Path-coupled Signaling for Dynamic Metering Configuration in IP-based Networks

Falko Dressler[1,2], Andreas Klenk[2], Cornelia Kappler[3], Ali Fessi[2], Georg Carle[2]
[1] Dept. of Computer Sciences, Computer Networks and Communication Systems, University of Erlangen, Germany
dressler@informatik.uni-erlangen.de
[2] Computer Networks and Internet, University of Tübingen, Germany
{dressler,klenk,fessi,carle}@informatik.uni-tuebingen.de
[3] Siemens Communications, Berlin, Germany
cornelia.kappler@siemens.com

Abstract

Metering for accounting, charging, and QoS measurements is an important functionality of modern IP-based networks. Many approaches have been published and some of the outcomes have been already deployed. So far, the configuration of the metering entities is based on centralized management systems. These systems usually have no knowledge about the ongoing routing decisions, and as a consequence do not allow to choose the metering entities based on algorithms that depend on the currently chosen data path. However, some scenarios require a path-dependent metering configuration functionality, e.g. for load-balancing between multiple meters. In this paper we present a path-coupled metering configuration that allows for sophisticated configuration options. Based on three different application scenarios, we discuss the requirements on a configuration signaling method, and present a path-coupled signaling approach which meets the identified requirements. Subsequently, we use the same application scenarios successfully assessing the approach.

1. Introduction

Advances in fixed and mobile network infrastructures are focusing on IPv4 and IPv6 protocol stacks, respectively. Metering in IP-based environments has been a research topic for a long time, leading to metering architectures for accounting, Quality of Service (QoS) measurement, and network security. Nevertheless, the interaction of individual metering components, as well as their configuration is still subject of ongoing research. For example, new services for 3G and Beyond 3G telecommunication networks were developed for which appropriate charging concepts require highly dynamic re-configuration of the involved accounting architecture [1]. 3GET[1] (3G Evolving Technologies) is a project that works on such real-time integrated accounting and charging architectures. Alternative application scenarios related to security are being investigated by projects such as DIADEM Firewall[2] that realize highly distributed network security environments based on network monitoring and attack detection. Accounting architecture frameworks were developed within the IRTF (Internet Research Task Force) AAAArch (Authentication, Authorization, and Accounting Architecture) working group [28], [24]. These activities lead to the standardization of a metering configuration framework. However, path-coupled metering configuration is not supported by this work. Such possibilities are currently discussed by the NSIS (Next Steps in Signaling) working group.

In this paper, we discuss a novel methodology for signaling metering configuration. We call this methodology the Metering NSLP (NSIS Signaling Layer Protocol). It addresses the question of how to configure efficiently appropriate meters by employing a path-coupled signaling. In the following, we introduce the Metering NSLP (M-NSLP) and discuss its applicability for different application scenarios.

The remaining sections of the paper are organized as follows. Related work is discussed in section 2. Then, the Metering NSLP and its correlation to the NSIS protocol suite are outlined in section 3, describing our proposed novel mechanism for configuration signaling. Section 4 describes different scenarios that benefit from path-coupled configuration of metering entities. We focus on three applications: accounting, measurement of QoS parameters, and monitoring for network security. Further discussions (section 5) and conclusions summarize the paper.

2. Related Work

In order to discuss possible solutions for configuring accounting and metering environments, a short overview of past work as well as the involved communities is needed. Measurement of parameters in communication networks, especially in the Internet, has a quite long history. It started with the collection of usage statistics and continued with quality of service (QoS) measurements [23]. Until today, such measurements dominate the accounting

[1] Project homepage: http://www.mobile-accounting.org/
[2] Project homepage: http://www.diadem-firewall.org/

and metering community.
Accounting is one of the most important metering applications. The IRTF AAAArch working group specified some mechanisms that can be used for accounting in large-scale networks based on a AAA infrastructure [7, 28]. It also specified how to initialize metering entities and how to distribute measured data. Other work on configuration of metering entities originates from the need to measure various network properties such as quality of service parameters. The IPPM working group of the IETF works on standardization of measurements such as one-way delay [3] or the one-way packet loss [4]. However, work is still needed to address the issue of how to choose appropriate measurement entities. Similar problems were addressed for the placement of multimedia servers in the Internet based on active and passive QoS measurements, see e.g. [11, 12].
Looking at existing accounting and measurement methodologies, the following configuration methods can be distinguished. Each method is associated with a configuration protocol.
SNMP (Simple Network Management Protocol, [8, 9]) allows for monitoring and configuration of network devices. So called NMS (Network Management System) servers use this protocol in order to query the configuration state as well as current operational parameters from networking entities. SNMP also allows to modify the configuration of these entities by writing individual configuration parameters. This configuration method is also envisioned for metering entities as defined by IPFIX (IP Flow Information Export) and PSAMP (Packet Sampling) [10]. Advantages of SNMP are the wide deployment and the widespread availability of tools. The fact that SNMP is a client-server protocol is a disadvantage in certain scenarios.
Diameter [6] is a AAA protocol focusing on authentication and authorization of network services and on transferring accounting data towards an accounting server. Additionally, parameters of metering entities can be configured using Diameter. The server-oriented nature of Diameter can also be regarded as disadvantage in certain scenarios.
Netconf [17] is a new and highly promising approach for configuration of network devices. Among others, Netconf can be used for metering configuration. Netconf transports configuration information using an XML-based encoding, thereby allowing for flexible configuration messages. For transport of the XML information, various transport protocols such as SOAP, SSH or BEEP are envisaged. The advantages of Netconf are its flexibility and its capability to use multiple transport mechanisms. Authentication and encryption is to be handled by the transport mechanism.
In summary, it can be said that all the mentioned configuration mechanisms have a server-oriented working principle. This means that state information must be kept up-to-date for optimizing configuration of available metering entities. Additionally, the configuration mechanisms presented here assume that the location of appropriate metering entities to meter a given data flow is known a priori. This can be realized if the configuring entity possesses knowledge about the data path chosen by a given data flow, or by configuring multiple or even all metering entities in the network with the same assignments. The first alternative fails in many scenarios, since it requires accurate and frequently updated knowledge about the network topology. The second alternative has scaling problems in large networks.
The goal of allowing dynamical, path-specific (re-)configuration of metering entities requires novel solutions. Starting at the primary operation of IP-based networks, the search for available meters should be done along the data path from the sender towards the receiver. This idea is the main concept behind the proposed path-coupled metering configuration that is described and discussed in detail in the following section.

