NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-118)TP/908

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-118**

SOA Recommendations for Disadvantaged Grids in the Tactical Domain

(Recommandations de SOA concernant les réseaux défavorisés dans le domaine tactique)

Final Report of RTG IST-118.

Published May 2020

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-118)TP/908

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-118**

SOA Recommendations for Disadvantaged Grids in the Tactical Domain

(Recommandations de SOA concernant les réseaux défavorisés dans le domaine tactique)

Final Report of RTG IST-118.

Edited by
Trude H. Bloebaum (NOR)
Frank T. Johnsen (NOR)
Peter-Paul Meiler (NLD)

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 May 2020

ISBN 978-92-837-2233-5

Table of Contents

List of Figures

List of Tables

List of Acronyms

C2IS	Command and Control Information Systems
CES	Core Enterprise Services
CFI	Connected Forces Initiative
CIA	Confidentiality, Integrity, and Availability
CIS	Communication and Information Systems
CNR	Combat Network Radio
CoNSIS	The Coalition Network for Secure Information Sharing
CORE	Common Open Research Emulator
COTS	Commercial off-the-shelf
DIL	Disconnected, Intermittent, and Limited
DSTL	Defence Science and Technology Laboratory
ebXML	Electronic Business Using XML
ESB	Enterprise Service Bus
FMN	Federated Mission Networking
FMV	Full Motion Video
JSON	JavaScript Object Notation
LOS	Line-of-Sight
MDC	Mobile Deployable Communications
NEC	Network Enabled Capabilities
NISP	NATO Interoperability Standards and Profiles
NNEC	NATO Network Enabled Capabilities
OASIS	Organization for the Advancement of Structured Information Standards
PER	Packet Error Rate
QoS	Quality of Service
REST	Representational State Transfer
SATCOM	Satellite Communication
SMC	Service Management and Control
SOA	Service Oriented Architecture
TIDE	Technology for Information, Decision and Execution superiority
TTB	TIDE Transformational Baseline
UDDI	Universal Description, Discovery and Integration
VTC	Video Teleconferencing

W3C	World Wide Web Consortium
WS-Discovery	WS-Dynamic Discovery
WSDL	Web Services Description Language
XML	eXtensible Markup Language

IST-118 Membership List

CHAIR

Mr. Peter-Paul MEILER,
TNO Defence, Safety and Security
NETHERLANDS
Email: peter-paul.meiler@tno.nl

MEMBERS

Mr. Christoph BARZ
Fraunhofer Institute for Communication-FKIE
GERMANY
Email: christoph.barz@fkie.fraunhofer.de

Dr. Jose Alcaraz CALERO
University of the West of Scotland (UWS)
UNITED KINGDOM
Email: josemaria.alcarazcalero@uws.ac.uk

Prof. Christos GRAIKOS
University of the West of Scotland
GREECE
Email: christos.grecos@uws.ac.uk

Ms. Trude Hafsoe BLOEBAUM
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: trude-hafsoe.bloebaum@ffi.no

Mr. Norman JANSEN
Fraunhofer Institute for Communication-FKIE
GERMANY
Email: norman.jansen@fkie.fraunhofer.de

Dr. Frank T. JOHNSEN
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: frank-trethan.johnsen@ffi.no

Mr. Marco MANSO
TEKEVER Communication Systems
PORTUGAL
Email: marco.manso@tekever.com

Mr. Daniel MARCO-MOMPEL
NCIA
SPAIN
Email: daniel.marco-mompel@ncia.nato.int

Mr. Ian OWENS
Cranfield University Defence Academy
UNITED KINGDOM
Email: i.owens@cranfield.ac.uk

Ms. Ayse Betul SASIOGLU
TUBITAK Scientific and Technical Research Council
TURKEY
Email: betul.sasioglu@uekae.tubitak.gov.tr

Dr. Joanna SLIWA
Military Communication Institute (MCI)
POLAND
Email: j.sliwa@wil.waw.pl

Dr. Qi WANG
University of the West of Scotland (UWS)
UNITED KINGDOM
Email: Qi.Wang@uws.ac.uk

ADDITIONAL CONTRIBUTORS

Dr. Kevin S. CHAN
US Army Research Laboratory (ARL)
UNITED STATES
Email: kevin.s.chan.civ@mail.mil

SOA Recommendations for Disadvantaged Grids in the Tactical Domain

(STO-TR-IST-118)

Executive Summary

The Service Oriented Architecture (SOA) Paradigm has been chosen by the NATO C3 Board as the method to achieve interoperability at the information infrastructure level. The current technologies used to implement SOA (e.g., Web Services, which is our focus) 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 battlespace.

