NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-090)TP/520

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-090**

SOA Challenges for Real-Time and Disadvantaged Grids

(Défis de la SOA pour les réseaux défavorisés et en temps réel)

Final Report of TR-IST-090.

Published April 2014

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-090)TP/520

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-090**

SOA Challenges for Real-Time and Disadvantaged Grids

(Défis de la SOA pour les réseaux défavorisés et en temps réel)

Final Report of TR-IST-090.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published April 2014

ISBN 978-92-837-0195-8

Table of Contents

List of Figures

List of Tables

List of Acronyms

AAO	AFRO Adaptation Ontology
ACT	Allied Command Transformation (NATO)
AFRO	Adaptation Framework foR web services prOvision
BFT	Blue Force Tracking
BRITE	Baseline for Rapid Iterative Transformational Experimentation
C2IS	Command and Control Information Systems
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCM	CORBA Component Model
CEP	Complex Event Processing
CES	Core Enterprise Services
CESMO	Cooperative ESM Operations
CESWG	Core Enterprise Services Working Group
CFF	Call For Fire
CNR	Combat Net Radio
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-The-Shelf
CR	Change Resolution
CSO	Collaboration Support Office
CWID	Coalition Warrior Interoperability Demonstration
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation and eXamination, eXercise
DA	Discard Attachment
DCD	Decrease Color Depth
DCPS	Data-Centric Publish-Subscribe
DDS	Data Distribution Service
DLRL	Data Local Reconstruction Layer
DQ	Decrease Quality
DSProxy	Delay and disruption tolerant SOAP Proxy
EFX	Efficient XML
ESB	Enterprise Service Bus
ESM	Electronic Support Measures
ESMTP	Extended Simple Mail Transfer Protocol
FFI	Forsvarets Forskningsinstitutt
FKIE	Fraunhofer Institute for Communication, Information Processing and Ergonomics
GPS	Global Positioning System
HQ	Headquarters
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IIS	Information and Integration Services
IOF	Information Originality Factor

ISCC	Initial Service Call Context
ISR	Intelligence Surveillance Recognition
IST	Information Systems Technology
ITM	Institute of Technology “La Marañosa”
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunications
LAN	Local Area Network
LGPL	Lesser General Public License
LOS	Line-Of-Sight
MAC	Medium Access Control
MAJIIC	Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition
MANET	Mobile Ad hoc Network
MCC	Military Communications Conference
MCI	Military Communication Institute
MEP	Message Exchange Pattern
MIP DMWG	MIP Data Modeling Working Group
MIP	Multilateral Interoperability Programme
MISA-EM	Multinational Inter-agency Situational Awareness – Extended Maritime
MMHS	Military Message Handling System
MNE	Multi National Experimentation
MTU	Maximum Transmission Unit
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation, Command and Control Agency
NC3B	NATO Consultation, Command and Control Board
NCIA	NATO Communications and Information Agency
NFFI	NATO Friendly Forces Information
NII	Networking and Information Infrastructure
NNEC	NATO Network-Enabled Capability
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
OWL	Web Ontology Language
PIM	Platform Independent Model
PSM	Platform Specific Model
QoS	Quality of Service
REST	Restful Web services
RTG	Research Task Group
RTO	Research and Technology Organization
RTPS	Real-Time Publish/Subscribe
SASD	Service Advertisement and Service Discovery
SATCOM	Satellite Communication
SGML	Standard Generalized Markup Language
SMTP	Simple Mail Transfer Protocol
SNIR	Signal-to-Noise plus Interference Ratio
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service-Oriented Computing

SQL	Structured Query Language
STANAG	Standardization Agreement
STO	Science and Technology Organization
SWRL	Semantic Web Rule Language
TCP/IP	Transmission Control Protocol / Internet Protocol
TIDE	Transforming Technology for Information, Decision and Execution
UAV	Unidentified Aerial Vehicle
UDDI	Universal Description, Discovery and Integration
UDP	User Data Protocol
UHF	Ultra High Frequency
URI	Uniform Resource Identifier
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
WISE	Web Interface of Search Engine
WSDL	Web Service Definition Language
WSN	WS-Notification
WWW	World Wide Web
XML	Extensible Markup Language

IST-090 Membership List

DENMARK

Dr. Jens STAVNSTRUP
Danish Defence Logistics and Acquisition (DALO)
Lautrupbjerg 1-5
DK-2750 Ballerup
Email: stavnstrup@mil.dk

FRANCE

Mr. Xavier DENIS
EADS
6 rue Dewoitine
78190 Velizy
Email: xavier.denis@eads.com

Mr. Jonas MARTIN
EADS/Defence and Security Systems
La Clef St Pierre 1
Boulevard Jean Moulin CS 40001
78996 Elancourt Cedex
Email: jonas.martin@eads.com

Mr. Olivier DE PEUFEILHOUX
CASSIDIAN Systems Integrated
1 Boulevard Jean Moulin
78990 Elancourt
Email: olivier.de-peufeilhoux@cassidian.com

GERMANY

Mr. Christoph BARZ
Fraunhofer-FKIE Communication Systems
Neuenahrer Strasse, 20
D-53343 Wachtberg-Werthhoven
Email: christoph.barz@fkie.fraunhofer.de

Mr. Norman JANSEN
Fraunhofer-FKIE
Neuenahrer Strasse, 20
D-53343 Wachtberg-Werthhoven
Email: norman.jansen@fkie.fraunhofer.de

ITALY

Dr. Francesca ANNUNZIATA
SELEX Sistemi Integrati SPA
Via Tiburtina Km 12.400
00131 Rome
Email: fannunziata@selex-si.com

NETHERLANDS

Mr. Peter-Paul MEILER (Chair)
TNO-FEL
P.O. Box 96864
2509 JG The Hague
Email: peter-paul.meiler@tno.nl

Dr. Leon C.P.M. SCHENKELS
NC3A CAT7 – Core Enterprise Services
P.O. Box 174
2501 CD The Hague
Email: leon.schenkels@nc3a.nato.int

NORWAY

Miss Trude HAFSØE
FFI (Norwegian Defence Research Establishment)
P.O. Box 25 Instituttvein 20
NO-2027 Kjeller
Email: trude.hafsoe@ffi.no

Mr. Frank Trethan JOHNSEN
Norwegian Defence Research Establishment (FFI)
Information Management Division
P.O. Box 25 Instituttveien 20
NO-2027 Kjeller
Email: frank-trethan.johnsen@ffi.no

POLAND

Mr. Przemyslaw CABAN
Military Communication Institute
Telecommunication Services Section
C4I Systems Department ul. Warszawska 22A
05-130 Zegrze
Email: p.caban@wil.waw.pl

Dr. Joanna SLIWA
Military Communication Institute
Communications Systems Department
Warszawska 22
05-130 Zegrze
Email: j.sliwa@wil.waw.pl

SPAIN

Eng. Ignacio HERNANDEZ NOVO
SDG TECEN
C/Arturo Soria
289 – 28033 Madrid
Email: ihernandez@isdefe.es

SPAIN (cont'd)

Mr. Luis SHAW MANERO
Spanish MOD R&D MoD/DGAM (SDGTECIN)
C/Arturo Soria
289 – 28033 Madrid
Email: lshaman@oc.mde.es

TURKEY

Ms. Burcu ARDIC
TUBITAK Scientific & Technological
Research Council
National Research Institute of Electronics
and Cryptography
PK 74 Gebze
41470 Kocaeli
Email: burcu.ardic@uekae.tubitak.gov.tr

Maj. Deniz KAYA
Turkish Land Forces Command
Department of Technical and Project Management
Akdeniz Caddesi Kocatepe
06630 Ankara
Email: dkaya@kkk.tsk.mil.tr

Ms. Ayse Betul SASIOGLU
TUBITAK Scientific & Technical Research
Council
TUBITAK UEKAE
National Research Institute of Electronics
and Cryptography
PK 74 Gebze
41470 Kocaeli
Email: betul.sasioglu@uekae.tubitak.gov.tr

Lt. Akif TOKUZ
Turkish Naval Research Center Command
Ankara Cad.
252 PK 46
34890 Pendik, Istanbul
Email: atokuz@armerk.tsk.tr

UNITED KINGDOM

Dr. Graham FLETCHER
Cranfield University
Department of Information Systems
College of Management & Technology
Shrivenham, SN6 8LA
Email: g.p.fletcher@cranfield.ac.uk

Mr. Ian OWENS
Cranfield University
Defence Academy
Department of Informatics & Systems Engineering
Shrivenham, Swindon SN6 8LA
Email: i.owens@cranfield.ac.uk

IST-090 Programme Committee

CHAIRMAN

- P.P. Meiler; NLD

EDITORS

- Bloebaum, Trude-Hafsoe; NOR
- Jansen, Norman; DEU
- Johnsen, Frank-Trethan; NOR
- Meiler, Peter-Paul; NLD
- Owens, Ian; GBR
- Schenkels, Leon; NCIA
- Sliwa, Joanna; POL

CHAPTER AUTHORS

Each chapter has a specific lead. But many editors have contributed to each chapter.

- Chapter 1 Introduction: IST-090 editors
- Chapter 2 Introduction to SOA at the Tactical Level: Lead by NOR
- Chapter 3 IST-090 Activities: Lead by NLD
- Chapter 4 Conclusions, Lessons Learned and Way Forward: IST-090 editors

Each of the annexes has one or more nations as main editor.

- Annex A Web Services: NOR
- Annex B DDS: ESP, POL (POL is lead)
- Annex C Interim Middleware: DEU
- Annex D SOA Over Disadvantaged Grids Experiment and Demonstrator: NCIA, NOR, POL (This annex is provided as a separate document)
- Annex E AFRO: POL
- Annex F IST-090 Meetings and Other Activities: NLD
- Annex G Terms of Reference: NLD
- Annex H References: IST-090 editors

ADDITIONAL AUTHORS

- Annex D: Przemysław Caban, Rui Fiske, Marc van Selm, Vincenzo de Sortis, Aad van der Zanden

SOA Challenges for Real-Time and Disadvantaged Grids

(STO-TR-IST-090)

Executive Summary

The Service Oriented Architecture (SOA) paradigm has been chosen by the NATO C3 Board (NC3B) as the method to achieve interoperability at the information infrastructure level. The current technologies used to implement SOA (e.g., Web Services and Data Distribution Services) were not specifically designed to handle the conditions found when working with tactical networks. This fact remains a major impediment to achieving interoperability among the nations in the battle space.

Therefore, the objective of IST-090 was to identify improvements to make SOA applicable at the tactical level, which typically includes communication grids that are disadvantaged by line-of-sight connections, low bandwidth, intermittent availability, etc. The goal was also to investigate how SOA could be used over disadvantaged grids, and to build demonstrations that show how the challenges that are posed by disadvantaged grids can be mitigated.

The overall research focused on the use of SOA in disadvantaged grids in 'near real time', as is the case at the tactical level in military operations. Sub-areas of research included:

- Efficient communication frameworks;
- Mechanisms to reduce needed bandwidth; and
- Mechanisms to improve reliability.

The results of IST-090 were focused around several demonstrations of SOA over disadvantaged grids. The following aspects were selected for consideration based on an analysis of where the biggest problems existed:

- Web Services across disadvantaged networks;
- The Data Distribution Service (DDS) at the tactical level (alternative to Web Services); and
- Interim solutions for use on the way toward an SOA-based information infrastructure.

Following these experiments, no single solution stood out as the 'magic bullet' to solve all the requirements for high-speed connectivity to the edge, but many of them do offer measurable improvements in messaging capability. A number of key success factors were identified, including the foundation on open standards, ease of management and configuration, and transparency to the user. The messaging infrastructure should be optimised for the consumers of services without the need to incorporate proprietary, ad hoc solutions that will ensure tighter coupling between providers and consumers of services, and therefore limit the range of potential partners. Where a protocol is not widely understood in another domain, gateways should be used to translate from one standard or protocol to another.

Défis de la SOA pour les réseaux défavorisés et en temps réel

(STO-TR-IST-090)

Synthèse

Le paradigme de l'architecture orientée service (SOA) a été choisi par le Bureau des C3 de l'OTAN (NC3B) comme méthode d'interopérabilité au niveau de l'infrastructure informatique. Les technologies servant actuellement à mettre en œuvre la SOA (par exemple, les services web et *Data Distribution Services*) n'étaient pas spécialement conçues pour faire face aux conditions qui prévalent dans le travail avec les réseaux tactiques. Ce fait reste un obstacle majeur à l'interopérabilité entre les pays sur le théâtre des opérations.

Par conséquent, l'objectif de l'IST-090 était d'identifier les améliorations à apporter pour que la SOA puisse s'appliquer au niveau tactique, ce qui inclut d'ordinaire les réseaux de communication qui sont défavorisés par les connexions à visibilité directe, une faible bande passante, une disponibilité intermittente, etc. L'objectif était également d'étudier comment la SOA pouvait être utilisée sur des réseaux défavorisés et de bâtir des scénarios montrant comment les problèmes posés par les réseaux défavorisés peuvent être résolus.

Dans leur ensemble, les recherches se sont concentrées sur l'utilisation de la SOA dans les réseaux défavorisés fonctionnant en « temps quasi réel », comme c'est le cas au niveau tactique dans les opérations militaires. Les sous-domaines de recherche comprenaient :

- L'efficacité des réseaux de communication;
- Les mécanismes réduisant la bande passante nécessaire ; et
- Les mécanismes améliorant la fiabilité.

Les résultats de l'IST-090 se sont concentrés sur plusieurs démonstrations de la SOA sur des réseaux défavorisés. Les aspects à étudier suivants ont été sélectionnés à partir d'une analyse indiquant les plus gros problèmes :

- Services web sur les réseaux défavorisés ;
- *Data Distribution Services (DDS)* au niveau tactique (alternative aux services web) ;
- Solutions intermédiaires à utiliser pendant la progression vers une infrastructure informatique basée sur la SOA.

Suite à ces expérimentations, aucune solution n'est apparue comme étant la solution miracle répondant à tous les besoins de connectivité à grande vitesse d'avant-garde, mais nombre d'entre elles offrent des améliorations mesurables de la capacité de traitement des messages. Plusieurs facteurs clés de réussite ont été identifiés, notamment l'utilisation de normes ouvertes, la facilité de gestion et de configuration et la transparence pour l'utilisateur. L'infrastructure de messagerie doit être optimisée pour l'utilisateur des services sans intégrer de solutions ad hoc exclusives qui créeraient un lien plus étroit entre fournisseurs et utilisateurs des services et limiteraient donc la gamme des partenaires potentiels. Lorsqu'un protocole n'est pas largement compris dans un autre domaine, des passerelles doivent être employées pour traduire la norme ou le protocole en question.

Chapter 1 – INTRODUCTION

This report presents the work done by the NATO CSO IST-090 research Task Group, also providing lessons learned, conclusions, guidelines and a way forward.

1.1 SCOPE OF WORK

The Service Oriented Architecture (SOA) paradigm has been chosen by NC3B as the method to achieve interoperability at the information infrastructure level. The current technologies used to implement SOA (e.g., Web Services and Data Distribution Services) were not specifically designed to handle the conditions found when working with tactical networks. This fact remains a major impediment to achieving interoperability among the nations in the battle space.

Therefore, the objective of IST-090 was to identify improvements to make SOA applicable at the tactical level, which typically includes communication grids that are disadvantaged by line-of-sight connections, low bandwidth, intermittent availability, etc. The goal was also to investigate how SOA could be used over disadvantaged grids and to build demonstrations that show how the challenges that are posed by disadvantaged grids can be mitigated.

The overall research focused on the use of SOA in disadvantaged grids in “near real time”, as is the case at the tactical level in military operations. Sub-areas of research included:

- Efficient communication frameworks;
- Mechanisms to reduce needed bandwidth; and
- Mechanisms to improve reliability.

The results of IST-090 were focused around several demonstrations of SOA over disadvantaged grids. The following aspects were selected for consideration based on an analysis of where the biggest problems existed:

- Web Services across disadvantaged networks,
- The Data Distribution Service (DDS) at the tactical level,
- Interim solutions for use on the way towards a SOA based information infrastructure.

The IST-090 group title implies a very large scope of study, as we were tasked with looking into service oriented architecture (SOA) challenges for both real time and disadvantaged grids. We limited our focus down to the topics that are unique to these network types, not topics that are generic SOA topics that happen to also feature in our network domains. We also only considered technical solutions that can be used to alleviate the issues that we face in disadvantaged grids. As an example, this implies that we did not look at service management issues and governance.

Furthermore, we did not address security issues, as this topic is already being addressed by other CSO groups. We have limited ourselves to looking at the technologies that can be used to implement a SOA solution on the middleware level and we have not looked at optimizations specific to one type of radio network.

When considering the real-time aspects of disadvantaged networks we needed to have a usable description or definition for both ‘real-time’ and ‘disadvantaged network’. In the context of IST-090 we used the following:

- The near-real-time aspect relates to the ‘timeliness’ of information. This ‘timeliness’ of information is directly related to the application area that requires the information. For example, the latency

acceptable for a chat application will be a matter of seconds, rather than minutes or hours. On the other hand, a latency of a few hours may be acceptable for a requirement to synchronize or update databases. We consider timely delivery but without hard-real-time guarantees.

- Disadvantaged grids are characterized by low bandwidth, variable throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that links the nodes [1]. The limited bandwidth at this level limits the possible amount of services and communication. Also the need for services will be location and mission specific. Similar grids impose different constraints depending on the level (Strategic, Operational, Tactical) and the domain (Land, Sea, Air, Space, Joint, Combined) where they are applied.

IST-090 investigated the feasibility of extending the use of the SOA paradigm to tactical networks, with special focus on disadvantaged grids. Rather than focusing work directly on the challenges of real-time networks, the group worked on a variety of solutions that can improve the timeliness of information in disadvantaged networks.

The advantage of SOA over current approaches (such as tightly coupled stovepipe solutions) is that it provides seamless information exchange based on different policies and loose coupling of its components. In a military domain it enables to make sensitive information resources available in the form of services, which can be discovered and used by all mission participants that do not need to be aware of these services in advance.

A SOA can be implemented using several different technologies such as Web Services [Annex A] and DDS (Data Distribution Service) [Annex B]. Both technologies have originated for use in civil systems, and both may be applicable when extending the SOA concept into the tactical domain: An interim solution on the way towards a SOA based information infrastructure is covered in more detail in [Annex C].

As a consequence, the IST-090 group has focused on identifying optimization techniques which can be applied to the technologies in order to extend their use to the tactical domain. The group had an experimental focus, resulting in demonstrations and experimental prototyping. The techniques employed have a varying degree of maturity, ranging from implementations of existing standards to novel research.

1.2 INTRODUCTION TO THE IST-090 TEAM

IST-090 was established as a result of the findings (in 2008) of the IST-ET-046 “Service Oriented Architecture (SOA) Challenges over disadvantaged grids” exploratory team.

IST-090 was established during the kick-off meeting on 27 April 2009 in Paris. The nations that initially established the IST were: DEU, DNK, FRA, ESP, GBR, ITA, NLD, POL and TUR. The group was later joined by NC3A and NOR. [Annex F] presents an overview of the topics and main results of each of the meetings and other activities.

1.3 SCOPE AND STRUCTURE OF REPORT

This report covers the work done by IST-090 and relates to other significant work, providing references where applicable.

Chapter 2 provides an introduction to SOA at the tactical level. It identifies two possible approaches to extend SOA to the tactical domain that we focussed on in IST-090.

Chapter 3 describes the activities by IST-090, focussing on three main areas: Interim solutions for use on the way towards a SOA based information infrastructure, Web Services across disadvantaged networks, and The Data Distribution Service (DDS) at the tactical level.

Chapter 4 provides practical recommendations based on the current results. Based on these results and on the lessons learned it describes what steps would or could be done to further investigate this area of research (the way forward).

For technical details and references, we provide the following annexes:

A WEB SERVICES

A Web Service is a software system designed to support interoperable machine-to-machine interaction over a network [2]: It has an interface described in a machine-processable format (specifically Web Services Description Language or WSDL). Other systems interact with the Web Service in a manner prescribed by its description using (SOAP (originally defined as Simple Object Access Protocol) messages, typically conveyed using Hypertext Transfer Protocol (HTTP) with an Extensible Markup Language (XML) serialization in conjunction with other Web-related standards.

B DDS

The Data Distribution Service (DDS) for real-time systems is a specification of a publish/subscribe middleware for distributed systems created by the Object Management Group (OMG) in response to the need to standardize a data-centric publish-subscribe programming model for distributed systems [3]. DDS allows the user to specify Quality of Service (QoS) parameters as a way to configure automatic-discovery mechanisms and specify the behavior used when sending and receiving messages. The mechanisms are configured up-front and require no further effort on the user's part. DDS was, however, not designed to be used over disadvantaged networks.

C INTERIM MIDDLEWARE

The objective of Task Group IST-090 “SOA Challenges for Disadvantaged Grids” is to identify solutions for making SOA applicable at the tactical level. Besides efficient mechanisms for service discovery and for reducing the overhead of Web Service communication [Annex A], an efficient transportation of the messages between a service consumer and a service provider, is essential. Thus, a middleware allowing for an adaptation of the applications’ communication behavior to the special needs of tactical networks could provide a basis for implementing a SOA infrastructure at the tactical level. As an example, DDS [Annex B] already provides many useful middleware features to be used in tactical network environments. However, it sees the network only as a transparent communication service. We argue that additionally, a better coordination between command and control information systems (C2IS) applications and network protocol layers is useful.

D SOA OVER DISADVANTAGED GRIDS EXPERIMENT AND DEMONSTRATOR

The Service Oriented Architecture (SOA) over disadvantaged grids experiment and demonstrator was linked to the CSO IST-090 group’s presentation during the 2011 MCC Conference in Amsterdam. The disadvantaged grid networking infrastructure used was based on mobile ad-hoc networking systems. This document describes the support plan for the exercise and describes the experimentation and the results of the various approaches for network optimisation as conducted by the Norwegian FFI, the Polish MCI and the NC3A.

[Annex D] is provided as a separate report.

E AFRO

MCI has developed a concept for an edge proxy: the Adaptation Framework foR Web Services prOvision (AFRO). This mediation service offers different levels of QoS to Web Services, through performance monitoring and application of the context-aware service provision paradigm (adapting the Web Services flow to the limitations of the network on the basis of semantic reasoning). This concept, though not demonstrated in IST-090 experiments, seems to be a promising approach as identified by Poland, and is discussed in detail in [Annex E].

F IST-090 MEETINGS AND OTHER ACTIVITIES

This annex presents an overview the topics and main results of each of the meetings and other activities.

H This annex provides the references.

1.4 SUMMARY

This chapter introduces the IST-090 approach of identifying SOA challenges for real time and disadvantaged grids. We focus on three main topics: Web Services across disadvantaged networks, DDS at the tactical level, and finally interim solutions for use on the way towards a SOA based information infrastructure.

Chapter 2 – INTRODUCTION TO SOA AT THE TACTICAL LEVEL

Disadvantaged grids are characterized by low bandwidth, variable throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that links the nodes [1]. Not only does the limited bandwidth at this level limit the possible amount of services and communication, but also the need for services will be location and mission specific.

The NATO Network Enabled Capability (NNEC) Feasibility Study [4], [5] presents a discussion of technology, focusing on the needs of future interoperable military communications. An information infrastructure will have to allow for communication across system and national boundaries while at the same time taking legacy systems into account. This leads to a requirement for a flexible, adaptable, and agile information infrastructure which can support all the information needs of national forces, and at the same time support interoperability. The study identifies the Service-Oriented Architecture (SOA) concept and Web Services technology as the key enablers for NNEC.

In the NNEC concept there is an ambitious requirement for users at all operational levels to seamlessly exchange information. In order to achieve efficient information exchange between these users, one needs to work with different types of information and communication systems. Systems and equipment used at the various levels are different, and the information exchange must be adapted to fit the capacity of the systems used.

2.1 SERVICE-ORIENTED COMPUTING

The Service-Oriented Computing [6] paradigm is based on the notion of a service, which is a networked piece of functionality (component) offered by a service provider. A service is specified by its service contract, interface, and semantics. The interface should be coarse-grained to accommodate internal change of the service implementation without affecting the interface. Building a system with a SOA [7] means to develop such stand-alone services and to compose them into a system.

In [8], SOA is defined as: "SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations."

There are three roles in a SOA; provider, consumer and registry (see Figure 2-1). Three operations define the interactions between these three roles; publish, find and bind.

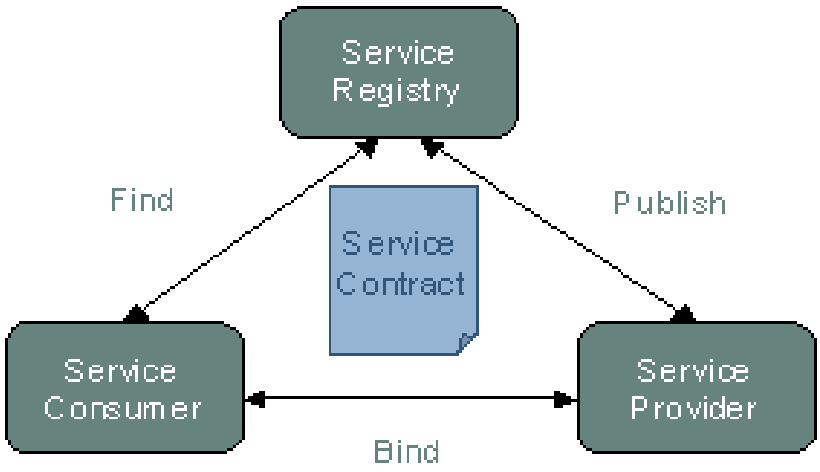

Figure 2-1: The Three Roles in a SOA.

Interoperability between provider, consumer, and registry is ensured by a standardized service contract. Following these principles, we get a loose coupling between the clients and the services, with respect to both time (enabling asynchronous communication) and place (the location of both client and service can be changed without need for reconfiguration):

- A service provider is responsible for creating a service description, publishing that description in a service registry, and receiving and answering bind requests (i.e., service invocations) from service consumers.
- A service consumer is responsible for finding a service description published in a service registry and using that description to bind to service providers. With the find operation the service consumer states search criteria such as the type of service it needs. The result of the find operation is a list of service descriptions that match the find criteria.
- A service registry is responsible for advertising service descriptions published to it by service providers and allowing service consumers to search for (i.e., find) service descriptions within the service registry.

The central concept in a SOA is the service, which [8] defines as: "A service is a mechanism to enable access to a set of one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description. A service is provided by one entity — the service provider — for use by others, but the eventual consumers of the service may not be known to the service provider and may demonstrate uses of the service beyond the scope originally conceived by the provider."

Thus, the principle of separating the service interface from the service implementation means that there are several different ways of realizing services. As illustrated in Figure 2-2, a service can be defined from scratch, allowing full control of the way the service is implemented. In addition, existing applications can be wrapped, and made available as services in a SOA. This approach requires an adaptation layer in order to adapt the existing interface of the application to the service interface. Finally, services of both types can be combined, in order to create new functionality in a more complex, composite service.

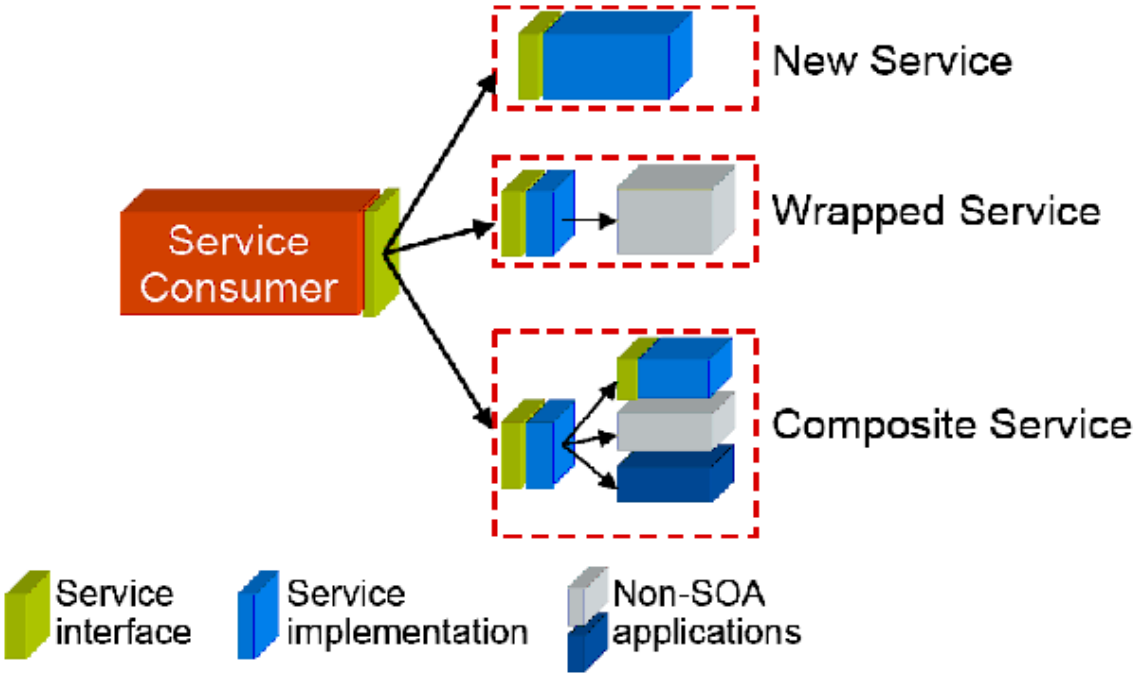

Figure 2-2: Creating Services (from [9]).

The SOA paradigm is not very new, it is a widely recognized approach to building loosely coupled distributed systems. In principle, it can be implemented using almost any middleware product. However, when keeping the interoperability requirements in mind, it is preferable to implement a SOA using open standards. Even if a SOA can be implemented using several different technologies, Web Services stand out as a preferred and widely adopted standard [10].

2.2 SOA ADVANTAGES

The SOA approach has demonstrated many advantages for the development and implementation of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems in general. SOA's greatest advantage is the ability to seamlessly exchange information based on different policies and on a loose coupling of the components.

A more specific list of advantages can be found in [12, page 6]:

- True interoperability: By allowing different categories of applications to interact with the same services, a highly cohesive interoperability environment is created. This allows normally disparate categories of applications, such as thin-client applications and legacy client-server applications, to share data they would not otherwise be able to share.
- Incremental functional improvement: Services can be added or refined without impact to existing operations. The risk inherent in new development can be constrained to smaller "chunks" of functionality.
- Broad reach: Service discovery allows potential business and integration partners to find deployed services they would not normally know about. This has the effect of reaching a broader market with little impact on existing infrastructure.
- Reuse potential: Existing services can be used again and again, thereby reducing the need for new development and the support requirements implied by that development.

- Technology transition: Highly decentralized and very loosely coupled, the SOA model allows for capabilities to be brought to and integrated within an operational environment with minimal impact to the existing system.

2.3 RELEVANCE OF SOA FOR NATO

The large number of legacy systems within NATO and within allied countries justifies any improvement to increase interoperability of existing applications in the overall frame of NNEC. Thus, SOA is unquestionably an area of interest for NATO C4ISR [4], [11], [12]. What is more, it is emphasized that Web Services implementation of SOA should be used where it is possible [5], [11].

To cover the whole spectrum of NATO systems from the strategic to the tactical level, some improvements have to be identified to make SOA applicable on battlefield disadvantaged grids.

In the tactical military environment the bandwidth may be quite low and the connectivity may be intermittent with widely ranging communication gaps (seconds to days). Very useful research in this field has already been performed [13], but this does not focus explicitly on SOA.

Service orientation is a conceptual architecture which asymmetrically provides services to arbitrary service consumers facilitating information sharing in heterogeneous environment and thus supports to some degree the open-ended aspects of net-centricity. That is why the Networking and Information Infrastructure (NII) strategy (technological background of NATO NEC – NNEC – implementation) assumes that the NII will be implemented as a Federation of Systems (FoS), involving the use of SOAs [4], [5], [12], [14]. NII is characterized by the use of SOAs to expose business functions as consumable services that can be discovered and invoked across the network. The use of SOAs ease application and data sharing and provide a flexible mechanism for reusing existing services to enable the development of new, value-added information services [14].