3. A Protocol for Meter Configuration

The metering configuration protocol proposed in this paper is based on the Next Steps In Signaling[3] (NSIS) protocol suite currently being standardized by the IETF (Internet Engineering Task Force). In the next two subsections we introduce the NSIS ideas and the metering configuration protocol. An overview of NSIS is given in [16].

3.1 NSIS Framework

The goal of the NSIS Working Group is the standardization of a general, flexible signaling protocol. NSIS signaling is path-coupled, i.e., it is a mechanism for sending signaling messages along the path of a data flow, in order to configure entities on this path to control or treat the flow is a particular manner. An example is signaling for providing QoS to a flow.
A flow is defined rather generally as a stream of packets that share a subset of a path and have something identifiable in common, e.g. source and destination IP address. For instance, a flow can include all packets of a user to a particular destination, or all packets from the ingress to the egress of a domain with the same DiffServ Code Point.
NSIS was inspired by the Resource Reservation Protocol (RSVP, [5]) where the

[3] NSIS charter: http://www.ietf.org/html.charters/nsis-charter.html

signaling messages request QoS for a data flow from the routers on the path. NSIS re-uses, where appropriate, the protocol mechanisms of RSVP. However, it supports more flexible signaling models, and is not restricted to QoS signaling. As opposed to RSVP, NSIS does not support multicast. This multicast support introduced considerable overhead for unicast applications, which are actually much more common than multicast applications.
The basic mechanism to achieve this flexibility is to divide the signaling protocol stack into two layers:

- A lower 'signaling transport' layer, providing common functionality for the routing of signaling messages, e.g. locating a suitable adjacent NSIS-aware node, and transporting signaling messages. This layer is independent of any particular signaling application. The protocol used in this layer is called NSIS Transport Layer Protocol (NTLP, [26]).
- An upper 'signaling application' layer, accommodating the actual information that is being signaled. It consists of a number of protocols for specific tasks, called NSLPs. Message formats and sequences are specific to each protocol.

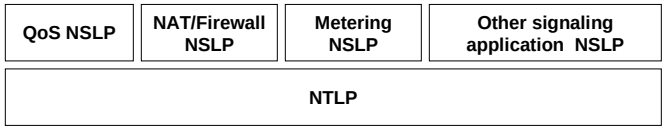

Fig 1. NSIS Protocol Stack

At the end, there will be one NTLP and several NSLPs on top of it as shown in Fig 1 [18]. The first NSLP being developed serves for signaling for QoS [22]. Simultaneously, an NSLP for controlling firewalls and Network Address Translators (NATs) is being developed [27]. In this paper, we propose a new NSLP, called the Metering NSLP, that is currently also being proposed at the IETF [13, 14].
The basic NSIS signaling scenario is shown in Fig. 2. A node, the NSIS Initiator (NI), initiates the signaling. Nodes along the signaling path, called NSIS Forwarders (NFs), intercept and then forward signaling messages. The NSIS Responder (NR) terminates the signaling. NI, NFs and NR all install signaling state which can be refreshed, updated or torn down by subsequent signaling. Backward routing state information is installed on the NFs, and hence the NR can also signal back to the NI. The signaling messages from the NR will be forwarded hop by hop towards the NI. NSIS aware nodes along the signaling path may also communicate among themselves, e.g. for error processing. Fig. 2 shows that not all nodes along the data path need to be NSIS aware. For Metering configuration signaling, this means only the subset of on-path nodes is included in a particular NSIS session which is necessary for the metering task, e.g. the first and the last node in the case of one-way-delay measurements.
There are different possible triggers for signaling, e.g. user applications, management actions, etc. The initiator and the receiver of NSIS signaling can be located anywhere in the network: on end nodes, proxies, edge routers etc. This allows for flexible localization of the signaling, e.g. end-to-edge, proxy-to-end, edge-to-edge etc. The messaging patterns are flexible: sender-initiated as well as receiver-initiated signaling is possible, i.e. a sender of a data flow can trigger the receiver to initiate the signaling. Additional requirements are independence of protocol machinery and the information that is being carried, the possibility to transparently carry the signaling through part of the network, and hooks to interwork with AAA and mobility protocols. All NSIS state is soft state; time-out values can be locally adjusted.

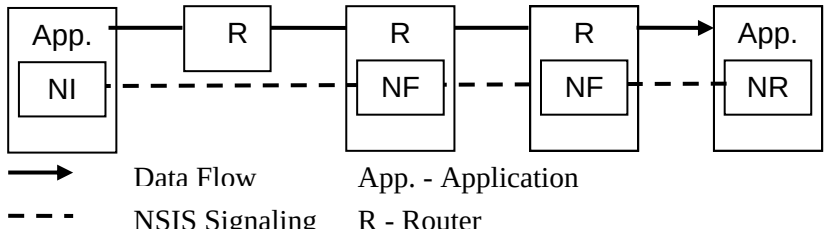

Fig 2. Basic NSIS signaling scenario

Security is a very important concern for NSIS protocols, although it is possible to use NSIS protocols in an unsecured fashion in safe environments, for example for intra-domain signaling. Means are provided for NSIS entities to authenticate each other. Messages can be integrity- and confidentiality-protected, and message replays can be detected. Suitable models for authorization of state set-up requests and defense against Denial of Service attacks are being worked on.
NAT traversal of NSIS messages is an open issue. The NSIS payload necessarily contains a flow identifier to define the flow being signaled for, e.g. by source and destination IP addresses. Usually, NATs only rewrite the header fields, in which case the flow identifier information contained in the NSIS payload becomes meaningless. An NSIS aware NAT could translate the payload, too. Alternative solutions are being worked on.
NSIS protocols can handle dynamic route changes. A number of triggers to detect a route change are conceivable, such as monitoring changes in routing

tables or inference from changes in signaling packet TTL. NTLP is responsible for detecting route changes and informs affected NSLPs. NSLPs are responsible for installing state along the new path. State along the old path will time out eventually because of soft state, however it may be desirable to tear it down faster, e.g. because it is tied to an accounting record or to release the resources reserved there.