IST-118 provides guidance on which technical modifications should be utilized in several different types of disadvantaged grids that are utilized by NATO member states. IST-118 builds on the findings by IST-090, which demonstrated that SOA can function better in disadvantaged conditions than previously thought. IST-090 also identified SOA challenges for real-time and disadvantaged grids and suggested technical modifications that can be used to overcome those challenges.

The work of IST-118 was performed in synergy with SOA-related specification and profiling work done as part of other NATO efforts such as Network Enabled Capabilities (NEC) and Federated Mission Networking (FMN). We reached our goal of involving the NATO and academic research community by publishing papers, presenting at conferences and providing demonstrations.

We focused on generating concrete recommendations for a subset of the core services from the NATO C3 Taxonomy, based on systematic testing and evaluation, rather than providing higher level recommendations for a wider set of services. This ensures that our work can have a direct impact on NATO operations.

For each of the chosen services we provide an overview of the current situation with respect to standardization and identify the main challenges of deploying these services in the tactical domain. Based on the results of our experiments (both real-life, emulated and combined), we identify possible optimizations, and provide recommendations for deployment of these services over disadvantaged grids. We also determined which further challenges remain for each of the services and recommend a road ahead.

Our real-life experiments were limited to the use of tactical broadband radios. Though we have emulated narrowband links, it would be preferable to perform further experiments using actual radios. Also, experiments in hybrid networks consisting of both broad- and narrowband radios would give an extra dimension to any recommendations given.

Also, we have focused on SOAP services in IST-118. Though we have some minor efforts related to REST, such services need further scrutiny in the tactical domain. As a consequence, we have proposed a follow-on group to IST-118 that should delve into the realm of both SOAP and REST services in hybrid tactical networks. At the time of finalizing this report, NATO CSO has approved RTG IST-150 to implement this research.

Note: Disadvantaged Grids are communication networks limited by line-of-sight connections, low bandwidth, intermittent availability, etc.

Recommandations de SOA concernant les réseaux défavorisés dans le domaine tactique

(STO-TR-IST-118)

Synthèse

Le paradigme de l'architecture orientée services (AOS – SOA en anglais) a été choisi par le Bureau des C3 de l'OTAN comme méthode permettant d'atteindre l'interopérabilité au niveau de l'infrastructure de l'information. Les technologies servant actuellement à mettre en œuvre la SOA (par exemple, les services web, notre sujet d'intérêt) 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 dans l'espace opérationnel.

L'IST-118 fournit des conseils sur les modifications techniques à apporter à différents types de réseaux défavorisés qui sont utilisés par les pays membres de l'OTAN. L'IST-118 s'appuie sur les conclusions de l'IST-090, qui a démontré que la SOA pouvait mieux fonctionner en conditions défavorables que ce que l'on pensait auparavant. L'IST-090 a également identifié les défis de la SOA sur les réseaux défavorisés et en temps réel, et a suggéré des modifications techniques pour surmonter ces problèmes.

Le travail de l'IST-118 a été réalisé en synergie avec la spécification relative à la SOA et le profilage effectué dans le cadre d'autres travaux de l'OTAN, tels que la capacité réseau-centrique (NEC) et le réseau de mission fédéré (FMN). Nous avons atteint notre but, qui consistait à impliquer l'OTAN et la communauté de la recherche universitaire, en publiant des articles, en réalisant des présentations lors de conférences et en effectuant des démonstrations.