The concept of every system viewing others as "services" in a loosely coupled manner is coherent with the concept of NNEC within the Federation of Systems. From a SOA perspective, it means that Information and Integration Services (IIS) Layer of NII architecture is to be thought of as a federation of services, where any NATO or national information system will be autonomous and provide specific services by means of implementing a standardized service interface [14]. Within this approach inclusion of a service-based system in the NII enables contributed systems to be independently managed and controlled by their owners within the framework of the FoS. For example, the Core Enterprise Services WG (CESWG) has already published a framework document that is highly relevant in this context. Even if our focus is on the tactical domain, it is vital that we also consider how the technologies we discuss will be able to interoperate with other systems on higher levels. CESWG points to SOA (implemented through Web Services) as the key enabling technology. That does not mean that we are limited to using Web Services in tactical systems, but we must take into account that we must co-exist with Web Service based systems.

As Web Services are developed for use in civilian networks, they will not necessarily perform satisfactorily in radio-based military networks. It is however vital that solutions used in tactical networks are able to fully interoperate with SOA solutions on other levels and there exist two possible approaches to achieve this:

First, one can use Web Services on the tactical level and make improvements to both the Web Services themselves and to underlying infrastructure to ensure that the Web Services become less bandwidth intensive. The benefits to this approach include:

- All services and clients, no matter where or how they are connected to the infrastructure, interact with each other using the same interfaces (so the same services can be used everywhere without modification).

- Cross network interoperability is easy, since the same technology is being used at the application level everywhere.
- Using the same solutions everywhere means fewer solutions that need to be maintained and monitored.

Second, we can use non-Web Service technology on the tactical level and provide interoperability through the use of gateways. The characteristics of this approach include the following benefits:

- A non-Web Service solution can be designed more specifically for the limitations of each individual network, and can potentially be optimized further than Web Services.
- Other solutions can provide functionality beyond what is supported by current Web Services standards, such as more fine-grained QoS support and support for real-time data. (This functionality, however, will be limited to working within the network the given solution is deployed in.)
- Gateways will handle interoperability. (Developing these gateways can generate significant overhead, as one gateway is needed per solution that is in use).

IST-090 investigates both these approaches, by both looking at how Web Services can be optimized for tactical networks, while at the same time looking at other technologies that can be used to implement a SOA at the tactical level. More specifically we are investigating the use of DDS on the tactical level.

2.4 AREA OF RESEARCH AND SCOPE

The overall research focuses on the use of SOA in disadvantaged grids in "near real time". Rather than focusing work directly on the challenges of real-time networks, the group worked on a variety of solutions that aimed to ensure the timeliness of information in disadvantaged networks. This 'timeliness' of information is directly related to the application area that requires the information. For example, the latency acceptable for a chat application will be a matter of seconds, rather than minutes or hours. On the other hand, a latency of a few hours may be acceptable for a requirement to synchronize or update databases. Sub-areas of research include:

- Communication paradigms.
- Mechanisms to reduce needed bandwidth.
- Mechanisms to improve reliability.
- Security: Security is not addressed by IST-090, as it is already the focus of other groups (IST-053, IST-061).

To evaluate our propositions for solutions we use a concrete scenario as a global context of the study. The scenario incorporates use cases and services (i.e. Blue Force Tracking, Observation report, Alert notification, video feed from an Unidentified Aerial vehicle (UAV), weather forecast…). An example of scenario is provided below.

In Figure 2-3 we have two kinds of SOA design and implementations: Regular (without Disadvantaged Grid limitations) and Adapted to tactical needs (with Disadvantaged Grid limitations). IST-090 takes into consideration the overall context of the scenario but focuses on SOA adapted to tactical needs.

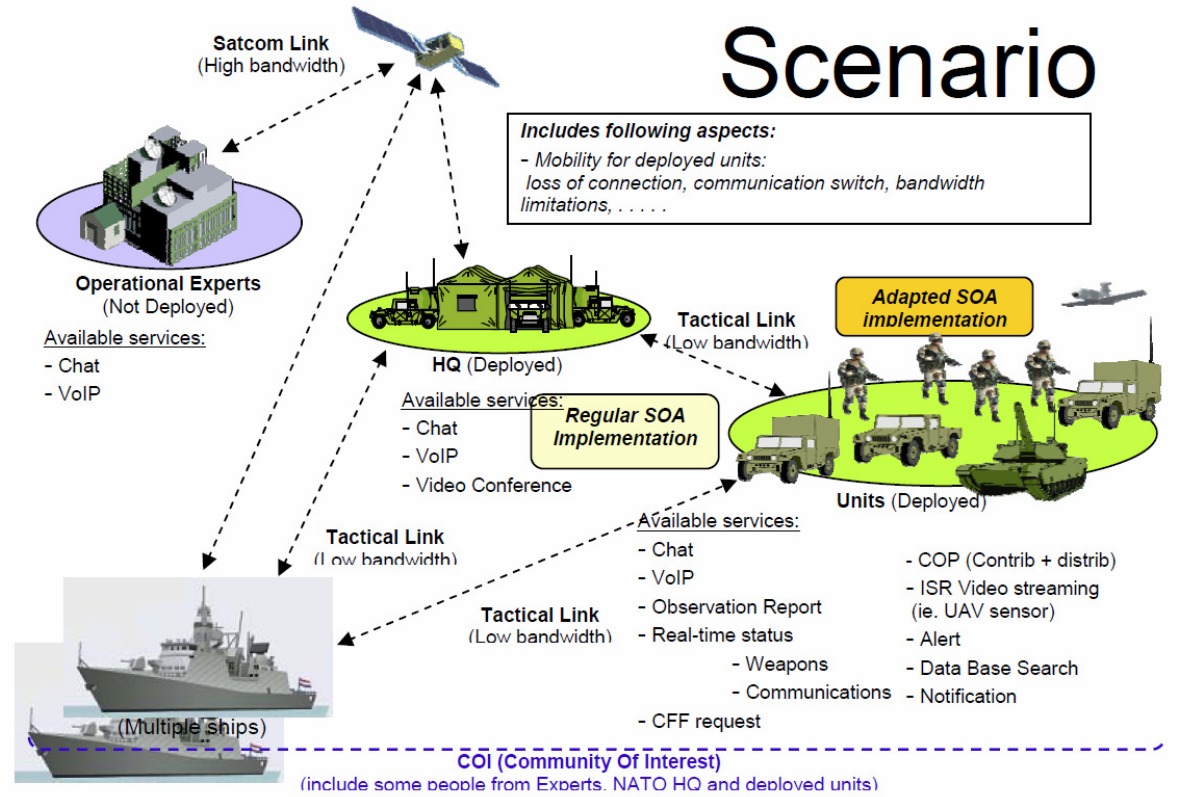

Figure 2-3: IST-090 Scenario Focus.

The tactical domain is the environment that needs to cope with disadvantaged grid conditions. Tactical communications can be defined as the infrastructure for the low-level forces that operate in the battlefield. It connects deployed command posts with mobile units and covers communications down to the individual soldier.

The main characteristic of the tactical domain is its unpredictability. Predictability is defined as the measure of the degree to which the state of the network can be reliably observed. Fixed-based terrestrial communications are highly predictable. Space-based networks (e.g. satellite networks) are moderately predictable, while tactical mobile networks are the least predictable.

Decrease in predictability is due to several factors and is reflected e.g. in the following network performance parameters:

- Connectivity – caused by topology changes and signal propagation.
- Links throughput – influenced by the distance of the communicating nodes and link type (dependent on the modulation, frequency, etc.).
- Links reliability – influenced by the variable error rate (Bit Error Rate or Packet Error Rate).
- Links latency – related to the communications technique (e.g. VHF radio link, satellite link). Often the delay caused by highly latent transport mediums will cause applications to timeout before receiving a response.

The above network performance parameters influence the success rate of the invocation and the delay of information transfer measured at the application layer.

In terms of communications techniques the NNEC FS clearly states that all heterogeneous networks forming the Networking Infrastructure (NI) should be able to transfer IP based traffic. The mobile radio networks that are considered in this report must also fulfil this requirement.

Military tactical communications are usually based on radios. Current tactical radios for individual soldier use VHF and UHF bands which provide good radio communications at ranges of tens of kilometres, depending on the terrain relief and equipment specifications. The military VHF band (30-88 MHz) is mostly used for Ground-to-Ground tactical communications as a Combat Net Radio (CNR). Most VHF waveforms nowadays transport analogue voice or low-rate data in simplex mode. The most recent military VHF systems provide digital voice and data capabilities (e.g. the digital F@stNet radios).In parallel to typical military communications more and more often civil standards are acquired to fulfil military requirements. The family of IEEE 802.11 standards offers efficient data communications and they give promising capabilities and are used by armies in point–to–point and ad–hoc scenarios for low level commanders' radio access (e.g. Rajant BreadCrumb radios). They are also very popular in reach-back connections based on the satellite links.

Something that also needs to be considered is the fact that it is rare for a single application flow to have the whole available end-to-end bandwidth at its disposal. There are a number of concurrent flows which share the bandwidth in a way which depends on the presence of a Quality of Service (QoS) mechanism (or lack thereof). In the case of a best-effort link, it seems reasonable to assume that the bandwidth available to the flow under test will vary in a randomized way, as the traffic patterns of other flows sharing the same link. If a QoS mechanism is in place, the flow under test may either be bandwidth-protected (if assigned to a priority category), or in the opposite case, suffer from bandwidth reduction caused by presence of priority flows.

To become a bit more concrete, we identified some examples of services that are applicable in this scenario. Common Operational Picture (COP), the Compilation, distribution and contribution of relevant information; Blue Force Tracking (BFT), providing information about own forces location; Intelligence Surveillance Recognition (ISR) Feed, the ability to access ISR Sensor information; Call For Fire (CFF), Fire support requests containing all information needed to determine the method of target attack. For the scenario the CFF comes from an observer; Alert Service, this is a high priority instant advertising of incoming emergencies and contingences; Observation Report, this involves the distribution of information collected on the battlefield through observation by deployed soldiers and a variety of electronic sensors; Database Search, this can consist of remote requests of information relevant to the operation by deployed units; Online Status, this involves monitoring the availability status of deployed units; Notification, this is the ability to be notified when a subscribed data changed. It is linked to a data subscription approach; Others: Chat, VoIP, Video, etc.

2.5 TECHNOLOGIES FOR REALIZING A SERVICE-ORIENTED SYSTEM

In IST-090 we focus on SOA as the key enabling technology for network centric operations. We have identified two possible approaches to extend SOA to the tactical domain:

1) Adapting existing Web Services standards for use in disadvantaged grids.
2) Employing other technologies in certain sub-systems, and then integrating these with Web Services through the use of gateways.

Web Services support both publish/subscribe and request/response communications, as opposed to DDS which has only publish/subscribe support. On the other hand, DDS supports QoS and real-time systems, which Web Services do not. All these capabilities should be available in a solution for real-time disadvantaged networks. For a comparison, see Table 2-1.

Table 2-1: Web Services and DDS Comparison.

Property	**Web Services**	**DDS**
Standardization	W3C, OASIS, WS-I	OMG
Real-time and QoS support	–	Yes
Request/response paradigm	Yes	–
Publish/subscribe paradigm	Yes	Yes
Current standard suitable for disadvantaged grids	No	No
Enabling support for disadvantaged grids	Experimental optimizations, e.g., proxies	Vendor specific tactical extensions

As Table 2-1 shows, no current technology is directly applicable in disadvantaged grids. Web Services are covered in [Annex A]. We also consider DDS as an alternative for certain networks in [Annex B], as well as present a current interim middleware solution in [Annex C].

Chapter 3 – IST-090 ACTIVITIES

IST-090 investigates the feasibility of extending the use of the SOA paradigm to tactical networks, with special focus on disadvantaged grids. There are a large number of possible approaches when looking to extend the SOA paradigm into tactical networks, and in IST-090 we have identified three main areas of focus:

- Interim solutions for use on the way towards a SOA based information infrastructure,
- Web Services across disadvantaged networks,
- The Data Distribution Service (DDS) at the tactical level.

The first item in this list, interim solutions, are, in their own right, not SOA solutions, but can rather be seen as a first step on the path from stove-pipe systems towards a service based infrastructure. The two remaining focus areas, Web Services and DDS, are alternative technology solutions that can both be used to implement a SOA-based infrastructure. In addition to these three main areas of focus other activities are listed in Section 3.4

IST-090 has had a strong experimental focus, where we have combined each nation's research in collaborative experiments or shared knowledge through demonstrations. In addition to the experiments performed, we have documented our work through a number of scientific papers, which were presented to the research community at MCC 2011.

3.1 INTERIM SOLUTIONS

As a stepping stone on the way towards full-fledged NNEC, it makes sense to consider middleware based interim solutions while working towards standardization of the necessary technology adaptations. A benefit of using such an interim solution is that it provides a cheaper and more flexible solution than today's stove-pipe systems.

The German Fraunhofer FKIE have developed such an interim solution, in the form of a middleware concept that allows for the coordination of C2IS applications and network protocol layers by using a cross-layer approach 0,0. In this middleware, several state of the art technologies and interfaces had to be combined to achieve a sound overall concept for network aware military applications, as well as a viable migration strategy for legacy systems. In addition to passing down the applications' communication and QoS requirements, an extended approach is followed that also provides the applications with well-adjusted information about the network environment. This can be used by the applications to adapt their functionality according to the available communication resources. Furthermore, the middleware is informed about application knowledge (e.g. mission information about the planned movement of troops). It enables the middleware to account for this additional information when configuring the network layers.

Germany developed a proxy-based interim solution for legacy systems that uses existing communication interfaces and network protocols in an intelligent way, and in doing so provides network awareness for legacy systems. Several state of the art technologies and interfaces had to be combined in a clever way to achieve a sound overall concept for network aware military applications, as well as a viable migration strategy for legacy systems. This was a challenge because the various commercial technologies employed were developed with very different goals in mind. What made it especially challenging is that no direct changes to the legacy applications were allowed. As a clever workaround, an application-based filter function was implemented on the existing platform as an additional software component. This filter function took the current state of the network into account and allowed for a semantic adaptation of the data sent by the application.

For a further description of this middleware, including the software demonstration given at MCC 2011, refer to [Annex C].

3.2 WEB SERVICES

Web Services is the most common and mature implementation technology for SOAs, and many nations are already implementing support for this technology in their information systems and infrastructures. In addition, Web Services has been identified as the key enabling technology for NNEC [15] because it offers loose coupling based on standards. By extending this technology into the tactical domain, interoperability with other systems is retained.

There are several aspects of Web Services that need to be adapted in order for the technology to function satisfactorily in disadvantaged grids, and the members of IST-090 have addressed these aspects both in the papers presented at MCC 2011, and through a common experiment, where the SOA solutions of several partners were connected together in order to achieve cross-domain information exchange.

The process of finding and identifying service, known as Service Discovery, is often implemented in the form of a service registry. Registry solution do however tend to have liveness and availability issues in disadvantaged networks, and because of this we have discussed and evaluated the performance of several non-registry based solutions for the use in radio based networks [16].

Once a service has been successfully discovered, the user of the service needs to invoke the service. In order to make Web Services invocation function satisfactorily in disadvantaged grids, there are three key requirements that have to be met [17]. One needs to:

1) Reduce the network traffic generated by Web Services,
2) Remove the dependency on end-to-end connections,
3) Hide network heterogeneity.

How to implement these requirements in practice will depend on how your Web Service infrastructure is realised. A Web Service deployment can be realised using an Enterprise Service Bus (ESB), which can be modified to improve performance in disadvantaged networks. Another possible solution is to introduce *proxies*, which can be used to adapt network traffic without having to change end systems. This approach has been investigated by Norway, through the use of the DSProxy [17], and by Poland, which has suggested the AFRO proxy [18]. For further details on the various approaches investigated in the context of IST-090, see [19] [Annexes A to E].

3.3 DDS

DDS is a standards based publish/subscribe middleware that focuses on providing support for real-time systems. It has also shown promise for use in resource constrained networks, where it leverages Quality-of-Service (QoS) support in order to provide reliable message exchange. These properties make DDS an interesting alternative to Web Services when attempting to extend the SOA paradigm into tactical networks. DDS uses knowledge about the schema of the messages it exchanges to reduce the overhead of message exchanges, and thus is able to implement SOA type services with little message overhead.

The DDS standard for exchanging messages ensures that different vendor implementations are interoperable. However, this standard is not efficient enough in disadvantaged grids, so different vendors implement different so-called tactical extensions. These extensions are proprietary optimizations of the communications protocol and they are not (always) interoperable.

In October 2010, the Spanish MoD, in cooperation with industry partners, demonstrated the use of DDS for the military [Annex B] [20]. Spain had prepared a live demonstration in their lab facilities showcasing their vision for the future Spanish SOA infrastructure: Using Web Services in conjunction with DDS, where DDS is used in the disadvantaged grid.

The demonstration successfully created interoperability among several legacy C2 applications from different vendors, and showcased the sharing of information among them in a disadvantaged grid scenario. A bridge was created to link two different SOA paradigms: Web Services and DDS. This bridge connected to the two technologically different SOA environments, enabling sharing information between them. It was a first step in solving the problem of interconnecting incompatible technologies, as well as sharing information among different operational levels (tactical and brigade). The demonstration also highlighted some challenges related to using DDS in bandwidth constrained networks – the need for vendor specific tactical extensions (i.e., optimizations to address bandwidth use), further described in [20].

When using DDS in the tactical domain, it is beneficial to be able to interconnect the tactical DDS domain with Web Services based solutions which might be in use in other information domains. This allows information to be exchanged between these technologically different domains, while at the same time leveraging the strengths of each solution within their respective domains. The Polish MCI has implemented and demonstrated a prototype WS-DDS Interface [21], which shows how this interconnection can be achieved using blue force tracking as an example service. For more information on using DDS in tactical networks, refer to [Annex B].

3.4 OTHER ACTIVITIES

This section provides information on various demonstrations that were done to investigate relevant topics.

3.4.1 Making Services Interoperable: SOA Over Disadvantaged Grids Experiment and Demonstrator

As part of the MCC 2011 conference, IST-090 was assigned a special area of the conference venue in order to demonstrate the benefits of the various solutions suggested by the IST-090 members. As part of this demonstration, further experiments were conducted over a dynamic network, provided by Norwegian and NC3A-owned MANET components. This provided a real, unreliable network environment in which we could assess the actual value of the suggested solutions.

During this experiment we interconnected two Web Service domains with a DDS domain in order to achieve cross-domain information exchange between domains that technologically different. We also demonstrated an experimental publish/subscribe protocol, tailored specifically for highly mobile networks, called MIST. For a detailed description of this joint experiment [Annex D].

In this experiment, no single solution stood out as the “magic bullet” to solve all the requirements for high speed connectivity to the edge, but many of them do offer measurable improvements in messaging capability. A number of key success factors were identified, including the foundation on open standards, ease of management and configuration, and transparency to the user. The messaging infrastructure should be optimised for the consumers of services without the need to incorporate proprietary, ad hoc solutions that will ensure tighter coupling between providers and consumers and therefore limit the range of potential partners. Where a protocol is not widely understood in another domain, gateways should be used to translate from one standard or protocol to another.

3.4.2 Sensor Network Integration Demonstration by Norway

In May 2011 at an IST-090 meeting in Oslo, a solution for Web Services integration of sensor networks was demonstrated to the IST-090 group, as an example on how to integrate networks that require the use of specialized hardware and software into a SOA environment. Sensor networks can be a valuable source of information to units in the field, but they often rely on specialized hardware and software solutions, making them challenging to integrate into a SOA infrastructure. In this demonstration, the sensor network sink (the node that connects the sensor network to other networks) was given a service interface allowing for both information extraction from the sensor network, and for configuring the sensor network from within the SOA domain. For further details [22].

3.5 SUMMARY

The IST-090 group has had an experimental focus, and this approach has enabled the group to gain practical experience with the originally suggested technologies and to expand their scope where useful.

Chapter 4 – CONCLUSIONS, LESSONS LEARNED AND WAY FORWARD

A SOA approach to interoperability provides agile C2 functionality through the provision of services on a network. It delivers flexibility, scalability and redundancy. However, SOA is currently only available at the higher levels of command such as (deployed) headquarters, and not at tactical levels. The work of IST-090 was a major step in extending the very valuable and flexible SOA to the tactical level [23].

The results of the RTG created an awareness of the challenges involved in extending a SOA to tactical networks and they provided possible solutions. The various demonstrations each made a valuable contribution to solving a difficult obstacle in the way of making NATO NEC a reality at the tactical level.

Following these experiments, no single solution stood out as the "magic bullet" to solve all the requirements for high speed connectivity to the edge, but many of them do offer measurable improvements in messaging capability. A number of key success factors were identified, including the foundation on open standards, ease of management and configuration, and transparency to the user. The messaging infrastructure should be optimised for the consumers of services without the need to incorporate proprietary, ad hoc solutions that will result in tighter coupling between providers and consumers of services and therefore limit the range of potential partners. Where a protocol is not widely understood in another domain, gateways should be used to translate from one standard or protocol to another.

4.1 CONCLUSIONS

Each of our 3 specific areas of our research warrants its own conclusions.

4.1.1 Interim Capabilities Towards End-to-End SOA Services

We found that a better coordination of C2IS applications with the different underlying network technologies can improve the overall user experience. The presented cross-layer middleware exchanges information between C2IS applications and the network protocol layers, to better coordinate application functionality with the capabilities of the different network technologies in use. This capability can also be applied to SOA based solutions.

We demonstrated that this approach can already be used for deployed legacy systems in disadvantaged networks.

4.1.2 Web Services

The application of Web Services to implement a service oriented system in a tactical environment requires a number of optimizations in order to reduce overhead. These optimizations can be of different types and can be on different levels, and can be combined for additional benefit. They are presented below.

Existing components can be configured in a more optimal manner. For example: configuring HTTP on the application server or ESB in a way that prevents time-outs.

Proprietary optimizations can be introduced in the form of intermediary components (proxies) that reduce communication overhead. These optimizations can for instance be compression (using SSL method or proxy compression) or implementing delay tolerance, to overcome network disruptions. Where proprietary optimizations are necessary, they should be implemented in gateways/proxies to ensure continued use of Commercial of the Shelf (COTS) clients and services.

When ESBs are used, we can abstract the optimizations away (i.e. make them transparent) from the developers and administrators of the services. Management of the communication becomes a separate concern, and additional optimization features can be deployed without the need to redevelop or recompile the applications themselves. In addition to this benefit, there are a number of features that are supported by ESBs that can greatly improve performance. Examples of such features include throttling and message prioritization. However, ESBs do not always comply with the standards and do not always deliver what they claim.

4.1.3 DDS

DDS is an interesting technology that can be applied if there is a need for real-time and QoS support. DDS is not a Web Service component so, if there is a need to use DDS, it becomes necessary to transfer data between the Web Service domain and the DDS domain. This was successfully demonstrated using the WS-DDS interface. Industry successfully demonstrated the interoperability among several different DDS implementations disseminating a service provided by the Spanish Army. The demonstration was however not run on a disadvantaged network. Therefore the robustness and usefulness of DDS will need to be validated in future events.

4.2 LESSONS LEARNED

There are two kinds of lessons learned: one related to the group collaboration and another related to dissemination of knowledge.

4.2.1 Group Collaboration

The task group was composed of 18 members from nine nations and NC3A. The group was fortunate in having members from industry, NC3A and academia. The NC3A members brought the group a stronger link to actual NATO systems.

IST-090 brought together the knowledge and experience of the member nations to better understand the SOA challenges and problems of disadvantaged networks. The nations worked together in sub-teams on the different aspects of the scientific challenges and in the development of the four main demonstrations. In addition, various specific experts from the different nations were invited and worked with us.

4.2.2 Dissemination of Knowledge

IST-090 disseminated its results, knowledge and experiences in different ways. We produced this NATO CSO report and we produced and presented numerous papers [Appendix H]. We also carried out demonstrations at ITM Madrid and at the MCC event. A CSO TG normally provides a report and sometimes also publishes papers, but usually does not provide a demonstration. This section discusses the lessons learned from the MCC 2011 demonstration.

Providing the demonstration brought us many benefits. We were forced, as a group, to present our material in a concise manner to the scientific community. The hands-on work that was needed to set up the demonstration was a challenge to our assumptions; we had to make sure that our assumptions were correct, and would have had to reconsider our assumptions if proven wrong. The combination of presentations and corresponding demonstrations provided theory as well as practice in a balanced way. A demonstration of tangible solutions proved also very useful, because it raised our profile in the community.

The demonstration also provided us with feedback and suggestions for improvements. The first observation is that, although improvements in our preparations are possible, in general the preparations went well. We now know that a CSO TG really should start preparing for the final presentation and, if it is decided to have

one, for a demonstration already at the start of the CSO TG. One of the practical things was that it is really important to arrange access to the facilities prior to the event.

The demonstration was comprised of two individual demonstrations, however it would be better to have more coordination between these demonstrations.

To increase visibility, we could assign a specific timeslot to each demonstration, preferably immediately after the corresponding presentation(s). We could also have sequences of presentations followed directly by one or more demonstration(s). In any case, the audience should be made aware which demonstrations will be done when and where. There is also a need for a realistic operational scenario that can be used as a common reference for each demonstration. Ideally, this scenario should be developed early on.

The demonstration at the MCC was well received. But we can still consider other options and improvements to our approach in engaging the community:

- We could put more effort into inviting stakeholders and other interested parties.
- We could consider events with a wider audience, or with a more specific audience such as the Coalition Warrior Interoperability eXploration, eXperimentation and eXamination, eXercise (CWIX).
- Instead of having a track within a conference it could be better to have a separate symposium, while also inviting external parties to contribute, to get more visibility. But this is also more difficult and requires more effort.
- We could also provide more promotional material to attract an audience (leaflets, pens, posters, etc.) and allow them to process our information also after the event.

4.3 WAY FORWARD

IST-118 CSO TG “SOA recommendations for disadvantaged grids in the tactical domain” has been initiated [24] as a follow-on to IST-090. This is based on the promising results of IST-090, the aspiration to do more work and with the goal to provide more results in this area of research.

The approach of IST-118 is to identify the types of information and the services to be used at the tactical level and use these to do experimenting and testing with possible SOA improvements. Based on the results, the goal is to provide guidance (best practices) to make SOA applicable on battlefield disadvantaged grids, in the form of a Tactical SOA Profile.

The approach will be:

- Identify the types of information that are exchanged at the tactical level in the SOA environment. These will be used in testing and prototyping. We will consider “future” systems and/or services, their expected communication needs, and the expected impact at the tactical level. This information will be documented in use cases.
- Identify tactical SOA foundation services needed to support the use cases. Examples: messages, security, discovery, management, mediation. Investigate how this baseline can be extended for use in tactical networks.
- Based on the identified types of information and the available technology we will propose a (set of) solution(s) for the use cases that we will be testing.
- Based on the information requirements the group will define their test plan. The test plan will incorporate well defined scenarios with predefined parameters. For the communication networks the

group will consider what techniques, throughputs and disruptions are relevant to the disadvantaged networks in the expected scenario. The group will employ a test framework that is based on (a combination of) simulation and/or emulation.

- To make the test plan realistic and relevant to the tactical environment, the group will consider the expected security overhead (signatures, added traffic) in the actually exchanged information.

Annex A – WEB SERVICES

There are many definitions of "Web Services". The core idea is the same (i.e., using XML [25] formatted data for information exchange), but some of the finer details may vary. For example, so-called restful Web Services [26] (REST) ignore most of the Web Services standards and specifications, providing only synchronous remote procedure call functionality using HTTP [27] over TCP [28]. TCP does not necessarily function in all disadvantaged grids, meaning that REST is too restrictive if one wants to implement a pervasive SOA for military networks. We need the flexibility of a broader spectrum of the Web Services specifications.

A.1 WEB SERVICES CHALLENGES IN HETEROGENEOUS NETWORKS

In Web Services, all communication is based on sending XML-based SOAP messages. A SOAP message is an "envelope" consisting of a header and a body. The header contains information related to the handling of the message, such as addressing and security information, while the body contains the application data. In regular Web Services, SOAP messages are transmitted using the HTTP protocol, which in turn uses the TCP protocol for reliable transfer of the messages. This protocol set is not suited for use in disadvantaged grids, and the main question is how to enable the use of Web Services in disadvantaged networks and across heterogeneous networks. Through our research on Web Services in disadvantaged grids, we have found that this question can be broken down into three requirements that must be met:

1) Reduce the network traffic generated by Web Services;
2) Remove the dependency on end-to-end connections; and
3) Hide network heterogeneity.

A.1.1 Addressing Web Services Overhead

The first problem is related to the amount of network traffic generated by Web Services. It is necessary to reduce both the size of the individual messages, and the number of messages being transmitted. XML is a rather verbose language, and tends to produce much larger messages than binary formats do. Using techniques such as compression will reduce the size, and thus the bandwidth requirements of each individual message, but will not reduce the number of messages sent between nodes. In our work, we have looked at several ways of limiting the number of messages:

1) Employing caching near the clients, which allows for reuse of older messages;
2) Using the publish/subscribe paradigm, where clients subscribe to information instead of requesting it, allowing the same message to be sent to multiple clients; and
3) Employing content filtering to ensure that only relevant data is transmitted.

A.1.2 End-To-End Connections

The second issue is that regular Web Services depend on a direct, end-to-end connection between the client and the service. TCP is connection-oriented, and designed for wired networks, which means that the control mechanisms are designed for handling congestion, and much less for handling errors. In tactical networks with high error rates and high latencies, the congestion control of TCP will therefore cause sub-optimal utilization of the network due to frequent connection timeouts. When multiple networks are interconnected (see Figure A-1), TCP's need for establishing an end-to-end connection increases this problem; each traversed network adds delay, increasing the risk of connection timeout. Similarly, HTTP is synchronous, which means that when a SOAP request is sent, the HTTP connection is kept open until the SOAP response

is returned in the HTTP acknowledgement message. If the connection times out the SOAP response cannot be routed back to the service consumer.

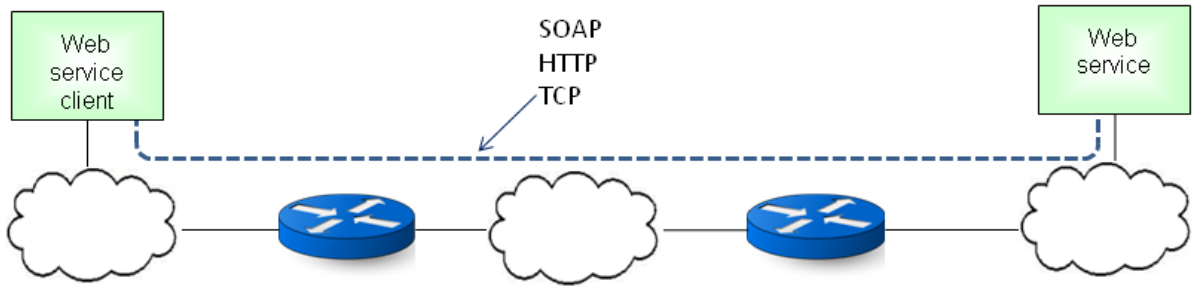

Figure A-1: HTTP and TCP Establish End-to-End Connections.

The obvious solution to this problem is to replace HTTP and TCP with other, more suitable protocols. However, this requires modifying the application software. Alternatively, an extra communication layer can be introduced. Within this layer, hidden from the applications, more suitable protocols can be used (e.g., tactical protocols such as STANAG 4406 Annex C & E), that are able to withstand long and variable round trip times, and have little communication overhead. There exist different approaches to implementing such a layer, for example one can implement support directly in clients and services, or one can introduce proxy servers.

