The CoNSIS Approaches to Network Management and Monitoring

Christoph Barz, Anne Diefenbach, Fatih Abut,
Matthias Wilmes, Peter Sevenich
Communication Systems Group
Fraunhofer FKIE
Wachtberg, Germany
christoph.barz@fkie.fraunhofer.de

Pierre Simon, Norbert Bret
Cogisys
Pertuis, France
pierre.simon@cogisys.fr

Abstract—**Secure information exchange is a key success factor for military operations. International coalition missions are especially challenging because of heterogeneous communication and C2IS equipment. The international project CoNSIS is targeted to fill in technical gaps regarding interoperability which occur in a reference scenario, consisting of a multinational convoy of military and non-governmental vehicles. The convoy forms an ad-hoc radio network and shares a common operational picture with an international headquarter mainly via a satellite link. This paper addresses network management challenges and technical solutions for this federated scenario. Both the core network interconnecting different national headquarters with an international headquarter as well as the ad-hoc radio network of the convoy are addressed in a single, seamless concept. In June 2012, field tests with the convoy were carried out in order to evaluate the different technical solutions.**

Keywords- network management; measurement architecture; federation; protected core networking; service level agreements

I. INTRODUCTION

CoNSIS – Coalition Networks for Secure Information Sharing – is an international project with France, Norway, Germany and the US currently participating. Based on the work done in INSC – Interoperable Networks for Secure Communications – it aims to work towards Network Enabled Capability (NEC). Heterogeneous networks from different nations are to be connected and form a federated environment in which to securely share information. CoNSIS concentrates on wireless networks in the tactical domain, but also considers deployed high speed networks as well as communication in-between. On the higher network layers, it places emphasis on a service-oriented architecture as stipulated in the NNEC Feasibility Study [1].

Work in CoNSIS is performed in five distinct groups. Task 1 is concerned with communication services. Task 2 is responsible for the integration of the SOA frameworks of the different nations. Task 3 is concerned with security, and task 4 with network management. Task 5 is responsible for the overall architecture and a field test scenario (see below) which serves as golden thread for all technical developments. The project concludes its first phase with the field tests in June 2012. This paper will concentrate on the work done in the network management task.

The CoNSIS scenario as depicted in Figure 1 is set in a country torn by civil war. International coalition troops are deployed in the country to stabilize the situation, protect the population and initiate the peace process. Larger cities are controlled by coalition forces, but the situation outside the cities is still unstable. Convoys and advanced outposts are constantly at risk of attack. The coalition troops have established an international headquarter (HQ) which has fixed network connections to several national headquarters. There are also naval forces from different nations patrolling the waters around the conflict area. The naval vessels form a wireless ad-hoc network and are connected to the other forces via satellite. There is also a backup HF radio connection.

In this situation, a natural disaster occurs in a part of the country not controlled by the coalition forces. The coalition decides to aid in disaster relief efforts by escorting the vehicles of a Non-Governmental humanitarian Organization (NGO) to the disaster site and secure the area. The military vehicles are connected by different broadband military radio technologies operating mainly in the UHF frequency spectrum, forming another ad-hoc network. As with the naval vessels, communication with the headquarters is ensured via satellite technology installed on a few specifically equipped vehicles. The NGO vehicles are also connected to the military convoy by terrestrial radio. Shortly after setting out, the convoy is joined by a second group of military vehicles from another nation. This group uses radios not compatible with the convoy's, but a few vehicles in both groups have radios with compatible waveforms to bridge the communication between the two groups. Following a reorganization of the network in the wireless domain, they now form a comprehensive ad-hoc network.

Making its way to the disaster area, the radio communication within the newly combined convoy is suddenly disrupted by a radio jammer. Satellite communication remains unaffected. The jamming is recognized, reported to the headquarters, and finally eliminated by an air strike.

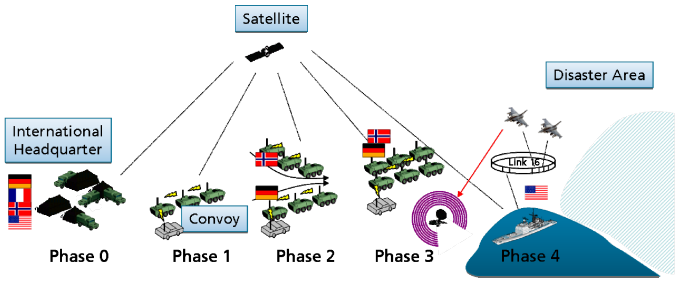

Figure 1: The CoNSIS network

The remainder of this paper is organized as follows. Section II will introduce related work which has been incorporated in the CoNSIS management concept. Section III will on this basis describe the CoNSIS management concepts, while section IV and V detail the test setup and the network management experiments performed in the field test.

II. Related Work

The CoNSIS reference model consists of a core network to which user domains are connected via IPsec crypto devices. The core network itself is composed of a number of interworking networks operated by different administrative authorities. Figure 2 shows the main elements of the CoNSIS architecture.