Work is in progress to enable NSIS protocols to cope with mobile end points [21]. A handover experienced by endpoints requires rerouting a section of the flow path up to a so-called cross-over router. Hence, NSIS state on the old section of the path must be torn down, and it must be installed on the new section of the path. In order to be able to recognize corresponding NSIS states and the cross-over router, NSIS state is not identified by the IP address of an endpoint – which may change due to mobility - but by a cryptographically random Session Identifier. Note here that RSVP identifies signaling state using IP addresses and hence can not cope with mobility.

3.2 Metering NSLP

Since the most appropriate metering entities (MEs) to measure/monitor a data flow are located along the path of this flow, NSIS is a good approach for discovering MEs and dynamically configuring them. Moreover, the MEs along the path can be easily coordinated using NSIS, for example, to distribute a correlation identifier for the same data flow (see below). Therefore a Metering NSLP to configure metering and monitoring entities along the path to record and export metering data seems to be a reasonable approach.

Fig 3 depicts the architecture of the Metering NSLP. The example scenario shows an ISP network that includes several routers with metering capabilities. Statistics about the data flows traversing the router are provided by Netflow, a protocol that is widely available in commercial routers.

To meter/monitor a specific data flow from Sender A towards Receiver B, only the MEs along the path from A to B are designated for this task. So, one or more MEs along this path need to be configured to perform the required metering/monitoring for this data flow.

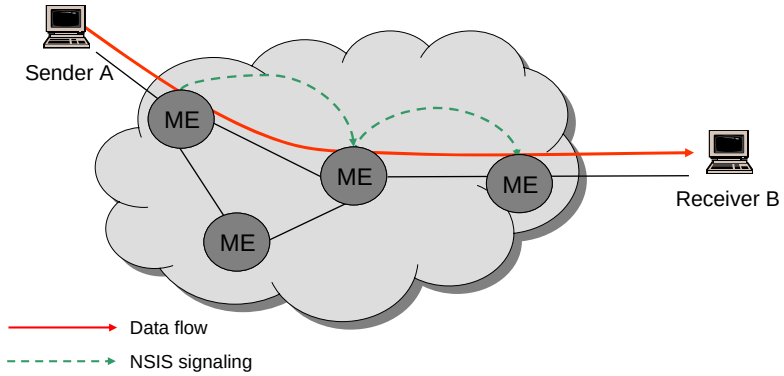

Fig 3. Metering NSLP: architecture

Which metering entities act as NSIS Initiator respectively NSIS Responder depends on the application. For example, for accounting purposes, Metering NSLP messages are initiated by the access router, and are forwarded NSIS-hop by NSIS-hop along the path. In many scenarios, e.g. in mobile networks where data flows are accounted and charged for, the end host can not be considered a trusted node due to eventual fraud. In such cases, the last router before the end host has to terminate the signaling and acts as NSIS Responder. In another scenarios, e.g. in which the end-to-end or the hop-by-hop delay on the path needs to be measured, the Metering NSLP session would be initiated by the data sender, and terminated by the data receiver. Therefore, depending on the application scenario, the data sender and the data receiver may or may not be the signaling initiator or signaling responder, respectively.

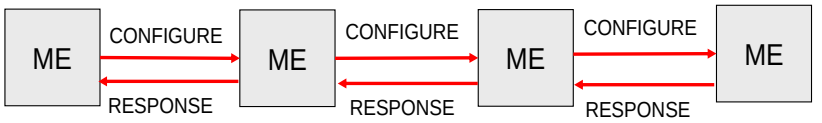

Fig 4. Simple Configuration scenario with the Metering NSLP

Fig 4 shows a simple configuration scenario with the Metering NSLP. The initiator of the metering configuration session issues a 'CONFIGURE' message, which contains a flow identifier and a description of the metering tasks, e.g. "One meter, count all packets of this flow". The destination address of the message is the address of the data receiver. Furthermore, the message carries a router-alert option which is specific to the Metering NSLP. The message thus travels along the data path towards the data receiver. Each router on the path

inspects the router alert option. If it implements Metering NSLP, the router inspects the message in more detail. If the router is eligible to perform a given task, e.g. it can count packets and no router upstream volunteered to do so, it sets a marker in the message. Furthermore it establishes a messaging association with the upstream Metering NSLP node from which it has received the message. This messaging association may be based on a TCP connection, a secured network layer security association, such as IPsec, or a transport layer security association such as TLS. The messaging association allows further messages for this metering configuration session (e.g. Metering NSLP state refreshing messages) to be sent directly peer-to-peer to the next upstream or downstream Metering NSLP node, without the processing overhead entailed by router alert options. In order to account for route changes or mobility events, still, from time to time, a routing state refreshing message on the NTLP layer with a router alert option needs to be sent along the path to discover if new or other NSIS nodes need to become involved in the signaling.
When all the metering tasks described in a CONFIGURE message have been allocated, the signaling message can be terminated - even before the NSIS Receiver has been reached. The ME terminating the signaling may send a 'RESPONSE' message upstream to the signaling initiator. Depending on the scenario, this message might be required to commit the configuration and to establish correct configuration state on the MEs.

3.3 A Possible Extension: Off-Path Signaling

While path-coupled signaling for meter configuration has numerous advantages as described above, some scenarios may call for the involvement of nodes that are not on the data path. For example, accounting configurations for data flows could be initiated by a central node in a network, or an off-path proxy (e.g. SIP proxy). The configuration message would then be initiated from the off-path node, and sent to the first NSIS node on the data path. From there it proceeds on-path as before. Of course, determining the first NSIS node on the data path is not a trivial task. It is in fact possible to generalize the NSIS protocol suite to also take into account such "path-related signaling". First thoughts are described in [19].