By implementing this extra communication layer in a *proxy* solution, standards compliance can be retained. A proxy is a node in the network between a client and a server through which the network traffic passes. A proxy can be used for several purposes, such as caching, firewalling and content adaptation. For example, HTTP proxies have been popular on the Internet for years, since they lower response times when surfing the WWW. Web Services proxies follow the same principle as HTTP proxies, in that they function as a "middle man" between the provider and the consumer of the service. However, they do not just understand the HTTP protocol, they must be able to recognize and process SOAP as well. For example, Norway has developed an initial SOAP proxy prototype [29].

Introducing an extra communication layer means increased flexibility when it comes to selecting which transport mechanism(s) to use. Additionally, using this approach means that the end-to-end connection dependency is removed in favor of a per-hop-behavior. In this case, the application software can often be left unmodified. However, there is a possibility for information corruption along the route, which may not be detected without an end-to-end connection. Also, since packets are acknowledged on a per-hop basis, you do not get end-to-end reliability. These two issues can be mitigated if the client uses application level solutions for error control and reliability. For example, using XML signatures will ensure that any modifications to a SOAP message is detected by the receiver, despite the lack of end-to-end error control. Furthermore, using for example the WS-ReliableMessaging specification provides application level acknowledgements, which mean that you do not need an end-to-end connection on the transport layer to acknowledge delivery. Thus, client software must use the appropriate Web Services specifications to add the desired level of resilience to their SOAP messages.

A.1.3 Network Heterogeneity

The third problem arises when heterogeneous networks are interconnected. In disadvantaged grids it is not uncommon to experience data rates of less than 1000 bits/s [30]. In particular, when several users are using the network simultaneously, the effective data rate can become very low because resources are shared. Connecting such networks to faster networks introduces a risk that the gateway between the networks has to drop packets due to its buffers filling up faster than the packets can be transmitted out onto the lower capacity network. In order to avoid this problem altogether, some information will have to be dropped by the

gateway, i.e., through content filtering. However, if the problem of congestion is temporary, then the problem can be countered by introducing store-and-forward capabilities into the network. In addition, a store-and-forward capability can help alleviate the problems that arise from frequent communication disruptions, which can prevent a message from being delivered immediately. Having store-and-forward support can ensure that the message is not dropped and subsequently having to be retransmitted.

When traversing heterogeneous networks, different communication protocols may be required. This means that a message traversing several networks may have to use multiple different protocols on its way from sender to recipient.

A.1.4 Goals and Solutions

The CSO group has come up with a number of solutions that mitigate some of these challenges and are being discussed in the following chapter. They are listed below:

• **Goal**		• **Possible Solutions**	
• Optimize information communication	• Store-and-forward overlay network	• Caching data	
• Optimize information representation	• Standardize the data model for information exchange		
• Reduce Message Size Overheads	• XML compression	• Binary XML	
• Reduce the amount of data traversing the network link	• Use of Proxy Server for caching and filtering	• Use of Federated Caching	• Use of multicast service discovery
• Increase the efficiency of information transfer	• Subscribing and Filtering for Pub/Sub: • Topic-based • Content-based • XML-based		
• Improve performance	• **Acceleration XML processing** • (Evaluation of different XML data parsing)	• Caching data	
• Improve Security	• Transportation-level security	• Message-level security	

A.2 WEB SERVICES

In total there are well over 150 specifications related to Web Services. However, only a few of these have become standards, or specifications mature enough to be widely supported by industry. Thus, only a select few of all these specifications are actually in use today. The most important standards are SOAP (messaging) and WSDL (service descriptions), since they form the foundation for all other Web Services specifications and interactions [31].

When we discuss Web Services in this report we use the definition by the World Wide Web Consortium (W3C) [32]: "A Web Service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web Service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."

Lifecycle

Figure A-2 shows the lifecycle of Web Services. We will now discuss this lifecycle in context of the SOA principles:

1) Assuming that a service has been implemented by a service provider, it first needs to make the service available through an advertisement. This means that after the service has been made available in the network, it needs to be published in a service registry.
2) Service clients, the so-called consumers, can now query the registry and find this and other available services (i.e., service discovery).
3) The list of services found in the discovery phase then need to go through a selection phase, where a service is selected. Service selection can be done either manually or automatically [34].
4) If multiple interesting services are found, then one can also create a new service through composition. This is an optional step, and is only applicable when using composite services.
5) The final step is invocation, where the service consumer binds to the service provided.

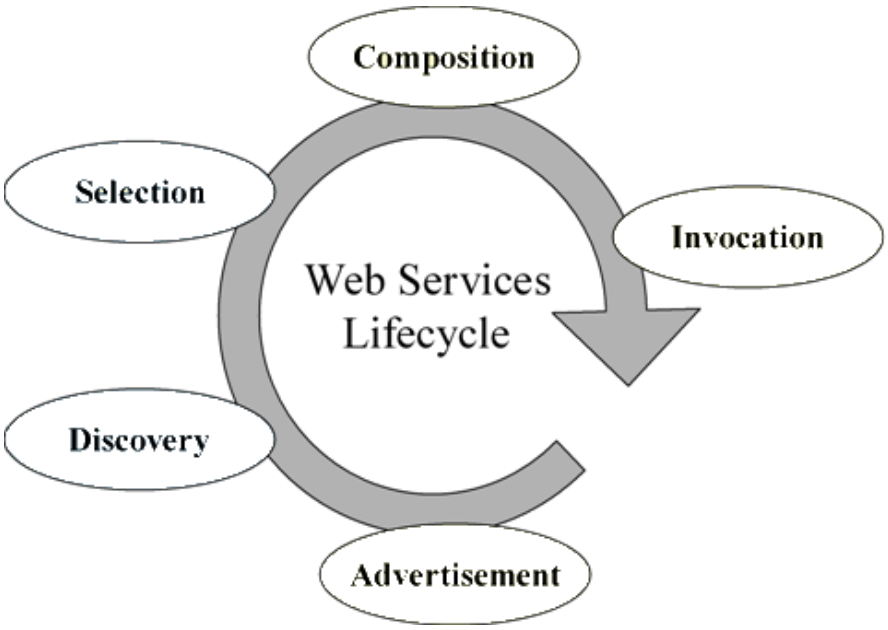

Figure A-2: Web Services Lifecycle (from [33]).

Only the last step has to be performed at run-time. When Web Services are used in businesses, the first four steps can be performed at design-time, when the SOA enabled system is implemented. This is because enterprises usually have fixed infrastructure where services are permanently available, so that the service address (i.e., binding) that was discovered and selected can be hard-coded in the client software. However, in dynamic systems, there is a need to be able to perform some of these steps at run-time. In this report we pay special attention to steps 1, 2, and 5.

The importance of step 5 is obvious, but since tactical networks are dynamic we also need to be able to perform steps 1 and 2 at run-time. Automated run-time selection and composition of Web Services is not supported by current Web Services standards, and is thus beyond the scope of this report. Step 3 can be solved easily – either by manual choice or for example choosing the first service in case of automated selection.

A.3 FOUNDATIONAL WEB SERVICES STANDARDS

One of the earliest Web Services standards, SOAP, was first introduced in 1999. Since then the number of Web Services related standards have been ever increasing and the Web Services standards now cover a large range of topics. The core standards, such as XML, SOAP and WSDL are widely supported, but the sheer number of available specifications means that it is difficult for developers to know which of them to adopt. This task is made even more complex when taking into consideration the fact that the maturity of the specifications vary. Some are fully ratified standards and have been released in several versions already, while others are early in their development cycle and are currently working drafts or have status as notes or recommendations.

In addition to the maturity issue, it is worth noting that there is not one single organization that controls all the on-going Web Services standardization work, and thus there is no set standardization process that ensures that all the standards adhere to a common “Web Services architecture”. As a consequence, some topics are covered by multiple, and in some cases competing standards, while other topics are not covered by a standard at all. Vendor support is crucial, so looking into which standards are currently supported by the major vendors such as IBM and Microsoft can function as a guideline when trying to determine if a standard is likely to ever see widespread use. The Web Services Interoperability Organization (WS-I) [35] is an open industry organization chartered to promote Web Services interoperability across platforms, operating systems and programming languages. The organization’s diverse community of Web Services leaders helps customers to develop interoperable Web Services by providing guidance, recommended practices and supporting resources.

Below we give an introduction to the foundational Web Services standards.

A.3.1 Extensible Mark-Up Language (XML)

XML is a simple, very flexible text format derived from SGML (Standard Generalized Markup Language) (ISO 8879) [25]. Originally it was designed to meet the challenges of large scale electronic publishing, but XML is playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. XML is often considered the base standard for Web Services, as most of the other standards use the encoding and format rules defined in this standard. There are multiple XML related standards, with the two most important being XML itself, and XML Schema. The latter standard is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntax constraints imposed by XML itself.

An XML document consists of data that are surrounded by tags. Tags describe the data they enclose. A tag may have other tags inside it, which allows for a nested structure. To illustrate the structure of an XML document, consider this simple example:

```
<?xml version="1.0" ?>
  <greeting>
      <greeting text>Hello world!</greeting text>
  </greeting>
```

One of the benefits of using XML is that an XML document contains metadata, that is, data about the data that are present in the document. In the example above, for instance, we can see that the text string "Hello world!" is a "greeting text", which in turn is a part of "greeting". Such tags can be standardized, which allows for the exchange and understanding of data in a standardized, machine-readable way. An XML document can be defined according to an XML Schema, which enables validation of XML documents according to rules defined in the schema.

A.3.2 SOAP

SOAP [36] is an XML based protocol for information exchange in a decentralized, distributed system. SOAP is an envelope for XML messages, functioning as a transport independent messaging protocol. It was called "simple object access protocol" up to and including its release as a W3C version 1.1 note, but this name did not describe exactly what SOAP was, and so it was later dropped.

In its current version, the W3C version 1.2 recommendation, the protocol is just called "SOAP". SOAP messages can be carried by a variety of protocols, the most common being HTTP. Other protocols can also be used — standardized SOAP bindings exist for User Data Protocol (UDP) [37] and Simple Mail Transfer Protocol (SMTP) [38] in addition to HTTP. Since SOAP is transport protocol agnostic, it can basically be used with any transport protocol. For example, experiments have shown that one can run SOAP over STANAG 4406 [39].

Current Web Services development tools usually support both SOAP version 1.1 and version 1.2. A SOAP message contains a header and a body. SOAP is an application level protocol. Compared to for example an IP packet, the SOAP header is the equivalent of the IP header, whereas the SOAP body is the equivalent of the packet payload. Thus, just like an IP header, the SOAP header can contain information that is necessary to achieve the desired per-hop behavior of the message. For example, WS-Addressing [40] information can be present in the SOAP header and be used to achieve transport protocol independent addressing of SOAP messages. Security related standards typically also add fields to the SOAP header [41].

A.3.3 Web Services Description Language (WSDL)

WSDL [31] is an XML language for describing Web Services. The current version is 2.0 [42], available as a W3C recommendation from 2007. However, version 1.1 [43] is still being used a lot, since several development tools work with this version of WSDL - this is because currently only WSDL 1.1 is addressed by the WS-I basic profile. Since XML is used, Web Services definitions can be utilized by any implementation language, platform, object model or messaging system. The specification defines a core language which can be used to describe Web Services based on an abstract model of what the service offers.

A WSDL service description indicates how clients are supposed to interact with the described service. It represents an assertion that the described service implements and conforms to what the WSDL document describes. A WSDL interface describes potential interactions with a Web Service, not required interactions. The declaration of an operation in a WSDL interface is not an assertion that the interaction described by the operation must occur. Rather it is an assertion that if such an interaction is initiated, then the declared operation describes how that interaction is intended to occur. By using WSDL, it is possible to create a formal, machine-readable description of a Web Service, making it possible for clients to invoke it.

WSDL service definitions provide documentation for distributed systems and serve as a recipe for automating the details involved in applications' communication. Thus, WSDLs are a crucial part of Web

Services, since they define the interface through which you access services, as well as information about where the service can be found in the form of an URL.

We will now take a closer look at a WSDL 1.1 document, since that is the foundation of all the Web Services implementations we discuss later in this report. A WSDL 1.1 document uses the following elements in the definition of network services:

- Types, which is a container for data type definitions using some type system, such as XML Schema Definition.
- Message, which is an abstract, typed definition of the data being communicated.
- Operation, which is an abstract description of an action supported by the service.
- PortType, i.e., an abstract set of operations supported by one or more endpoints.
- Binding, containing a concrete protocol and data format specification for a particular PortType.
- Port, which is a single endpoint defined as a combination of a binding and a network address.
- Service, which is a collection of related endpoints.

A.3.4 WS-Notification

Currently there are two standardization efforts regarding publish/subscribe for Web Services: OASIS has its Web Services Notification (WS-Notification, WSN) standard [44], whereas W3C has produced a similar framework called Web Services Eventing (WS-Eventing) [45]. Both of these protocols are based on SOAP, and use the functionality provided by SOAP rather than building their own messaging protocols. Here we focus on WS-Notification, because it has been identified as the standard of choice by NATO CESWG.

There are three parts in the specification: WS-BaseNotification, WS-BrokeredNotification and WS-Topics. The WS-BaseNotification specification unifies the principles and concepts of SOA with those of event based programming.

WS-BaseNotification provides the foundation for the WSN family of specifications. It defines the basic roles and message exchanges needed to express the notification pattern. The specification can be used on its own, or it can be used in combination with the WS-Topics and WSBrokeredNotification specifications in more sophisticated scenarios. The specification defines the message exchanges between notification producer, notification consumer, subscriber, and subscription manager.

The simplest form of a subscribe request message just contains an endpoint reference for a notification consumer. This form of request instructs the notification producer to send each and every notification that it produces to the notification consumer.

The subscribe request message can optionally contain one or more filter expressions. The filter expressions indicate the kind of notification that the consumer requires by restricting the kinds of notification that are to be sent for this subscription.

WS-Notification encompasses the following standards:

- WS-BaseNotification defines standard message exchanges that allow one service to subscribe and unsubscribe to another, and to receive notification messages from that service.
- WS-BrokeredNotification defines the interface for notification intermediaries. A Notification Broker is an intermediary that decouples the publishers of notification messages from the consumers of those messages. This allows publication of messages from entities that are not themselves Web Service providers.

- WS-Topics defines an XML model to organize and categorize classes of events into “Topics”, enabling users of WS-BaseNotification or WS-BrokeredNotification to specify the types of events in which they are interested.

The WSN specifications standardize the syntax and semantics of the message exchanges that establish and manage subscriptions and the message exchanges that distribute information to subscribers. An information provider, known as a notification producer, that conforms to WSN can be subscribed to by any WSN-compliant subscriber.

A.4 WEB SERVICES DISCOVERY STANDARDS

There are three standards related to service discovery, all by OASIS: Universal Description, Discovery and Integration (UDDI), electronic business using XML (ebXML), and WS-Dynamic Discovery (WS-Discovery). UDDI is the oldest and most widely known, which is why it is almost always mentioned when one talks about service discovery in the context of Web Services. So far, it is the only discovery related standard that is addressed by the WS-I. This means that UDDI is also the most mature and widely supported of these standards. Currently, UDDI is being considered for the role of service registry by NATO CESWG, and ebXML is being considered for use as a metadata registry.

A.4.1 UDDI

UDDI [46] allows service providers to register their services and service consumers to discover these services both at design-time and run-time. In principle, UDDI is centralized, but mechanisms for federating several registries have also been specified in newer versions of the specification.

Having multiple registries, or letting a registry consist of several nodes that replicate data, increases the robustness of the discovery solution. In UDDI, replication between registry nodes must be configured manually. It is also possible to let several separate UDDI registries exist independently of each other, but information will not be replicated unless a custom scheme is designed. Additionally, a hierarchical model may be used, using a root registry and affiliate registries. In this case, a root registry must be chosen, and affiliate registries may be defined as child registries of the root registry.

This must be done to avoid duplicate identifiers or keys. A replication scheme for intra-registry replication between nodes is defined, which allows for fault tolerance. The replication topology must be configured.

UDDI supports rich service descriptions, and one can find services by name, type, binding and according to a taxonomy. UDDI provides a flexible model in that specific service types can be registered with the registry and referenced by service instances that implement the service type.

This is called a technical model, or tModel, in the UDDI information model. A tModel can include pointers to further description of a service, such as a WSDL description and bindings. Since UDDI is designed to be general, OASIS describes ways to map WSDL documents and also BPEL4WS abstract processes to the tModel fields of the UDDI registry. Especially the former facilitates a number of interesting queries, where searches can be based on WSDL port types and bindings, that is, the signature of the service. This is very important for run-time selection of services.

The tModels give flexibility, but that is also one of the drawbacks with UDDI, as proprietary use of the field can occur. Many solutions use the tModels to store such proprietary information, for example about QoS issues [47]. However, if such proprietary solutions are to work, all publishers and consumers using the registry must understand the information in the tModel and know how to handle it. Another limitation is that tModels are not stored in UDDI registries themselves. A unique identifier referencing a tModel is contained in the registries, and you need a separate repository to store the actual data in.

The UDDI registry supports reconfiguration as long as services do not go down unexpectedly. If so, advertisements will be in the registry forever because there is no liveness information in the current versions of UDDI. UDDI does not include a repository mechanism. It can only hold Uniform Resource Identifiers (URIs) pointing to content which has to be stored somewhere else, such as on the WWW.

Since UDDI is the most mature of the Web Services registry standards, several vendors offer UDDI implementations. Some support the newest specification UDDI version 3, whereas others implement the older UDDI version 2. There also exist several open source implementations that implement UDDI, for example, Apache jUDDI, which is a Java implementation of UDDI v3. It is freely available from http://ws.apache.org/juddi/.

A.4.2 ebXML

Another service discovery standard is ebXML [48]. It is a collection of specifications for conducting business-to-business integration over the Web. It allows registering services in a similar way as UDDI according to its own registry specification. The ebXML registry also defines inter-registry interaction, or cooperation between registries, a so-called federation of registries. Note that an ebXML federation is different from that of a UDDI federation, because ebXML supports a non-hierarchical multi-registry topology. Here, each registry has the same role, and registries may join or leave a federation at any time. This allows flexible deployment. Federated queries are supported, enabling query forwarding to other registries without the need to replicate data first. Since the federation model is P2P based, there is no single point of failure. The ebXML registry is meant to support both discovery and business collaboration, as opposed to UDDI, which mainly targets discovery.

The ebXML registry information model is similar to that of UDDI but somewhat more flexible. Business capabilities such as processes and services can be published in the registry. It is possible to use taxonomies to classify the registered items. Support for rich service descriptions in ebXML is currently very similar to that of UDDI. Both support finding services by name, type, binding and according to a taxonomy. However, ebXML supports more advanced (i.e., Structured Query Language (SQL) based) queries.

Just like UDDI, ebXML has issues with liveness, in that it supports reconfiguration as long as services do not go down unexpectedly. Unlike UDDI, the ebXML registry can store vocabularies like XML Schema or ontologies since it also specifies a repository for such items. This standard is less mature than UDDI and is not as widely supported by industry as UDDI is. There exists an open source reference implementation of ebXML 3, which is the most recent specification. That implementation, called Omar, is freely downloadable from http://sourceforge.net/projects/ebxmlrr/files/.

A.4.3 WS-Discovery

WS-Discovery is a standardized Web Services discovery mechanism. After first becoming a draft in 2005 [49], it became a standard in 2009 [50]. This makes WS-Discovery the most recent of the Web Services discovery standards, meaning that there are few implementations available that adhere to the standard. For example, the implementation of WS-Discovery in Windows Vista pre-dates the standard, and is thus only draft compliant.

An open source implementation of WS-Discovery written in Java which supports the standard is available from http://code.google.com/p/java-ws-discovery/.

WS-Discovery is based on local-scoped multicast, using SOAP over UDP [37] as the advertisement transport protocol. Query messages are called probe messages. Services in the network evaluate probes, and respond if they can match them. To ease the burden on the network, WS-Discovery specifies a discovery proxy (DP) that can be used instead of multicast (e.g., if a registry such as UDDI or ebXML is present, it should be used

instead). This means that WS-Discovery can run in two modes, depending on whether there is a DP available or not. However, this DP is not well defined in the standard. The standard fully describes the decentralized operation of WS-Discovery, but the functionality of (and integration with) the DP is left to be implemented in a proprietary manner for now.

WS-Discovery is suited for service discovery in a LAN only, since it is based on local scoped multicast. However, if a DP is present, then WS-Discovery enables you to find that DP in your LAN. That DP can in turn allow you to find services in the WAN. WS-Discovery, when operating without a DP, is fully decentralized. However, when a DP is present, it should be used instead, and then the robustness of the DP solution is important. As none of the registry standards take liveness into account, WS-Discovery will only accurately reflect the service network in its decentralized mode.

With WS-Discovery, service matching is based mainly on the WSDL port type supported by the service and administrative scope. The port type is described by a namespace URI, and some scope limitation can be done through a simple filter. Since WS-Discovery cannot provide a complete WSDL, it is not suited for design-time discovery. WS-Discovery has no repository mechanism, and information referenced in discovered descriptions (i.e., WSDL includes and XML schema includes) need to be fetched from somewhere else.

A.5 ADAPTING WEB SERVICES FOR USE IN DISADVANTAGED GRIDS

Web Services is a technology or more specifically a collection of standards. This technology is the most common way (but not the only way) to implement SOAs. Figure A-3 shows a high-level view of the Web Services communication stack.

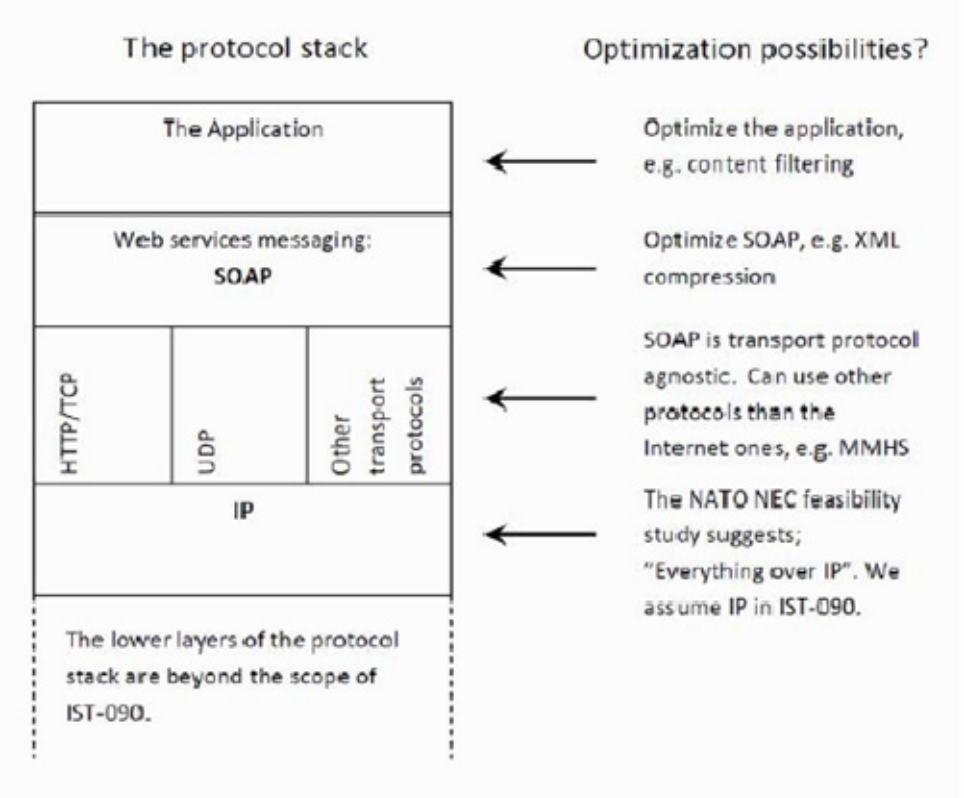

Figure A-3: Optimizing the Protocol Stack.

As we can see, there is room for optimizations several places in the protocol stack. At the application level, it is possible to limit the applications' need to exchange data by changing the data representation and performing content filtering [51]. Below the application level we need some sort of standardized middleware to ensure interoperability across different systems. The NNEC feasibility study has identified SOA implemented by Web Services technology as the key enabler for NNEC [52]. Web Services are based on open standards and define an XML based messaging protocol called SOAP. Being based on XML, SOAP messages can be quite large. However, the benefit of SOAP is that it can be handled by COTS development tools and thus COTS clients and services. It is possible to reduce the footprint of XML by using compression. A previous study has shown that standards, such as GZIP and the emerging standard for efficient XML (EFX), compress XML quite well [53]. SOAP is transport protocol agnostic, meaning that it can be carried by any transport protocol. In civil systems, the standardized SOAP binding to HTTP over TCP is used most of the time. There also exist bindings to other transport protocols such as UDP and SMTP. In a military network other protocols could be used, for example Military Message Handling System (MMHS) which is based on tactical transport protocols and adds store-and-forward capabilities [39]. Thus, there are several techniques that can be investigated in order to make Web Services better suited to the tactical environment. In IST-090 we do not concern ourselves with radio technology or link layer issues, as this is being covered by other NATO groups. We assume that IP is used on the network layer, since the NNEC feasibility study has identified this as the common protocol for network interoperability – the so-called "Everything over IP" idea.

For an extended discussion on Web Services standards and solutions for use in military networks, see [54].

A.5.1 Current SOA-Based C2 Functionalities

Many SOA-based C2 functionalities are being prototyped or are already available. The whole NATO concept is being developed based on the SOA concept (Core G, FFT, NMMR, IEG, NIRIS, MCCIS, BRITE – BWS). Many other countries have also shown their SOA-based implementations (Germany – SPC SOA, France – FoCCs-SOA, Finland – Mevat) [55]. Utilization of SOA-based implementation of Web Services in an NEC environment has been shown in many international experiments. These prove that SOA technology improves collaboration, interoperation and information sharing in a Federation of Systems (FoS) [56].

Together, the nations that participate in IST-090 have much relevant experience in implementing SOA in the area of C2. Some examples are provided below:

Example: *Coalition Warrior Interoperability Demonstration (CWID)*

The CWID demonstration [55] evaluates technologies and capabilities for exchanging information among coalition partners, military services, government agencies, first responders and U.S. combatant commanders. Information sharing technologies leverage decision-making and operational flexibility on the battlefield and during crisis response on the home front. Two specific CWID examples are described:

CWID 2006

SOA solutions need to work with different types of information and communication systems. During CWID exercises in 2006 tests of SOAP Web Services were performed that resulted in the conclusion that "service-oriented architecture implemented via the technology of Web Services is the strategic means to achieving interoperability". However particular problems related to the utilization of protocols of the SOA stack like TCP/HTTP/SOAP have been recognized [57].

CWID 2007

Another example of SOA-enabling of C2 software is an experiment [58] that took place at NATO CWID 2007, in which a hand held soldier system was connected to an already existing national C2 system using a Web Service interface.

Example: *BRITE*

> The Baseline for Rapid Iterative Transformational Experimentation (BRITE) is an experimentation framework which allows for the rapid implementation of new ideas and capabilities to support experimentation. It fits into the Transforming Technology for Information, Decision and Execution (TIDE) superiority concept. Its goal is to rapidly improve the IT capabilities of the NATO Alliance by reusing existing systems/components and by steering current and future projects towards greater openness and cooperation in a common framework. WISE 2.0 is part of this BRITE framework. These components are implemented as a SOA.

Example: *Multi National Experimentation 6 (MNE 6) in phase A.2*

> This experiment is used to test technical possibilities in sharing maritime situational awareness between systems of the Baltic Sea. It encompasses Multinational Inter-agency Situational Awareness – Extended Maritime (MISA–EM). It includes e.g. the following systems: FIN: Mevat; SWE: Sucbas; POL: SWIBZ, NATO: BRITE, all based on Web Services and SOA based solutions [59].

Example: *Norwegian national experiment*

> Figure 2-2 shows the many ways SOA services can be constructed, either as a new SOA service, as a wrapped legacy service or as a composite service. During a Norwegian national experiment [60] several of these mechanisms were tested using an experimental Cooperative ESM Operations (CESMO) software. This software was wrapped using Web Service standards and was thus made available to new users. In addition, new functionality, in the form of a NATO Friendly Forces Information (NFFI) blue force tracking service, was created from scratch using the same data sources.

Example: *Joint NC3A/NOR experiment at Combined Endeavor 2009*

> At Combined Endeavor (CE) in the Netherlands, 2009, experiments were performed using Web Services in mobile networks and over reach-back links back to deployed infrastructure (i.e., the HQ) [61]. Here, we were able to show the feasibility of employing Web Services in an operational experiment for a specific set of communications hardware: NC3A used Rajant Breadcrumbs, whereas NOR used the KDA WM600 tactical radio. We were able to successfully discover and invoke Web Services across the heterogeneous networks, through the use of proxies for delay tolerance and gateways for network- and discovery protocol interoperability.

A.5.2 Web Services Experimentation in Context of IST-090

The IST-090 member nations have performed much Web Services related research during the course of IST-090 as presented below.

A.5.2.1 Independent Evaluation of a Number of Published Approaches that Purport to Improve the Reach of Web Services into Locations with Disadvantaged Networks

In [62] we report on a project that has independently evaluated a number of published approaches that purport to improve the reach of Web Services into locations with disadvantaged networks. The original analyses produced were incompatible and thus of limited value. This project has brought them into a directly comparable framework. We also analyse raw Web Service and other very low cost solutions to provide a context in which to view the results of the published solutions. The output of the work is advice on how and where to use each of the solutions in order to facilitate the delivery of Web Service based SOA systems over disadvantaged networks.

A.5.2.2 Mediation of Network Load Over Disadvantaged Grids Using Enterprise Service Bus (ESB) Technology

One of the main aspects of a SOA, and thus the future NNEC, is that of the dynamic discovery and utilization of services. However, it is likely that different versions of a service will be offered, physically located within separate parts of the enterprise infrastructure. If the SOA infrastructure could be designed to be "network aware" then the user could be automatically directed to the proper instance of a service based upon the status of the end-to-end connection between the user and service, and the required quality of service. A network-aware SOA would need to facilitate the adaptation of a service depending on the status of the connection between the client and the server or between two end users (depending on the scenario). With the goal to provide a ubiquitous, global, seamless, pervasive, fully managed, resilient, secure and flexible Internet Protocol (IP) based communications capability including wired, wireless and Satellite Communication (SATCOM) bearer services, the services in a service-oriented architecture need to have the ability to adapt to the current network conditions. This especially applies for disadvantaged users, such as in a MANET (mobile ad-hoc networking) extension of a fixed network. Depending on the available data rates, error rates, delays etc. different variants of services can be supported [19].

A.5.2.3 Review of Service Advertisement and Service Discovery (SASD) Algorithms

SOA is an approach to designing information systems that promotes good management and cost effectiveness through reuse and easy reconfiguration. The concept being that through a thorough understanding of service level agreements, service descriptions and finding new service providers you are able to allow competition between IT suppliers to drive down costs and drive up value. However, although many of the technologies exist to support these goals, and they are even embedded within most of the SOA implementations offered by the major vendors, they are rarely used in commercial projects. Instead, commercial IS system developers prefer to pre-configure the SOA interconnections. We believe that this gives them greater confidence in the stability of their system.

One major issue is that the system houses do not trust the service advertisement and service discovery (SASD) algorithms to correctly find the "correct" provider at any given time. One issue they face is that although there are many SASD algorithms they have not been evaluated in a common framework that allows direct comparison of the results. GBR reviewed such SASD algorithms. Several SASD algorithms were identified that were considered to demonstrate very different approaches to the problem. This work still needs more consideration.

A.5.2.4 Semantic Description of QoS Framework for Context-Aware Web Service Provision

In [63], we present a semantic description of Web Service QoS profiles that is part of the larger framework for context – aware service provision. It consists of upper level ontology that defines basic concepts and their relationships generally known from ITU-T recommendations and domain ontology for Web Service provision that specifies user QoS profile, service QoS profile and network performance. This Quality of Web Services (QoWS) model can be used for (1) service discovery enabling to match user QoS requirements and service QoS offerings, and (2) service delivery, including adaptation actions in order to support QoS provision for Web Services in disadvantaged wireless environment. The model is based on existing ITU-T QoS descriptions and Web Service QoS models defined e.g. by OASIS and W3C.

