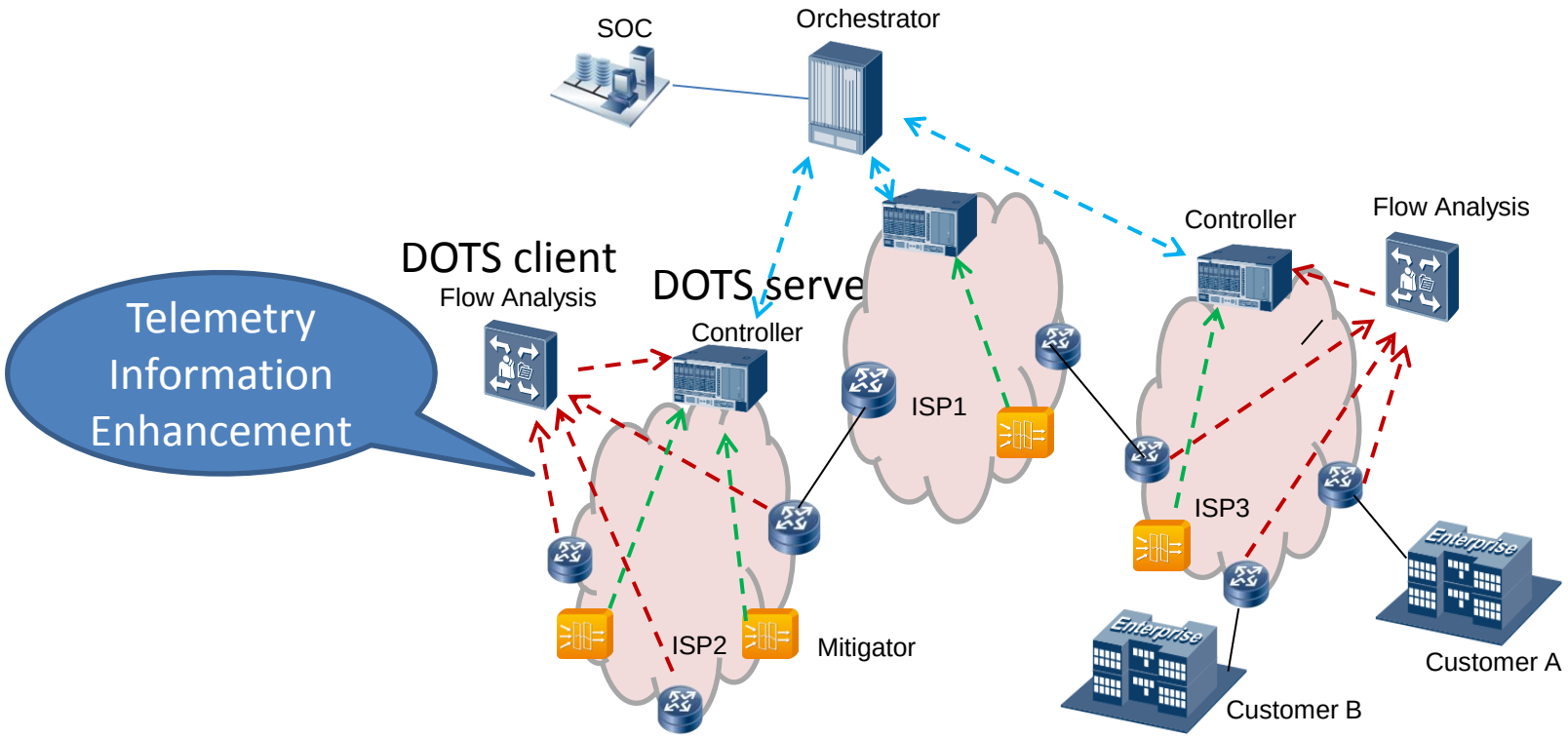
IPFIX IE Extensions for DDoS Attack Detection draft-fu-dots-ipfix-extension-01 (Bo Zhang)

Tianfu Fu	futianfu@huawei.com
Dacheng Zhang	dacheng.zdc@alibaba-inc.com
Liang Xia (Frank)	frank.xialiang@huawei.com
Min Li	l.min@huawei.com

Telemetry Information Value for Operators



- Chances for Operators to be involved in DDoS attack detection
- No need for additional specific devices
- Telemetry information enhancement improve attack detection ability

From -00 to -01

- Remove incorrect examples and related IEs
- Improve the clarification for the differences between packet sampling and connection sampling
- Add new exceptions (for server or client side) with the new IEs, such as: out of order attack, abnormal TCP state, RTT timeout, Http Slowloris Attack, etc

Challenges of Using IPFIX in DDoS Attack Detection

- **Packet sampling**

✓ Can not be aware of the session related information: statistics, status, duration, other metrics;

✓ Low packet sampling probability for small sessions: the smaller packet sampling probability leads to big difficulty to detect small session based attacks (http slowloris, 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;

- **IPFIX Information Elements (IEs)**

✓ Current information is not fully sufficient: without detailed information, it's impossible to distinguish some attacks and exceptions, such as IP fragment attack, out of order attack, HTTP Slowloris attack, etc

Key features of Connection Sampling

- Session semantics: association of two flows in sampling, if one flow is sampled, the flow in the reverse direction should also be sampled
- Capture all packets of sampled connections
- Resilience in deployment: change sampling hash value periodically or using ACL to deal with elephant sessions, VPN or tunnel
- Appropriate for detecting DDoS attacks
- Appropriate for detecting server side exceptions

New IPFIX IEs

fragmentPacketCount
fragmentFirstTooShortCount
fragmentFlagErrorCount
fragmentOffestErrorCount

To detect fragment attack

icmpEchoDeltaCount
icmpEchoReplyDeltaCount

To detect ICMP reflection attack

tcpControlStateBits
tcpOutoforderTotalCount

To detect out of order attack (session exception)

octetVariance
pktTimeInterval
pktTimeIntervalVariance

To detect slowloris attack

serverResponseTime
clientResponseTime
sessionResponseTime

To detect client or server exception (just for TCP)

Note: attacks should be identified by new IEs together with some existing IPFIX IEs

Performance Comparison with Current IPFIX in Operator's Networks

- High detection rate
- Increase by 5 times in detection rate, compared with current IPFIX
- Low false alarm
- 80% decrease in false alarms, especially for the classical DDoS attacks such as SYN flood, ACK flood, etc
- Exception discovery ability
- IPFIX extension has the ability to detect server side exceptions such as out of order attack, abnormal TCP state, RTT timeout, HTTP Slowloris Attack.

Next Steps

- Comments and Suggestions
- Do more measuring and experiments in real life networks
- More clarification for the new IEs
- More exception examples

Thanks!

Bo Zhang (Alex)