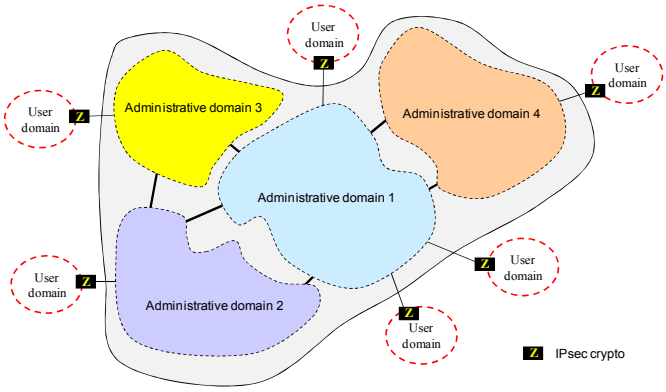

Figure 2: Administrative Domains

This architecture is close to the Protected Core Network (PCN) [2] approach.

A. Protected Core Networking

In the PCN concept, secure red networks are represented by the Coloured Clouds (CCs), while the unprotected black network represents the Protected Core. PCN now requires the existence of certain distinguished nodes, the E-nodes, in the black network, which ensure availability and offer reliable transport to the CCs. These routers may be clustered to Protected Core Segments (PCSs) which together form the PCN. There are certain functionalities like traffic concealment that are associated with the E-nodes. In addition, the PCN concept defines interfaces between different PCS and between PCS and the Coloured Clouds.

The CoNSIS network architecture is based on this concept, but the two reference models are not identical. In particular, CoNSIS administrative domains are not assumed to have exactly the same functions as PCSs regarding e.g. security protection and the management of SLAs. The administrative domains interwork via interfaces which are not supposed to have the same features as the PCS-1 interface. Likewise, the generic interface between CoNSIS user domains and the core network is not necessarily compliant with the PCS-2 interface.

In order to reflect the above-mentioned divergence, objects of the CoNSIS reference model are given names intentionally different from their PCN counterparts (see Figure 3):

- The core network (counterpart of the PCN protected core) is referred to as the **Transport Network** (TN).
- The TN is a collection of interworking **Transport Network Segments** (TNS) (counterpart of PCSs), each TNS being defined as a set of network elements under a single administrative authority. A segment administered by a national authority is referred to as an N-TNS while a segment administered by the coalition is a C-TNS.
- User domains are referred to as **Coloured Enclaves** (CE) (counterparts of coloured clouds), separated from the TNS by IPSec. A CE can be embedded within another CE; in that case it is called an **Inner Coloured Enclave** (ICE).

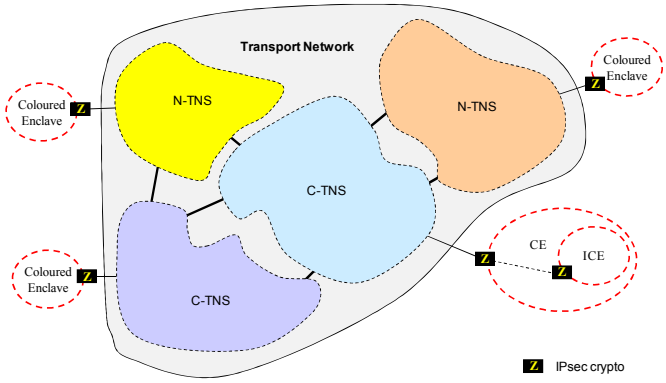

Figure 3: Network Segments and Colored Enclaves

B. Federated Sharing of Management Data

The TN with its individually-administered TNSs poses a challenge to management because there is no single authority to determine how, where and when the network should be monitored, and some nations may hesitate to reveal their network structure. This situation is similar to civil federated networks, such as research networks administered by different organizations. For these, there is a monitoring framework available.

PerfSONAR [3] is a network performance monitoring framework that is developed by an international consortium from the research and education community. GÉANT (Europe), ESnet, Internet 2 (USA) and RNP (Brazil) offer their customers advanced inter-domain QoS services. Delivering end-to-end QoS in a hierarchical multi-provider structure results in challenges similar to the ones occurring in a coalition

network. The perfSONAR framework is an infrastructure for network performance monitoring, making it easier to solve end-to-end performance problems on paths crossing several networks.

PerfSONAR uses a service-oriented architecture. The SOAP and XML based messages between the different service types are standardized by the Network Measurement Working Group of the Open Grid Forum. There is already a variety of service implementations available. In addition, the open, standardized interfaces allow for an integration of additional measurement tools, including existing solutions like Cacti [12]. PerfSONAR is already deployed at many National Research and Education Networks (NREN) around the world.