4. Application Scenarios

Path-coupled metering is beneficial for different scenarios in the Internet, not only for supervision of existing connections but also for fault diagnosis and even for the analysis of malicious behavior. The following sections describe three scenarios for the usage of path-coupled configuration of Metering Entities: accounting, QoS monitoring, and monitoring for network security.
All scenarios have certain properties in common. Metering on-path helps to measure characteristics which cannot be measured at central spots. Dynamic policy-based configuration keeps the system easily extensible. Distribution of the measurements and of the processing leads to a better overall processing capacity and lower bandwidth for exchange of metered data and avoids central bottlenecks. Load balancing helps to increase system utilization of the meters. Fault tolerance is achieved, because the mechanism allows to replace a non-functioning meter by another meter on the data path.
The meters can be kept agnostic of the particular purpose they serve. A meter with packet counting and delay measurement capabilities, for example, does not have to be aware that its output is used for QoS measurements, accounting and intrusion detection at the same time. In this example, it may notice that it must report the same measurements to three different collectors. Hence configuration of meters depends to a large degree on the scenario.
This section will discuss three scenarios: Accounting Configuration for IP-based Networks, QoS Monitoring and Monitoring Configuration for Intrusion Detection. First, the requirements are elaborated, then the particularities of the scenarios are discussed and subsequently, an assessment of the applicability of the M-NSLP is presented.

4.1 Accounting Configuration for IP-based Networks

Network operators rely on accurate accounting and charging mechanisms for their services. This holds especially with the integration of existing networks while providing services based on IP technology. With the advent of new technologies in the context of Beyond 3G (B3G) networks, new charging mechanisms must be introduced into the system. The All-IP perspective of Beyond 3G networks [2] requires accounting mechanisms which can cope with the packet switched nature of the core network. While the 3GPP already specified solutions to many accounting problems, we describe in this scenario how on-path accounting mechanism can serve the same purposes and provide some additional benefits.

4.1.1 Scenario Details

Usage-based charging as well as flow-based accounting have been identified to be of high importance in future IP-based networks. The evolution of 3GPP networks towards an IP-based core foreseen for B3G networks fosters the need for new accounting mechanisms, both flexible and efficient..

Different aspects of accounting in IP-based networks could benefit from path-coupled metering and configuration signaling. Meters along the data-path can be dynamically setup to measure flow-specific parameters as required. They are discovered on the fly during the session initialization and are configured based on their capabilities and the requirements of the session.
In order to provide accounting and charging functionality in such networks, meters need to be appropriately configured. Due to limited resources, load balancing and minimization of metering tasks are the primary goals for the configuration step. The following scenarios will highlight how path-coupled accounting helps to introduce new capabilities into the system and how it can act as an alternative to the existing accounting mechanisms.
Metering entities can be situated at routers on the data-path at the monitoring port. Others might be integrated at specialized components, for instance, at a content server to account for content access.
Online accounting, real-time information of the user on accumulated costs and QoS aware accounting are among the functionalities that benefit from path-coupled accounting. Basic characteristics of these scenarios are dynamic metering configuration and scalable processing of the metering records.
Online charging in IP networks is especially challenging for usage metering. Different parameters of a session must be accounted in nearly real-time: Access and transport is typically charged based on time and volume at the bearer level. Triggers signal chargeable events, for instance, the service usage or content access. The accounting must process the generated accounting data records in a short period and send the results to the charging. The distributed approach can help to perform a demanding accounting in terms of generated metering records and freshness of the gathered accounting data. Distribution of the accounting over the meters on the data path and distributed pre-processing of the metering records enables online accounting capabilities.
A growing demand for Quality of Service (QoS) guarantees raises the need of QoS-based charging. Customers of services with QoS support require information about the fulfillment of QoS guarantees. In the case QoS guarantees were broken, a customer might demand a refund for the degradation of his service. This scenario is especially challenging if traffic crosses multiple provider networks. The following subsection 4.2 discusses how path-coupled metering helps to measure QoS. QoS aware accounting can be implemented by using a collector with QoS and accounting capabilities.
Complex usage-based charging can be accomplished by path-coupled metering and distribution of the charging processing. A session can consist of many sub-sessions with different accounting requirements. To reduce the burden of the charging infrastructure, a collector can perform pre-processing, e.g. by aggregating metering data records of sub-sessions into a single session-specific metering data record. Hence less processing is required at the charging infrastructure itself if the pre-processing is done by the collector.

4.1.2 Requirements

The requirements differ depending on the purpose of the accounting. Accounting is required for informational purposes in the network as well as for charging of service usage.
Charging requires a high accuracy of the underlying accounting mechanisms and must operate reliably. Accounting must be scalable and fault tolerant to provide its service at any time and under any traffic condition. As a charging system needs to rely on the accounting data, the accuracy of the gathered data is very important. Frequently accounting entities must provide their output data with very low latency.
Advice of charge is a highly challenging task, as the user receives information about his service usage and the respective costs in real time. Advice of charge strongly depends on the timeliness of the accounting and charging information.
As already stated, the accuracy of the accounting mechanism is of high importance. Still, the mechanisms must scale for high bandwidth. The system must be able to handle traffic peaks. The treatment of the generated metering records must scale and must be reliable.
A flexible accounting mechanisms should not make any assumptions about the topology of the network and must therefore be able to adapt to any network structure as wells as changes thereof. Route pinning should be avoided because it results in inefficient routing decisions and bottlenecks. New functionalities might only work at certain processing units of the network, say at ingress/egress nodes or at proxies. Hence a mechanism is required to discover those entities.
An accounting system must be easily extensible to allow the seamless introduction of new accounting functionalities without the need to change the existing system. A provider typically avoids replacing an existing accounting infrastructure, and rather aims to add new capabilities.
Accounting can also serve for data analysis of the network behavior. Network planning can use the information about bottlenecks and traffic peaks. In the case of traffic sampling it is important that the sampled data is representative.