Nous nous sommes attachés à formuler des recommandations concrètes pour un sous-ensemble des services centraux issus de la taxonomie C3 de l'OTAN, recommandations fondées sur des essais et une évaluation systématiques, au lieu de fournir des recommandations de niveau supérieur pour un ensemble de services plus large. De la sorte, notre travail pourra avoir un effet direct sur les opérations de l'OTAN.

Nous donnons une vue d'ensemble de l'état de la normalisation de chacun des services choisis et identifions les principaux défis liés à leur déploiement dans le domaine tactique. À partir des résultats de nos expériences (à la fois en conditions réelles, par l'émulation et en associant les deux), nous identifions les optimisations possibles et émettons des recommandations pour le déploiement de ces services sur les réseaux défavorisés. Nous avons également déterminé les défis restants pour chacun des services et recommandons une voie à suivre.

Nos expériences en conduitions réelles se sont limitées à l'utilisation de radios tactiques à large bande. Bien que nous ayons émulé des liaisons en bande étroite, il serait préférable de réaliser d'autres expériences à l'aide de radios réelles. De plus, des expériences sur des réseaux hybrides composés de radios à bandes large et étroite donneraient une dimension supplémentaire à toute recommandation.

L'IST-118 s'est également concentré sur les services SOAP (Simple Object Access Protocol). Même si nous avons de petits travaux liés à REST (Representational State Transfer), ce type de service doit être examiné de plus près dans le domaine tactique. En conséquence, nous avons proposé un groupe de suivi de l'IST-118, qui devrait approfondir le domaine des services SOAP et REST sur les réseaux tactiques hybrides.

Au moment de l'achèvement du présent rapport, le CSO de l'OTAN a approuvé la création du RTG-150 pour mettre en œuvre les recherches en question.

Nota : les réseaux défavorisés sont des réseaux de communication limités par la portée visuelle, par la largeur de la bande passante, par une disponibilité intermitente, etc.

SOA RECOMMENDATIONS FOR DISADVANTAGED GRIDS IN THE TACTICAL DOMAIN

1.0 INTRODUCTION

This report presents the work done by the NATO CSO IST-118 research task group "SOA Recommendations for Disadvantaged Grids in the Tactical Domain."

1.1 Scope

The Service-Oriented Architecture (SOA) approach has been chosen by the NATO C3 Board as the recommended method to achieve information interoperability in NATO. Especially, utilizing a service-oriented approach can help increase the level of interoperability between independent systems by leveraging agreed upon interfaces. However, Web Services technology was originally designed for civil use over robust, high-bandwidth networks, and it was clear that it could not properly function in the deployed military environment, which suffers in many instances from inadequate or unstable connectivity. This fact remains a major impediment to achieving interoperability among the nations in the battlespace.

IST-118 is the second IST research task group to focus on SOA in the tactical domain. The primary objective of IST-090, the predecessor to IST-118, was to identify challenges and show how to make SOA applicable at the tactical level. The results of IST-090 created an awareness of the challenges related to extending a SOA to tactical networks and provided some possible solutions. The results also demonstrated that SOA can function better in disadvantaged conditions than previously thought.

IST-118 builds on the findings from IST-090, which focused on SOA challenges for real-time and disadvantaged grids. The aim of IST-090 was not only to identify the challenges that arise when one applies the service-oriented paradigm in limited capacity networks, but also to suggest technical modifications that can be used to overcome those challenges. IST-118 builds upon the findings of IST-090 and aims to provide guidance on which technical modifications should be utilized in a number of different types of disadvantaged grids.

An important goal for IST-118 is to ensure that the work performed by the group was not done in isolation, but rather in synergy with the SOA-related specification and profiling work done as part of other NATO efforts such as Network-Enabled Capabilities (NEC) and Federated Mission Networking (FMN).

The scope of investigating SOA in the tactical domain is quite large, and the IST-118 group members agreed to limit the focus area of the group to a specific set of services. The rationale behind this decision was that it would be more useful to be able to give concrete recommendations for some services, based on systematic testing and evaluation, rather than give more high-level recommendations for a wider set of services. IST-118 has thus focused on a subset of the core services from the NATO C3 Taxonomy [1].