The PerfSONAR multi-domain monitoring (MDM) service allows cross-domain performance monitoring with standardized metrics. The perfSONAR infrastructure consists of a User Interface Layer, a Web Service Layer, and a Measurement Layer. There are already several visualization tool implementations that are designed for different scenarios. At the Service Layer, the following Web services have been implemented:

- **Lookup WS** – allows the discovery of available services and information sources
- **Authentication WS** – provides authentication for clients and protects privacy
- **Measurement Archive WS** – is a family of WS that allow access to measurement data from different sources (e.g. databases, files, etc.)
- **Measurement Point WS** – allows integration of measurement tools and publishing the collected data in Measurement Archives

Depending on the measurement tools used, packet based measurements with IPv4, IPv6 and different QoS configurations are supported. In addition to the WS presented above, a Transformation WS has been defined but not implemented yet. For further information, a compact survey of the perfSONAR features is presented in [4]. An overview of the perfSONAR architecture can be found in [5] and [7].

III. CONSIS MANAGEMENT CONCEPTS

As mentioned in section II.B, the concept of a Transport Network consisting of Transport Network Segments which are managed under the administrative authority of different countries can be conceived as a multi-provider network. In general, the challenges of delivering end-to-end inter-provider QoS that were addressed in the network research community (e.g. [8]) also apply to the context of coalition networks. In addition to the standard information hiding requirements of network providers, special security considerations regarding the Coloured Enclaves have to be addressed when sharing monitoring data and managing the Transport Network Segments for military use. The general challenges that were identified in [8] are:

- *Common service definitions* for all administrative domains
- *Common performance metrics* to support end-to-end SLAs

Common service definitions are already addressed by CoNSIS task 1 in [11] (DSCP/Application Requirements). Without this standardisation a meaningful end-to-end service is hard to obtain.

Common performance metrics must be used if performance information needs to be concatenated across the different providers. This does not only include the definition of the metrics themselves, but also the definition of common aggregation periods for samples and the use of reference times. Concatenation of measurements of different network segments enables a scalable approach to the control of end-to-end SLAs. This can be achieved by sectioning the network into multiple measurement segments, allowing the reuse of these measurements for different end-to-end paths. Note that the segmentation of the Transport Network already induces measurement segments. A framework for the concatenation of performance metrics [13][14] has been under development by the IETF.

Multi-provider/multi-segment QoS paths result in the need for mechanisms to allocate budgets for different network impairments (e.g. delay, jitter, …) that are defined on an end-to-end basis along the path to the different network segments which are separate administrative domains. Here, approaches include a static, a dynamic and a hybrid allocation of the acceptable end-to-end impairments. In the static approach, the maximum number of Transport Network Segments could be assumed in the path. The impairments are then equally distributed between these segments. However, this approach is less efficient and may rule out possible inter-TNS paths. The dynamic negotiation approach is most efficient but requires signalling between the TNSs. In the hybrid approach, all impairments are shared equally only with segments on the path. Thus, it does not support situations in which only an unequal distribution of impairments would result in an acceptable SLA.

This leads to the discussion of provider/segment interconnection models for dynamic QoS negotiation. Here, a hierarchical third party model (e.g. realized by the NATO in the form of NATO service classes) can be envisioned, as well as a cooperative model. To respect the autonomy of the different countries managing the Transport Network Segments as well as for resilience reasons, the distributed cooperative negotiation model in combination with a centralized definition of common service classes and performance metrics seems to be the most appropriate solution. In addition, a distributed approach may be more resilient to outages. Here, knowledge of the E-Node topology might be beneficial for assessing the end-to-end connectivity and for finding an impairment allocation.

A similar challenge may arise within Transport TNSs if they are also organized as overlay networks. Links between E-Nodes may be realized by several lower layer links by one or more independent providers. If these providers do not offer common NATO service classes the next better national service classes have to be chosen.

As described in section II, the management and monitoring architecture is defined for coalition networks on the basis of TNSs and Technical Management Areas (TMAs) within the TNSs. As depicted in the following sections, the concept comprises three different interfaces related to monitoring (see

Figure 4). Other management interfaces regarding configuration management are still to be defined in detail. However, Figure 5 and the description MI 4 and MI 5 provide first suggestions regarding a configuration architecture.

MI 1: The network monitoring interface MI 1 specifies the communication between measurement points and measurement archives and is national concern. It might be either based on standard network management protocols like SNMP, a proprietary solution or based on a standardized Web service interface. The latter case should be preferred. For existing tools a wrapper to encapsulate implementation specific communication has to be implemented.

MI 2 is used to transport monitoring information from measurement archives in the TMAs to the corresponding measurement archives in the national CEs. A transformation service can be used to transform raw measurement data into a format that can be shared between the different CEs. Task 3 will provide the transfer channel for the national monitoring data. Ways to accomplish this without compromising the confidentiality of red data are discussed in [6].

MI 3 specifies the communication for distributing measurement and monitoring information between the CEs. A lookup service is responsible for advertising available measurements and to make the results available to search queries. The service will be based on SOA. Details of the monitoring Web service definitions will be part of a task 2 document. Task 2 is responsible to provide the monitoring UI.