A.5.2.5 WS-DDS Interface (Gateway) for Tactical Network

In [64], we present results of the study on the exchange of data between Web Services (WS) and Data Distribution Service (DDS) using WS-DDS Interface. WS-DDS Interface connects two architecturally different message exchange solutions dedicated for two different environments. Web Service is system-independent application very often used in over-provisioned network. DDS is designed for real time applications. It works in publish-subscribe mode providing efficient solution for resource constrained

networks. The WS-DDS Interface enables bi-directional traffic between WS and DDS, with regard to the timeframe of the protocol and data transformation, which is a very important factor in success of a mission.

DDS is discussed further in [Annex B].

A.5.2.6 Service Advertisements in MANETs (SAM)

Service Advertisements in MANETs (SAM) is a service discovery protocol that we have designed and implemented for use in MANETs [65]. It addresses the high resource use of WS-Discovery, and uses periodic service advertisements. The advertisements are compressed to reduce overhead, and caching with timeouts is used to address the liveness issue. The protocol offers a fairly up to date view of available services (in the local cache), and may significantly reduce discovery communication overhead because there is no need to query the network. Instead, service advertisements are sent at fixed intervals using IP multicast to reach all nodes. This spreads out the service discovery traffic over time, and eliminates traffic bursts due to frequent searches for services. The protocol is released as open source at: http://sourceforge.net/projects/servicead/.

A.5.2.7 Mist

As multicast is not always available in MANETs, we have designed a delay tolerant, publish/subscribe mechanism that we call Mist [66]. Using this protocol, we have implemented a Web Services discovery solution, Mist-SD (http://mist-sd.googlecode.com/), which is suitable for use in large MANETs. Like SAM it is based on periodic updates, but instead of completely distributing all information to all nodes, it uses a combined broadcast and subscription scheme which ensures that only relevant information is propagated through the network.

A.5.2.8 An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield

To successfully discover Web Services, we need to find the service signature and the corresponding service address. For Web Services, the service is defined by the WSDL, where the unique combination of defined messages, methods, and protocol binding is the service signature. Web Services discovery can be divided into two sub-classes: Design-time discovery and run-time discovery. The former is needed when designing a new service oriented system, whereas the latter is needed in a dynamic environment to identify which services currently are available.

In [16] we consider service discovery for a squad in the network-centric battlefield, i.e., a small MANET. We do not anticipate that new services and clients are implemented and deployed on-the-fly during an operation. Thus, we focus on run-time discovery in this paper, where we test both reactive and proactive discovery protocols. The above mentioned SAM and Mist are included in the evaluation, and perform better than the standards tested.

A.5.2.9 Integrating Wireless Sensor Networks in the NATO Network-Enabled Capability Using Web Services

Wireless Sensor Networks are expected to provide greatly enhanced situational awareness for war fighters in the battlefield. Sensors widespread in the battlefield are, however, of very limited value unless the sensors are reliable during the entire operation and the information produced is accessed in a timely manner. We focused on these issues by enabling wireless sensor networks as a capability in NNEC using Web Services. This work was presented to the IST-090 group during a meeting in Oslo in 2011. We demonstrated that Web Services are an enabling technology for information-sharing, facilitating presentation of sensed data and alarms to a battlefield management system. In addition, we could show the feasibility of using a Web Services approach as a query processing tool enabling multi-sensor fusion and data aggregation in the WSN

domain. The networking protocols can in this way inherently adjust data-aggregation and -processing criteria according to the requirements posed by external subscriber systems. In this way, energy efficiency, which is paramount in wireless sensor networks, is optimized without sacrificing the flexibility of Web Services. Our proposed methods were tested using practical experiments with TelosB sensing nodes. For further experiment details, see [67].

A.5.2.10 Cross-Layer Quality of Service-Based Admission Control for Web Services

Web Services are in widespread use today. In [68] we discuss Quality of Service (QoS) concepts which are not covered by existing Web Services standards, and focus on application level solutions that will be important building blocks in the future. Here, a QoS based admission control Mechanism is presented, which provides priority based access to the network, while at the same time avoiding overloading the limited network capacity that is available. We use cross-layer mechanisms to combine QoS mechanisms at the network layer with our Web Services admission control broker. The preliminary experiments we have performed with Web Services over emulated wireless links are discussed.

A.5.2.11 DSProxy

FFI has developed the Delay and disruption tolerant SOAP Proxy (DSProxy) [69], a proxy solution which transports SOAP messages across disadvantaged grids. This is made possible by employing different optimization techniques (e.g., compression) to reduce bandwidth needs. Furthermore, it provides delay tolerance meaning that COTS Web Services and clients can function across disadvantaged grids. The DSProxy is now a fully implemented prototype which has been tested multiple times, amongst others at IST-090's MCC 2011 demonstration.

A.5.2.12 AFRO

MCI has developed a concept for an edge proxy: the Adaptation Framework foR Web Services prOvision (AFRO). This mediation service offers different levels of QoS to Web Services, through performance monitoring and application of the context-aware service provision paradigm. This concept, though not demonstrated in IST-090 experiments, seems to be a promising approach as identified by Poland, and is discussed in detail in [Annex E].

A.6 IST-090 COLLABORATIVE DEMO AT THE MCC 2011

The NC3A, Poland, and Norway collaborated on a joint experiment and demo at the MCC 2011 in Amsterdam, the Netherlands. This effort is documented in [Annex D].

A.7 SUMMARY

There are some clear benefits to taking the "adapting Web Services approach" to using SOA in disadvantaged grids. Using Web Services eases integration with other systems, and allows using the same implementation of clients and services in the entire information infrastructure, thus reducing development and maintenance costs.

In order to employ Web Services technology in disadvantaged grids, it needs to be adapted in order to handle low bandwidth and frequent connection disruptions. By implementing the adaptations in proxies, we can gain this flexibility while retaining the SOA benefits such as loose coupling and interoperability.

We have identified three areas needing addressing:

1) Reduce the network traffic generated by Web Services;

2) Remove the dependency on end-to-end connections; and
3) Hide network heterogeneity.

In IST-090 we have addressed these issues both through national efforts and experiments, as well as through collaboration and the final IST-090 demonstration at the MCC 2011.

Annex B – DDS

This Annex provides a general introduction to DDS and related technologies. It provides an overall description of how to adapt to the technology of disadvantaged grids. The MCC experiments are elaborated in more detail in [Annex D].

DDS Demonstration at the Tactical Level

As already described in the results section, in this demonstration it was necessary to interoperate several legacy (already built) applications, from different vendors. These applications were not designed to share information with other applications, so it was necessary to design a mechanism that allowed information sharing. There were several commercial solutions that might have fulfilled the above requirements, but the IST-090 scenario had very specific requirements, such the capability to cope with low bandwidth (57.6 kbps) and with frequent loss of signal. These difficult requirements needed specific (software) solutions, which were not commercially available. So it was necessary to customize the available commercial middleware to make it work properly at the tactical level.

The innovation of the experiment consisted of the sharing of information among C2 legacy systems in a disadvantaged-grid scenario, which couldn't be done up until that point.

DDS stands for *Data Distribution Service for real time systems* [70] which is a standards-based middleware that shows promise for use in low capacity networks and could be considered as an alternative for Web Service implementation of SOA in tactical communications networks. It is dedicated for real – time systems and enables the distribution of data from many sources to many destinations at the same time. Moreover, it does not require the network to be over-provisioned since the data overhead is rather small. This is very important in operational scenarios, where mobile users act dynamically and need to exchange information quickly. They usually use mobile wireless networks with limited resources, such as, e.g. tactical networks.

This chapter briefly describes characteristics of DDS that make it interesting technology for SOA implementation in disadvantaged networks. It also provides information about two activities of IST 090 participants:

- The DDS demonstration that was organized by the Institute of Technology "La Marañosa" (ITM) in Madrid, Spain during one of the IST 090 regular meetings; and
- The prototype of WS-DDS Interface that enables to share information between the Web Service and DDS domains.

DDS was also used in the joint IST090 experiment that was demonstrated during the MCC 2011 conference in Amsterdam. Results of this experiment are presented in [Annex D].

B.1 DATA DISTRIBUTION SERVICE

The Data Distribution Service (DDS) is a middleware standard created by the Object Management Group (OMG) for integrating real-time systems. DDS promotes loose coupling between system components. It enables data distribution between many sources and many destinations using the publish-subscribe mode.

The DDS introduces a virtual Global Data Space, which allows applications to communicate with each other by reading and writing data objects. Data providers publish typed data, defined by a *topic* that consumers can subscribe to. The DDS enables an extensive control of QoS parameters such as priority, reliability, delivery deadlines, etc. that can be used to configure the service (see subchapter B.1.1).

The DDS is based on the Peer-to-Peer (P2P) architecture. Data flow in the DDS is illustrated in Figure B-1. A *data publisher* first creates a *topic*, which is an aggregation of a structured data type, a key list, and a specific QoS contract. Then, it may instantiate a *data writer*, used to actually publish data. On the receiver side, a domain participant uses the topic to create a *subscriber* and then employs a *data reader* for data reception from other domain participants. The DDS is responsible for handling failures (such as inaccessible data receiver).

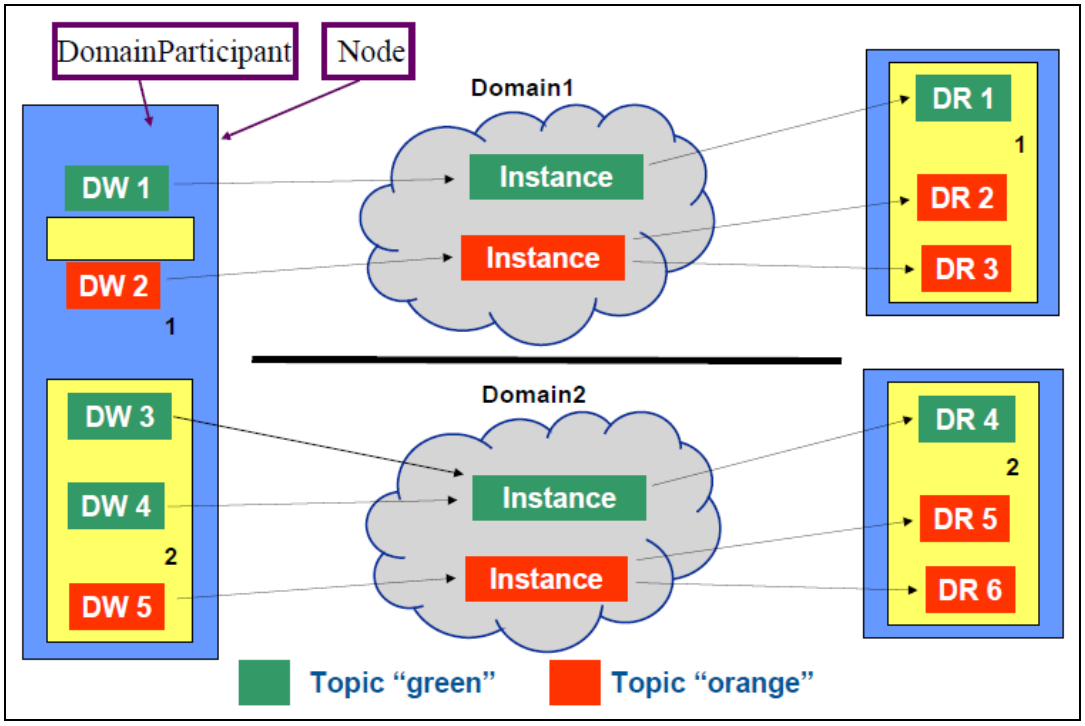

Figure B-1: DDS Data Flow (DW – Data Writer, DR –Data Reader).

The DDS specification describes two levels of interfaces:

- A lower Data-Centric Publish-Subscribe (DCPS) level that is targeted towards the efficient delivery of the proper information to the proper recipients.
- An optional higher Data Local Reconstruction Layer (DLRL) level, which allows for a simple integration of the Service into the application layer.

A separate specification, called the Real-Time Publish/Subscribe (RTPS) DDS interoperability wire protocol, defines the standard network protocol used to exchange data between publishers and subscribers that use different implementations of DDS. [71].

In result, communications among participants can be distributed:

- In space – participants can be located anywhere,
- In time – delivery of message can be in the moment of publication or later,
- In flow – QoS requirements can very precisely control the data flow,
- On many platforms – participants can have DDS data writers/readers implementations on different platforms, in different programming languages,
- Among many participants – there can be many readers and writers to particular topic.

Additionally, DDS provides a mechanism that allows for data filtering on the basis of topic contents. Specifically it enables to create requests using topics concatenation and SQL queries.

The DDS standard describes interfaces on the basis of PIM (Platform Independent Model), which allows for abstract API specification that can be further on mapped to many existing Platform Specific Models (PSM). This approach supports Model Driven Engineering that simplifies the process of software design.

Data Distribution Service has been standardized by the Object Management Group, the body that has coordinated work on Common Object Request Broker Architecture (CORBA), and, specifically, its Notification Service, which has also been designed as a publish-subscribe solution. Additionally, the Notification Service has multiple COTS implementations and many commercial deployments (see sub-chapter B.1.4).

B.1.1 DDS QoS Policy

In net-centric systems on tactical level, publishers and subscribers correspond to a range of domain participants such as embedded devices, Unmanned Air Vehicles (UAVs), soldiers' equipment, as well as planning and simulation services in operations centers. DDS applications use data writers to publish data values to the global data space of a domain and data readers to receive data.

The data-distribution service relies on the use of QoS (Quality of Service) to tailor the service to the application requirements (See Figure B-2 below). A QoS is actually a set of characteristics that drives a given behaviour of the service. It is made of individual QoS policies (objects of type deriving from *QoSPolicy*).

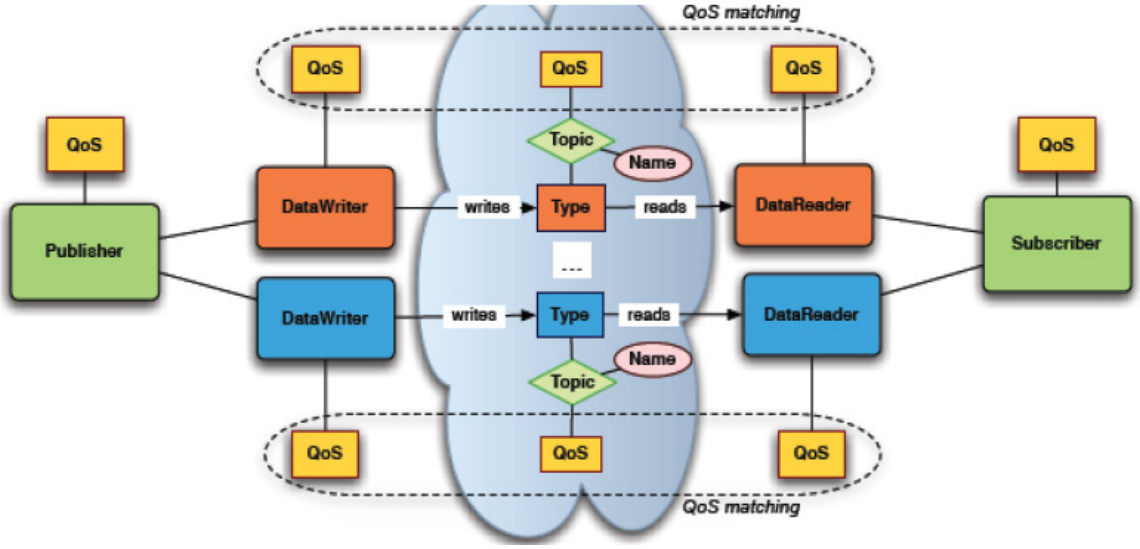

Figure B-2: QoS Support in DDS [72].

Publishers can declare their intent to produce data on particular topics with associated *QoSPolicy*, and they distribute the data on those topics to the global data space. Subscribers receive topic data in the global data space that match their subscriptions. QoS policies allow publishers and subscribers to define, first, their local behaviour, such as the number of historical data samples they require and the maximum update-rate at which they want to receive data, and, second, how data should be treated once in transit with respect to reliability, urgency, importance, and durability. Topics can also be annotated with these QoS policies to drive the behaviour of the data-distribution. The QoS policies of pre-defined topics serve as defaults for publishers and subscribers and can therefore ensure consistency between requested and offered QoS.

A *QoSPolicy* can be set on all DCPSEntity objects. In many cases, for communications to occur properly, a *QoSPolicy* on the publisher side must be compatible with a corresponding policy on the subscriber side. For example, if a Subscriber requests to receive data reliably while the corresponding Publisher defines a best-effort policy, communication will not happen as requested. To address this issue and maintain the desirable decoupling of publication and subscription as much as possible, the specification for *QoSPolicy* follows the subscriber-requested, publisher-offered pattern. In this pattern, the subscriber side can specify an ordered list of "requested" values for a particular *QoSPolicy* in decreasing order of preference. The Publisher side then specifies a set of "offered" values for that *QoSPolicy*. The DDS middleware will then select the most-preferred value requested by the subscriber side that is offered by the publisher side, or may reject the establishment of communications between the two DCPSEntity objects if the QoS requested and offered cannot be resolved.

The following Table B-1 lists the supported *QoSPolicy* options.

Table B-1: The Key QoS Policies [72], T – Topic, DR- Data Reader, DW – Data Writer.

QoS Policy	Applicability	RxO	Modifiable	
DURABILITY	T, DR, DW	Y	N	Data Availability
DURABILITY SERVICE	T, DW	N	N	
LIFESPAN	T, DW	-	Y	
HISTORY	T, DR, DW	N	N	
PRESENTATION	P, S	Y	N	Data Delivery
RELIABILITY	T, DR, DW	Y	N	
PARTITION	P, S	N	Y	
DESTINATION ORDER	T, DR, DW	Y	N	
OWNERSHIP	T, DR, DW	Y	N	
OWNERSHIP STRENGTH	DW	-	Y	
DEADLINE	T, DR, DW	Y	Y	Data Timeliness
LATENCY BUDGET	T, DR, DW	Y	Y	
TRANSPORT PRIORITY	T, DW	-	Y	
TIME BASED FILTER	DR	-	Y	Resources
RESOURCE LIMITS	T, DR, DW	N	N	
USER_DATA	DP, DR, DW	N	Y	Configuration
TOPIC_DATA	T	N	Y	
GROUP_DATA	P, S	N	Y	

The *QosPolicy* objects that need to be set in a compatible manner between the publisher and subscriber ends are indicated by the setting of the 'RxO' (Requested/Offered) property:

- An 'RxO' setting of "Yes" indicates that the policy can be set both at the publishing and subscribing ends and the values must be set in a compatible manner. In this case the compatible values are explicitly defined.
- An 'RxO' setting of "No" indicates that the policy can be set both at the publishing and subscribing ends but the two settings are independent. That is, all combinations of values are compatible.
- An 'RxO' setting of "-" indicates that the policy can only be specified at either the publishing or the subscribing end, but not at both ends. So compatibility does not apply.

The 'modifiable' property determines whether the *QosPolicy* can be changed after the *Entity* is enabled. In other words, a policy with 'changeable' setting of 'NO' is considered "immutable" and can only be specified either at *Entity* creation time or else prior to calling the *enable* operation on the *Entity*.

B.1.2 DDS Compliance Profiles

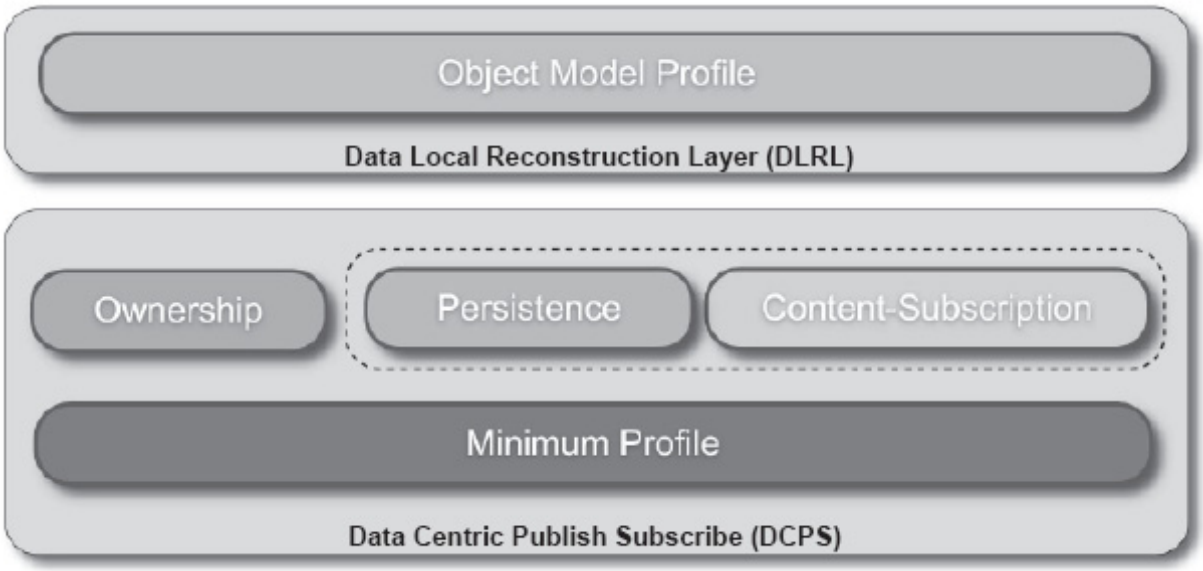

Figure B-3: DDS Compliance Profiles [72].

The DDS specification includes the following profiles, which define level of compliance with the standard.

- Minimum profile: This profile contains just the mandatory features of the DCPS layer. None of the optional features are included.
- Content-subscription profile: This profile adds the optional classes: ContentFilteredTopic, QueryCondition, MultiTopic. This profile enables subscriptions by content.
- Persistence profile: This profile adds the optional QoS policy DURABILITY_SERVICE as well as the optional settings 'TRANSIENT' and 'PERSISTENT' of the DURABILITY QoS policy kind. This profile enables saving data into either TRANSIENT memory or permanent storage so that it can survive the lifecycle of the DataWriter and system outings.
- Ownership profile: This profile adds:
  - The optional setting 'EXCLUSIVE' of the OWNERSHIP kind;
  - Support for the optional OWNERSHIP_STRENGTH policy; and
  - The ability to set a depth > 1 for the HISTORY QoS policy.
- Object model profile: This profile includes the DLRL and also includes support for the PRESENTATION access_scope setting of 'GROUP'.

B.1.3 Web Services and DDS Comparison

In order to understand the DDS characteristic features and the approach of SOA implementation using these standards, it is important to demonstrate how it relates to the most often used implementation of SOA systems: Web Services.

Web Service is a software component independent from the platform and the implementation, delivering definite functionality (-ies) through a unique, well described in a machine-processable format and easily accessible interface. The interface is described using Web Services Description Language (WSDL). Other systems interact with the Web Service according to its description using the SOAP protocol.

Web Services are built based on the client - server architecture, mainly in two message exchange patterns (MEPs) – request – response and publish - subscribe (see Figure B-4). In the first case service consumer (so called client stub) sends to the well-known address (so called endpoint) a request message and receives a response message. The major and largest disadvantage of this architecture is the lack of service accessibility when the application server is damaged, switched off or when some problems with the network connection have appeared.

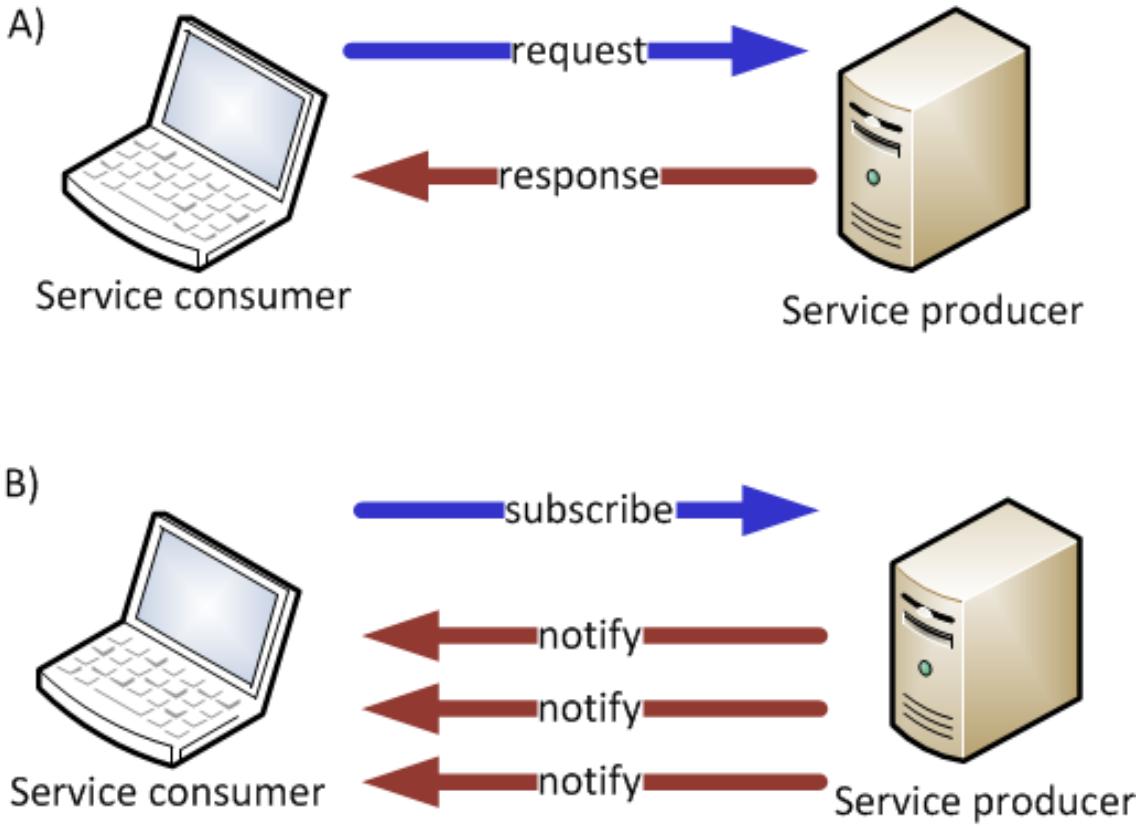

Figure B-4: Client-Server Architecture. WS Message Exchange Patterns.
A) Request – Response; B) Publish/Subscribe.

In the second MEP user subscribes to messages on specific interface and the messages are returned to him as notifications. In both cases service consumer exchanges messages with the service producer (which can be also notification broker).

Data Distribution Service for Real-time Systems (DDS) [73] is the first open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems. It is built based on the Peer-to-Peer (P2P) architecture (see Figure B-5). DDS is asynchronous. It enables publishing of data in so called *Topics*. Data defined by Topics is sent in one direction from Publishers to Subscribers. The main advantage of this architecture is loose coupling between DDS elements. If one of the participants publishing data is inaccessible, the DDS service is still accessible. Subscribers can receive data on the same topic from different publishers.

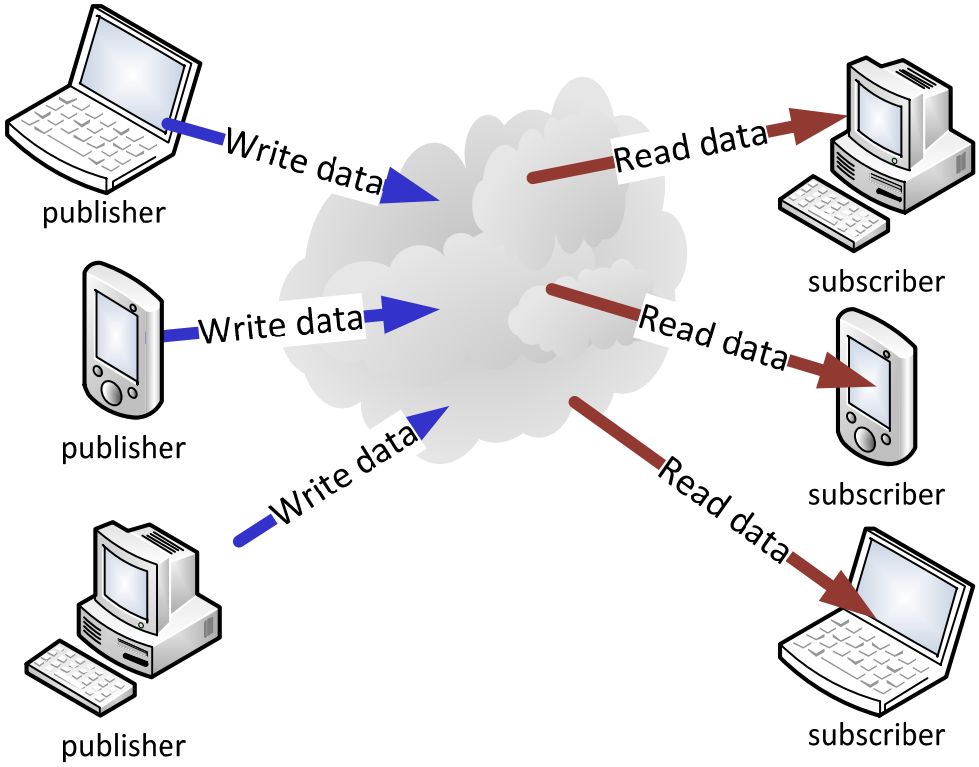

Figure B-5: P2P Architecture.

The WS – DDS comparison is shown in Table B-2. Significant difference between DDS and Web Service is the possibility of creating, by the DDS application, Client subscriber object to the topic that have not started publishing yet. It is very important when the dynamics of an action in the battlefield is high. When one of the battle participants begins publishing data, the DDS Global Space subscribers will receive it immediately. Web Service technology does not enable creation of a client stub for receiving SOAP messages when the Web Service provider does not make the WSDL description accessible.

Table B-2: WS and DDS Comparison.

Feature	Web Service	DDS
Architectural elements	- Provider, - Requester, - Broker (optional).	- Publisher, - Subscriber.
Architecture	Client-Server	P2P
Message Exchange Patterns	Request-Response Publish-Subscribe	Publish-Subscribe
Data flow	Remote method calls	One-way messages
Data model	SOAP Message	Data-Object
Data description	WSDL description	Topic description
QoS	------	QoS Policy
Use cases	Best for: - Configuration, - File transfer, - None-real-time systems, - Soft-real-time systems, - Synchronous transactions, - Sporadic request-response, - Military networks – strategic / operational level.	Best for: - Hi-performance one-to-many, - Dynamic, unreliable transports, - Hard-real-time systems, - Extreme-real-time systems, - Flexible delivery requirements, - Events, High performance messaging - Military tactical network.

Web Services are the most often used means of service oriented architecture (SOA) realization. WS related standards are being quickly applied in software development tools (also in the open source) which bring great benefit for the software developers. They are also being extended by additional recommendations and standards (thanks to OASIS and W3C organizations) which result in fast enhancement of their functionality. They are very often used in modern military command and control systems on high command levels to distribute information among different subsystems and users. They are also applied by the civil units that need easy and quickly implementable solutions.

However, WS application in standard implementations (with no adaptation – see chapter 4) on low command levels, where mobile operators act in a dynamic environment usually utilizing wireless devices is limited. In this environment DDS gives satisfactory results allowing the exchange of information among mission participants in real time.

B.1.4 OMG DDS Implementations Comparison

The DDS has a number of significant commercial deployments in military, communications, financial and public sectors (listed on vendors' websites). DDS standard has been implemented by at least three companies that made it available for customers, namely:

- Twin Oak – CoreDX DDS,
- RTI – RTI DDS, DDS,
- PrismTech - OpenSplice DDS.

Recently, a communication protocol has been standardized [74] and interoperability between leading vendors has been demonstrated. [74].