4.1.3 Applicability of M-NSLP

All these requirements make it necessary to design an innovative accounting concept for IP-based networks which is more flexible and scalable than today's approaches and can be applied to future B3G networks as well (see also [15,

20]). The most appropriate location to perform flow based accounting is on the data path itself. Accounting entities can be dynamically configured depending on the particular accounting scenario.
Instead of usage metering at central points, a distributed approach is envisioned. Meters at different locations inside the network will use load balancing to divide the burden of metering. The collectors in the network perform pre-processing of the metering records to relieve the charging system. Thus the on-path accounting scales with the capacity of the meters and the collectors in the network.
In a representative scenario, the task of accounting one session may be assigned to different meters. Meters are chosen to monitor particular parameters depending on their capabilities. Different meters report their measurements to a collector which aggregates them into a single metering record. Hence charging must only process this single metering record instead of metering records from different sources.
An advantage of the dynamic configuration of metering entities is the more efficient utilization of resources, leading to smaller total accounting costs. For charging, only parameters relevant to the charging function of a particular data flow must be accounted. Here, configurable accounting is more efficient than static accounting that collects data which has to support a variety of charging functions.
It is of high importance for the charging infrastructure to assure that all relevant packets are accounted unambiguously and none can pass without being accounted. Before a service is initiated, the meters along the data path must be configured for metering all important aspects of the service. Fault tolerance can be enhanced by redundant accounting at different meters. In case that a meter ceases its operation unexpectedly the M-NSLP will detect the failure and will configure an alternative meter for the metering task autonomously.

4.2 QoS Monitoring

Guarantees for real-time traffic are hard to establish and maybe even harder to maintain in complex networks. Subtle changes inside the network may easily disrupt the reserved QoS parameters. Therefore the need arises to constantly monitor the established QoS parameters to detect the loss or the degradation of the connection quality. Important parameters to assess the QoS are usually quantified by bit rate, packet loss, jitter, delay and other parameters. The contract between user and provider determines the parameters that need to be monitored.

4.2.1 Scenario Details

Especially ISPs that want to guarantee a certain level of QoS contained in a S*ervice Level Agreement* (SLA) need to constantly monitor if the provided service meets this agreement. If it does not they must quickly find out the cause and the location of the degradation of the QoS. Monitoring at all routers in the network may help to detect this kind of problem but is too costly to be constantly performed in sufficient detail. Furthermore it raises the problem of correlating the degraded performance of a service session with the behavior of specific routers. Lastly, a huge burden is put onto the network by permanent monitoring and reporting also the vast majority of the traffic with has no specific QoS demand.
Path-coupled monitoring techniques imply a direct correlation of the metered data with a specific data path and assure that only the required metering entities are configured. Therefore, the M-NSLP is a good candidate to control the compliance of the network behavior with QoS requirements. First of all it is of interest if a connection matches the requested QoS parameters inside a specific domain, for example the core network of an ISP. Path-coupled monitoring can be used by specifying the first and the last node in the network on the data path to monitor the packet flow [25].
In case of QoS non-conformance, further analysis can be undertaken. Different meters on the path can collaborate to localize segments of the network responsible for QoS violation (see Fig 5). Subsequently, additional data can be gathered on the identified segments. Depending on the service type, meters can be configured differently to determine the behavior of the link. Meters inside a suspect section can be configured to measure delay of individual packets between all meters in the section.

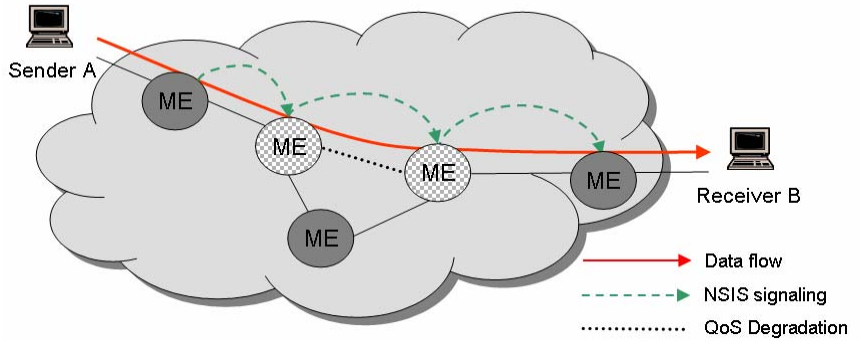

Fig 5. QoS Degradation

4.2.2 Requirements

An important requirement for QoS measurements is sufficient accuracy. It is important to avoid impact on the measured traffic. Accuracy additionally depends on the location of the meters. E.g., to measure end-to-end delay, the meters should be situated as close as possible to source and destination of traffic.

4.2.3 Applicability of M-NSLP

Monitoring QoS of a session is highly related to the chosen data path. M-NSLP is a good choice to setup the metering to measure particular characteristics of a flow. Depending on the parameters that should be metered, different meters become involved. For hop-by-hop delay or packet loss measurement, all the meters on this particular data path get involved. For end-to-end delay measurement meters close to the source and the destination are configured, while bandwidth measurements can be performed at a single meter.

4.3 Monitoring Configuration for Intrusion Detection

Intrusion Detection Systems (IDS) are an important part of effective security architectures. They provide means to detect and prevent unauthorized behavior which might be harmful. Especially network based intrusion detection systems can detect malicious traffic and prevent negative impacts. Usually, their efficiency depends largely on the quality of the analysis of the network traffic if it can be considered hostile or as authorized communication. Only if network traffic can be classified as hostile with a high confidentiality, intrusion response can be put in action. The classification depends on the quality and amount of analyzed data.

Many network security mechanisms such as intrusion detection are based on the capability to monitor the network behavior. Monitoring on the path enables new means to detect ongoing attacks and intrusion attempts.

Different meters can report to a single collector which can draw further conclusions about the suspicious traffic. More data can be analyzed due to the distributed processing in comparison with the centralized approaches. Prior inaccessible information like topology data can now be taken into account to trace down attackers. The merging of information from different sources in the network can show the pattern of an intrusion or an attack.

4.3.1 Scenario Details

Including the network meters into the available information base of the intrusion detection provides better means to detect patterns of malicious behavior in the traffic flows. M-NSLP offers mechanisms to distribute the sensors across the network instead of monitoring a limited scope of the traffic.

The basic idea of intrusion detection systems is to constantly monitor the data flows and traffic patterns for known intrusions and suspicious anomalies. In case suspicious traffic patterns were detected further analysis is triggered. The intrusion detection system examines particular flows by configuring the appropriate meters along the data path.