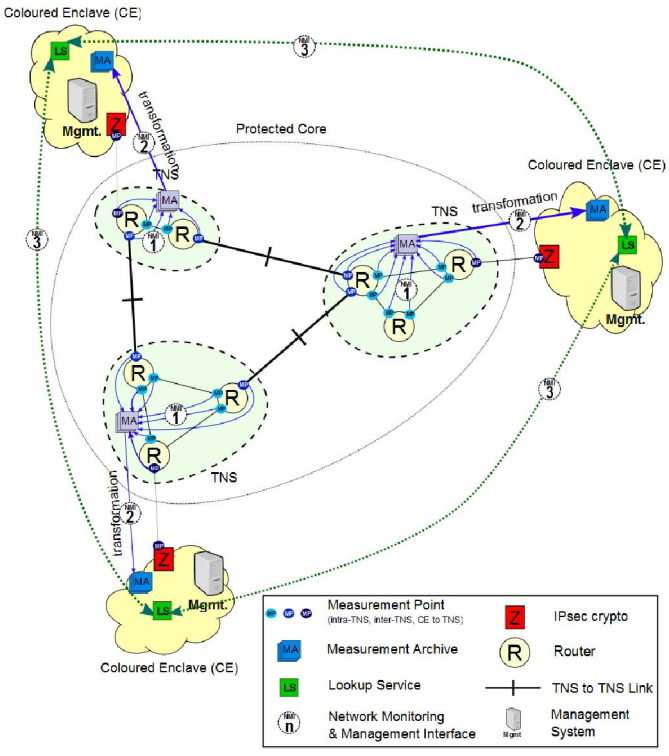

Figure 4: Refined Performance Monitoring Architecture

MI 4 specifies an SLA negotiation/agreement interface between an Overall Coalition Manager and the different TNS Managers. This multi-domain QoS negotiation mechanism will work via bilateral communication between the Overall Coalition Manager and the Local TNS Managers. The communication resources are under the authority of the local TNS Managers which act as a "management decision point". [9] presents a similar approach.

MI 5 specifies a configuration interface between the local TNS Managers and the Technical Management Areas under their administration. It is assumed that each TMA has special configuration management tools that might be proprietary. The TNS Manager will act as "management enforcement points". MI 5 should comprise high level technology agnostic configuration commands that need to be translated into a technology specific configuration by the appropriate configuration management tools.

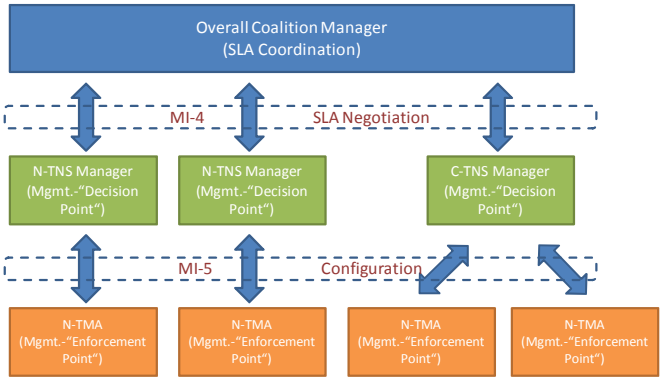

Figure 5: SLA Negotiation and Configuration Architecture

IV. CoNSIS Field Test Setup

Experimentation in CoNSIS has a strong focus on the mobile part of the network, i.e. the convoy. It consists of three parts: NGO vehicles, Norwegian military vehicles (the original convoy), and German military vehicles (which join the convoy in phase 2). The German vehicles use three different types of radio, HiMoNN (IABG), FlexNet-4 (Rockwell Collins) and Harris radios. The Norwegian part uses Kongsberg WM600 radios and the NGOs commercial WLAN. None of these radio types are interoperable, which is why one Kongsberg radio is passed to the German convoy and one FlexNet-4 to the Norwegian one. In addition, at least one German and one Norwegian vehicle have a satellite connection. All UHF military radios in our scenario perform ad-hoc routing within their technology domain, which normally cannot be deactivated and provides no information about the internal topology. In addition, multi topology routing is not supported so far. Thus, these incompatible technologies need to be tied together in an overlay network with multi topology routing [10] support to cope for the heterogeneity of the different technologies. To overcome these limitations, a liaison with COALWND, the interoperable coalition wideband networking waveform for military radios under development, is planned to eliminate the need for a second layer of routing.

Jammer detection is usually done by dedicated, strategically placed units. In CoNSIS, there is an experimental option of the jammed systems doing the detection themselves. To detect a jamming incident locally, information from different network

layers must be correlated, which requires a cross-layer information architecture. Besides reporting the incident to the international headquarter, local measures may be taken to circumvent the jamming, such as changing frequency or modulation or reconfiguring the routing.