The comparison of the three aforementioned implementations is shown in Table B-3. These implementations are compliant with DDS version 1.2. They have different additional features (e.g. interfaces to databases and other software integration support) and Operating Systems support (although each of them supports the most popular OSs – Windows and Linux). However, the only open source version is offered by the Prism Tech as the DDS OpenSplice Community Edition under the LGPL Commercial license. The other two companies offer 30-days trial versions for researches and tests.

Table B-3: DDS Implementations Comparison.

Implementation DDS / Parameters	CoreDX DDS	RTI DDS	OpenSplice DDS
STANDARD INTERFACES, LANGUAGES SUPPORT	C C++ Java	C, C++, C# Java, Ada RTPS wire protocol JMS WSDL/SOAP REST SQL Lightweight CORBA Component Model (CCM) Sockets Custom via adapter interface	C/C++ C# Java Real-Time Specification for Java SOAP-Connector DBMS-Connector
OMG DDS COMPLIANCE	OMG DDS v1.2 specification, including the Data Centric Publish/ Subscribe(DCPD) and the Data Local Reconstruction Layer (DLRL) profiles. Wire Protocol (RTPS) 2.1	DDS API 1.2 – Minimum profile – Persistence profile – Ownership profile ContentFilteredTopic & QueryCondition DDS Interoperability Wire Protocol (RTPS) 2.1 Web-enabled DDS (draft) Extensible and Dynamic Topic Types (draft)	OMG DDS v1.2 specification, including the Data Centric Publish/ Subscribe(DCPD) and the Data Local Reconstruction Layer (DLRL) profiles. Wire Protocol (RTPS) 2.1
Tools	CoreDX DDS Spy CoreDX DDS Multiplexor CoreDX DDS Centralized Discovery	Relational databases Microsoft Excel Complex Event Processing (CEP) engines Visualization platforms Application Servers and ESBs	Relational databases MDE PowerTools Tuner DDS TouchStone
PLATFORMS INTEGRITY	Linux 2.6 Windows Solaris 10 LynxOS-SE QNX 6.4 VxWorks 5.5 VxWorks 6.6 NexusWare Android	INTEGRITY, Linux, SELinux and Embedded Linux LynxOS and LynxOS-SE Mac OS X QNX Unix – AIX and Solaris VxWorks , VxWorks 653 and VxWorks MILS Windows and Windows CE/Mobile	AIX Linux Solaris Windows INTEGRITY VxWorks
PROCESSOR FAMILIES	x86 (32bit, 64bit) i686pc sun4u ARM v5 ARM v7 MIPS PPC	x86 (32bit, 64bit) ARM PowerPC / Cell SPARC	x86 (32bit, 64bit) SPARC
LICENSING	Commercial	Commercial	LGPL Commercial

B.1.5 DDS for Real-Time Systems

It is interesting to notice the DDS application for various time requirements. In Figure B-6 one can see that DDS covers the whole spectrum of time requirements: from near – real time to extreme real time. It is the main technology taken into account for integration of real-time systems and especially promising for integration of systems with different time requirements. For comparison, Web Services, the other important SOA technology offers messages delivery in near real time and soft-real time, assuming that the transmission in provided through the fast transmissions media (like Ethernet).

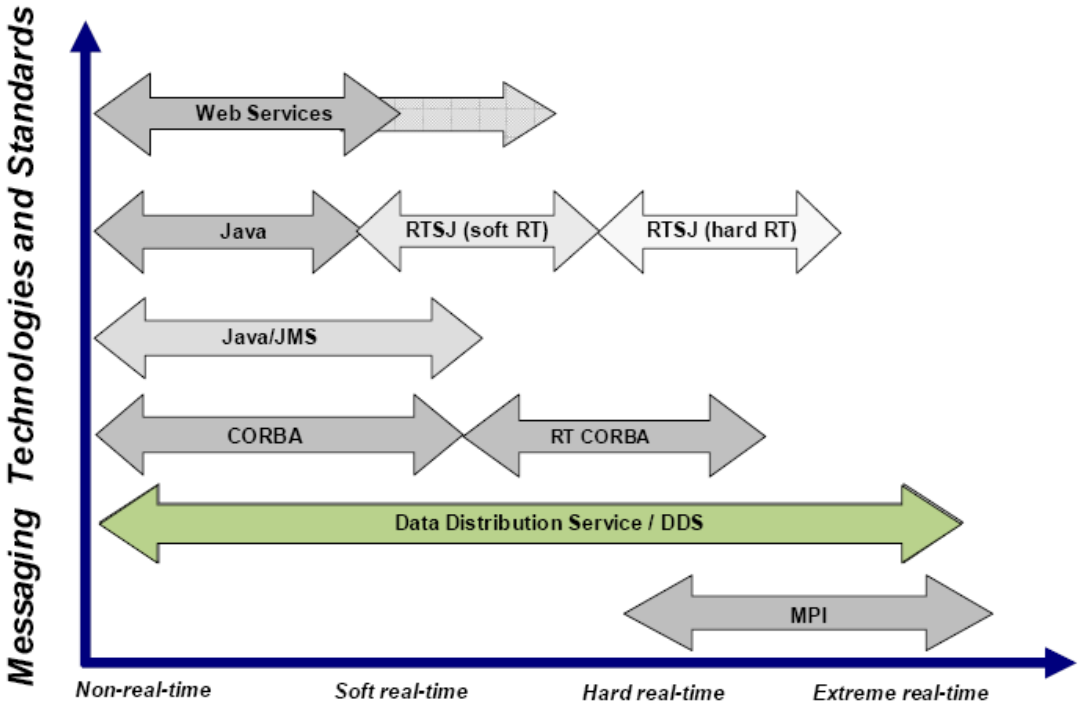

Figure B-6: Messaging Oriented Technologies and Standards in Time Requirements [75].

B.2 DDS DEMONSTRATION AT THE TACTICAL LEVEL

During October 2010 a NATO IST-090 meeting took place at the Institute of Technology "La Marañosa" (ITM) in Madrid, Spain. At this meeting a Technology Demonstration was set up to demonstrate the capability of DDS middleware (Data Distribution Service) as integrator of different legacy systems in the context of military operations.

In this demonstration it was necessary to interoperate several legacy (already built) applications, from different vendors. These applications were not designed to share information with other applications, so it was necessary to design a mechanism that allowed information sharing. There were several commercial solutions that might have fulfilled the above requirements, but the IST-090 scenario had very specific requirements, such the capability to cope with low bandwidth (57.6 kbps) and with frequent loss of signal. These difficult requirements needed specific (software) solutions, which were not commercially available. So it was necessary to customize the available commercial middleware to make it work properly at the tactical level.

The innovation of the experiment consisted of the sharing of information among C2 legacy systems in a disadvantaged-grid scenario, which couldn't be done up until that point.

B.2.1 Introduction

The key concept of the demonstration was to test the interoperability among several different real legacy systems, just to test that these legacy systems can actually exchange information.

The initial aim was to run the demo in a real tactical network using PR4G v3 radios. This wasn't possible during the demonstration, because this kind of radio has crypto hardware and the facilities of ITM were unable to manage the crypto keys. The required facilities at the needed classification level were not available.

So it was used a regular LAN for communicating the systems and there were not considered issues such as low network bandwidth, loss of connectivity, etcetera. Implementation of real radios for networking was too complex, and simulation of disadvantaged grids using a tool was too difficult.

The core of the demonstration was a set of DDS services designed by the Spanish Army. These DDS services (Unit Information, Tactical Messaging, File Distribution and Video Distribution) are currently being implemented in real systems and several Spanish companies were invited to participate in developing and testing in a joint environment to recreate a tactical scenario using those services in its existing systems.

A Web Service was implemented in parallel to the DDS services and a gateway between the DDS services and the Web Service was implemented. This gateway could transform information from the Unit Information Service (DDS data model) to the COP's (Common Operational Picture) Web Service data model.

IGECIS is the Spanish MoD organism responsible of the Web Service and INTEGRA, a tool developed at the ITM, was able to make such transformations.

A relatively easy and simple, but realistic, scenario was designed and used. The scenario encompasses an attack that consists of two enemy units which land on the beach of the Naval Base of Rota, carrying out manoeuvres of approaching and attack on the airport. The manoeuvres are resisted by both ground units and air support.

B.2.2 Demonstration

B.2.2.1 Scenario

IST-090 uses a generic scenario for its context (see Chapter 2). But for the demonstration, that generic scenario was mapped into a more detail specific scenario (Figure B-7):

- Set: Rota, Cádiz (Spain).
- Defending an enemy disembarkation.
- Roles:
  - Link-16: Generating naval enemy troops.
  - COSMOS: Radar Simulator: Detect troops disembarking.
  - HALO detects the explosion at the airport.
  - JCISAT and NEON troops will get to the airport to eliminate the enemy ones.
  - Link-16: Air units from the Naval Base.

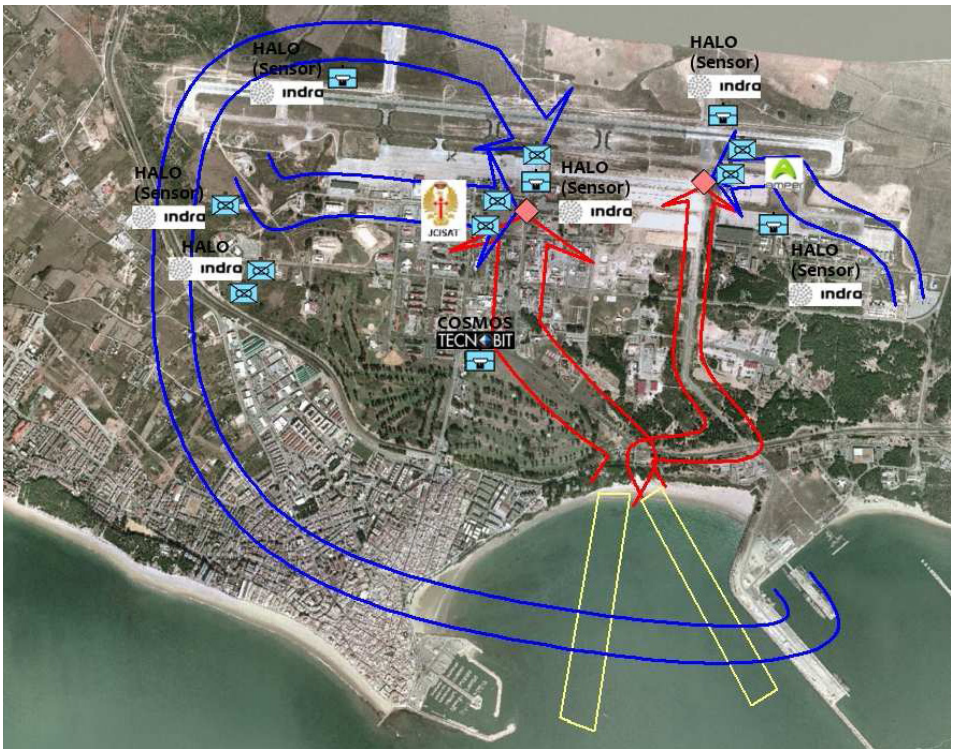

Figure B-7: Specific Scenario.

B.2.2.2 Executed Script

The COSMOS system, after detecting enemy units with its radar, reports the landing to the HALO, a system that is also part of the tactical network. The HALO system alerts the explosions made by the enemy to the rest of the participants in the DDS network system. As response to this alarm, ground units, using both systems BFT (Blue Force Tracking) and ESP DDS Evaluation Platform, report their positions and LINPRO reports the position of the air unit. All of this positioning information is presented at the web system COP of the IGECIS through the gateway INTEGRA.

B.2.2.3 Implemented Services

The Spanish Army has created, for internal purposes, an interface for sharing information named Tactical Data Interface. This Tactical Data Interface is a definition of what information has to be share among units in the battle field and how that information is going to be transmitted. It defines:

- Services to be implemented.
- Data to be transmitted, specifying the information model of each service.
- DDS as the information distribution paradigm.

For the demonstration it was decided to use some of the services described in this tactical interface. These services were: Unit information service, Tactical Messaging Service, File Distribution Service and Video Distribution Service. Systems involving in the demo had to implement these 4 services at least.

B.2.2.4 QoS

The QoS settings for the demonstration were the default QoS settings of the RTI DDS implementation. They are described in the *RTI Data Distribution Service* documentation.

Due to the use of a regular LAN, it was known that the discovery performance and available bandwidth was going to be excellent. So, in this case, it was not needed to change any QoS setting.

If some kind of radio or some kind of simulation software could be used to implement a disadvantaged grid, QoS should be tuned for getting good discovery performance. ESP company eProsima, as national distributor of RTI in Spain, has worked with ESP Army in several ESP systems to get the appropriate QoS settings.

A summary of the results of eProsima work with PR4G radios is:

- Low Discovery times:
  - Grid: 6 nodes, 4800 bps shared bandwidth.
  - Result: Less than 20 seconds.
- Good use of available bandwidth:
  - Grid: 6 nodes, 4800 bps shared bandwidth.
  - Transmitting JC3 positions (200 bytes).
  - Result: An update from every node every 10 seconds (or less).
- A lot faster than previous middleware for the PR4G Radios.

B.2.2.5 Participants and Products

The participating companies with the systems that they brought to the demo are listed in Table B-4 below.

Table B-4: Components of the DDS Demo.

Company	Product	Description
AMPER	NE.ON family (network enabled.on) BFT	A BFT system using the JCISAT interface.
Spanish Army JCISAT	DDS service that provides BFT	An implementation of BFT using the JCISAT interface.
INDRA	HALO (Hostile Artillery LOcating)	Radar sensor to detect enemy explosions
TECNOBIT	LINPRO (Data LINk PROcessor)	Link 16: BFT for air units
TECNOBIT	COSMOS (COmprehensive Surveillance MObile System)	BFT for ground units
TECNOBIT	Optronic camera	For video transmission
EPROSIMA	National Distributor of RTI	
NEC Unit of ITM	INTEGRA	Gateway DDS - WS
Spanish Army IGECIS	COP	Common Operational Picture
University of Granada	Video transmission by DDS	

B.2.2.6 Communications Environment

The Communications Environment intended to use included the following radios:

- PR4G v3 Radios,
- IPSAP mode. 6 Kb/s,
- 1 grid. 7 nodes.

It was the intention to actually use the radio communications environment as described above but that, due the radio crypto implementation problems, a regular LAN was used instead.

B.2.3 Conclusions

Although PR4G radios were not used, the primary goals were successfully accomplished. The exercise showed that legacy C2 systems can share information using a common service oriented middleware (DDS in this case) at a tactical level.

ESP army promoted the definition of a common interface data at a tactical level. Systems implemented this interface and the communication was set with no problems. Now, we know how to define a common interface data and if this could be a solution to the interoperability problem of many systems in the army.

Moreover, for the IST – 090 group was provided a disadvantaged scenario to test other solutions (Web Services, etcetera).

B.3 WS-DDS INTERFACE

Work devoted to application of DDS in tactical networks carried out by MCI concluded with a statement that DDS can be efficient middleware technology that offers interesting functionality to mobile units on the field. Web Services are also efficient technology for information distribution in military networks. The specifics of these two technical (WS and DDS) domains hinder their interoperability. DDS defines a specific API for the messages and subscription handling but cannot natively interoperate with SOAP Web Services. In order to exchange information it is necessary to provide a special interface that would enable connection of these domains, without limiting their independence and functionality. Therefore MCI started researches on development of proof of concept WS-DDS interface.

WS-DDS Interface has been designed and implemented to solve this problem. It enables exchange of information between two technologically different domains – DDS domain and WS domain.

The WS-DDS dedicated interface proof of concept is the application that enables transformation of XML data (NFFI SOAP messages) from the Web Service domain to the data format sent in the DDS system. The opposite direction requires transformation of the DDS data format to SOAP messages sent in the Web Services domain. Apart from data transformation, it provides architectural and protocol transformations.

For the purpose of the proof of concept both sides (Web Service domain and DDS domain) send NNFI messages (NATO Friendly Forces Information) according to the STANAG 5527.

WS-DDS has a Web Service interface that enables calling web methods providing appropriate functions. This is a front-end to the proxy functionality that connects the Web Service application (run on the GlassFish application server) with the OpenSplice DDS middleware. WS-DDS Interface enables the following operations:

- Authorization operations:
  - Login – login to WS-DDS Interface,

    - Logout – logout form WS-DDS Interface,
- Functional operations:
    - createTopic – creates object Topic of DDS system,
    - getTopics – lists accessible Topics from the WS-DDS Topic repository,
    - createPublisher – creates Publisher object in DDS domain,
    - createSubscriber – creates Subscriber object in the DDS domain,
    - writeData – publishes data in DDS,
    - readData – reads data from DDS (pull mode).

The WS-DDS Interface Architecture has been depicted in Figure B-8 below.

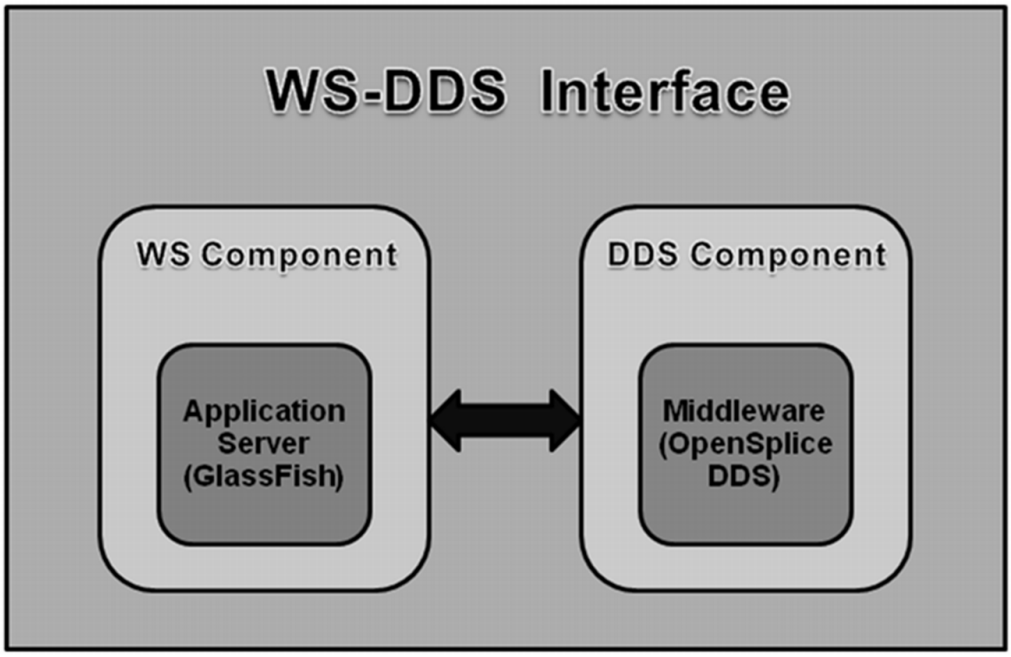

Figure B-8: WS-DDS Interface Architecture.

The WS-DDS interface requires that the architecture of the DDS domain is mapped to the WS domain and vice versa. For this purpose the WS-DDS interface executes the following tasks:

- It translates SOAP messages into DDS data objects (WS→DDS communications) and DDS data objects into SOAP messages (DDS→WS communications),
- It processes WSDL descriptions (the NFFI service in case of the proof of concept) and creates Topic data description (when the user calls createTopic operation). Additionally, it enables setting QoS parameters for the data to be sent,
- It creates registry of Topics that were created by the WS-DDS users. The list of Topics is then available for other users by the getTopics operation. This reflects the registry (or the service discovery functionality) that exists in the WS domain.

Due to the fact that the OMG is currently working on the security extensions for the DDS, the security aspects have not been analysed.

The WS-DDS interface has been tested against performance of processing user requests and connecting WS and DDS domains [21]. The tests were mainly focused on the efficiency of the WS-DDS implementation meaning the time that the appropriate transformations from the WS domain to the DDS domain were performed.

Interoperability tests of WS-DDS were performed during the MCC 2011 conference in the joint IST 090 experiment. The results of the tests are presented in [Annex D].

B.4 SUMMARY

The DDS standard is an interesting messaging middleware that can be used to share information in military systems used at the tactical level. It is language and platform neutral, offers several enhanced capabilities with respect to data filtering and transformation, (near) real-time delivery effort and Quality of Service.

Interoperability of different vendors DDS implementations, even though demonstrated by the companies in [76] should be subject to further investigation, especially in terms of QoS Profiles interoperability and vendor – specific enhancements.

The DDS demonstration that was performed in ITM, Spain shows true possibilities of this technology that was used as main middleware for information distribution in C4I systems taking part in the demo, including delivery of reports, incidents, unit positions and video. Moreover, what is worth mentioning Spain has defined their Tactical Data Interface on the basis of DDS.

During the IST 090 activity there has been also tested WS-DDS interface, which implements a SOAP Web Service interface on the top of the DDS API so that a standard SOAP data consumer/producer can directly use this interface. The experiment with the WS-DDS interface was very successful and NC3A is keen to build upon the knowledge gained with this prototype.

Annex C – INTERIM MIDDLEWARE

The objective of Task Group IST-090 "SOA Challenges for Disadvantaged Grids" is to identify solutions for making SOA applicable at the tactical level. Besides efficient mechanisms for service discovery and for reducing the overhead of Web service communication as discussed in chapter 4, an efficient transportation of the messages between a service consumer and a service provider, is essential. Thus, a middleware allowing for an adaptation of the applications' communication behavior to the special needs of tactical networks could provide a basis for implementing a SOA infrastructure at the tactical level. As an example, DDS described in chapter 5 already provides many useful middleware features to be used in tactical network environments. However, it sees the network only as a transparent communication service. We argue that additionally, a better coordination between Command and Control Information Systems (C2IS) applications and network protocol layers is useful.

In this chapter, we describe an approach of the German Fraunhofer FKIE to a middleware concept that allows for the coordination of C2IS applications and network protocol layers by using a cross-layer approach [77], [78]. Besides passing down the applications' communication and QoS requirements, an extended approach is followed that also provides the applications with well-adjusted information about the network environment. This can be used by the applications to adapt their functionality according to the available communication resources. Furthermore, the middleware is informed about application knowledge (e.g. mission information about the planned movement of troops). It enables the middleware to account for this additional information when configuring the network layers. In the following we present a middleware design that comprises these functionalities and discuss its main interfaces and components.

C.1 INTRODUCTION

A major goal regarding future C2IS is to provide ubiquitous access to all mission-relevant information in a timely manner. A crucial aspect will be the full integration of the tactical level and its communication technologies. Currently, mobile units deployed on the tactical level are often connected by low-speed legacy VHF radio equipment. Therefore, to alleviate the problem of scarce communication resources, efficient utilization is essential. However, many of today's C2IS were built originally for Ethernet-like communication networks, e.g., located inside command posts, ignoring the additional challenges of wireless communication systems operating in high-interference environments at low data rates at the tactical level.

To fill the gap between C2IS built for high-speed LANs and tactical networks based on narrow-band radio links, a middleware for military heterogeneous networks is needed, which mediates between C2IS and the underlying military network technologies [79].

Such a middleware should be aware of the communication requirements of military applications (blue force tracking, military message handling, Voice over IP (VoIP), etc.) and utilize the network in a conscious way to increase the overall user experience. One should keep in mind that different military applications have different requirements regarding the network service. For instance, VoIP applications highly depend on low delay and jitter, whereas military message handling systems benefit mainly from a high average data rate. To prioritize the different data streams of C2IS applications, the middleware should assess the relevance of these data streams in relation to the current mission state and tag the data dynamically. The network may then put this prioritization of the different data streams into effect.

Additionally, the middleware should be aware of the current network conditions and enable the adaptation of C2IS applications to the current communication resources. For this purpose, the middleware should provide the applications with information about the current network conditions (available communication resources, data rates, etc.). By doing so, it should shield C2IS from the details of the communications services and provide information in a technology-independent manner.

In this chapter we present first steps towards a middleware for military network environments. The middleware can be seen as a mediator between C2IS and the tactical network infrastructure. To this end, a high-level, cross-layer design has been developed featuring a direct exchange of status information between C2IS and lower network protocol layers. In the design, the middleware supports the adaption of C2IS functionality according to the deployed network technologies and their currently available communication resources. At the same time, the middleware enables the configuration of the network protocol layers, reflecting the current military objectives and the communication requirements of C2IS.

To show the benefit of such a cross-layer approach even for current C2IS and communication systems, we describe three approaches for interim solutions for improving the coordination of C2IS and communication systems. These approaches may be used even without modifications of the original systems.

C.2 MIDDLEWARE DESIGN

A high-level overview of our cross-layer design of a middleware and supporting components for military networks is shown in Figure C-1 [80]. Two new convergence layers complementing the existing network layers of the ISO/OSI protocol stack are introduced (Transport Convergence and Technology Convergence in Figure C-1).

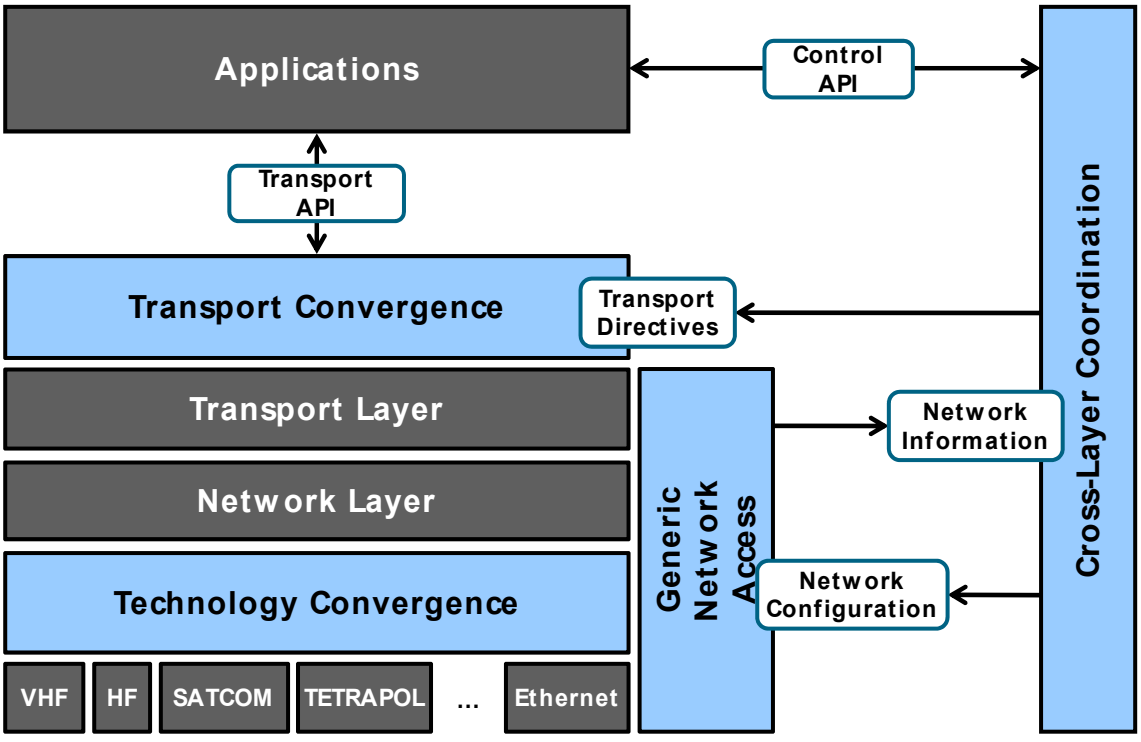

Figure C-1: Cross-Layer Design (High-Level View) of a Middleware for Military Networks.

Purpose of the technology convergence layer is to unify the access to different communication technologies. In order to utilize the QoS potential of the different communication technologies, the technology convergence layer should select and configure the different technologies according to the user/application requirements. To be able to realize an automatic mapping between user/application requirements and the QoS mechanisms of the communication technologies, a unified QoS model for the middleware is needed. The application requirements are then mapped to the unified QoS model which is itself mapped to the capabilities of the different technologies.

The role of the transport convergence layer is to choose the right transport protocol to cope with specific channel properties. It should offer transparent proxy services to change the transport protocol and to split sessions, e.g. to use tailored transport protocols and congestion control mechanisms in different sections of the communication path. Cross-Layer Coordination (see below) may provide the transport convergence layer with QoS requirements of the applications by using the Transport Directives interface (Figure C-1). This enables the transport convergence layer to choose the right transport protocol according to the communication needs of the applications.

Additionally, to realize the above-mentioned exchange of status information between C2IS and lower network protocol layers, a new cross-layer component (Cross-Layer Coordination in Figure C-1) coordinates the exchange of status information and provides mechanisms for adapting the application and network behavior. The network stack is accessed by Cross-Layer Coordination via technology-independent interfaces (Network Information and Network Configuration in Figure C-1) of the Generic Network Access component. This allows shielding Cross-Layer Coordination from technical details of the different network technologies.

A major purpose of the middleware is to provide mechanisms to adapt the application behavior to the currently available communication resources. To access these new mechanisms (services), our design incorporates new interfaces between C2IS applications and the middleware (Transport API and Control API in Figure C-1). In the long-term this will stimulate the further development of C2IS applications which are deployed on the tactical level towards network-sensitive applications. In the following, we will describe the requirements for the different interfaces (Control API, Network Information and Network Configuration) in more detail and thereby describe some functional responsibilities of Cross-Layer Coordination.

C.2.1 Control API

The Control API is used for the coordination of applications and the middleware. There are four constituent parts of this interface. These sub interfaces of the Control API are shown in Figure C-2 and will be described in the following.

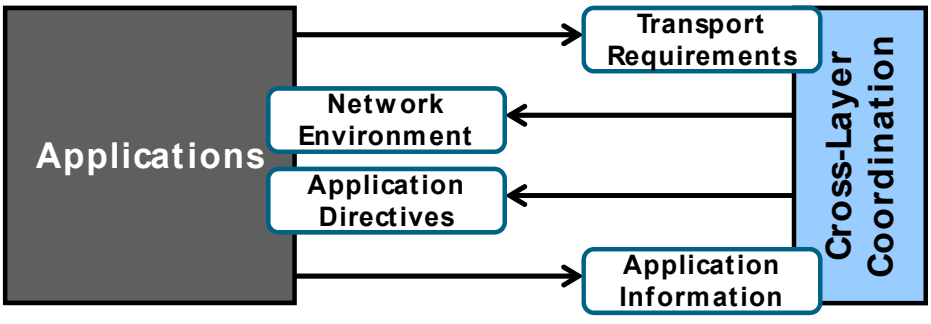

Figure C-2: Sub Interfaces of the Control API Used to Coordinate C2IS Applications and Middleware.

As part of the API, applications should be able to specify their communication requirements (Transport Requirements in Figure C-2) to allow for optimizations by the middleware. For example, if strict delay constraints are specified by the application, this information can be used by the middleware to discard messages which are obsolete from message queues. There are several ways in formulating the communication needs of applications. For example, in [81] the authors suggest the use of a specific language (called CAPRI) to specify the utility for an application as a function of measurable attributes of the connection (e.g. throughput, delay, packet loss rate, bit error rate and jitter). This allows an application to specify its QoS requirements and thus enables utility-based optimizations by the middleware.

As a further part of the application interface, the Cross-Layer Coordination provides the applications with information about the current network state (Network Environment in Figure C-2). This information enables applications to dynamically adapt their functionality according to the current network state. However, it should not be assumed that all applications have to be fully aware of the network. Instead, different levels of abstractions should be supported. While some applications can benefit from detailed information about the abstract structure and the state of the network, other applications might only be interested in information about the end-to-end connectivity. In general, the information about the network environment should be designed to be independent of the network technologies in use, since applications should not be concerned with technical details. Furthermore, this information has to generalize from the fluctuating network state by using an appropriate statistical description (e.g. including the variance), since applications usually operate in larger time scales than communication layers.

As an additional part of the application interface, the middleware should be enabled to provide applications with directives concerning the use of communication resources (Application Directives in Figure C-2) before applying a strict admission control. This cooperative way would enable the middleware to assign different amounts of communication resources to the different applications if the network utilization changes.