1.2 Introduction to the IST-118 Team

IST-118 was, as previously mentioned, a follow-on to IST-090. A subset of the members from IST-090, namely DEU, GBR, NLD, NOR and POL were the initial members of IST-118. Most of these nations were represented by the same organizations as those who participated in IST-090, but GBR later increased their participation by bringing in both an industry and an academic national partner. Additionally, the USA later joined the group.

1.3 Scope and Structure of This Report

This report provides an overview of the work done by IST-118, including recommendations based on national efforts. As the results that form the basis for the recommendations provided in this report have been

documented through a number of peer reviewed publications, we have chosen to not include all the details of the technical experiments in this final report, but rather provide references to the publications where applicable.

Section 2 describes the methodology on which we have based our work. This includes information about the operational scenario used as a background for experiments, the different types of network technologies we have considered, and information about our approach to testing and evaluation.

Section 3 gives a short introduction to the concept of core services, and how the work done in IST-118 relates to other NATO efforts on SOA. This includes information about which core services we have considered in IST-118.

Section 4 contains the actual recommendations for each of the services IST-118 has addressed. For each service we give an overview of the current situation with respect to standardization, and identify the main challenges of deploying these services in the tactical domain. Based on this we identify possible optimizations, and give our recommendations. We also look at which further challenges remain for each service, and recommend a road ahead.

Section 5 describes all the activities that have taken place as a part of IST-118. In addition to the normal group meetings, this includes several workshops, presentations to other communities and the publications the group has produced.

2.0 METHODOLOGY

This section covers the methodology the group adopted for its research and experiment work. First, we agreed on the purpose of the work, and then we developed a spiral approach to experimentation. This approach was used for all activities in the group's testing and evaluation.

2.1 Purpose

The main purpose of the work is to create recommendations for how to support SOA in the tactical domain. In short, this means giving recommendations for how to adapt services to the network limitations found in this domain. The services we seek to give recommendations for are primarily the common infrastructure services that are needed in a service-oriented distributed system.

A recommendation is a suggestion for how one should adapt the core services before deploying them in a tactical network. As there are large variations in the networking conditions services experience when running over the different networking technologies that are used in the tactical domain, a recommendation will consist of a number of different adaptations that should be applied in different use cases.

To improve the performance of Web Services in tactical networks, it is important to understand their limitations. The DIL concept refers to three characteristics of a network: Disconnected, Intermittent and Limited, as shown in Figure 1:

- **Disconnected:** Military units that participate in a tactical network may be highly mobile and may disconnect from a network either voluntarily or not. Unplanned loss of connectivity can be due to various reasons, such as loss of signal or equipment malfunction. The term *disconnected* refers to the fact that units may be disconnected for a long time, possibly for multiple hours or even days.
- **Intermittent:** Units operating in a DIL environment may lose connection temporarily before reconnecting again. The duration can range from milliseconds to seconds. As an example, consider a military vehicle that is driving on a countryside road. It may temporarily lose connection due to the signal being obstructed by trees beside the road, driving into tunnels or having a bad radio signal.

- **Limited:** Limited refers to various ways a network can be constrained. The available data rate may be low, the network delay may be high, and the packet error rate (PER) may be high. The term *data rate* refers to the speed that data that can be transmitted over a network. Delay means the time it takes for data to travel from machine to machine. The PER refers to the percent of packets being sent incorrectly due to the data being erroneous altered in transmission. A packet is considered as incorrect if at least one bit error in the data occurs.