V. CoNSIS Management Experiments

Not all of the concepts described above can be realized in the CoNSIS field test. However, there are several experiments which will lay the foundations and serve as proof-of-concept:

A. Core Network Experiments

1) MA-Basic: Maintain a common network picture

Purpose: Show how monitoring information can be shared between the HQs of the different nations regarding the network state within the different non-mobile ASs and on the inter-ASs links/tunnels. The experiment helps to identify problems within the TNSs and the inter-TNS links.

Test setup: PerfSONAR measurement archives collecting SNMP information from core TNS routers within each AS are installed as depicted in Figure 6.

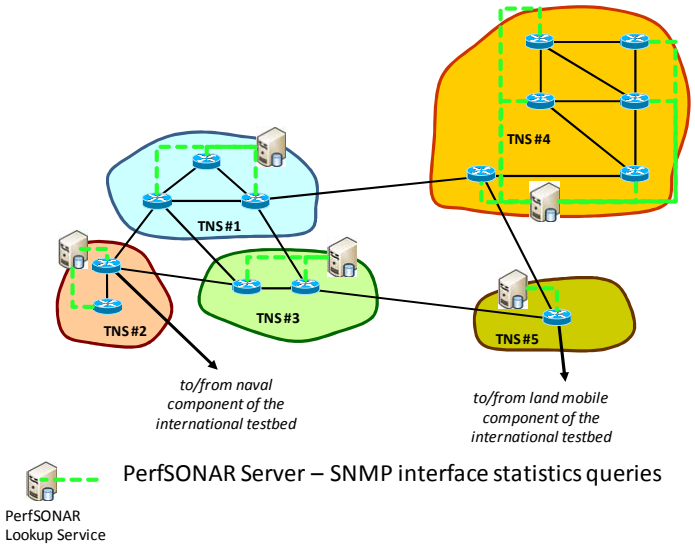

Figure 6: PerfSONAR SNMP Interface Statistic Queries

In addition, measurement archives collecting Iperf and OWAMP measurements from the inter-TNS links are installed. The information will be archived so the experiment also supports an offline analysis also regarding other experiments.

Walkthrough: Deployment and activation of the service is performed prior to the experiment. All nations can access the information via a Web based client during the whole experiment. All information is stored in local measurement archives. If necessary, measurement archives have to be cleared before the experimentation so there is be enough storage capacity. In regular intervals the archives were backed up.

Prerequisites and special requirements: For autonomy reasons, PerfSONAR Measurement Archives (and a Lookup Service) were installed in every AS participating in the measurements (see Figure 7). Participating nations set up one or more virtual machines. In addition, an NTP server was needed to synchronize the measurements.

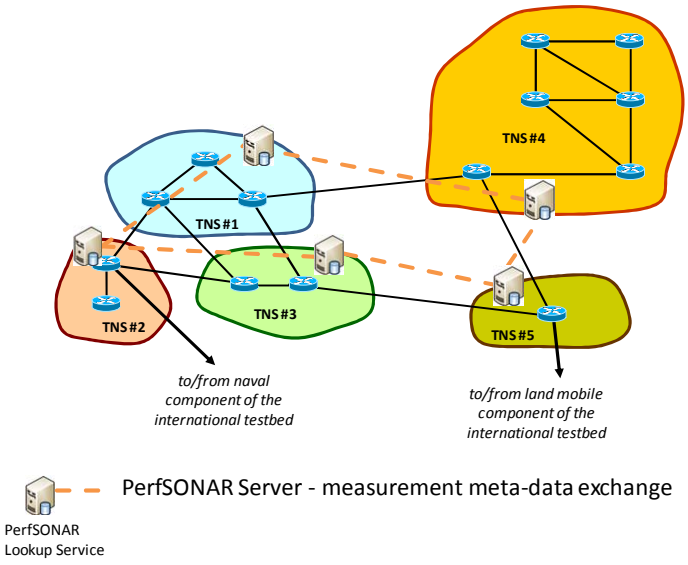

Figure 7: PerfSONAR Measurement Metadata Exchange

Findings: Sharing monitoring data between the different TNSs worked well in general. The performance of intra- and inter-TNS links in the non-mobile part of the network was accessible. Some performance issues querying data from within the US TNS will be analyzed as future work.

2) MA-SOA: Provide access to PerfSONAR data via the SOA Architecture

Purpose: Access to OWAMP data stored by PerfSONAR in a MA via a standard Web service as utilized in the CoNSIS SOA architecture. One application is the provision of data for generating technical profiles (see experiment 4) in this section).

Test setup: A SOA service acts as consumer to the PerfSONAR OWAMP measurement archives of the different nations. In turn, it offers access to the latest packet loss rate in a queried TNS for a queried class of service.

One particular client application that uses the data is the technical profile process in one or several TNSs. The communication is based on SOAP messages (standard Web service).

