SIPFIX

Using IPFIX for VoIP monitoring

Sven Anderson

Institute of Computer Science
University of Göttingen

in cooperation with

NEC Laboratories Europe
Heidelberg

EMANICS/IRTF-NMRG Workshop on
Netflow/IPFIX Usage in Network Management
Munich, October 2008

Outline

Motivation

- VoIP deployment increasing fast (long distance calls, "last mile", NGN/IMS, ...)
- Increased attack surface
- "Best effort" brings unreliablility
- Control- and user data plane are decoupled
- Routes change and hard to predict

Monitoring:

- required for QoS, call integrity, attack and abuse detection, ...
- must be distributed
- must inspect application layer (DPI)

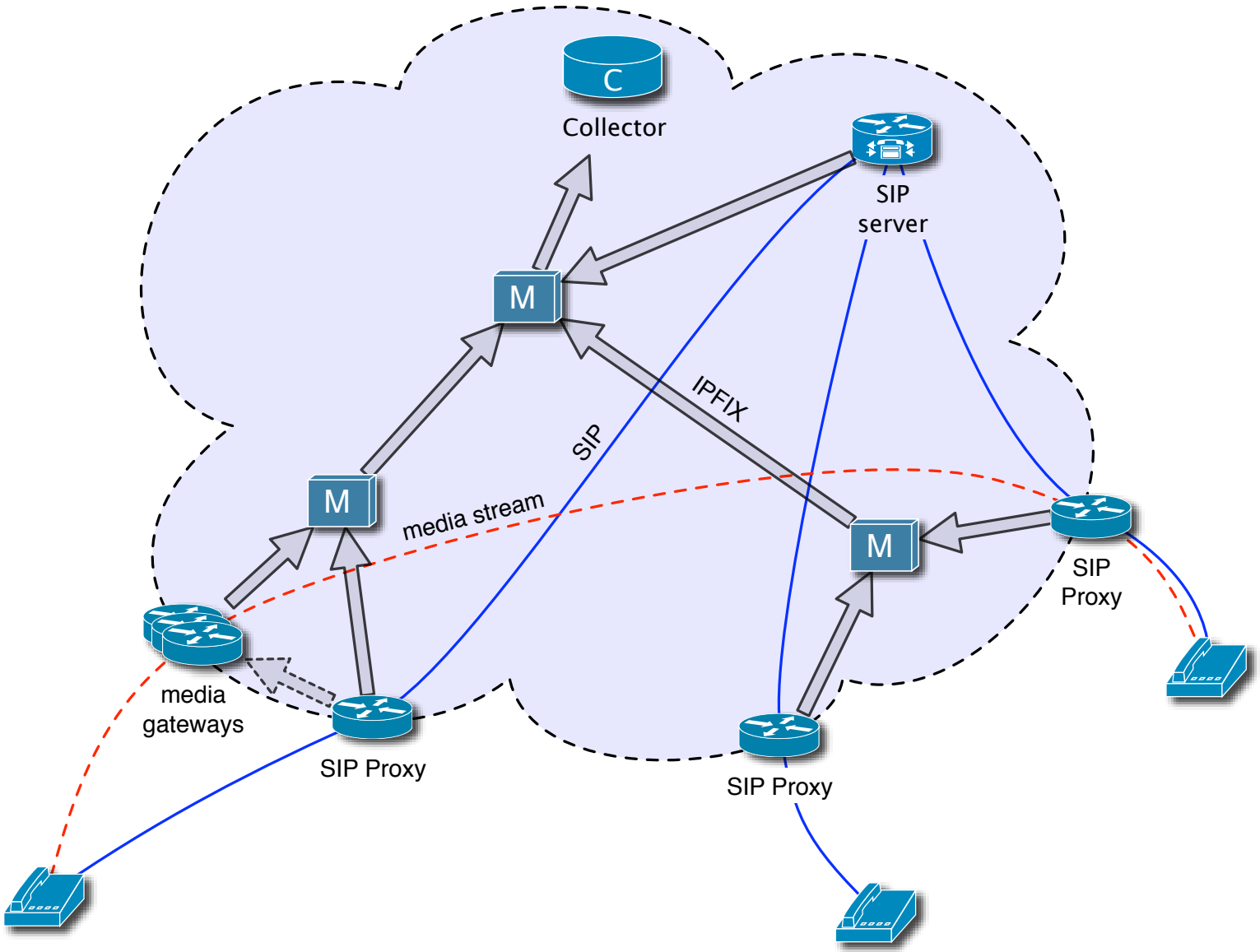
Challenges of SIP Monitoring

- Signalling and media may take different paths
- Media detection needs session description (SIP content)
- SIP and media probes may not know each others location
- Correlation of distributed measurements (e.g. OWD)

Requirements:

- Distributed measurements
- Application layer inspection (SIP, SDP, Media)
- Export of data in appropriate time intervals
- Efficient convergence of data

Reference Scenario



SIP Header IEs

Mandatory:

- sipFrom (`alice@example.com`)
- sipTo (`bob@example.org`)
- sipCallId (`xyz@192.168.0.1`)

  tuple referred to as "sipDialogId"

Further examples:

- sipRequestMethod (INVITE, REGISTER, BYE, ...)
- sipRequestURI (`sip:bob@example.org`)
- sipResponseStatus (2xx, 4xx, 5xx, ...)

Media IEs

Derived from SIP content (SDP):

- sipMediaId (mandatory)
  - Unique identifier for media stream descriptions
- sipMediaProtocol (e.g. RTP/AVP)
- sipMediaType (audio, video, ...)
- sipMediaEncoding (G722, GSM, PCMU, ...)
- ...

Derived from SDP or RTP:

- rtpPayloadType
- ...