Finally, the application interface should enable the applications to provide the middleware with application knowledge (Application Information in Figure C-2). Consider, for example, mission information like the planned relocation of military units or the change of the mission state of units (e.g. on the move, engaging, etc.). If such application knowledge is made available to the middleware, this information can be used by the middleware to configure the network according to the prospective situation in advance. Knowledge about the current and commanded location and movements of tactical units might also be beneficial for delay/disruption tolerant networking [82] for predicted or scheduled contacts [83]. To the best of our knowledge, the use of application knowledge in the middleware is a new functionality which has not been considered in other approaches so far.

C.2.2 Generic Network Access

The Generic Network Access component is used by the Cross-Layer Coordination to get a technology independent description of the current network state. Furthermore, the Cross-Layer Coordination can use this component to configure the network stack. We will describe these two aspects of the Generic Network Access component in the following.

The Network Information (see Figure C-1) should contain a description of both static and dynamic network properties. To get a basic technology independent model of the local network behavior it is crucial to have at least a coarse classification of the physical and link layers. Starting with the channel directionality (simplex, half duplex or full duplex) and the communication pattern, the Medium Access Control (MAC) mechanism plays an important role. The MAC mechanism strongly influences the tolerance of the local network to an increasing number of stations and to an increasing traffic load. In addition, the MAC mechanism also determines the capabilities to prioritize traffic of different units on the same communication channel. Regarding the dynamic network properties, there are some technology-spanning parameters that can be observed. Decisive factors for the delay of a communication channel are the signal propagation delay, the effective data rate and the distribution of medium access times. They have direct influence on the data rate, the delay, the jitter, and the channel reliability. The effective data rate can either be predicted by monitoring the Signal-to-Noise plus Interference Ratio (SNIR) or determined by monitoring the data sent on the channel. Here, the frame size plays an important role for an effective channel usage. Random Access-based link layers often provide channel load statistics. Note, that it is crucial that applications on higher tactical levels directly connected to high-speed network technologies do not overload remote tactical links. End-to-end probing can be used to assess the communication channel capacity of the link with the least capacity on a network path down to the tactical units. In addition, information about the local network state in the tactical level can be propagated to higher levels proactively if enough bandwidth is available.

Besides providing network information, the Generic Network Access should enable the Cross-Layer Coordination to configure the network according to the application requirements. This is done by setting values of network parameters via the Network Configuration interface (Network Configuration in Figure C-1). One should keep in mind that these parameters have to be technology-independent, since the Cross-Layer Coordination is assumed to be technology-agnostic. For example, the interface can be used by the Cross-Layer Coordination to provide the degree of mobility of a node (i.e. military unit). This information could then be used to configure a hybrid routing protocol.

C.3 INTERIM SOLUTIONS FOR IMPROVING COMMUNICATION FOR LEGACY SYSTEMS

To show the benefit of the cross-layer design shown in Figure C-1 even for legacy C2IS and communication systems, which can't be modified to support the new middleware interfaces, we describe three approaches for interim solutions. These approaches allow for improving the coordination of C2IS and communication systems and thereby for a more effective use of the communication resources.

Generally the communication behavior of legacy C2IS applications can be influenced in different ways. In this section we present three different approaches:

- Use of C2IS application adapters: In this approach additional adapters are used, which may modify data exchanged between C2IS applications and the communication system;
- Influencing the user behavior by providing network information: This approach is based on the visualization of the current network status or the status of message delivery for the user. This shall enable the user to defer less important messages if the channel utilization is very high (e.g. due to higher important military messages);
- Situation- and role-specific configuration of the communication system: In this approach the configuration of the communication system is adapted according to the hierarchy level of the assigned unit. An example is link layer protocols that use static, preconfigured frame sizes. A reduction of the frame size reduces the delay of the communication channel (e.g. for transfer of VoIP communication, which is especially important at the tactical level), while an increase of the frame size reduces the protocol overhead and thus improves the efficiency of communication (e.g., for transfer of military messages, which is more important at higher hierarchy levels). This adaptation is especially important for radio links which are used both for transfer of data and voice.

C.3.1 German Legacy Communication Systems

Prior to presenting approaches for interim solutions, we take a look at a German C2IS and communication infrastructure, which is used in this section as exemplary system for deploying the proposed solutions.

Figure C-3 shows a typical example for the deployment of the German C2IS and the Communication Server in a military vehicle. The Communication Server is a separated device which is responsible for delivering messages. For this purpose, a Communication Server is connected to different communication technologies like SATCOM, trunked radio systems and legacy VHF based radios. Additionally, the Communication Server is connected to the German C2IS (deployed on a separate host) via a local area network (Ethernet). The Communication Server offers interfaces for configuration and message transfer. Military messages are exchanged between C2IS and the Communication Server via the Extended Simple Mail Transfer Protocol (ESMTP) protocol.

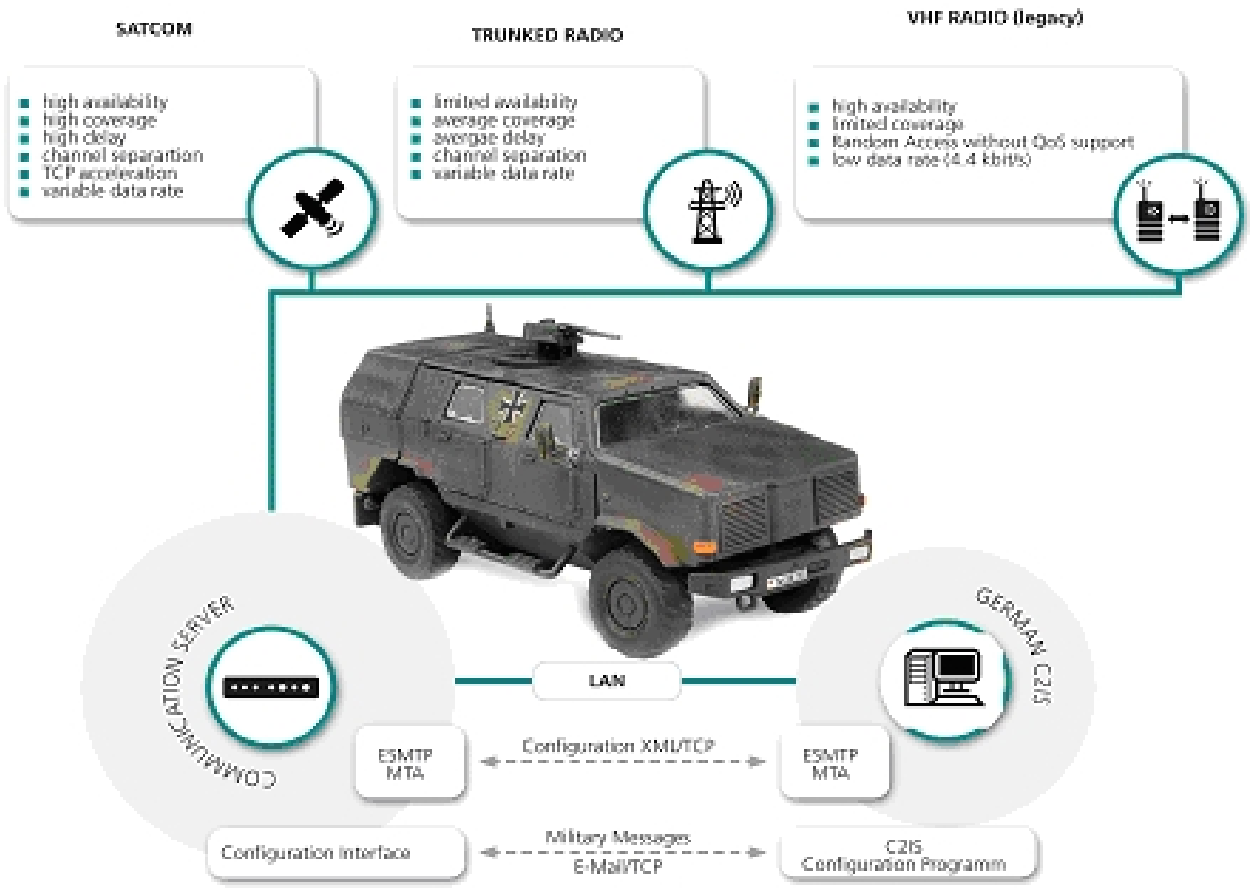

Figure C-3: A German C2IS Using Different Communication Technologies Including Legacy VHF Communication.

In the following, we consider solutions to be deployed in the short-term. Thus, we assume that no additional hardware can be deployed in military vehicles and no direct modifications of legacy software components can be made. Additional software components have to be deployed on existing hosts (C2IS host or Communication Server host) and must use existing interfaces of legacy applications.

Figure C-4 shows our test bed for legacy systems. Two C2IS systems (see both monitors) each connected to a Communication Server (small form factor version on top of the radio devices) communicate via SEM 80 VHF radios. Instead of antennas we uses dummy loads that still allow for short range radio communication.

Figure C-4: Demonstrator and Test Bed for Legacy Systems.

C.3.2 Use of C2IS Application Adapter

We introduce an approach utilizing adapters which may modify the data exchanged between C2IS applications and the Communication Server. These adapters can be installed as additional software on the different systems (C2IS or the Communication Server).

Figure C-5 shows our design of this approach with adapters installed on the Communication Server host. The adapters are informed by the middleware (Cross-Layer Coordination) about the current network conditions and may delay, discard or modify messages of the C2IS. In this approach the adapters can be seen as local proxies for the C2IS applications and therefore correspond to the application layer in Figure C-1. The provision of network information for the adapters corresponds to Control API in Figure C-1.

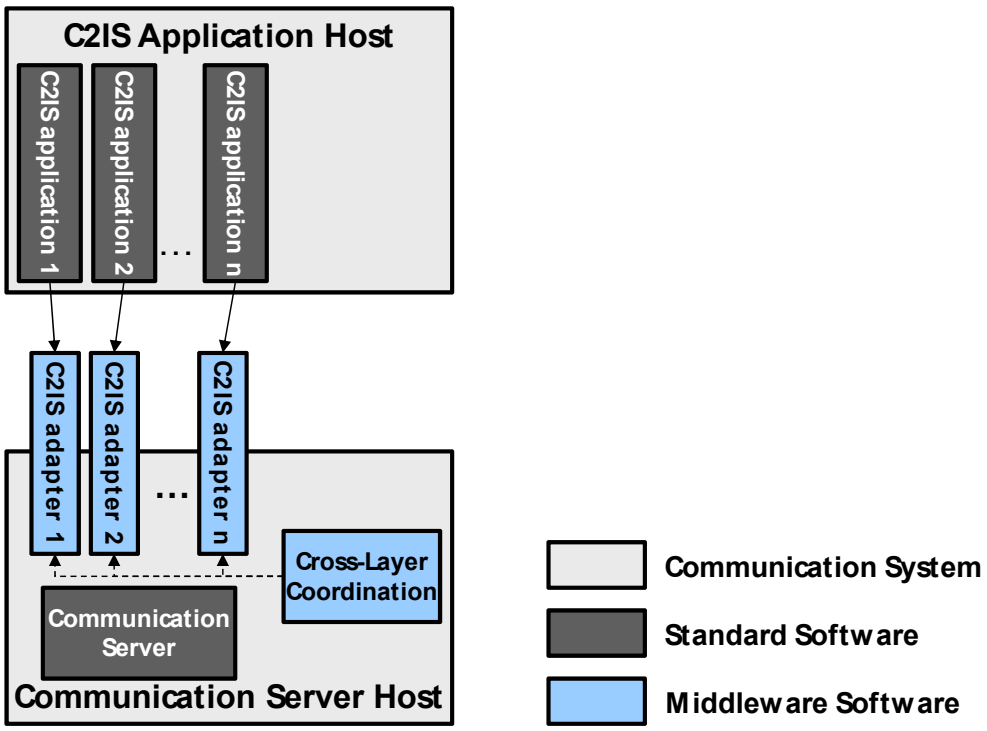

Figure C-5: C2IS Adapter Design.

In this way the communication behavior of the C2IS can be adapted to the current network status. For this purpose the behavior of each adapter should be adjusted to the communication requirements of the C2IS system it is responsible for. For example, an adapter for Blue Force Tracking (BFT) could discard some GPS messages in case of overloaded radio links. This is feasible, because GPS messages usually do not require reliable transport. Figure C-6 shows an example of the interaction of the different software components according to this approach. Figure C-7 shows the same approach and message flows applied to our legacy test bed.

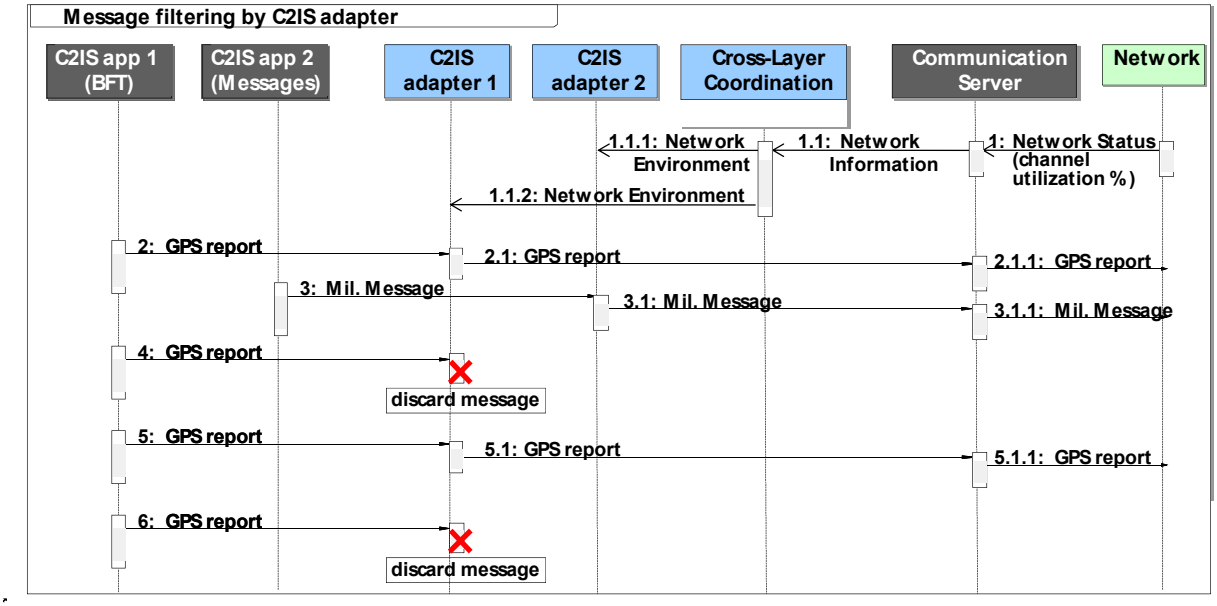

Figure C-6: Message Filtering by C2IS Adapters.

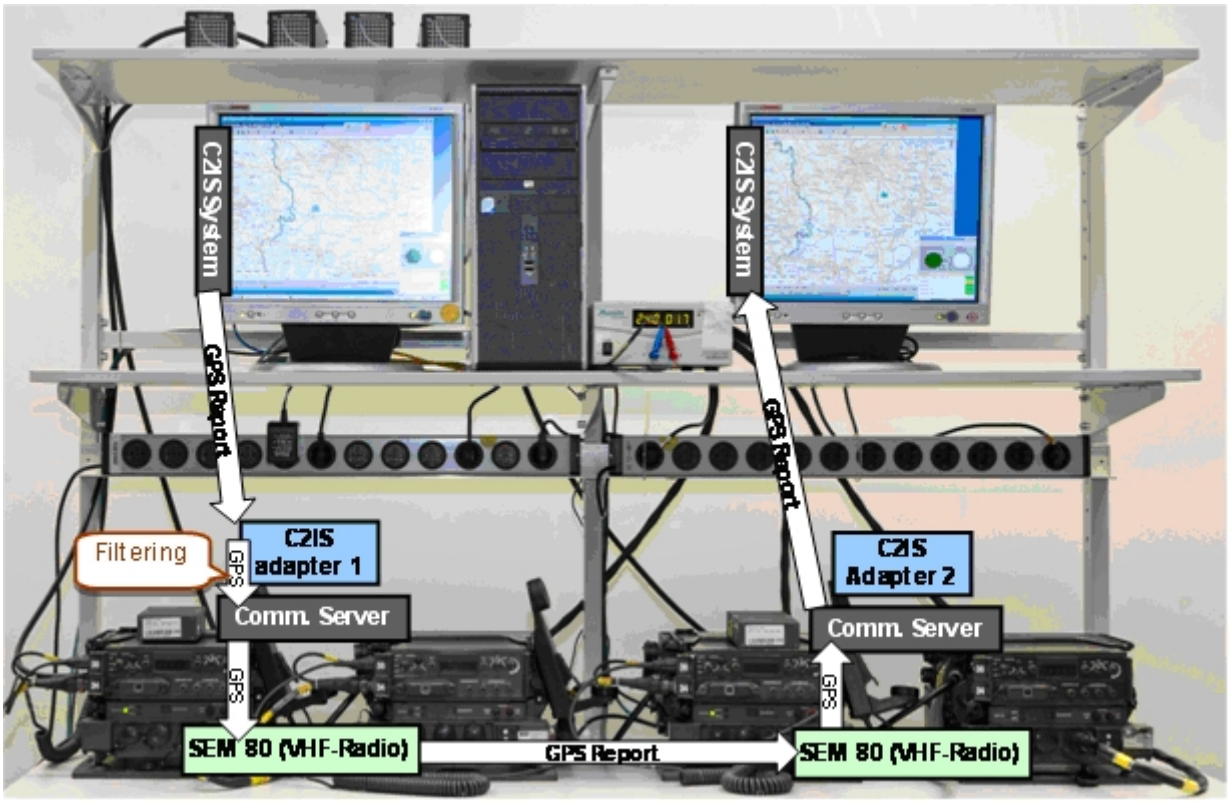

Figure C-7: Message Filtering by C2IS Adapters in the Test Bed Setup.

As shown in Figure C-6, the Communication Server gets information about the current network status from the radio link (i.e. the channel utilization) and provides this information to Cross-Layer Coordination (see 1 and 1.1 in Figure C-6). Cross-Layer Coordination hereafter provides the different application adapters with

this information (see 1.1.1 and 1.1.2 in Figure C-6). A GPS report sent from the BFT application to the corresponding BFT adapter (see 2 and 4 in Figure C-6) may be delivered to the Communication Server and further transmitted by the radio link (see 2.1 and 2.1.1 in Figure C-6) or be discarded by the BFT adapter depending on the current radio link status (see 4 in Figure C-6). Contrarily, high prioritized military messages are always passed by the corresponding application adapter to the Communication Server and then transmitted via the radio link (see 3.1 and 3.1.1 in Figure C-6). The BFT adapter may configure the maximal sending rate of BFT messages depending on the network information (channel utilization) provided by Cross-Layer Coordination.

C.3.3 Influencing the User Behavior by Providing Network Information

The German C2IS does provide little information about the status of message delivery (only “successful delivered”, “failed” or “to be delivered” on the basis of end to end acknowledgements) and no information about the channel utilization of deployed communication technologies. Thus, an impatient user tends to send messages which are not confirmed more than once. This leads to a higher utilization of the radio links, increased time of waiting and less message throughput.

Therefore, this approach aims at influencing the communication behavior of the user by visualizing the network conditions and/or the status of message transfers respectively. This status information may be displayed by an additional application installed on the legacy C2IS host. Thus, no modification of the C2IS software itself is necessary. If acting cooperatively, users are enabled to defer less urgent messages in the case of scarce communication resources. This helps to deliver urgent messages in a timely manner.

Figure C-8 shows an approach for visualizing information about the current network status for the user. Cross-Layer Coordination gets information about the current network status (e.g. the current channel utilization) from the Communication Server and provides a visualization component (Network Info in Figure C-8) deployed on the C2IS application host with this information. For this purpose the Communication Server offers a configuration interface. It allows inquiring the delivery status for each message which afterwards may be visualized by Network Info. Network Info shows which message is currently being transmitted and which messages are stored in the sending queue. Additionally, statistical information about the receiving quality, channel utilization and the occupancy of the radio channels by the unit itself and by other units is available via the configuration interface of the Communication Server and hence can be displayed to the user (see Figure C-8). Furthermore, based on the channel utilization, the delivery time for the messages which are stored in the message queue can be calculated and shown on a predictive basis (see Figure C-8). In general, a higher degree of transparency regarding the status of message transfers and utilization of communication links is expected to achieve better communication behavior of the user.

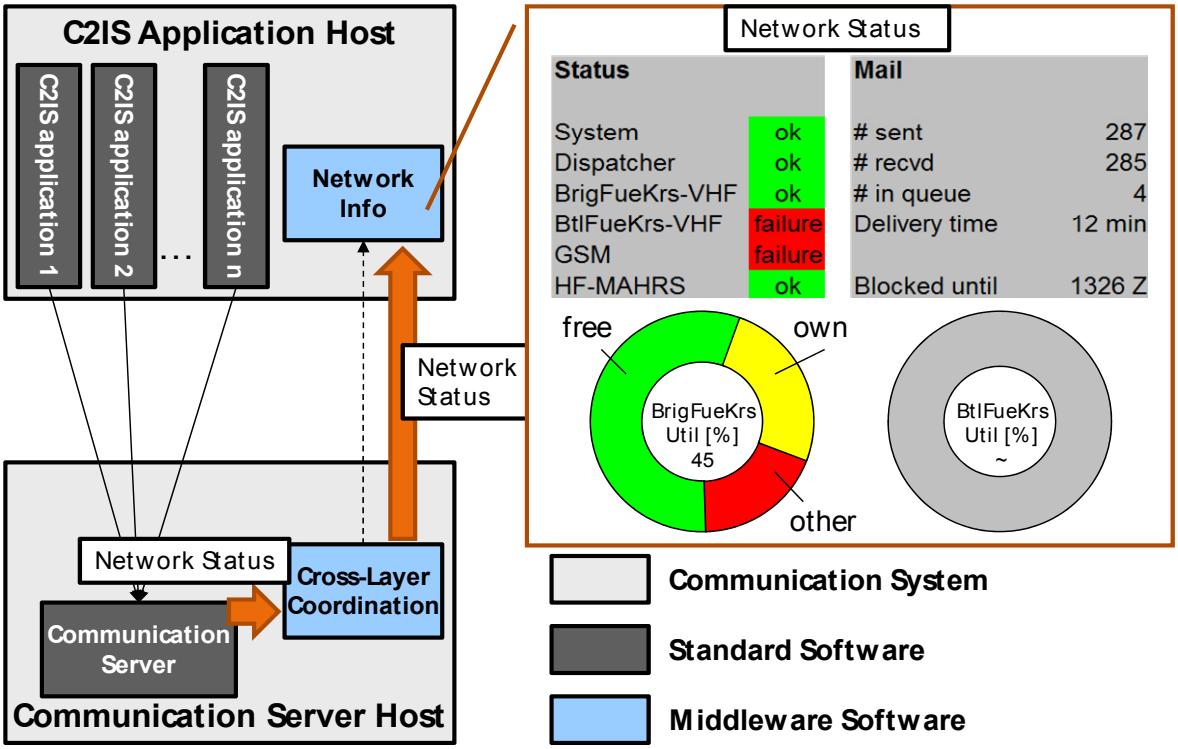

Figure C-8: Visualization of the Network Status.

C.3.4 Situation- and Role-Specific Configuration of the Communication System

In this approach the communication system is configured dependent on the hierarchy level of the corresponding military unit. For link layer protocols with a static, preconfigured frame length, this length could be reduced for military units at lower hierarchy levels to decrease the communication delay (e.g., for transfer of VoIP packets). At higher hierarchy levels, where voice communication is less important, the frames should be larger to improve the efficiency of communication (e.g., for transfer of military messages).

To deploy different configuration profiles, a couple of configuration profiles may be predefined. By the use of the configuration interface of the Communication Server (Configuration Interface in Figure C-3 and Network Configuration in Figure C-1), Cross-Layer Coordination can specify the configuration profile to be used by the corresponding Communication Servers. To preserve the communication compatibility of different hosts, only a few fixed communication profiles should be used. These profiles should be chosen in an automated manner, to assure that each host uses the right profile.

C.4 SUMMARY

In this chapter, we argued that a better coordination of C2IS applications with the different network technologies in use can improve the overall user experience.

We presented a cross-layer middleware design, which aims at exchanging information between C2IS applications and the network protocol layers to better coordinate application functionality with the capabilities of the different network technologies in use. In our design, we extended existing approaches to achieve a better information exchange between applications and communication layers. Our middleware concept contains a Control API that is used by the applications to specify their communication requirements

as well as to provide mission information. It also offers technology independent information about the network environment to the applications, which is retrieved from the network stack by a Generic Network Access component.

Additionally, we showed how the cross-layer middleware approach can be used for current C2IS and communication systems. We presented three approaches for interim solutions to improve the communication behavior even if no modifications of the systems are feasible.

Annex D – SOA OVER DISADVANTAGED GRIDS EXPERIMENT AND DEMONSTRATOR

Annex D is provided as a separate report “SOA Over Disadvantaged Grids Experiment and Demonstrator”; Przemysław Caban, Rui Fiske, Trude H. Bloebaum, Frank T. Johnsen, Leon Schenkels, Marc van Selm, Joanna Śliwa, Vincenzo de Sortis, Aad van der Zanden; NCIA; December 2011, The Hague. It can be obtained through NCIA, The Hague, Netherlands.

Keywords:

Service Oriented Architecture, Disadvantaged Grids, Data Distribution Service, DSProxy, Mist, Enterprise Service Bus

Abstract:

The Service Oriented Architecture (SOA) over disadvantaged grids experiment and demonstrator was linked to the CSO IST-090 group’s presentation during the 2011 MCC Conference in Amsterdam. The disadvantaged grid networking infrastructure used was based on mobile ad-hoc networking systems. This document describes the support plan for the exercise and describes the experimentation and the results of the various approaches for network optimisation as conducted by the Norwegian FFI, the Polish MCI and the NC3A.

Annex E – AFRO

Under the umbrella of IST 090, POL have carried out research on the possibility of adapting the Web Services flow to the limitations of the network on the basis of semantic reasoning. This is a promising candidate (interesting and related to IST-090 work) for further testing. This work is placed as a separate annex because it was not incorporated in the demonstrations or tests by IST-090 [Annex D]. This annex relates to the discussion of proxies in [Annex A].

For this purpose there has been proposed the Adaptation Framework For Web Services Provision (AFRO) that defines a mechanism for effective Web Services invocation in tactical networks, which are considered disadvantaged in terms of available throughput, delay and error rate. Its implementation, in the form of AFRO Proxy, performs so called adaptation actions, which are modifications of the SOAP XML messages by changing their encoding to more efficient or cutting out information that are accepted to be removed by the service requester. The proposed adaptation mechanism gives promising effects for low level commanders located at the battlefield. They can be supplied with information generally available on high command levels which, up to now, were very rarely distributed to tactical networks.

The solution is to enable the client to use the service in disadvantaged network in a limited way (with limited number of information provided or provided by a different mechanism) and adapt the service provision mechanism to the client's software and hardware possibilities.

E.1 CONTEXT – AWARE SERVICE PROVISION

Context – aware applications refer to a general class of mobile systems that can sense their physical environment, and adapt their behavior accordingly. They derive from the ubiquitous (or pervasive) computing concept that was presented in 1991 by Mark Weiser [84] who set its foundation. This concept developed for the commercial applications began the new field of interest of many researchers where the area of context-aware applications became an important part.

In context – aware service provision it is generally important where the client is, what are his actions/duties, what terminal is he using, what resources are nearby, etc. [85]. In many applications the most important aspect is location but this can be extended to include different characteristics (user actions, device, surrounding environment, etc.). Context recognition allows users to take full advantage of the local capabilities within a given environment, and be able to seamlessly roam between several environments, choose different services, even as the defined context change.

The idea of context – aware service provision was used in the development of the Adaptation Framework for Web Service provision in disadvantaged environment (AFRO). It is aimed at improving the chance of success of SOAP Web Services invocation in tactical environment, which is characterized by dynamic changes in throughput, error rate and delay. Successful service invocation in this case is understood as the possibility to deliver response message requested by the client from the target service.

AFRO follows the assumption that in order for a Web Service to function more efficiently it is necessary to minimize the amount of data transmitted to the user. The actual traffic flow related to Web Services' interactions is burdened with the XML overhead which greatly limits communication link output. It is highly recommended therefore: to improve encoding efficiency, i.e. enhancing the ratio of the user data to the management data in the SOAP message, and to reduce the number of unnecessary data (or data that cannot be consumed) to the users of degraded networks.

Limiting the size of traffic flow to the users of wireless networks will improve the successability of Web Service calls and will support users with information crucial for their operation in the battlefield.

Message adaptation actions can be therefore twofold: lossless – e.g. actions that improve message encoding enabling the consumer's side to decode it without losing any of the data or without the transport protocol change (e.g. HTTP to MMHS), and lossy – cutting out information that the user agrees to be filtered out.

The selection of an appropriate adaptation action is not a trivial task and must be based on several types of information. First, adaptation does not have to be performed when the connections are stable, the network has high bandwidth, acceptable delay, no losses, and therefore, does not provide limitations for Web Service provision. The information about the network state is important in order not to spoil time on unnecessary actions.

The second important aspect is necessity to take into account users' preferences in terms of adaptation. They will be included in, so called, user profile, within which the user will state his adaptation preferences, and device profile, which defines his terminal's software and hardware possibilities. This set of information is necessary for selecting the actions that would meet the user intentions and, at the same time, would not make it impossible for the user terminal to receive and decode the message. This results from the fact that when the message is received at the user terminal it is firstly processed by the software libraries installed on it. Existence of particular software libraries implies therefore possibility of particular message encoding actions. Additionally, terminal information can help in parameterizing images and video streams that would be directed to the user working on a particular device.

Such an approach makes it necessary to provide a mechanism for provisioning and then efficiently using information about the user, his terminal, the network and service invoked. This problem has been defined as the need to identify the context of the service call. It has been proposed in the form of ontology that allows to clearly define parameters of entities taking part in the information distribution process and then, on the basis of the set of rules and the rule engine, efficiently support the decision process enabling to take adaptation actions improving service successability.

On the basis of those considerations the architecture of the Adaptation Framework for Web Service Provision (AFRO) has been proposed (see Figure E-1). It bases on the Decision Support Engine that uses information about the context of the service call as the input data, and, on the basis of ontology rules, defines the adaptation actions to be triggered on the SOAP body and SOAP attachments by the Adaptation engine. Such a modified SOAP message has smaller size than the original one and as such, is sent to the requester.

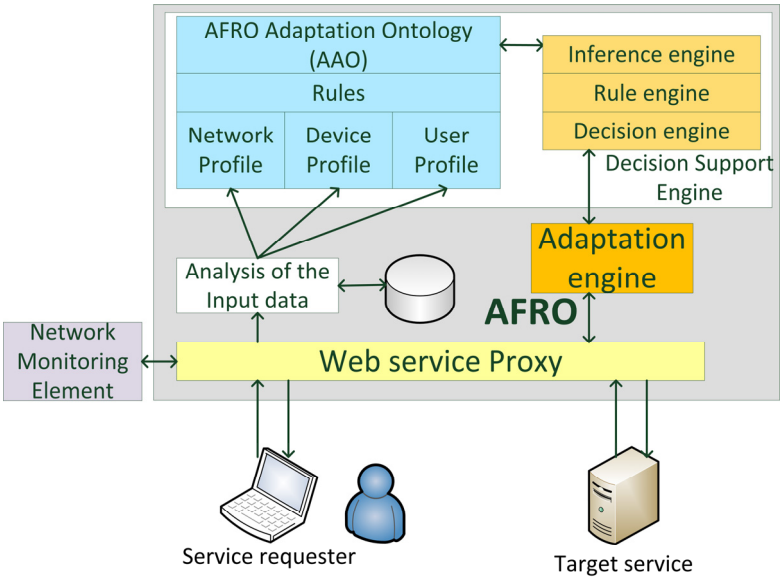

Figure E-1: AFRO Architecture Framework.