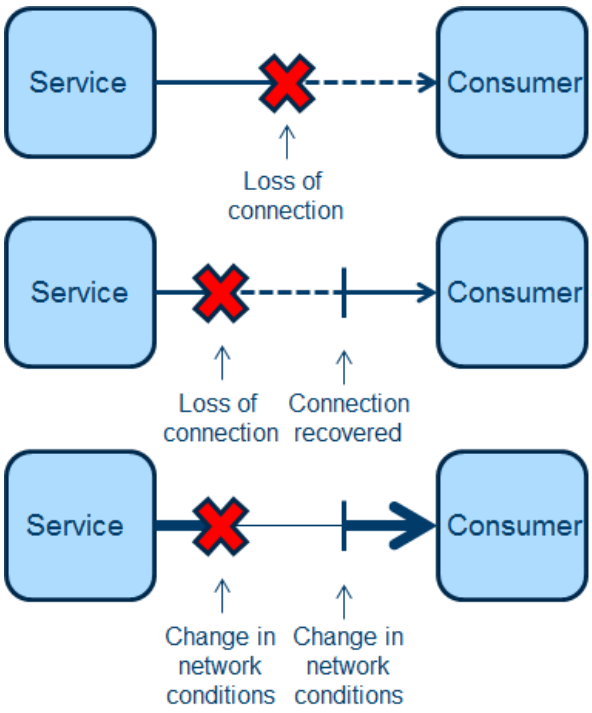


Figure 1: DIL Networks, from Top to Bottom: D (Disconnected), I (Intermittent) and L (Limited).

In addition to network limitations, other factors may also limit communication for military units. As an example, consider a military foot patrol that is operating out in the field. To communicate critical information with other units they use radios. The radio communication equipment is powered by batteries, which the soldiers have to carry with them. Running applications and the sending and receiving of data can consume a considerable amount of power. Thus, the battery could be a scarce resource for units operating in a DIL environment.

2.2 Spiral Approach

When addressing how to support SOA in the tactical domain there are a number of different services that need to be investigated. Additionally, for each service there are also a large number of possible adaptations that must be investigated to determine their suitability as optimizations in different network types. The goal for IST-118 is to give recommendations based primarily on experimental results, so we decided to use an incremental spiral approach to organize our experiments.

In each spiral we aimed to test one specific service, after having identified a scenario or use case appropriate for that service. We would then test one or more optimizations for that service and apply that to at least one representative networking topology. We tested the optimizations using both synthetic environments and real communications equipment using a common scenario for the experiments. We also defined a number of network parameter configurations that we used across tests to ensure that the results from each spiral

would be comparable. The common scenario, the network configurations and experiment setup are further described in the following sections.

The number of different experiments performed varied per service; some services were tested in multiple experiments in order to test different optimizations, while others were only tested once. The experiments performed and results achieved are described further in Section 4.

2.3 Scenario

The Coalition Network for Secure Information Sharing (CoNSIS) [2] was one of the first examples of an international collaboration project which performed extensive tests of Web Services technology in a real tactical environment. As part of this project an operational scenario, suitable in size for being deployed on real radio systems and intended to showcase the flexibility of SOA-based systems was developed. IST-118 chose to use a modified version of this scenario as the operational setting for the group's experiments.

In the original scenario, two vehicle convoys from two different nations need to collaborate to solve a common mission, which is escorting a civilian aid convoy through an area with a high hostile activity level. As the two convoy elements are from different nations, they have different technical systems both with respect to communications equipment and software systems. In order to be able to exchange information between the applications used in either convoy, Web Services technology was used [3].

CoNSIS included a significant networking focus, which meant that the scenario included steps which require the use of prototype multi-topology routing and other advanced networking features that are not commonly supported by today's military communications equipment. The topology of the underlying network changed during the experiment, and the information flow between the applications was altered on the fly to ensure efficient information as the network topology changed.

In IST-118 we do not have the same networking focus as in CoNSIS, but we rather look at service adaptations that can be utilized at the service level. Because of this, IST-118 uses a simplified version of this same scenario that better corresponds to the fact that our main focus is on the interoperability and optimization of services.

The modified CoNSIS scenario used during the IST-118 experiments includes two convoys, each consisting of four vehicles, which exchange information internally between the nodes, but also make this information available to others. This is done by the lead vehicle in each convoy, which aggregates the convoy internal information, and reports this to its own national headquarters through a reach-back link. The information is then shared with partner nations at the headquarters level, and the national headquarters are then responsible for distributing this information as needed within their own nation. Note that the technologies we test in IST-118 do not rely on information being shared in such a hierarchical manner, but as this deployment illustrates how the information flow between services needs to traverse multiple hops across hybrid networks, it is well suited for testing service optimizations suitable at different points in the service deployment.