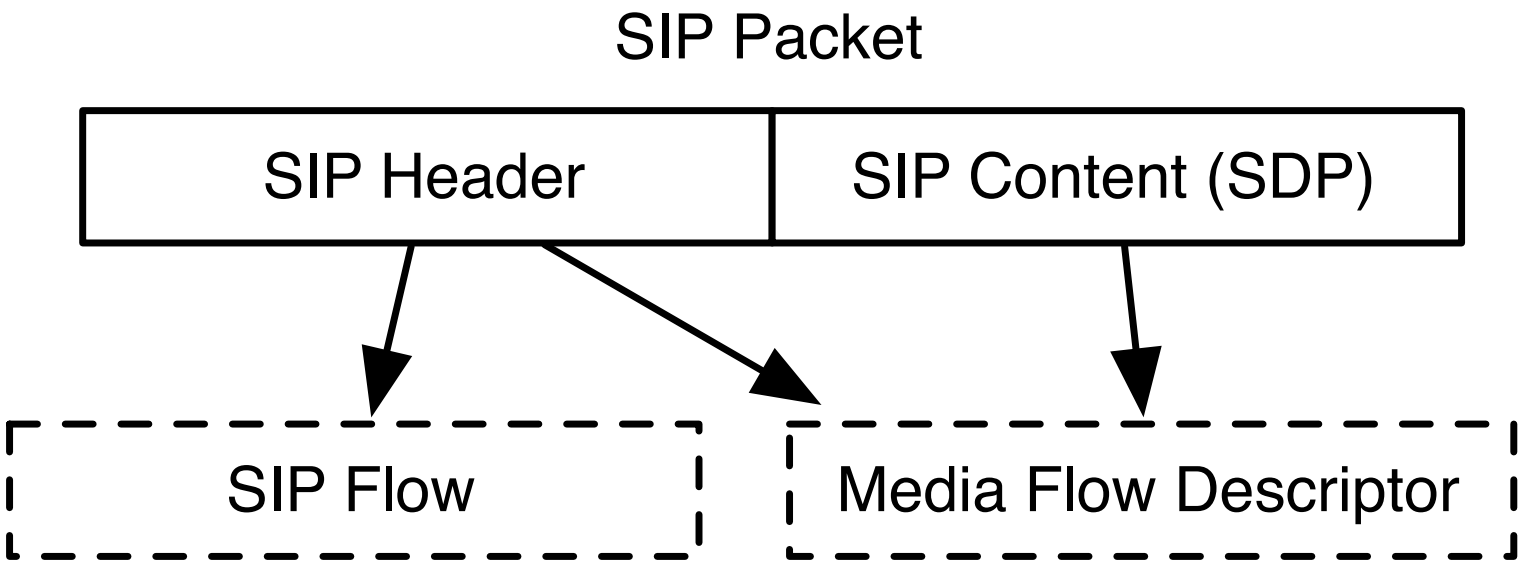
Performance Metric IEs

- mediaPacketLoss
  - ratio of lost packets to total packets
- mediaDelayFromTerminal
- mediaDelayToTerminal
  - OWD from media gateway to the terminal and vice versa
- mediaDelayMGW
  - OWD from ingress to egess media gateway
- rtpJitter
  - interarrival jitter as defined by the RTP
- ...

Flow Type Definitions

- SIP Flow
  - Flow of SIP packets
  - Must include "sipDialogId" (sipFrom, sipTo, sipCallId)
  - May include other SIP header IEs
- Media Flow
  - Flow of media packets
  - No mandatory IEs
  - Can be exported by standard IPFIX device
- Media Flow Descriptor
  - Pseudo flow (expected, not observed)
  - Extracted from media descriptors (SIP content)
  - Must contain "sipDialogId" and sipMediaId
  - No counter IEs

Flow Type Dependencies



IPFIX Probe Extensions

- Efficient deep packet inspection
- SIP Flows: SIP header parser
- Media Flow Descriptors: SIP & SDP parser
- Media Flow: no requirements in general
- Media Flow identification:
  - RTP detection if feasible, or
  - import of Media Flow Descriptors
- Optional:
  - SIP metric measurement
  - Media metric measurement

Mediator/Collector Extensions

Processing of SIP related data, for example:

- Calculation of metrics deriving from different probes (e.g. timestamps for OWD)
- Correlation of Media Flows and Media FLow Descriptors
- Correlation of SIP Flows and Media Flow Descriptors by "sipDialogId"
- Forwarding of uncorrelatable data to next Mediator
- Creation of "call records"
- Real-time display of current calls (Collector frontend)