Walkthrough: The client process queries the information needed to generate a technical profile from the SOA service. This will be packet loss rates on various links and tunnels. The SOA service determines the archives holding the relevant information and retrieves the data. The retrieved data is processed and the packet loss rate is forwarded to the client.

Prerequisites and special requirements: The SOA service needs to be available in the TNS part of the network (not in the CEs). It does not use WS-Discovery but is statically configured.

3) Measurement Probes: Assess the usability and trustworthiness of various measurement probes

Purpose: Determine how and to what extent software probes can be used in a tactical network to provide measurement information.

Because they require in-depth investigation and comprehensive procedures, tests of this series were actually performed before the field experimentations described in this article, but on the same testbed and with the same technical means. They paved the way for the use of appropriate measurement tools during the field tests themselves.

Test setup: A broad array of measurement tools were tested, including Iperf, Internet2 OWAMP and Cisco IP SLAs which turned out to be the best ones.

Software probes have a special interest in a tactical environment for the obvious reason that they do not imply additional hardware and thus have no detrimental effect on the compactness of deployed assets. Conversely, they have the downside of providing results with a lower precision, and of requiring active test flows (i.e. specific measurement packets) which may be a source of overhead.

The precision and trustworthiness of software probes was assessed whenever needed by comparing the results they supply with those provided by hardware measurement tools such as Smartbit or Ipanema whose performances in terms of accuracy are acknowledged.

Findings: The major lessons learnt through the tests concern the precautions a network operator should take when using software probes, the precision that can be expected in measurements, and the consistency of results supplied by probes of different types.

Overall, all three above-mentioned software tools proved to be usable and to provide valuable information as long as they are operated in an appropriate environment and within their normal range. It was indeed an important discovery that *each measurement probe has a range* (e.g. of data rates, of number of packets per second) within which it will work properly, but beyond which it may supply erroneous, incomplete or inconsistent data. The recommendation is thus that a network operator should only use measurement devices whose range of valid operation has been duly tested prior to deployment.

It was also shown that, with appropriate procedures, the overhead due to active measurement flows could be kept under control and remains marginal as compared to user traffic, even in a narrow-bandwidth network.

Finally, special care must be taken when conducting active measurements in IP systems which implement such mechanisms as weighted fair queuing (WFQ). As WFQ creates a dissymmetry in the treatment of flows even if they belong to the same class of service, it may result in active test flows experiencing a different quality of service than the user flows they are intended to represent, and thus lead to erroneous conclusions in network performance monitoring. This is but one more illustration of the well known principle that measurements cannot be performed in total ignorance of the system they apply to.

Another important finding is that a given probe will provide results which are consistent with themselves, but not always as consistent with those of other probes. For example, Internet2 OWAMP used in two different segments of a network will indicate jitter values which can directly be compared together, and so will Iperf, but the measurements supplied by the two tools may not be consistent with one another. This bias which may exist between two different probes is no serious hindrance per se since a theoretical study leads to the conclusion that high precision in the measurements conducted in an IP network is not needed and should not be sought. However, when comparisons are made between measured values within a network, or when measurements are composed in space or in time, the same type of tool should be used throughout the system. PerfSONAR and its message format provides the means to distinguish measurements of different tools.

4) Technical Profiles: Use measurement results to automatically update the description of network capabilities

Purpose: A technical profile is a data set which describes the current capabilities of a TNS (e.g. the quality of service it is able to support, whether it is subject to sudden major alterations due to e.g. high mobility, jamming). This data set is intended to be communicated to users or adjacent networks so they will optimize the way they use the services of the relevant TNS.

Technical profiles were studied under the task 1 of CoNSIS (communication services), but an important aspect of their definition is that they should be kept up to date automatically so as to actually reflect the current transport conditions prevailing in a TNS. One essential way to update a technical profile is of course to use the results of measurements conducted according to the methods and procedures recommended by task 4.

Test setup: Host A is a Web server, host B is a web client. They are located in two different colored enclaves respectively connected to TNS 1 and TNS 4.

The technical profiles of these two TNSs are held by their respective Network Management Systems (NMSs). They are kept up to date thanks to measurements periodically performed by probes deployed throughout the two networks.

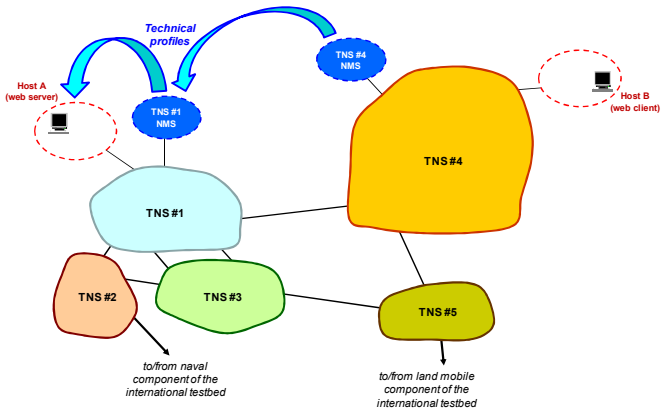

Figure 8: Technical profile repositories and user systems which will use these technical profiles

Walkthrough: When technical profile mechanisms are not enabled and when traffic conditions in TNS 4 are adverse, it takes an unacceptable time for host B to download a HTML page from host A.