Network monitoring can provide statistics by collecting statistical measures such as packet rate, bit rate, and others. An in-depth analysis of the packet payload for signatures of well known patterns can identify an intrusion attempt.

Anomaly detection is one method of intrusion detection systems to detect priory unknown attacks by inspecting the difference with network behavior considered as normal. Malicious behavior can be identified by comparing it with regular traffic data without intrusion attempts. This technique profits especially from the larger available information base and the correlation between topological location and monitored behavior.

If an attack is being assumed the monitoring devices can be re-configured dynamically to gather more information about specific data flows. Depending on the assumed intrusion the meters can be configured to inspect special packets in more depth, say ICMP packets during an ICMP flood.

In contrast to the two previous scenarios the collector plays a different role for intrusion detection, because the more specific the data is about the malicious traffic the better the analysis gets. Aggregation might harm the chances of the intrusion detection system to detect a security violation. Hence one might expect an intrusion detection system to be co-located with the collector to gather all the data from the meters but that the collector only issues reports in case of detected intrusions.

One can take self-replicating malicious code like internet worms as an example how the intrusion detection could work. The distribution of internet worms like W.32/Blaster can be detected as it distributes itself. Pre-configured meters at the network constantly monitor the traffic for anomalies and known intrusions. When a priory unknown worm is released the malicious code would probably be undetected during a first short time. As some computers get infected and try to infect other machines the traffic patterns change. The meters would detect these anomalies and start further analysis by configuring additional rules for the meters. As more and more traffic emerges in the network showing the same behavior it can be concluded that the traffic is potentially malicious and demands for further, maybe manual analysis.

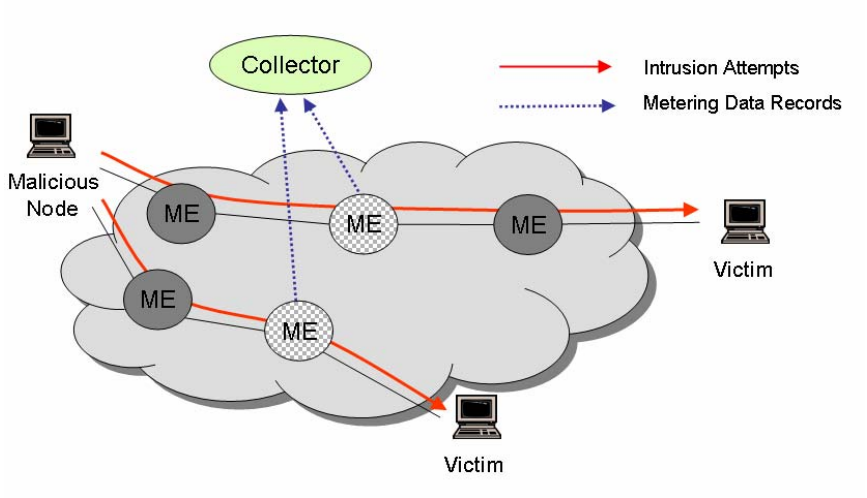

Fig 6. IDS correlating simultaneous intrusion attempts

4.3.2 Requirements

Intrusion detection must be able to detect attacks and intrusion attempts as early as possible. A constant surveillance of the traffic is mandatory to detect these events right from the start. If suspicious traffic patterns are detected an alarm is to be triggered. However, before intrusion response is initiated a high confidence in the malicious nature of network traffic is required. Say traffic might be rate limited or even blocked if the traffic is proven to be malicious. Otherwise the intrusion detection system might content with examining the traffic further if no ultimate conclusion about the nature can be reached.

Sufficient monitoring capacity must be available to prevent an overflow of measurements which could be used actively to disguise an intrusion. After an intrusion is detected advice should be deduced on how to cope with the intrusion and what countermeasures are advisable.

Intrusion detection systems should not be detectable by intruders to make it harder for the intruder to fool the sensors. An intruder can conclude if an intrusion detection system is active from changes of the network characteristics, for example, additional delay can be observed. Hence the intrusion detection system should impose no changes of the network behavior.

4.3.3 Applicability of M-NSLP

The benefits of using M-NSLP are manifold for intrusion detection systems. Improved network monitoring capabilities increase the chance of detecting an intrusion. The intrusion detection system can derive detailed statistics from the meter records which are generated at different points in the network. The correlation between topology information and packet statistics provides new analysis capabilities.

The gathered information about the network traffic can be used for an analysis of packet's payload for known attack/intrusion patterns as well as for anomaly detection mechanisms. It is desirable that monitoring devices can be re-configured dynamically, depending on the state of the network to know more about a specific data flow when an attack is being assumed. Note, that the configuration may be different depending on the nature of the attack, for example an ICMP flood.

The distribution of the metering provides enhanced resources for the analysis of the traffic. Collectors help to pre-process the data to avoid overloading the intrusion detection system. Suspicious traffic can be traced by utilizing the flow based configuration of the meters. Correlation between different suspicious data flows (as depicted in Fig 6) can provide useful information especially for anomaly detection.

Monitoring of different network capabilities serves as an input for the intrusion detection: Statistics are generated, for example by the collection of statistical measures, such as packet rate, bit rate, number of connections, and other parameters. Not all traffic is equally relevant for the intrusion detection. M-NSLP can configure metering entities to sample packets based on specified sampling algorithms in order to analyze only those packets.

5. Discussion

In the last section, we presented different scenarios where the path-coupled configuration of the metering entities is advantageous. The benefits of using path-coupled signaling for metering configuration are manifold:

- Configuring all the MEs in the network of the ISP to meter a data flow from A to B would be a tremendous waist of resources, since most of the MEs in the network will not be traversed by this flow, and therefore are unable to perform any metering/monitoring for it anyway. The configuration of the MEs using the Metering NSLP is a smart solution to solve this problem, since only MEs along the data path will be configured.
- Dynamic configuration signaling can setup flow-based metering mechanisms without knowledge of the particular address of the meters. The autonomous discovery of applicable meters at the data path provides an abstraction of the metering specification from the implementation of the

traffic measurements at specialized nodes.