2.4 Network Types

IST-118 has defined the following network types for use in our experiments. These have been chosen because they represent technologies that are relevant at the tactical edge. Note that the network configurations given in Figure 2 are intended to provide the services we investigate with realistic network behavior as seen from the application layer, and they are thus not intended to be completely accurate representations of any given networking technology.

The last column in Figure 2 shows the primary deployment of the different networking technologies. This is further illustrated in Figure 3, which shows the different network technologies applied in an operational scenario. Here, a typical satellite communication (SATCOM) link and a line-of-sight (LOS) link is shown

functioning at transit or reach-back links for information traveling from the tactical domain and back to the backbone networks.

Network	Data Rate	Delay	PER	Type of Network
Satellite Communications (SATCOM)	250 kbps	550 ms	0	Transit
Line of Sight (LOS)	2 Mbps	5 ms	0	Transit
WiFi 1	2 Mbps	100 ms	1 %	Tactical edge
WiFi 2	2 Mbps	100 ms	20 %	Tactical edge
Combat Net Radio (CNR) with Forward Error Correction (FEC)	9.6 kbps	100 ms	1 %	Transit

Figure 2: Network Parameters for the Five Network Types Used in the IST-118 Experiments.

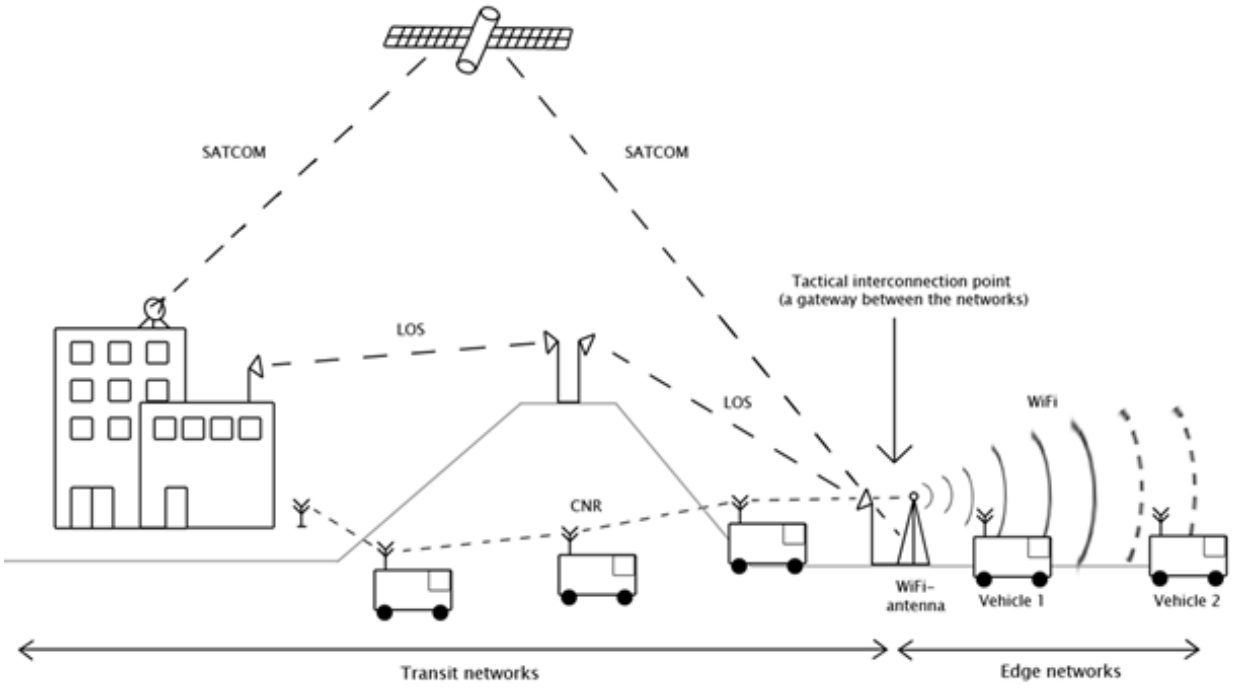


Figure 3: Different Network Technologies Used as Either a Transit Network or an Edge Network.