The ontology proposed and the rule engine strongly support dynamic selection of adaptation actions appropriate for the user. They are used by the Decision Support Engine that returns in response a set of actions. These actions derive from the Proxy functionality. They can be embedded (e.g. take the form of the Adaptation engine, see Figure E-1) or, taking different approach, distributed. The latter one can be implemented using SOA services orchestration. After the Proxy selects appropriate actions for the user, it searches for the services that will provide appropriate mediation (will carry out the action).

Whatever approach to Proxy implementation one can take, the application of the Decision Support Algorithm and the proposed adaptation ontology (AAO) will supply him with the dynamic selection of actions to be taken.

It is also assumed that the Proxy will make use of information provided by external element – Network Monitoring Element that will support it with information about currently observed network performance on the link to the user. This performance information (in terms of throughput, delay and error rate) will be used by the decision support algorithm. In case the network is categorized as disadvantaged, the Proxy will make the modifications stronger, decreasing the amount of information that is sent to the user (in terms of image modifications), however making it more probable to be transferred to the consumer.

E.2 REFLECTING USER REQUIREMENTS

One of the elements of the proposed method is the context of the service call. In the case of the AFRO proxy, this context is perceived as collections of information about the user, the device, the service and the underlining network.

Information about the user:

- What modifications of the SOAP messages' content is the user willing to accept?
- What device is he using as his end terminal?
- What access network is he using?

Information about the device:

- What are the characteristics of the device hardware (resolution of the screen, CPU frequency)?
- What are the characteristics of the device software (operating system, supported libraries)?

Information about the service:

- What is the service description?

Information about underlining network:

- What is the network type?
- What is the current link performance?

The reason for the dynamic adaptation to be based on the pre-distributed information is that the user – from the point of view of his activities – may not wish the mechanism to modify contents of the message and modify the attachment (resize, compress, decrease color depth). In order for the non-standard XML encoding to be used at the receiver, the device must be equipped with appropriate libraries. It is very often an issue in mobile devices that use limited operating systems and limited set of libraries and do not support software implementations regularly used in laptops or PCs. The environment the adaptation framework is to be used in assumes utilization of mobile hand-held devices the configuration of which (software and hardware) is important in terms of successful Web Services adaptation.

The context of the service call has been modeled semantically with the Web Ontology Language, (OWL DL [86]) which is the most powerful ontology description language and promising in terms of further processing, rule enforcement and inference.

The context information in AAO has static and dynamic elements. It generally consists of: user context (adaptation preferences – static), device profile (static), service context (QoS profile – static), network context (Link performance – dynamic).

For the purpose of selecting the adaptation actions the decision engine uses the AFRO Adaptation Ontology (AAO) describing all the actions that can be taken by the proxy, reflecting the user preferences. In order to make use of the adaptation ontology a set of rules has been defined. Rules are important in OWL to state facts about instances of classes.

The rules in AFRO define requirements for particular actions based on information that are provided in the context of the service call. They have been defined using the Semantic Web Rule Language (SWRL) [87], combining sublanguages of the OWL DL and Lite with those of the Rule Markup Language.

Adaptation actions are modifications of the SOAP XML messages. In the proof of concept GZIP compression algorithm and Efficient XML were used for XML messages. Images attached to SOAP messages were modified by hanging their resolution, color depth and limiting their quality. With these actions, the sizes of messages are significantly diminished making them better tailored to the tactical networks.

The dynamic elements of the context should be gathered at run time by agent entities and forwarded to the proxy (see Figure E-2). In this case they relate to the current link performance.

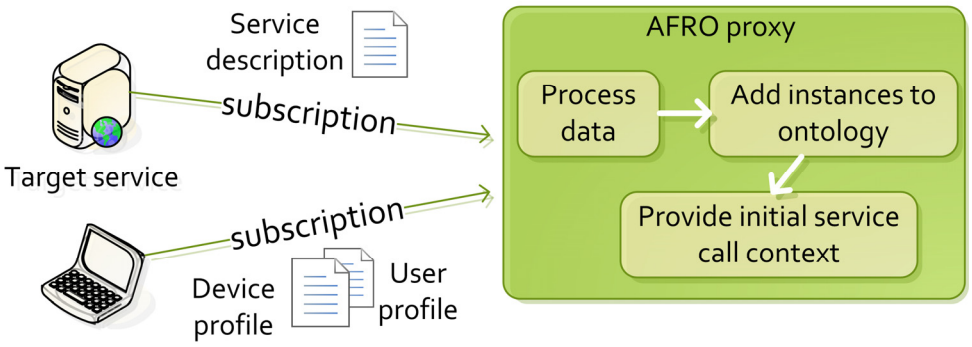

Figure E-2: Pre-Processing of the Data Gathered During the Subscription Process.

After the user logs in, his every request is perceived as a Service call. On the basis of rules defined in the Proxy, appropriate adaptation actions are selected. An exemplary rule defining the ChangeResolutionAction as preferred for the user when his device has low CPU is as follows:

uses(?x, ?y)^hasHWlimitations(?y, ?z)^LowCPU(?z)→
hasPreferredAction(?x, ChangeResolutionAction)

In AFRO Adaptation Ontology (AAO) the Action class is divided into two subclasses: SOAPAdaptationAction and AttachmentAdaptationAction. They allow for creating different actions that the Proxy can provide (or can invoke in an external entity).

The adaptation ontology can be further expanded as additional components reflecting actions available in the AFRO proxy will be introduced.

E.3 VERIFICATION

In order to verify its correctness of the adaptation process functionality and compare with the regular Web Service invocation, the verification phase has been taken up. In general, it aims at proving that the proposed method improves successability and application response time parameters of Web Service realization in disadvantaged networks. However particular steps are devoted to check different elements of AFRO. The verification phase was to answer the following questions in 4 Experiments: Experiment 1: AAO ontology evaluation; Experiment 2: Verification of information originality after running attachment adaptation actions; Experiment 3: Verification of the Method in Disadvantaged Environment.

E.3.1 Results of Experiment 1

The scope of the AFRO adaptation ontology (AAO) has been set up by the problem it is designed to solve. It is aimed at supporting the dynamic selection of adaptation actions taken on the SOAP messages exchanged between the Web Service client and server. It defines:

- Entities that take part in the service invocation as classes (User, Device, Network, Service, Action class),
- Relationships among entities as object properties (connects ↔ isConnectedBy, hasAdaptationPreferences, hasDeviceProperties, hasPreferredAction, hasProhibitedAction, usedBy ↔ uses, hasNetworkType, isInvokedBy ↔ invokes),
- Characteristics of entities as data type properties (userName, deviceName, qualityValue, resolutionValue, colorDepthValue).

The TBox ontology model describes relationships among defined entities. On its basis knowledge about the service call context (defined in ABox entries) is collected. After each user registers to the proxy, the knowledge about the user preferred, prohibited actions and his device properties are saved in ABox entries. This allows to set the Initial Service Call Context (ISCC). After the network state is checked, the final AFRO defined actions set (ADA) is defined.

The AAO is the basis for running the decision support algorithm and setting the actions that should be performed by the AFRO Proxy.

Ontology rules defined for the purpose of selecting the actions take into account the following cases:

- The terminal does not support particular file format → the attachment is discarded (rule 1 – 5),
- The terminal supports particular encoding techniques → the encoding actions is added to the list of preferred (rule 11 – 13),
- The terminal has too low CPU frequency (processing power) → big images will be difficult to be processed – change image resolution (rule 6),
- The terminal has limited color display – decrease color depth (rule 7 – 9),
- The terminal is connected by disadvantaged network link (general rule – true for all cases) – decrease quality (rule 10).

Moreover, the preferred and prohibited actions that the user defined are also taken into account. They may derive from the role of the user and his duties at the battlefield.

The AAO defines all entities that are necessary to take appropriate adaptation decision and enables to automatically select appropriate adaptation actions. Its scope covers the required level of detail in describing the entities and relationships among them taken in the initial phase of ontology development. It covers so called competency questions [88] defined for the purpose of AAO. Additionally, the set of rules monitor all basic terminal characteristics that may influence usability of messages delivered to the user.

The second ontology evaluation step consists in checking the ontology consistency. According to [89] ontology is consistent (also called satisfiable) when it does not contain a contradiction. The lack of contradiction can be defined in either semantic or syntactic terms. The syntactic definition states that a theory is consistent if there is no formula P such that both P and its negation are provable from the axioms of the theory under its associated deductive system.

The ontology model that contains formal definitions of classes, properties and individuals allows inferring new knowledge from knowledge that is already present. The fact that it is based on formal description logic makes it prone to logical reasoning and enables to infer knowledge from existing facts and axioms, as stated in [86]: "Fact states information about a particular individual, in the form of classes that the individual belongs to plus properties and values of that individual" and "Axioms are used to associate class and property identifiers with either partial or complete specifications of their characteristics, and to give other information about classes and properties. Axioms used to be called definitions, but they are not all definitions in the common sense of the term and thus a more neutral name has been chosen".

The aao.owl model has been verified in the Protegè 3.4.6 using the Pellet 1.5.2 reasoner for consistency on the machine with following configuration: Processor: Intel Core i7 (2 cores 2,8 GHz each); RAM: 6 GB; Operating System: Windows 7 (64 bit). The consistency check on this machine was successful. AAO has been proven consistent.

E.3.2 Results of Experiment 2

Attachment adaptation actions are lossy. That is why Experiment 3 was aimed at verification of the information degradation factor when particular attachment adaptation actions are performed. For the purpose of Experiment 3 there has been defined the Information Originality Factor (IOF) that is aimed at measuring how big are changes that have been done in the original attachment.

For original attachments the IOF = 1, which means that no changes have occurred. When the image is discarded, IOF = 0, which means that no original data will be transferred back to the client. The adaptation actions defined for the AFRO Proxy are: Discard Attachment (DA), Decrease Quality (DQ), Change Resolution (CR), Decrease Color Depth (DCD). The IOF will therefore be dependent on these four actions in the following way:

$$IOF = \begin{cases} 0 \; if \; DiscardAttachment \in ADA \\ \frac{1}{3} * cr + \frac{1}{3} * dq * cr + \frac{1}{3} * dcd \end{cases} \quad (1)$$

Cr – change resolution factor, which measures the ratio of the area of adapted image to the area of original image. It means how much the image's size (in pixels) was reduced.

$$cr = \frac{area \; of \; the \; adapted \; image}{area \; of \; the \; original \; image} \quad (2)$$

Dq – decrease quality factor, which measures the ratio of the quality of adapted and original images. It means how much was the quality of the image reduces.

$$dq = \frac{quality \; of \; the \; adapted \; image}{quality \; of \; the \; original \; image} \quad (3)$$

Dcd – decrease color depth factor, which measures the ratio of the color depth in bits for the adapted and original images. It means how much was the color depth reduced.

$$dcd = \frac{color \; depth \; in \; bits \; for \; the \; adapted \; image}{color \; depth \; in \; bits \; for \; the \; original \; image} \quad (4)$$

The values of IOF for adapted images are shown in Figure E-3. The IOF for images prepared for degraded network is lower than for constrained network which means that this image has limited detail. However when the network resources are scarce, the message size has great influence on the successability of its delivery. Therefore it is strongly recommended to use the AFRO adaptation mechanism and deliver adapted images, even though their Information Originality Factor is below 1.

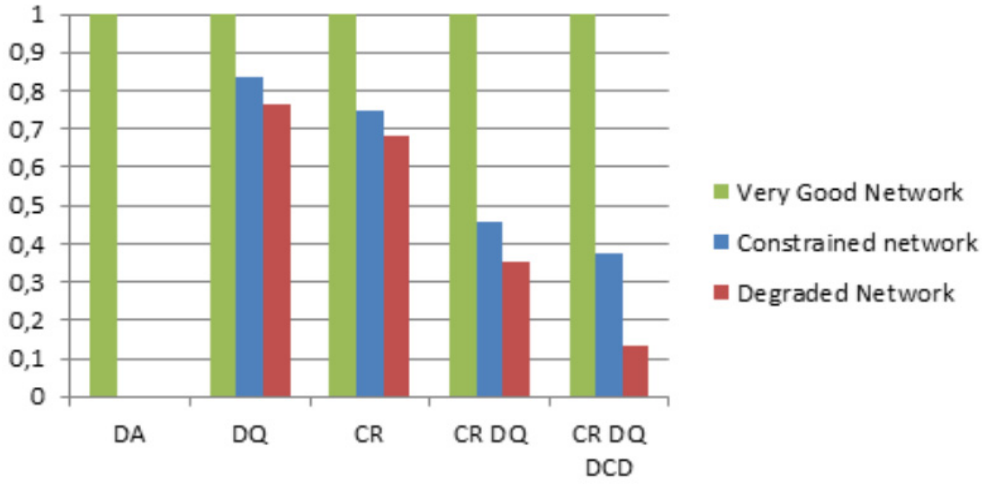

Figure E-3: Results of IOF for Images Adaptation.

E.3.3 Results of Experiment 3

The efficiency of assumed adaptation actions was verified in the Experiment 4 which measured two Web Services performance metrics - the response time and successability - for invocations of Web Services directly and through the AFRO Proxy. The Experiment 4 has been divided into 10 scenarios, each devoted to checking the AFRO adaptation mechanism efficiency for two exemplary target Web Services and five exemplary network performance conditions. The selected network types are the most often used in modern communications systems, prepared to be working in NEC military operations, delivering information to users on low levels of command [90]. These are the most representative examples from within the disadvantaged networks. They give the worst case in terms of delay – SATCOM, throughput – CNR and error rate – WIFI2. There is also an example of a very good performance network – LOS, with relatively high throughput, small delay and no errors, and constrained network – WIFI2 – with relatively high throughput, medium delay and small PER.

Since the adaptation actions consider modifications of SOAP messages and image attachments, there has been considered evaluation of two Web Service types: The NFFI service that returns tracks of objects as SOAP XML messages (5 messages from 1kB to 93kB were sent), and the Image service that returns still image files in JPEG format (an image of 900kB was sent).

Additionally the test investigates the measured response times in terms of their adherence to the requirement set in the G.1010 [85] ITU-T recommendation. It states that in order for the user to be satisfied with the transfer of the bulk data, it should be delivered in time less than 15s, without errors. It was the reference level for evaluating results. Any result above 15 s is given so called “penalty” equal one point for each second. If invocation is 100% unsuccessful, penalty of 1000 points is given.

Table E-1 and Table E-2 show a summary of results. The AFRO Proxy SOAP adaptation actions provide a very big advantage, especially in case of networks that are classified as degraded (SATCOM, WIFI2, CNR). In a very good network (LOS) there was almost no difference of response time for SOAP XML and

encoding techniques. It results from the fact that message modifications are also time consuming, but when the transmission lasts a few seconds, they can be a significant coefficient of the total observed response time. In networks that the network state classification algorithm would classify as having enough performance (very good networks) no adaptation would occur. The results proved that in such a network all original messages would be sent in satisfactory time (less than 15 seconds) and with 100% successability. In constrained network it is visible that the SOAP adaptation gives additional benefit in case of big messages (message 4 and 5).

Table E-1: Summary of Results Achieved for Experiment 4 in Case of NFFI Service Invocation.

Network	AFRO			Original Web Service Invocation	
	Response time	*Successability*	*Penalty*	*Successability*	*Penalty*
SATCOM	Improved (by 2 times for small mess. By 10 times for large message)	100% for all messages with GZIP and EXI	0 for all messages adapted with GZIP and EXI	100% for all messages	0 for all messages
LOS	The same – no adaptation	100% for all messages with GZIP and EXI	0 for all messages adapted with GZIP and EXI	100% for all messages	0 for all messages
WIFI1	Improved (20-40 ms for small message 2 times for large message)	100% for all messages with GZIP and EXI	0 for all messages adapted with GZIP and EXI	100% for all messages	0 for all messages
WIFI2	Improved (~2-3 times for small message 31 times for GZIP and large message)	100% for all messages with GZIP and EXI	7 for Message5 encoded with EXI; 0 for the rest of messages adapted with GZIP and EXI	100% for Message1 87,3% for Message2 90,4% for Message3 52,3% for Message4 44,4% for Message5	0 for Message1 5 for Message2 22 for Message3 76 for Message4 297 for Message5
CNR	Improved (about 30 times for GZIP and large messages)	100% for all messages with GZIP and EXI	0 for all messages adapted with GZIP and EXI	100% for all messages	0 for Message1 0 for Message2 0 for Message3 37 for Message4 81 for Message5

Table E-2: Summary of Results Achieved for Experiment 4 in Case of Image Service Invocation.

Network	AFRO			Original Web Service Invocation	
	Response time	*Successability*	*Penalty*	*Successability*	*Penalty*
SATCOM	Improved 3-12 times shorter	100% for all images	22 for D3; 0 for all other images	100% for image1	38 for image1
LOS	The same – no adaptation	100% for all images	0 for all images	100% for image1	0 for image1
WIFI1	Improved 2,5-6 times shorter	100% for all images	0 for all images	100% for image1	0 for image1
WIFI2	Improved	Av. 91,5%	Av.90,45	0% for image1	1000 for image1
CNR	Improved	0% for D3; Other images: 100%	44 for D2; 1000 for D3; 0 for D4; 0 for D5	0% for image1	1000 for image1

In case of image service invocation the attachment adaptation actions give response time improvement and successability increase in all scenarios. However for degraded networks with high error rate (WIFI2) and low available throughput (CNR) the attachment adaptation action that only decreases image quality is not sufficient (this is the case of sending file D3). It is necessary to provide at least two adaptation actions, i.e. change resolution and decrease quality.

The results of using AFRO prove that this method improves Web Service application response time and successability of Web Services invocations in networks that suffer from low throughput, high delay, error rate and are classified as constrained or degraded. The efficiency of the Method is however also dependent on the accuracy of the network performance evaluation by the Network Monitoring Element. It is especially important in case of attachment adaptation actions that take different adaptation preferences in case of constrained and degraded networks. The Adaptation Decision Support Algorithm is composed in such a way to give the user information with the highest fidelity (highest IOF value) so that stronger actions are performed in case of degraded networks.

In general, the attachment adaptation actions triggered by the Proxy will be dependent on the user and device profile. Moreover, the resulting files will be also dependent on the original file sent in response. In the tests done in Experiment 4 the original file has high resolution and large size (904 kB). Therefore, the results collected give the overview of the AFRO functionality in the worst case scenario.

The results also show that the packet error rate has higher influence on response times and successability of Web Services invocations than delay and throughput. In conclusion it has been assumed that, given an erroneous channel with quite high throughput (like WIFI2), in order to get better response time and successability, it is better to employ some error correction techniques and decrease channel throughput. When the error rate is high, so many packets are lost that the communications parties interpret losses as disconnections. When the adaptation is introduced, messages are significantly smaller and the successability as well as application response time of Web Services invoked through the AFRO Proxy is increased.

High delay in channels (like SATCOM) is interpreted by the TCP as congestion, so the source is decreasing its speed of sending data. This results in higher transmission times, however does not influence

successability. In case of low throughput the transmission times are longer, which is caused by the physical performance of the channel, however decreasing the amount of information sent results in improving the application response time in case of SOAP Web Service invocations and improving successability and response time in case of image Web Service.

E.4 SUMMARY

This chapter presents researches on using semantic description of the service call context defined for the purpose of the Adaptation Framework For Web Services Provision (AFRO) to improve effectiveness of Web Services invocation in tactical networks that are considered disadvantaged in terms of available throughput, delay and error rate. Its implementation, in the form of AFRO Proxy, performs so called adaptation actions, which are modifications of the SOAP XML messages by changing their encoding to more efficient or cutting out information that are accepted to be removed by the service requester. With these actions, the sizes of messages are significantly diminished making them better tailored to the tactical networks.

The results of tests confirmed that the proposed AAO model is semantically and syntactically correct and consistent. Reasoning over it provides the possibility to support the adaptation actions decisions taking into account the user preferences deriving from his role and limitations of his terminal. The SWRL rules defined for AFRO strongly support the automatic process of defining the preferred actions.

The proposed adaptation mechanism gives promising effects for low level commanders located at the battlefield, which can be supplied with information generally available on high command levels which, up to now, were very rarely distributed to tactical networks.

Following the loosely – coupled architecture of the AFRO proxy the idea of dynamic Web Services adaptation can be extended with the orchestration engine that would search for services that would carry out the adaptation action defined by the decision algorithm. Additionally, it would be interesting to combine the results of work in terms of Delay Tolerant Networking and DSProxy (see Section 3.2 and Annex A.5.2.11) with the idea of AFRO Proxy that works in the application layer to assess what is the benefit of applying such a combination in a disadvantaged environment.

Annex F – IST-090 MEETINGS AND OTHER ACTIVITIES

IST-090 organized 2 working meetings in each of 2009, 2010 and 2011. A few smaller meetings were held among nations that were working together on specific topics and/or demonstrators. The last meeting of 2011 was preceded by the Military Communications Conference (MCC) conference, where IST-090 presented 8 papers and showcased 3 demonstrations. A final meeting dedicated to producing the final report was held in 2012.

F.1 2009-04-27 PARIS

IST-090 was established during the kick-off meeting on 27 April 2009 in Paris. The nations that initially established the IST were: DEU, DNK, FRA, ESP, GBR, ITA, NLD, POL and TUR. The group was later joined by NC3A and NOR.

Topics:

- Member introduction and presentation;
- Presentation of IST-ET-046 work and subject (SOA) understanding;
- Discussion on goals and demonstrations. Includes taxonomy, criteria, use cases and scenarios, best practices,
- Work organization (TAP, POW, also TOR);
- Meeting schedule.

Main results:

- Agreement on goals and way of working.

F.2 2009-10-15 SHRIVENHAM DCC

Topics:

- Identification of inputs for IST-090 and of ongoing studies and developments:
  - Introduction and discussion on existing / available systems:
    - DSProxy;
    - Core Enterprise Services (CES) Test bed;
    - Other.
  - Introduction and discussion on related exercises / experiments:
    - Combined Endeavour 2009 – DSProxy;
    - Combined Endeavour 2009 – Service Discovery;
    - Other.
- Simulation tools.
- Scenario / Use case + mapping to research / experiments.
- Specific applications of for SOA over disadvantaged grids:
  - Maritime Force Level Functions;
  - Geographical services.

- Demonstration / tour:
  - EDS demonstrator;
  - Overtask Battle Lab in the DCC (15th);
  - EDS/HP presentation on simulated disadvantaged networks and SOA.
- Work organization + schedule and programme of work.

Main results:

- Overview of systems, simulation tools, experiments and ongoing research;
- Step taken towards a scenario;
- Work organization + schedule and programme of work.

F.3 2010-06-30 THE HAGUE

Topics:

- IST-090 Working Groups (WGs):
  - WG – General;
  - WG – SD;
  - WG - Synthetic environment;
  - WG - WS implementation.
- Report back on ICCRTS paper.
- Discussion around the goals of IST-090 and how to reach them:
  - Determine how to coordinate and apply studies and demonstrations;
  - Synchronise final demonstration, report;
  - Evaluation of possible solutions (preparation for).
- Presentations:
  - Presentation of WS and SD by GBR and NOR;
  - FFI's recent work on Web services information exchange (DSProxy) and service discovery;
  - NC3A introduction.
  - OSGi presentation;
  - MIP introduction;
  - Prepare plan for symposium.

Main results:

- POW iteration done;
- IST-090 working groups instantiated;
- Plans for symposium started;
- Plans for demonstration started.

F.4 2010-10-05 MADRID

Topics:

- Prepare for an experiment at the next meeting (equipment, configurations, investigate cooperation issues);
- Investigation for remote collaboration:
  - Now only point-to-point connections available;
  - Investigate VPN link or VM (Virtual Machine) for experiments;
  - Test framework + DS Proxy.
- Tools / simulators:
  - NC3A: Network simulator: Dummynet;
  - POL: Simulator / evaluation tool;
  - NLD: Ad Hoc Network Emulator (AHNEMO);
  - ESP: EXATA (Antycip);
  - GBR: NETem.
- DDS WG:
  - Experiment was prepared for (equipment, configurations, investigate cooperation issues);
  - Not enough preparation time to actually do the experiment this meeting;
  - Discuss about doing an experiment at the next meeting.
- POL demonstration:
  - DDS proxy;
  - Network emulator WANEM emulation / evaluation tool;
  - Afro proxy.
- ESP overview: Tactical Data Interface.
- ESP talks and demonstrations at ITM by industry OMG, AMPER, INDRA, TECNOBIT, University of Grenada, GMV, IGECIS, EPROSIMA, RTI, PrismTech and NEXTEL.

Main results:

- MAJIIC + industry interaction;
- Agreement to do an experiment at the next meeting + preparations for it;
- Refinement on IST-090 symposium / demonstration;
- Demonstrations by ESP.

F.5 2011-05-10 OSLO

Topics:

- Experiments:
  - Experimentation preparation day;
  - NOR Demonstration / experiment: SOA-pilot & SOA-Wireless sensor network presentation;

    - ESP and POL DDS interoperability;
    - NOR + NC3A (test harness) + WG WS results;
    - WS – DDS translator.
- Scenario update:
    - Align the scenario elements that are applicable for each demo.
    - The final scenario('s) should not be too complex, but should put the demo elements in the right context, also for a non-expert.
- Discussion of the framework for the final report;
- Determine what still must be done and how we do this. Timeline;
- Try-out of the presentations for the papers.

Main results:

- Experiments done;
- Symposium / demonstration chosen MCC 2011 Amsterdam:
    - Determined what we want to do at the MCC;
    - Determined what we need to prepare for the MCC;
    - Briefing of MCC TPC meeting;
    - Briefing of MCC conference environment and organization.
- IST-090 papers: try-outs done.

F.6 2011-10-17 AMSTERDAM MCC

This event was the culmination of the IST-090 work. We presented the IST-090 papers, which are referred to in this report and referenced in Section H.2 "Publications derived from work of IST-090".

We also performed the actual demonstrations. These are described in:

- Annex C - Interim Middleware;
- Annex D - SOA over Disadvantaged Grids Experiment and Demonstrator.

F.7 2011-10-19 THE HAGUE

Topics:

- Work on final report:
    - Discuss framework;
    - Divide the work.
- Progress report (for CSO panel meeting 9 November);
- Adaptation of IST-090 overview at MCC for DefenceIQ's Interoperable Open Architecture Conference;
- Evaluation of MCC:
    - Own experiences;

    - Useful input;
    - Feedback / improvements.
- Evaluation of experiments:
    - Own experiences;
    - Useful input;
    - Feedback / improvements.
- Follow-on steps for after this IST-090.

Main results:

- MCC symposium evaluation results;
- Experiment / demonstration evaluation results;
- Follow-on steps for after this IST-090. This would results in IST-118 as it is currently operating.

F.8 2012-04-02 SHRIVENHAM DCC

Topics:

- IST-090 report editing session;
- Future IST-118 IST TAP editing session.

Main results:

- Iteration of IST-090 report. A lot of work was done, but still a lot of work needed to be done by the nations after this meeting;
- TAP for follow-on IST.

Annex G – TERMS OF REFERENCE

G.1 ORIGIN

It should be noted that the TOR as represented below was defined, as it should be, at the start of the project. Whilst the TG gained more knowledge and insight, the planning and goals were improved and adapted to the available resources. For instance, the requirements coverage matrix was not elaborated as detailed as we originally planned, but several papers were generated and presented, for instance at the ICCRTS and MCC conferences. Also the demonstrations were successfully performed at a symposium (ITM Madrid 2010) and a conference (MCC 2011). Because the actual work of the TG continued until the end of the planned period, much material remained to be processed, and with little resources. This resulted in a later than planned delivery of the report.

G.1.1 Background

The SOA approach has demonstrated many advantages for the development and implementation of C4ISR systems in general:

- SOA's greatest advantage is the ability to seamlessly exchange information based on different policies and on a loose coupling of the components. [91].
- SOA can be realized by the use of open standards:
  - Asynchronous mode of exchange through the SOAP protocol offers a simple way to build interoperability with a good level of decoupling between presentation and transportation of information;
  - Common use of XML as a basis for the different description languages of the different levels of abstraction (SOAP for exchanges, WSDL for services description, UDDI for directories) resulted in the development of a wide offer of (COTS or open source) products;
  - Most of the commercial programming environments offer tools to easily realise "wrappers" to use legacy applications in Web Services.

There are some drawbacks which become apparent in a disadvantaged (constrained) military network:

- The use of XML as a message exchange format is a problem, because it is verbose and therefore needs a high bandwidth. Compression technologies can be used to mitigate this, but they need to be improved. The use of SOAP messages may be unfeasible in tactical networks with highly limited communication links. Since the use of a SOA does not require the use of SOAP, other protocols (more efficient in terms of bandwidth use) could be used instead (e.g. Data Distribution Service (DDS) or Military Message Handling System (MMHS)).
- The currently used implementations of SOA result in a high latency, especially for the discovery and invocation of services. This is caused by the high levels of decoupling that are used to facilitate the creation of interoperable solutions.
- The existing products are not designed for use in disadvantaged grids with a significant probability of unanticipated disconnections, because their development is mainly driven by the commercial market of WAN enterprise information systems.

G.1.2 Justification (Relevance for NATO)

The large number of legacy systems within NATO and within allied countries justifies any improvement to increase interoperability of existing applications in the overall frame of NNEC. Thus, SOA is unquestionable an area of interest for NATO C4ISR.

To cover the whole spectrum of NATO systems from the strategic to the tactical level, some improvements have to be identified to make SOA applicable on battlefield disadvantaged grids.

In the tactical military environment the bandwidth may be quite low and the connectivity may be intermittent with widely ranging communication gaps (seconds to days).

G.2 OBJECTIVES

G.2.1 Area of Research and Scope

The overall research focuses on the use of SOA on disadvantaged grids (e.g. Mobile Ad-hoc Networks) in "near real time". Sub-areas of research include:

- Communication paradigms;
- Mechanisms to reduce needed bandwidth;
- Mechanisms to improve reliability;
- Security: Requirements posed by security will only be taken into account as far as relevant. Security is already the focus of other groups (IST-053, IST-061).

To evaluate our propositions for solutions we will use a concrete scenario as a global context of the study. The scenario will incorporate use cases and services (i.e. Blue Force Tracking, Observation report, Alert notification, UAV video feed, weather forecast…). An example of scenario is provided below.

In Figure G-1 we have two kinds of SOA design and implementations:

- Regular (without Disadvantaged Grid limitations);
- Adapted to tactical needs (with Disadvantaged Grid limitations).