When technical profile mechanisms are enabled, measurements permanently conducted in all TNSs allow the detection of a degradation of transport conditions (in this case a high packet loss rate in TNS 4), and this situation is reflected in the relevant technical profiles.

Whenever it receives a request from host B, host A first determines which TNSs will be traversed by the data flow it is about to send to the Web client. Then it fetches the technical profiles of TNSs 1 and 4 and composes them to find out that the path will be affected by a high packet loss rate.

Knowing this information, it decides to send to host B a HTML page with skimmed contents (i.e. with lower-resolution pictures). The time it takes for host B to download the page returns to an acceptable value.

At the end of this test, the best compromise has been automatically discovered to ensure end-to-end quality of service in the presence of degraded transport conditions detected through measurements.

Prerequisites and special requirements: Interface MI 2, as described in section III of this article, is required to convey to the colored domain information pertinent to the black networks.

B. Experiments Regarding the Convoy

1) SNMP-Mob: Extend the common operational picture to the convoy – SNMP

Purpose: Collect SNMP-based information from the mobile domain.

Test setup: A PerfSONAR SNMP measurement archive is installed on the border router of the mobile domain. Data about interface/tunnel statistics is requested from the mobile MTR routers that have a direct SAT connection to the border router of the mobile domain.

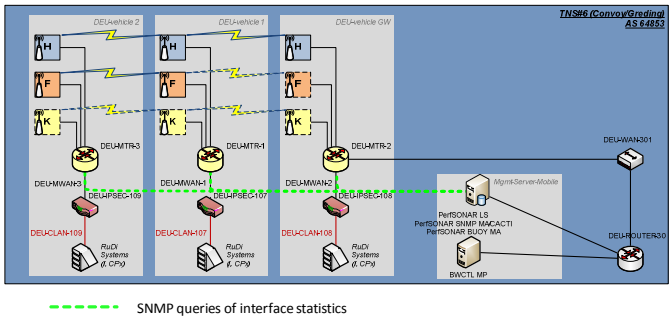

Figure 9: SNMP Interface Statistics Queries in the Wireless Domain

Walkthrough: Periodic queries via SNMP from the measurement archive co-located with the border router of the mobile domain are performed. This data can be accessed via the PerfSONAR framework.

Prerequisites and special requirements: SNMP data is fetched remotely via the satellite links. This has to be taken into account by experiments related to the convoy part of the network. The impact on the satellite links is supposed to be not relevant.

Findings: Throughput from the mobile domain was extracted without overloading the mobile links. Because of the full mesh of overlay tunnels for every radio technology, it was even possible to identify traffic to/from different nodes just using interface statistics. The results also clearly showed when nodes were isolated. Follow-up measurement samples need to be interpreted accordingly. However, identifying the cause (limited transmission range vs. jamming) will only be possible by correlating this data with cross layer information like the noise level.

2) OSPF-Topo: Monitoring of the OSPF Topology of the mobile domain

Purpose: Providing real time information about the communication status and connectivity within the convoy with minimal/no communication overhead to the mobile components OSPF domain. This includes the terrestrial radio links as well as the satellite links to the HQ.

Test setup: The OSPFv2 MIB of the non-mobile MTR located at the Multi National Deployed HQ is queried via SNMP by a software tool running also in the HQ. The OSPFv3 MIB is not yet supported by the MTR implementation based on Vyatta Linux. The information provided consists of a snapshot of the Links State Database of the MTR and thus provides a local view of the OSPFv2 topology of the mobile domain.

Walkthrough: The OSPFv2 Link State Information was shown on a computer located at the Multi National Deployed HQ and continuously provided information regarding the communication status of the convoy to the other experiments.

In addition, a packet capturing process was started at the MTR in the HQ to allow for an offline analysis of the Routing Protocol behavior (OSPFv2 and OSPFv3) in the post processing of the experiments.

Prerequisites and special requirements: Remote access to the MTR is needed.

3) Jammer-Basic: Cooperative detection of the jammer

Purpose: Show that the detection of a jammer is possible within the convoy with cross-layer information aggregation of data from the radios.

Test setup: A cross-layer framework called CRAWLER [15][16] was installed on two dedicated routers equipped with WIFI cards. One of the nodes was located in a German military vehicle. The other node is located at an NGO vehicle.

Walkthrough:

The CRAWLER framework needed to be installed and configured on both ends of the communication. The connection between the German military vehicle and the German NGO vehicle was established. Special jamming equipment was placed between both nodes. In addition, plausibility checks of cross-layer information were performed via the CRAWLER

framework. Thus, the presence of a possible jamming incident was detected based on this local information.