The combat network radio (CNR) can be used as a transit network, as shown in the figure, but can also be utilized as the primary network at the tactical edge. WiFi technology can also be utilized in a military context, but then primarily to provide a local communication capability. In the IST-118 experiments, we used two different WiFi configurations, one indicating operation in the "sweet spot" (less than 100 m range, called WiFi1) and one indicating operating near the edge of network reach (more than 100 m range, called WiFi2).

2.5 Testing and Evaluation

Our tests have been made in several ways:

1) We have investigated solutions in lab environments, leveraging network emulation with Netem [4] to support the above-mentioned network characteristics.
2) We have leveraged the Common Open Research Emulator (CORE) [5] for large-scale tests in a cloud-enabled lab environment.
3) We have performed experiments using actual radio equipment.

Netem is built into the kernel of modern Linux distributions, so it is quite easy to get started with. It is a tool that allows you to control the characteristics of an emulated link, hence the name "network emulator" or "Netem" for short. This tool is handy for evaluating protocols across a point-to-point link, but does not allow for more elaborate tests involving mobility or multi-hop networking. For such scenarios more advanced tools are needed, e.g., CORE.

CORE is an open source project being developed by the US Naval Research Laboratory. It allows emulating complex networks, and also allows hybrid setups where a part of the network is emulated in CORE and a part of the network consists of actual physical nodes. In IST-118 we used an instance of CORE installed, maintained and operated at UWS, leveraging their expert knowledge on emulation and cloud computing to enable us to run large-scale emulations in their testbed. This instance of CORE was a valuable tool during the group's work.

As for radios, each nation has considered national resources and some have provided their national resources for testing in context of the group's experimentation. Examples here include Rinicom PodNode from the UK and KDA WM600 from Norway.

3.0 SERVICES

The goal of IST-118 is to generate recommendations for how to support the SOA concept in tactical networks by suggesting optimizations to the various services we expect to need support for at the tactical level. In our work, we have utilized the definitions from the Organization for the Advancement of Structured Information Standards (OASIS) reference model for SOA [6] for what SOA and services are:

- "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."
- "A service is a mechanism to enable access to resources, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description."

Due to the importance of prescribed interfaces, the group has looked closely at NATO's work and recommendations in this area. Hence, we do not do our work in isolation, but build on the work done elsewhere in NATO and by the nations and look at how to make the services identified there applicable to the tactical domain while retaining interoperability with the non-adapted versions of the standards.

3.1 NATO Core Services

NATO has for a number of years been providing guidance on the usage of Web service technology in federated environments. Here, the term "Web Services" refers to the technology first defined by the

World Wide Web Consortium (W3C), which is, standardized interfaces (using the Web Services Description Language (WSDL)), standardized messaging (using SOAP), all realized using eXtensible Markup Language (XML) serialization. The NATO NEC (NNEC) was the first effort to identify the SOA paradigm, implemented primarily as Web Services, as a key enabler for interoperability between partners [7]. As a part of this effort the concept of Core Enterprise Services (CES) arose as a way of identifying and categorizing common functionality that a large number of Web Services will depend upon. These CES can been seen as shared components of the service infrastructure that should be available throughout the enterprise, as they provide a uniform means of access to central functionality such as discovery of services, message routing and translation, and messaging security.

Both NNEC and the more recent FMN initiatives focus on interoperability at the strategic and operational levels, where network resources are abundant. Due to this, the standards recommended for realization of the various CES are chosen based on their suitability as a federation mechanism, rather than their resource consumption.

3.1.1 Technical Background

Web Services technology is in widespread use, both commercially and in the military domain. The main benefit of using Web Services is that they enable loose coupling, i.e., that services and clients can be developed independently of each other, but still be interoperable due to the explicitly defined interfaces the technology is based on. “Web Services” is a term that is generally applied to services built using Web technologies, and encompasses many different approaches. Here, we look at two such technologies; Simple Object Access Protocol (SOAP) and Representational State Transfer (REST).