- The distribution of the metering tasks over a large pool of meters provides a higher overall capacity in comparison with centralized approaches. Load balancing techniques which can be implemented on top of the Metering NSLP enhance the available capacity and avoid bottlenecks. Many applications can profit from the extended information source. Furthermore the collector implements a distributed pre-processing of metering records and relieves the load at central recipients like, for example, charging systems and network management tools.
- Fault tolerance can be easily accomplished by the regular refresh messages sent along the data path. In case of an error the system will autonomously reconfigure itself and assign the metering task to another meter.
- The MEs that will be configured are located along the topologically optimal route. For example, in current accounting architectures, the traffic is enforced to pass via statically configured nodes that perform the accounting and that are not necessarily located on the topologically optimal data path. In contrast, Metering NSLP allows a dynamic and automated discovery of MEs on the optimal data path.
- Finally, the Metering NSLP allows the distribution of the metering tasks along all the MEs in the network making use of the resources and capabilities of the existing network infrastructure.

However, using the Metering NSLP has also some issues that still need further investigation and improvement.

- The time required to establish the required state information for the Metering NSLP along the path might be too long. As mentioned above, the signaling path is constructed hop by hop. At each hop, a route discovery message with router alert options needs to be sent along the path. After processing the router alert option, a messaging association needs to be established with the previous hop. If this messaging association needs to be secured, then further messages exchange and processing is required to establish the security association. This can cause a considerable delay that is no affordable for real-time applications or for very short sessions. However, in the ideal case, security associations will be already established between neighboring NSIS hops. Moreover, security associations might be optional if the signaling messages do not leave the trusted domain, for example, within an operator network.
- Another problem for the Metering NSLP is route changes. If a route change can be detected after a few seconds, this might be not critical for QoS measurement. Depending on the environment, it might be also not critical for intrusion detection if some packets pass by unmonitored as long as a potential intruder possesses no means to trigger route changes. However besides these scenarios route changes must be detected as soon as possible. As already mentioned above, the NSIS transport protocol (NTLP) detects dynamic route changes using different triggers, such as monitoring changes in routing tables or inference from changes in signaling packet TTL. NTLP is responsible for detecting route changes and informs the local Metering NSLP on the same node, which in turn must send an asynchronous notification to the signaling initiator. The signaling initiator needs then to re-initiate the signaling. Therefore, if for instance, a metering entity performing accounting is not on the path anymore, a new metering entity on the new path must be elected to take over the currently unassigned accounting tasks. The accounting scenario requires more accurate monitoring and can not afford to miss packets during route changes. The strategy make-before-break, if applicable, can establish the accounting configuration on the future data path before the path change occurs.

Route changes are in fact a general problem for path-coupled signaling. However, some optimizations can be investigated to cope with the problem efficiently. For instance, in mobility scenarios the necessary configuration information could be moved from the old access point to the new one during the handover. The new access point can then re-initiate the signaling for each of the involved NSLPs, in particular the Metering NSLP. In the ideal case, this could happen before the handover is achieved and packets are routed via the new access points (make-before-break).

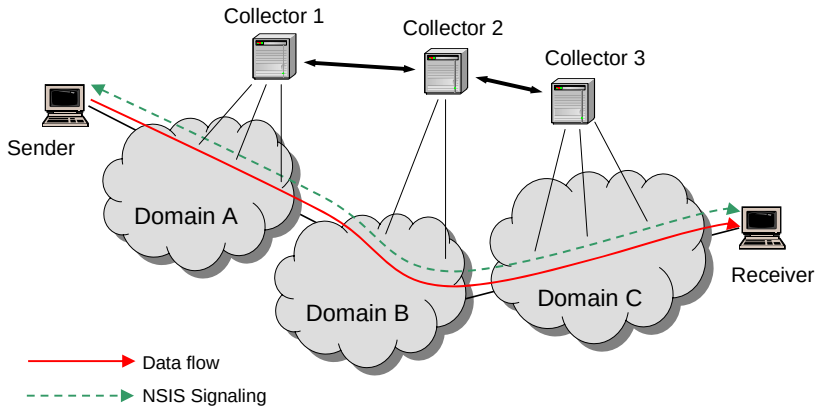

Fig 7. Multiple Domain Signaling with NSIS

Another challenge for the Metering NSLP is the inter-working between multiple domains. Fig 7 shows an example how the Metering NSLP could operate across several domains. The signaling messages go beyond one network domain and configure the metering entities on the path in the other domains. Metering entities along the path that participate in the metering process send their metering records to the appropriate collector. There might be one or more collectors per domain. The collectors of different domains exchange the metering records between each other.

For example, network domain A might want to collect resource records in network domain B to offer the user a more consistent bill covering both the price of the network resource consumption and the application usage. A high degree of trust is required to allow other domains to configure metering entities and to collect the resource usage of particular users.

Metering across the border of a single domain would also add significant and helpful information in the intrusion detection scenario. By cooperating together, neighboring network domain can resist better against attacks. Also, it would be useful to measure QoS parameters across several domains. For example, it would be useful to measure the delay or packet loss per domain, or simply to measure the end-to-end delay. For these tasks an end-to-end signaling of metering configuration is required.

However, the process of configuring an Internet-wide metering system is a challenging task. Administrators of other domains will not be easily willing to allow data traffic to be sent and redirected to a collector outside the domain. Customer privacy comes into question. Exchanging monitoring data between different domains might severely impact the users trust perception about the attached domain. For this reason, concepts for the confidentiality and privacy of the monitoring data need to be investigated.

6. Conclusions

In conclusion it can be said that we were able to present and assess an approach for metering configuration that has numerous advantages compared to existing solutions. The configuration of distributed meters or monitors, especially in large scale IP-based networks with a complex topology always required costly operation and management. As the complexity of the network architectures increases with the introduction of new services, the need for a flexible and easily maintainable configuration mechanism becomes urgent.