Prerequisites and special requirements: Jamming equipment for WIFI as well as a military and an NGO vehicle equipped with WIFI devices connected to the black part of the network and as well as the CRAWLER service. No dynamic routing was performed on this link.

4) Jammer-Notification: Automated notification of the HQ by the CRAWLER application via the Operational Message Service (OMS)

Purpose: Provided by task 2, the Operational Message Service (OMS) is a notification-based service intended to distribute commands, information, warnings and alerts. By using the OMS to raise the alarm about a suspected jamming incident, two purposes are answered: One, the OMS is notification-enabled and allows any interested party to subscribe to the alerts, without the necessity of setting up any new information structures or configurations; and two, it is a good example of a task-comprehensive test. Note: Since the OMS provider and the notification broker are located in the red network and CRAWLER in the black, a cross domain guard was needed to allow for a controlled forwarding of the message.

Test setup: The CRAWLER application includes a WS-Notification client with a publish method set up for the Operational Message Service to send an alert about a detected potential jamming attack to a WS-Notification broker. The German portable Command and Control Information System (C2IS) subscribed to alerts of this kind and was capable of displaying the jamming incident at the geographic location in the GUI.

Walkthrough: Upon the detection of a potential jamming incident an alert was sent via Operational Message Service. Subscribers, namely the German portable C2IS system, received the alert and processed it. The content eas displayed in the C2IS GUI.

VI. Conclusions and Future Work

In this paper, we introduce both challenges and technical solutions for federated network management with special requirements regarding security and information hiding, as well as addressing the wireless and core domains. Building on the Protected Core Networking concept, we showed how a well established framework PerfSONAR for sharing network performance measurements between different research networks can be extended and applied to the CoNSIS scenario. In addition, we presented the first prototype of an architecture that can use the performance measurements to adjust SLAs between the different nations of the coalition.

The paper concludes with details about the experiments performed within the CoNSIS field tests. These tests lay the foundations and serve as proof-of-concept. The results will set the agenda for the second phase of the CoNSIS project.

Acknowledgment

This work has been performed within the CoNSIS project.

References

[1] NATO Network Enabled Capability Feasibility Study Executive Summary v. 2.0, October 2005.

[2] G. Hallingstad and S. Oudkerk, “Protected core networking: an architectural approach to secure and flexible communications”, Communications Magazine, IEEE, 2008, 46, pp. 35 -41

[3] PerfSONAR Homepage <http://www.perfsonar.net/> (last accessed May 24, 2012).

[4] perfSONAR MDM release 3.0 – Product Brief.

[5] Instantiating a Global Network Measurement Framework http://acs.lbl.gov/~tierney/papers/perfsonar-LBNL-report.pdf.

[6] P. Steinmetz, “Use of Cross Domain Guards for CoNSIS network management“, MCC 2012, Gdansk, Poland, in press.

[7] PerfSONAR: A Service Oriented Architecture for Multi-domain Network Monitoring.

[8] P. Jacobs and B. Davie , “Technical challenges in the delivery of interprovider QoS”, Communication Magazine, IEEE, Vol. 43, No. 6, 2005, pp. 112-118.

[9] D. Duda et al., “The QoS Policy Agreement System for Federation of Communications and Information Systems”, MCC 2011, Amsterdam, The Netherlands, Oct. 2011.

[10] M. Hauge, M.A. Brose, J. Sander, and J. Andersson, "Multi-topology routing for improved network resource utilization in mobile tactical networks," *Military Communications Conference, 2010 - MILCOM 2010* , pp. 2223-2228, Oct. 31 2010-Nov. 3 2010.

[11] M. Hauge, CoNSIS Task 1, “QoS-classes for the CoNSIS test and demonstration architecture”.

[12] “Cacti - The Complete RRDTool-based Graphing Solution”, http://www.cacti.net/ (last accessed June 13, 2012).

[13] A. Morton and S. Van den Berghe, “Framework for Metric Composition”, December 2009, <http://www.ietf.org/id/draft-ietf-ippm-framework-compagg-09.txt>.

[14] A. Morton and E.Stephan, “Spacial Composition of Metrics”, IETF-RFC6049 January 2011.

[15] I. Aktas, J. Otten, F. Schmidt, and K. Wehrle, “Towards a Flexible and Versatile Cross-Layer-Coordination Architecture,” Proceedings of the 29th International Conference on Computer Communications (INFOCOM 2010), pp. 1-5, March 2010.

[16] I. Aktas, F. Schmidt, M. H. Alizai, T. Drüner, and K. Wehrle, “CRAWLER: An Experimentation Architecture for System Monitoring and Cross-Layer-Coordination,” Proceedings of the 13th International Symposium on a World of Wireless, Mobile and MultimediaNetworks (WoWMoM'12), pp. 1-9, June 2012, in press.