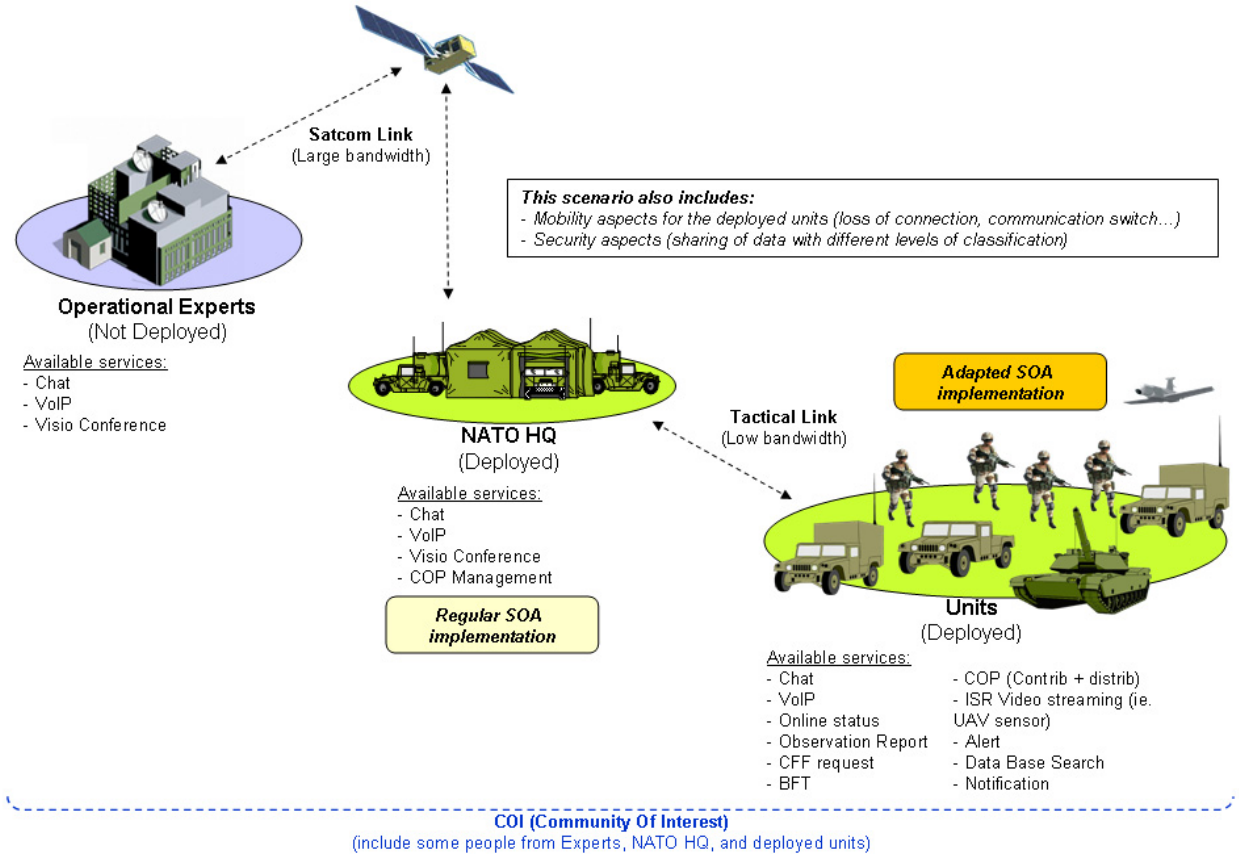

Figure G-1: Example of Scenario.

The TG will take in consideration the overall context of the scenario but will focus on SOA adapted to tactical needs.

Examples of Scenario Services:

- COP – Common Operational Picture
  Compilation, distribution and contribution of relevant information.
- BFT – Blue Force Tracking
  Provide information about own forces location.
- ISR Feed – Intelligence Surveillance Recognition
  Ability to access ISR Sensor information.
- CFF – Call For Fire
  Fire support requests containing all information needed to determine the method of target attack. For the scenario the CFF comes from an observer.
- Alert Service
  High priority instant advertising of incoming emergencies and contingences.
- Observation Report
  Distribution of information collected on the battlefield through observation by deployed soldiers and a variety of electronic sensors.
- Database Search
  Remote requests of information relevant to the operation by deployed units.

- Online Status
  Availability status monitoring of deployed units.
- Notification
  Ability to be notified when a subscribed data changed. It is linked to a data subscription approach.
- Others: Chat, VoIP, Video

G.2.2 The Specific Goals and Topics to be Covered by the TG

In the scenario described in Figure G-1 it is possible to discern the following issues that should be analyzed to find the solution for making SOA applicable to Disadvantaged Grids.

Areas of research that are proposed to investigate include (but are not limited to):

- Communication paradigms:
  - Request/Response, Publish/Subscribe (Message-centric approach, Data-centric approach);
  - Reduced dynamic service discovery.
- Mechanisms to reduce needed bandwidth:
  - Compression;
  - Content based routing and filtering;
  - Optimal synchronization of information;
  - Caching.
- Mechanisms to improve reliability (deal with intermittent connectivity / link instability and high latency):
  - Caching;
  - Data Replication.

G.2.3 Expected End Products and/or Deliverables

- Requirements for the use of SOA over Disadvantaged Grids;
- Demonstrations;
- Final report (Test results, Proposed solutions, Requirements Coverage Matrix).

G.2.4 Preliminary Planning

The duration of the Task Group will be three years starting in early 2009 with the final report submitted in 2011.

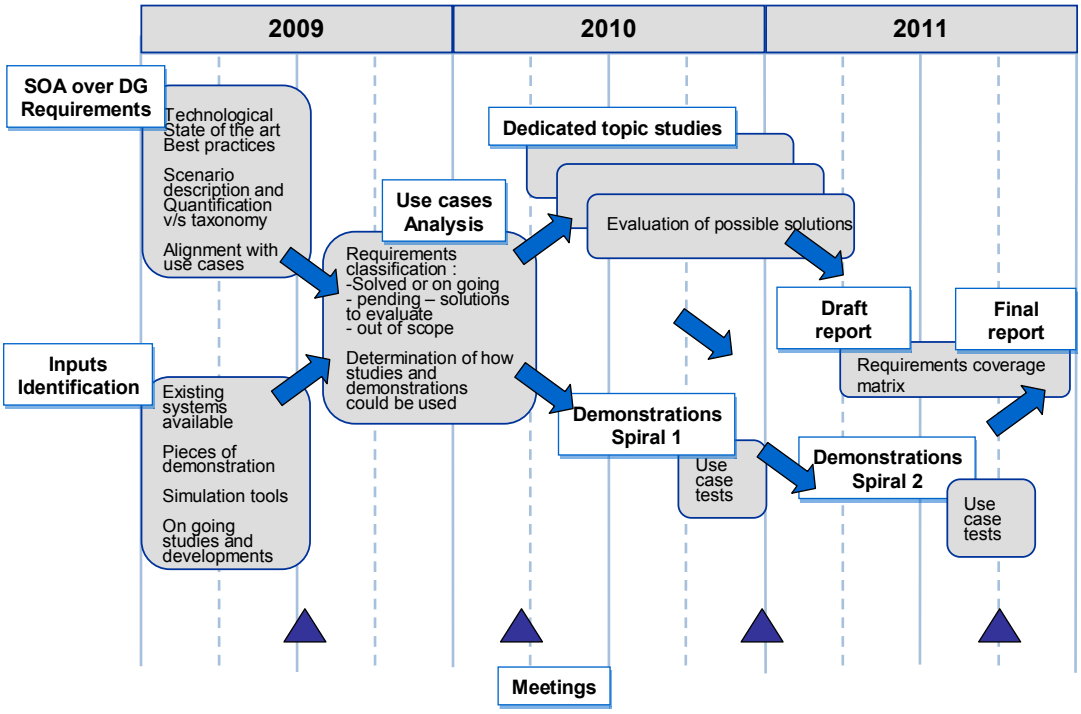

Figure G-2: Planning.

G.3 RESOURCES

G.3.1 Membership

Initial list of Nations which have expressed a willingness to participate: DEU, DNK, ESP, FRA, GBR, ITA, NLD, POL and TUR. NCIA and NOR became members later.

Mode of operation:

- Two to three meetings (for one to two days) per year and additional workshops when required.
- Workshop Sessions could be organized to spend some time on specific technical topics that may not require all group members to attend.
- In addition to face-to-face meetings, the ability to conduct distance collaboration (VTC, audio conference, …).
- Use of scientific/technical/military experts by the nations as needed.
- Team Leader : a team leader will be elected during the first meeting of the TG.

G.3.2 National and/or NATO Resources Needed

Nations are requested to resource:

- Personnel resources (technical/scientific and military);
- Travel costs;
- Provision/adaptation of their national participating systems/tools.

Nations or NATO are requested to resource:

- Contribution to integration, testing, performing experiments;
- Contribution to the final demonstration and lessons learned report;
- Hosting an implementation.

NATO is requested to resource:

- Provision/modifications to their participating systems and tools if needed;
- Travel costs (e.g. for conferences).

G.4 SECURITY CLASSIFICATION LEVELS

Originally the Security classification levels were set to:

- NATO Unclassified and commercially confidential;
- Recommended for the publication: NATO Unclassified.

Note that it was later decided to expand the classification to:

- Approved for Public Release.

In addition to the above, this manuscript is (check all that apply):

- Releasable to Partner for Peace Nations (PfP);
- Releasable to Mediterranean Dialogue (MD) Nations;
- Releasable to Global Partners;
- Releasable to the following non-NATO countries: All nations.

G.5 PARTICIPATION BY PARTNER NATIONS

The Technical Team work remains open to partner nations.

G.6 LIAISON

- CSO Panels;
- ACT (Allied Command Transformation);
- NC3A (NATO Consultation, Command and Control Agency), now NCIA (NATO Communications and Information Agency);
- MIP DMWG (Multilateral Interoperability Programme Data Modeling Working Group).

A liaison with the MCC conference was established and a presentation was also given for a MAJIIC representative.

G.7 TERMS AND DEFINITIONS

SOA – SOA is a paradigm for organizing and utilizing distributed capabilities that enables the creation of applications that are built by combining loosely coupled and interoperable services to support the

requirements of the business processes. In a SOA environment resources are made available as independent services that can be accessed without knowledge of their underlying platform implementation. The key is independent services with defined interfaces that can be called to perform their tasks in a standard way, without the service having pre-knowledge of the calling application, and without the application having or needing knowledge of how the service actually performs its tasks. In this way, SOA supports the integration and consolidation activities within complex enterprise systems [92].

Annex H – REFERENCES

Section H.1 of this Annex contains the general references as they are used in this report. Section H.2 of this Annex contains a list of publications that have been derived from work of IST-090. Some references in Section H.1 refer to a more detailed reference as provided in Section H.2.

H.1 REFERENCES

[1] A. Gibb, H. Fassbender, M. Schmeing, J. Michalak, and J. E. Wieselthier. Information management over disadvantaged grids. Final report of the RTO Information Systems Technology Panel, Task Group IST-030 / RTG-012, RTO-TR-IST-030, 2007.

[2] W3CWS , http://www.w3.org/TR/ws-arch/#whatis <abb => full).

[3] OMGDDS, http://portals.omg.org/dds/ <abb => full).

[4] NATO Network Enabled Feasibility Study Volume I: Overview of the NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions, version 2.0, 2005.

[5] NATO Network Enabled Feasibility Study Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII), version 2.0, 2005.

[6] M. N. Huhns and M. P. Singh. Service-oriented computing: key concepts and principles. Internet Computing, IEEE, 9(1):75–81, Jan-Feb 2005.

[7] T. Erl. Service-Oriented Architecture — Concepts, Technology, and Design. Prentice hall, 2005.

[8] OASIS. Reference model for service oriented architecture 1.0 OASIS standard, 12 october 2006. C. Matthew MacKenzie, Ken Laskey, Francis McCabe, Peter F. Brown, and Rebekah Metz (eds.), http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf.

[9] Yefim Natis, Gartner Research, "Service-Oriented Architecture Under the Magnifying Glass", Application Integration & Web Service, Summit 2005, April 18-20, 2005.

[10] T. Erl. Service-Oriented Architecture—A Field Guide to Integrating XML and Web Services. Prentice hall, 2004.

[11] J. Bush An Investigation Into Deploying Web Services TN1229, The Hague, December 2006.

[12] NATO Architecture Framework (NAF) version 3.0, June 2007; The Essence of Net-Centricity – A system Implementer's Perspective, Hans Polzer, AFEI DS3WG, October 2006.

[13] Niranjan Suri and Erika Benvegnù, Florida Institute for Human and Machine Cognition, Mauro Tortonesi and Cesare Stefanelli, University of Ferrara, Jesse Kovach, U.S. Army Research Laboratory, James Hanna, U.S. Air Force Research Laboratory; "Communications Middleware for Tactical Environments: Observations, Experiences and Lessons Learned"; IEEE Communications Magazine; October 2009.

[14] NATO Interoperability Standards and Profiles (ADatP-34) Volume 1, Introduction and management, Version 0.94, February 2007.

[15] NATO Network Enabled Feasibility Study Volume I: Overview of the NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions, version 2.0, 2005 and Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII), version 2.0, 2005.

[16] See IST-090 Publications in H.2: IST-090 – 03 [EvalWS].

[17] See IST-090 Publications in H.2: IST-090 – 01 [COMMAG].

[18] Śliwa J., Gleba K., Amanowicz M., "Adaptation Framework foR web services prOvision in tactical environment", MCC 2010: Military Communications and Information Systems Conference, Wrocław, Poland.

[19] See IST-090 Publications in H.2: IST-090 – 08 [MedNetLoad].

[20] See IST-090 Publications in H.2: IST-090 – 02 [DDSDemo].

[21] P. Caban, J.Śliwa, Dedicated WS-DDS Interface for Sharing Information Between Civil and Military Domains. MCC 2011: Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011. In: Military Communications and Information Technology: A Comprehensive Approach Enabler. Editor: M.Amanowicz, Warszawa: Redakcja Wydawnictw Wojskowej Akademii Technicznej, 2011. ISBN 978-83-62954-20-9, s. 27-38 (MK-312).

[22] J. Flathagen and F.T. Johnsen, " Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web Services", IEEE MILCOM 2011.

[23] See IST-090 Publications in H.2: IST-090 – 06 [IQPC IOA2012].

[24] IST-118 Technical Activity Proposal (TAP), Activity Title: SOA recommendations for disadvantaged grids in the tactical domain; Activity Reference Number: IST-118; 2012; NATO-CSO.

[25] W3C. Extensible markup language (XML). http://www.w3.org/XML/.

[26] L. Richardson and S. Ruby. RESTful Web Services. O'Reilly Media, 2007.

[27] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616 (Draft Standard), June 1999. Updated by RFC 2817.

[28] J. Postel. Transmission Control Protocol. RFC 793 (Standard), Sept. 1981. Updated by RFCs 1122, 3168.

[29] E. Skjervold, T. Hafsøe, F. T. Johnsen, and K. Lund. "Delay and disruption tolerant web services for heterogeneous networks," IEEE MILCOM, Boston, MA, USA, October 2009.

[30] J.-C. St-Jacques, "Challenges for a distributed collaborative environment functioning over mobile wireless networks," NATO IST-030/RTG-012 Workshop on Role of Middleware in Systems Functioning over Mobile Communication Networks, 2003.

[31] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi, and S. Weerawarana. Unraveling the Web Services Web, An Introduction to SOAP, WSDL, and UDDI. Internet Computing, IEEE, 6(2):86–93, April 2002.

[32] W3C. Web services glossary W3C working group note 11 february 2004. Hugo Haas and Allen Brown (eds.), http://www.w3.org/TR/ws-gloss/.

[33] J. Cardoso. Semantic Web Services: Theory, Tools and Applications. IGI Global, 2007.

[34] G. Babakhani et al. Web trends and technologies and NNEC core enterprise services —version 2.0. NATO C3 Agency, Technical Note 1143, December 2006.

[35] Web Services Interoperability Organization (WS-I). WS-I organization's web site. http://www.ws-i.org/.

[36] W3C. SOAP specifications. http://www.w3.org/TR/soap/.

[37] OASIS. SOAP-over-UDP version 1.1 OASIS standard 1 july 2009. Ram Jeyaraman (ed.), http://docs.oasis-open.org/ws-dd/soapoverudp/1.1/os/wsdd-soapoverudp-1.1-spec-os.pdf.

[38] R. Cunnings, S. Fell, and P. Kulchenko. SMTP transport binding for SOAP 1.1. http://www.pocketsoap.com/specs/smtpbinding/.

[39] F. T. Johnsen, A. Eggen, T. Hafsøe, and K. Lund. Utilizing military message handling systems as a transport mechanism for soa in military tactical networks. NATO IST-083 Symposium on Military Communications with a special focus on Tactical Communications for Network Centric Operations, Prague, Czech republic, April 2008.

[40] W3C. Web services addressing (ws-addressing) W3C member submission 10 august 2004. Don Box, Francisco Curbera (eds.), http://www.w3.org/Submission/ws-addressing/.

[41] N. A. Nordbotten. XML and Web Services Security. FFI report 2008/00413, 2008. http://rapporter.ffi.no/rapporter/2008/00413.pdf.

[42] W3C. Web services description language (wsdl) version 2.0 - W3C recommendation 26 june 2007. Roberto Chinnici, Jean-Jacques Moreau, Arthur Ryman, and Sanjiva Weerawarana (eds.), http://www.w3.org/TR/wsdl20/.

[43] W3C. Web services description language (wsdl) 1.1 - W3C note 15 march 2001. Erik Christensen, Francisco Curbera, Greg Meredith, and Sanjiva Weerawarana (eds.), http://www.w3.org/TR/wsdl.

[44] OASIS. WS-Notification (2006) tc. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn.

[45] W3C. Web services eventing (ws-eventing) W3C recommendation. Doug Davis, Ashok Malhotra, Katy Warr, and Wu Chou (eds.), http://www.w3.org/TR/ws-eventing/.

[46] OASIS. UDDI Version 3.0.2, UDDI Spec Technical Committee Draft. Luc Clement, Andrew Hately, Claus von Riegen, and Tony Rogers (eds.), http://uddi.org/pubs/uddi_v3.htm, 2004.

[47] T. Min. QoS integration in Web services with the WS-QoS framework. PhD thesis, Freie Universität Berlin, 2005.

[48] OASIS. ebXML registry information model version 3.0 OASIS standard, 2 may, 2005. Sally Fuger, Farrukh Najmi, Nikola Stojanovic (eds.), http://docs.oasis-open.org/regrep/v3.0/specs/regrep-rim-3.0-os.pdf.

[49] J. Schlimmer (editor). Web Services Dynamic Discovery (WS-Discovery). http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf.

[50] OASIS. Web services dynamic discovery (ws-discovery) version 1.1 OASIS standard 1 july 2009. Vipul Modi, and Devon Kemp (eds.), http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.pdf.

[51] Trude Hafsøe, Frank T. Johnsen, Ketil Lund and Anders Eggen. "Adapting web services for limited bandwidth tactical networks", 12th International Command and Control Research and Technology Symposium (ICCRTS), Newport, RI, USA, 2007.

[52] NATO Network Enabled Feasibility Study Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII), version 2.0, 2005.

[53] Frank T. Johnsen and Trude Hafsøe. "Using NFFI Web Services on the tactical level: An evaluation of compression techniques", 13th International Command and Control Research and Technology Symposium (ICCRTS), Seattle, WA, USA, June 2008.

[54] F.T. Johnsen, "Pervasive web services discovery and invocation in military networks", FFI Report 2011/00257, http://rapporter.ffi.no/rapporter/2011/00257.pdf.

[55] CWID home page, http://www.cwid.org.

[56] Joanna Śliwa, Marek Amanowicz, A mediation service for WEB services provision in tactical disadvantaged environment, MILCOM, San Diego, November 17 - 19, 2008.

[57] J. Bush An Investigation Into Deploying Web Services TN1229, The Hague, December 2006.

[58] Raymond Haakseth, Tommy Gagnes, Dinko Hadzic, Trude Hafsøe, Frank T. Johnsen, Ketil Lund and Bård Karsten Reitan. "SOA - cross domain and disadvantaged grids - NATO CWID 2007", FFI report 2007/02301, ISBN 978-82-464-1272-6, 2007.

[59] tide.act.nato.int.

[60] Trude Hafsøe, Frank T. Johnsen, Nils A. Nordbotten and Espen Skjervold. "Using Web Services and XML Security to Increase Agility in an Operational Experiment featuring Cooperative ESM Operations", 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington DC, USA, June 2009.

[61] F.T. Johnsen and T. Hafsøe, “Experiments with Web services at Combined Endeavor”, 15th International Command and Control Research and Technology Symposium (ICCRTS), Santa Monica, CA, USA, June 2010.

[62] See IST-090 Publications in Section H.2: IST-090 - 14 [WSReach].

[63] See IST-090 Publications in Section H.2: IST-090 – 10 [SemDes].

[64] See IST-090 Publications in Section H.2: IST-090 – 13 [WS-DDS].

[65] Johnsen F.T. and Hafsøe T., Service Advertisements in MANETs (SAM): A decentralized web services discovery protocol, Workshop on Ubiquitous Computing and Networks (UbiCoNet), Dec. 2010.

[66] Skjegstad M., Johnsen F.T., Hafsøe T., and Lund K., Robust and efficient service discovery in highly mobile radio networks using the Mist protocol, IEEE Military Communications Conference (MILCOM 2010), Oct. 2010.

[67] J. Flathagen and F.T. Johnsen, " Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web Services", IEEE MILCOM 2011.

[68] "Cross-layer Quality of Service Based Admission Control for Web Services", Frank T. Johnsen, Trude Hafsøe, Mariann Hauge, Øyvind Kolbu, IEEE GLOBECOM workshop HeterWMN 2011, Houston, TX, USA, December 9 2011.

[69] "Robust Web Services in Heterogeneous Military Networks", Ketil Lund, Espen Skjervold, Frank T. Johnsen, Trude Hafsøe, and Anders Eggen, IEEE Communications Magazine, Special Issue on Military communications, October 2010.

[70] OMG Data-Distribution Service for Real-Time Systems. OMG Available Specification, formal/07-01-01.

[71] OMG. "Real-Time Publish Subscribe Protocol – DDS Interoperability Wire Protocol Specification.", available: http://www.omg.org/cgi-bin/doc?formal/10-11-01.pdf.

[72] Dr. Douglas C. Schmidt, Dr. Angelo Corsaro, and Hans van't Hag, Addressing the Challenges of Tactical Information Management in Net-Centric Systems With DDS, CROSSTALK - The Journal of Defense Software Engineering, 2008.

[73] OMG Data-Distribution Service for Real-Time Systems. OMG Available Specification, formal/07-01-01.

[74] OMG, The Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification (DDS-RTPS, Version 2.1, 2009.

[75] RTI. The Data-Centric Future, www.rti.com, 2006.

[76] PrismTech, RTI, TwinOaks, DDS InteroperabilityDemo, 2009, Available: http://www.omg.org/news/meetings/GOV-WS/pr/rte-pres/ddsi-demo.pdf.

[77] Fortuna, C.; Mohorcic, M., "Trends in the development of communication networks: Cognitive networks," Computer Networks, 53(9), 1354–1376, 2009.

[78] Srivastava, V.; Motani, M., "Cross-layer design: A survey and the road ahead," Communications Magazine, IEEE, 43(12), 112–119, 2005.

[79] Suri, N.; Benvegnu, E.; Tortonesi, M.; Stefanelli, C.; Kovach, J.; Hanna, J., "Communications middleware for tactical environments: Observations, experiences, and lessons learned," Communications Magazine, IEEE, vol.47, no.10, pp.56-63, October 2009.

[80] Barz, C.; Jansen, N.; Thomas, D., "Middleware for Tactical Military Networks," Military Communications and Information Systems Conference, MCC 2010, September, Wroclaw, Poland.

[81] Riihijärvi, J.; Petrova, M. & Mähönen, P. "A Common Application Requirement Interface for Cognitive Wireless Networks," 4th IEEE Workshop on Networking Technologies for SDR Networks in conjunction with SECON 2009, 2009.

[82] Fall, K. “A delay-tolerant network architecture for challenged internets,” Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications, SIGCOMM '03, Karlsruhe, Germany, 2003.

[83] Cerf, V., et al. “Delay-tolerant networking architecture,” IETF, RFC 4838, 2007.

[84] M. Weiser; "The Computer for the 21st Century"; Scientific American special Issue on Communications, Computers, and Networks; USA, 1991.

[85] ITU-T Recommendation G.1010, Series G: Transmission systems and media, digital systems and networks. Quality of service performance. End – user multimedia QoS categories, ITU 2002.

[86] P. F. Patel-Schneider, I. Horrocks, OWL Web Ontology Language Semantics and Abstract Syntax Section 2. Abstract Syntax, 2004, http://www.w3.org/TR/owl-semantics/syntax.html.

[87] I. Horrocks et al., SWRL: A Semantic Web Rule Language. Combining OWL and RuleML, W3C Member Submission 21 May 2004, http://www.w3.org/Submission/SWRL/.

[88] J. Sliwa, K. Gleba, W. Chmiel, P. Szwed, A. Glowacz, IOEM- ontology engineering methodology for large systems, Lecture Notes in Computer Science, volume 6922, 2011.

[89] A. Tarski, Introduction to Logic and to the Methodology of Deductive Sciences, Second Edition, Dover Publications, Inc., New York 1946, ISBN 0-486-28462-X.

[90] M. van Selm, A. van der Zanden, P. Copeland, M. Winkler, Infrastructure-Free Information Exchange At Combined Endeavor 2009 - Final Reviewed Draft, NC3A Technical Note 1426, 2009.

[91] A mediation service for web services provision in tactical disadvantaged environment, Joanna Sliwa, Marek Amanowicz, Military Communication Institute, 05-130 Zegrze, Poland, 2008.

[92] IST-061 Secure Service Oriented Architectures (SOA) Supporting NEC, NATO-RTO Research task Group, 2008.

H.2 PUBLICATIONS DERIVED FROM WORK OF IST-090

IST-090 - 01 [COMMAG] “Robust Web Services in Heterogeneous Military Networks”, Ketil Lund, Espen Skjervold, Frank T. Johnsen, Trude Hafsoe and Anders Eggen, IEEE Communications Magazine, Special Issue on Military communications, October 2010.

IST-090 - 02 [DDSDemo] “DDS technology demonstrations related to IST-090”, IST-090 members: Hernández Novo, Ignacio; Meiler, Peter-Paul; Shaw Manero, Luis. MCC 2011, 17-18 October 2011, Amsterdam, NLD. ESP contribution.

IST-090 - 03 [EvalWS] “An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield”, Magnus Skjegstad, Frank T. Johnsen, Trude Hafsøe. MCC 2011, 17-18 October 2011, Amsterdam, NLD. NOR contribution.

IST-090 - 04 [IST-090ICCRTS] “IST-090 SOA Challenges for Disadvantaged Grids”, Annunziata, Francesca; Ardic, Burcu; Denis, Xavier; Fletcher, Graham; Hafsøe, Trude; Hernández Novo, Ignacio; Jansen, Norman; Johnsen, Frank Trethan; Meiler, Peter-Paul; Owens, Ian; Sasioglu, Betül; Sliwa, Joanna; Stavnstrup, Jens; Tokuz, Akif, 15 International Command and Control Research and Technology Symposium (ICCRTS) – The Evolution of C2, Santa Monica, June 2011, USA. IST-090 team contribution.

IST-090 - 05 [IQPC IOA2011] “An overview of IST-090 - SOA Challenges for Disadvantaged Grids”, P.P. Meiler, Interoperable Open Architecture Conference, 26 - 28 October 2011, London, GBR. http://www.iqpc.com/Event.aspx?id=659378. IST-090 chair contribution.

IST-090 - 06 [IQPC IOA2012] “IST-118 SOA recommendations for disadvantaged grids in the tactical domain”, P.P. Meiler, Interoperable Open Architecture Conference, 30 - 31 October 2012, London, GBR. http://www.iqpc.com. IST-090 chair contribution.

IST-090 - 07 [MCC2011] “An overview of the research and experimentation of IST-090: SOA over Disadvantaged Grids”, IST-090 team. Military Communications and Information Technology Conference (MCC), 17-18 October 2011, Amsterdam, NLD. IST-090 team contribution.

IST-090 - 08 [MedNetLoad] “Mediation of network load over disadvantaged grids using Enterprise Service Bus (ESB) technology”, IST-090 member Leon Schenkels. Rui Fiske, NC3A and Tomasz Rogula, NC3A. MCC 2011, 17-18 October 2011, Amsterdam, NLD. NATO C3 Agency contribution.

IST-090 - 09 [Pervasive] “Pervasive Web Services Discovery and Innovation in Military networks”, Frank T. Johnsen, FFI Report 2011/00257, January 2011.

IST-090 - 10 [SemDes] “Semantic description of QoS framework for context–aware Web Service provision”, IST-090 member Joanna Śliwa. Marek Amanowicz, Military Communication Institute. ul. Warszawska 22a, 05-130 Zegrze, Poland, m.amanowicz@will.waw.pl. MCC 2011, 17-18 October 2011, Amsterdam, NLD. POL contribution.

IST-090 - 11 [SemModCon] “Semantic Model for Context-Aware Service Provision in Disadvantaged Network Environment”, J.Sliwa, M.Amanowicz, Semantic & Domain Based Interoperability Symposium, IST – 101/RSY-024, 7-8.11.2011, Oslo, NOR.

IST-090 - 12 [TacMiddle] “Towards a Middleware for Tactical Military Networks – Interim Solutions for Improving Communication for Legacy Systems”. IST-090 members Christoph Barz and Norman Jansen, Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Neuenahrer Straße 20, 53343 Wachtberg, Germany. MCC 2011, 17-18 October 2011, Amsterdam, NLD. DEU contribution.

IST-090 - 13 [WS-DDS] “WS-DDS Interface (gateway) for tactical network”, IST-090 members Przemyslaw Caban, Joanna Sliwa. MCC 2011, 17-18 October 2011, Amsterdam, NLD. POL contribution.

IST-090 - 14 [WSReach] “Independent evaluation of a number of published approaches that purport to improve the reach of Web Services into locations with disadvantaged networks”. IST-090 members Graham Fletcher and Ian Owens. Antonio Hidalgo Lander, Cranfield Defence and Security. Defence Academy of the United Kingdom. Shrivenham, SN6 8LA, UK. MCC 2011, 17-18 October 2011, Amsterdam, NLD. GBR contribution.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-IST-090 AC/323(IST-090)TP/520	ISBN 978-92-837-0195-8	UNCLASSIFIED/ UNLIMITED

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

SOA Challenges for Real-Time and Disadvantaged Grids

7. Presented at/Sponsored by

Final Report of TR-IST-090.

8. Author(s)/Editor(s)	9. Date
Multiple	April 2014
10. Author's/Editor's Address	**11. Pages**
Multiple	122

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Common distributed databases	Line-of-sight	Reliability
Cross-layer design	Low bandwidth	Service discovery
Data Distribution Services (DDS)	Military operations	Service-Oriented Architecture (SOA)
Demonstration	Mobile Ad-Hoc Network (MANET)	Tactical level
Disadvantaged grid	Near-real-time	Web Services (WS)
Interoperability	Performance	

14. Abstract

The Service-Oriented Architecture (SOA) paradigm has been chosen by NC3B as the recommended method to achieve interoperability at the information infrastructure level within NATO. Current technologies to implement SOA were designed for civilian use over robust, high-bandwidth networks and consequently not designed to work over the disadvantaged grids that are employed at the military tactical level. This makes it hard to achieve interoperability among the Nations in the battle space.

The disadvantaged grids that IST-090 considered are mobile ad-hoc networks that are characterized by line-of-sight connections, low bandwidth, intermittent availability, etcetera.

IST-090 identified improvements to make SOA work while using disadvantaged grids and built demonstrations that show how the challenges that arise because of the use of disadvantaged grids in near-real-time, as is the case at the tactical level in military operations, can be mitigated. IST-090 used a concrete military scenario as a global context for the study.

Areas of research included: efficient communication frameworks, mechanisms to reduce needed bandwidth and mechanisms to improve reliability. IST-090 specifically considered the following technologies: Web Services and Service Discovery, Data Distribution Services, Common Distributed Databases and Cross-layer design.

The results demonstrated that SOA can be applied at lower levels than previously thought.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

CANADA
DSIGRD2 – Bibliothécaire des ressources du savoir
R et D pour la défense Canada
Ministère de la Défense nationale
305, rue Rideau, 9e étage
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
SDG TECIN / DGAM
C/ Arturo Soria 289
Madrid 28033

ESTONIE
Estonian Ministry of Defence
Estonian National Coordinator for NATO STO
Sakala 1
Tallinn 15094

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc - BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALIE
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Knowledge and Information
Services
Building 247
Porton Down, Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

CANADA
DRDKIM2 – Knowledge Resources Librarian
Defence R&D Canada
Department of National Defence
305 Rideau Street, 9th Floor
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian Ministry of Defence
Estonian National Coordinator for NATO STO
Sakala 1, Tallinn 15094

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc - BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GRECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALY
Centro Gestione Conoscenza
Secretariat General of Defence
National Armaments Directorate
Via XX Settembre 123/A, 00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6, 061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen
M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
SDG TECIN / DGAM
C/ Arturo Soria 289
Madrid 28033

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Knowledge and Information Services
Building 247
Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-0195-8