Path-coupled signaling for metering configuration is a viable candidate for the dynamic configuration of the distributed monitoring. Using on-path signaling covers existing configuration demands but requires noticeably less overhead. The dynamic discovery of monitoring capabilities can keep network management functions agnostic of the site of the meters in the network topology. It solely must specify the tasks that must be metered but does not have to care which monitor will provide the measurements in the end. Network architectures can employ new services more flexible than nowadays. As shown for the application scenarios, our approach is applicable to a widespread spectrum of configuration tasks, since it is flexible and extensible to new requirements. By using the Metering NSLP for the configuration for QoS, Accounting, and Intrusion Detection at the same time, the network operator can leverage synergetic effects due to the lower operational costs of joint monitoring of usage parameters.

Acknowledgments

Parts of this work are an outcome of the standardization work within the IETF. Besides the authors of this paper, Jürgen Quittek and Hannes Tschofenig are main contributors to the proposed Metering NSLP protocol standard.

References

[1] 3GPP, "Telecommunication management; Charging management; On line Charging System (OCS) architecture study," 3GPP, TR 32.815, 2003.

[2] 3GPP, "All-IP network (AIPN) feasibility study," 3GPP, TR 22.978, 2005.

[3] G. Almes, S. Kalidindi, and M. Zekauskas, "A One-way Delay Metric for IPPM," RFC 2679, September 1999.

[4] G. Almes, S. Kalidindi, and M. Zekauskas, "A One-way Packet Loss Metric for IPPM," RFC 2680, September 1999.

[5] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," RFC 2205, September 1997.

[6] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588, September 2003.

[7] G. Carle, F. Hartanto, M. Smirnov, and T. Zseby, "Charging and Accounting Architecture for QoS-enhanced IP Services," Competence Center for Global Networking (GloNe), GMD FOKUS, Berlin, Germany, Technical Report 11-98, 1998.

[8] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)," RFC 1157, May 1990.

[9] J. Case, M. McCloghrie, M. Rose, and S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network

Management Protocol (SNMPv2)," RFC 1902, January 1996.
[10] T. Dietz and B. Claise, "Definitions of Managed Objects for Packet Sampling," Internet-Draft, draft-ietf-psamp-mib-04.txt, February 2005.
[11] F. Dressler, "An Approach to Select a Best Suitable Video Server," Proceedings of International Conference on Advances in Infrastructure for Electronic Business, Education, Science, Medicine, and Mobile Technologies on the Internet (SSGRR 2003w), L'Aquila, Italy, January 2003.
[12] F. Dressler, "A Metric for Numerical Evaluation of the QoS of an Internet Connection," Proceedings of 18th International Teletraffic Congress (ITC18), vol. 5b, Berlin, Germany, August 2003, pp. 1221-1230.
[13] F. Dressler, A. Fessi, J. Quittek, C. Kappler, and H. Tschofenig, "NSLP for Metering Configuration Signaling," Internet-Draft, draft-dressler-nsis-metering-nslp-02.txt, July 2005.
[14] A. Fessi, C. Kappler, C. Fan, F. Dressler, and A. Klenk, "Framework for Metering NSLP," Internet-Draft, draft-fessi-nsis-m-nslp-framework-01.txt, July 2005.
[15] U. Foell, C. Fan, G. Carle, F. Dressler, and M. Roshandel, "Service-Oriented Accounting and Charging for 3G and B3G Mobile Environments," Proceedings of 9th IFIP/IEEE International Symposium on Integrated Network Management (IM 2005), Nice, France, May 2005.
[16] X. Fu, A. Bader, D. Hogrefe, C. Kappler, G. Karagiannis, H. Schulzrinne, H. Tschofenig, and S. van den Bosch, "NSIS: A New Extensible IP Signaling Protocol Suite," *IEEE Communications Magazine*, 2005. (to appear)
[17] S. Hallé, R. Deca, O. Cherkaoui, R. Villemaire, and D. Puche, "A Formal Validation Model for the Netconf Protocol," Proceedings of 15th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2004), Davis, CA, USA, November 2004, pp. 147-158.
[18] R. Hancock, G. Karagiannis, J. Loughney, and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework," RFC 4080, June 2005.
[19] R. Hancock, C. Kappler, J. Quittek, and M. Stiermerling, "A Problem Statement for Path-Decoupled Signalling in NSIS," Internet-Draft, draft-hancock-nsis-pds-problem-01.txt, July 2005.
[20] M. Koutsopoulou, A. Kalaoxylos, and A. Alonistioti, "Charging, Accounting and Billing as a Sophisticated and Reconfigurable Discrete Service for next Generation Mobile Networks," Proceedings of IEEE Semiannual Vehicular Technology Conference (Fall VTC2002), Vancouver, Canada, September 2002.
[21] S. Lee, S. Jeong, H. Tschofenig, X. Fu, and J. Manner, "Applicability Statement of NSIS Protocols in Mobile Environments," Internet-Draft, draft-ietf-nsis-applicability-mobility-signaling-02.txt, July 2005.
[22] J. Manner, G. Karagiannis, A. McDonald, and S. Van den Bosch, "NSLP for Quality-of-Service signalling," Internet-Draft, draft-ietf-nsis-qos-nslp-07.txt, July 2005.
[23] V. Paxson, J. Mahdavi, A. Adams, and M. Mathis, "An Architecture for Large-Scale Internet Measurement," *IEEE Communications Magazine*, vol. 31 (8), August 1998.
[24] A. Pras, B.-J. van Beijnum, R. Sprenkels, and R. Parhony, "Internet Accounting," *IEEE Communications Magazine*, vol. 39 (5), pp. 108-113, May 2001.
[25] F. Raspall, Q. J, M. Brunner, and M. Martin, "Path-Coupled Configuration of Passive Measurements," Proceedings of Inter-domain Performance and Simulation Workshop, Budapest, Hungary, March 2004.
[26] H. Schulzrinne and R. Hancock, "GIMPS: General Internet Messaging Protocol for Signaling," Internet-Draft, draft-ietf-nsis-ntlp-04.txt, October 2004.
[27] M. Stiermerling, H. Tschofenig, and C. Aoun, "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)," Internet Draft, draft-ietf-nsis-nslp-natfw-07.txt, July 2005.
[28] T. Zseby, S. Zander, and G. Carle, "Policy-Based Accounting," RFC 3334, October 2002.