Use Of Existing IPFIX Extensions

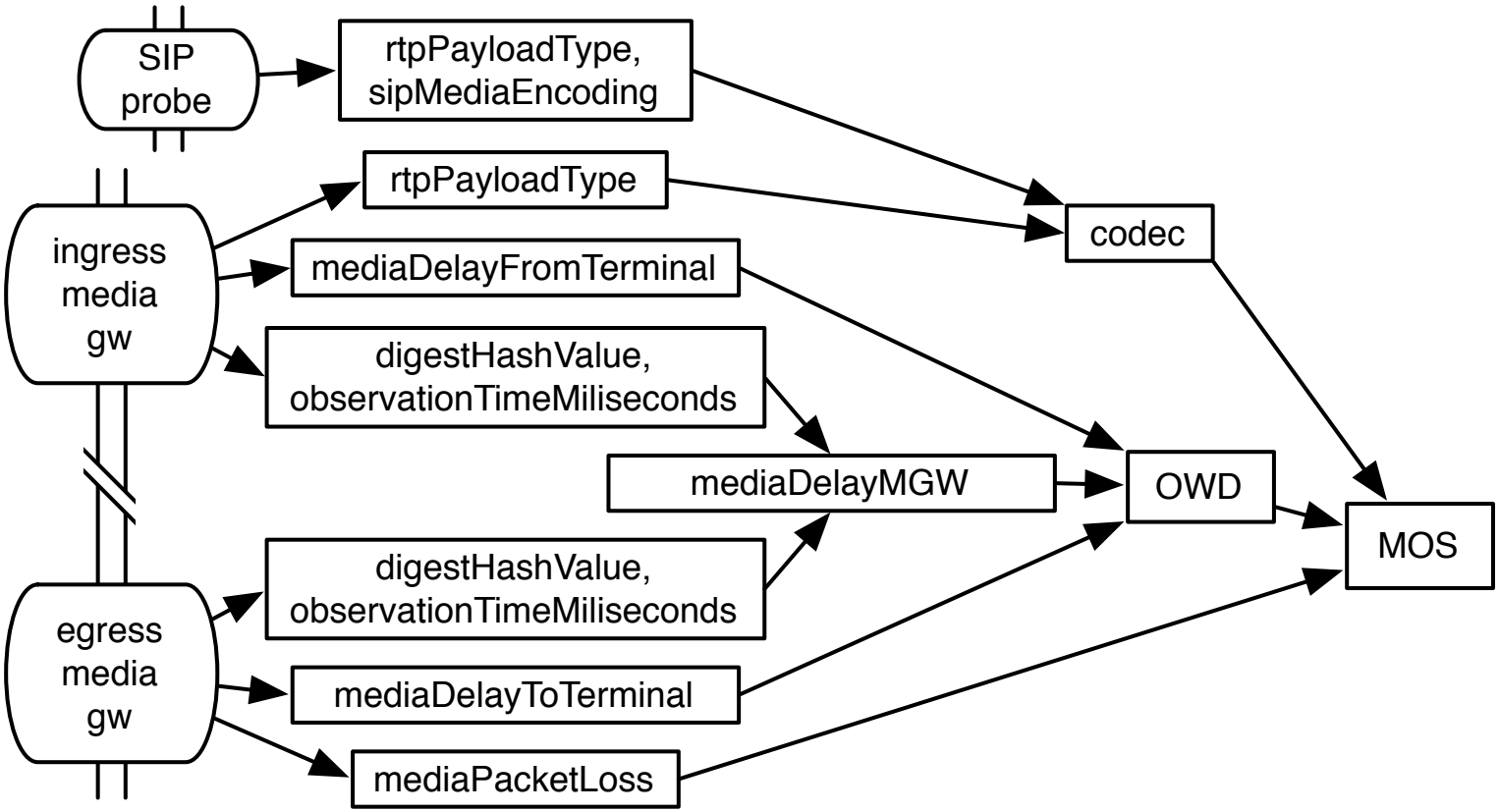
- Bidirectional Flows
  - Directional information of SIP Flows can be kept
  - Normal counters refer to SIP requests
  - Reverse counters refer to SIP responses
- Common Properties
  - "sipDialogId" can be represented by a commonPropertiesId with the template <commonPropertiesId | sipFrom, sipTo, sipCallerId>
  - often exported status updates can be "attached" to SIP Flows
  - performance metrics can be "attached" to Media Flows
  - several possible codecs "attached" to a Media Flow Descriptor

Use Case Examples I

- Seperate SIP and Media Flows
  - Mediator correlates Media and SIP by Media Flow Descriptors
- Asymmetric Routing
  - Mediator correlates SIP requests and responses by "sipDialogID"
- Security Inspections
  - Spoofed Media Sender
    - Detection of multiple Media Flows fitting to one Media Flow Descriptor
  - Stateful Cross-Protocol IDS
    - SIP Flows contain multi-layer information
  - DoS Detection and Prevention
    - Detection close to source
    - DDoS can be detected by flow aggregates
- Realtime Status Display

Use Case Examples II

- Quality-of-Service Monitoring



Summary

- Key ideas of SIPFIX:
  - Probes inspect and export application layer info
  - Media description (SDP) is exported as Media Flow Descriptors
  - "sipDialogId" ties SIP Flows and Media Flow Descriptors
  - Media Flow Descriptors tie SIP Flows and Media Flows
  - Correlation and processing by distributed Mediators
- Many open detail questions, like:
  - What data types for which IEs? (string, integers...)
  - Use of Option Templates for Media Flow Descriptors?

Summary

- Key ideas of SIPFIX:
  - Probes inspect and export application layer info
  - Media description (SDP) is exported as Media Flow Descriptors
  - "sipDialogId" ties SIP Flows and Media Flow Descriptors
  - Media Flow Descriptors tie SIP Flows and Media Flows
  - Correlation and processing by distributed Mediators
- Many open detail questions, like:
  - What data types for which IEs? (string, integers...)
  - Use of Option Templates for Media Flow Descriptors?

Thank you!

Sven Anderson
<anderson@cs.uni-goettingen.de>
University of Göttingen / NEC Labs