SOAP is a transport layer independent messaging protocol that provides an envelope for sending information via a network [8]. It is the messaging protocol used in W3C’s Web Services [9], and forms the basis of a complete and standardized message-oriented middleware using XML. In SOAP Web Services one standardizes on the service interface according to SOA principles.

REST is a software architecture style that incorporates a set of principles that determine how networked resources should be defined and addressed. A RESTful architecture uses the HTTP operations GET, POST, PUT, or DELETE to exchange information via the network [10]. REST also permits many different data formats unlike SOAP which is XML only. The data format most commonly used with REST is JavaScript Object Notation (JSON).

The current trend in civil systems is to leverage both SOAP and REST technology where applicable. For example, SOAP is the single most used technology for realizing a SOA today, and the technology benefits from mature standards and proven interoperability across vendors, operating systems, and programming languages. SOAP’s main strength is in machine-to-machine communication, and its XML foundation makes it easy to parse and process. REST is also much used, but for slightly different purposes. For example, it is natively supported by all smart devices. Also, it is used from clients written in JavaScript, where JSON is much easier to work with than XML. REST is very straightforward to use since it builds directly on HTTP constructs, and it is often used for simplistic point-to-point connections where one needs to submit data to a server’s database, for example. So, in short, SOAP is good for the infrastructure whereas REST is employed nearer to the user. Given a holistic approach to building an information infrastructure, it makes sense to build on the standardized, proven SOAP. Acknowledging the need for the occasional REST client, one can accommodate those by writing REST wrappers to the existing SOAP services. Similarities and differences between the technologies are discussed further below.

3.1.2 W3C’s Web Services – NATO’s Choice

Web Services are currently identified as the technology that should be used to achieve interoperability with respect to machine-to-machine message-oriented information exchange in NATO, both for request/response

and publish/subscribe. SOAP-based Web Services constitute the foundation for an interoperable message-oriented middleware, and NATO's CES are to a large extent based on Web Services technology (as defined by the W3C). This approach and the relevant standards are further discussed in the NATO C3 Board's SOA Baseline [11]. The SOA baseline is being further refined in NATO's current work on defining Service Interface Profiles (SIPs). The SIPs vary in maturity, but their development is foundational for the Connected Forces Initiative (CFI) and FMN.

Work on specifying further profiles for the various core services is also ongoing in ACT's venue for Technology for Information, Decision and Execution (TIDE) superiority, which amongst other things produce the TIDE Transformational Baseline (TTB) which contains profiles for a number of core services. The services addressed here are not limited to only SOAP-based Web Services, but also include technologies such as REST.

3.2 Selected Core Services

Core services provide generic, domain independent, technical functionality that enables using IT resources. These services can be broken up further into: Business Support Services, SOA Platform Services, and Infrastructure Services. Permeating the core services are the concepts of CIS security and Service Management and Control (SMC). All these services and further subdivisions into more specific services under each category are deemed applicable to support various aspects of NATO's communication needs, see e.g., the C3 Taxonomy [1]. In IST-118 we chose to focus on a subset of these services in an attempt to bring selected core services to the tactical domain. That subset was considered the very minimum of services needed to get distributed systems running in the tactical domain, but that is not to say that other services are not needed. The selection merely provided a starting point for the group to focus its efforts on.

From the Business Support Services, the core services we chose to pursue were Video- and Text-Based Communication Services from the Unified Communication and Collaboration Services subcategory (see Figure 4).

From the SOA Platform Services we chose to introduce aspects of SOA Platform Communication and Information Systems (CIS) Security Services, namely investigating single sign on in the tactical domain. Further, we chose to investigate Service Discovery from the SOA Platform SMC Services. Finally, we included parts of the Message-Oriented Middleware Services to enable both pull (request/response) and push (publish/subscribe) communication patterns. We considered this subset of core services enable enough functionality to get started building a distributed system in a disadvantaged environment, and made it the focus of the group's efforts. Figure 5 highlights the selected services subcategories under the SOA Platform Services umbrella.

4.0 CORE SERVICES RECOMMENDATIONS

In this section, we summarize our recommendations for how one should adapt the selected core services before deploying them in tactical networks. The level of detail varies between the different recommendations depending on the maturity of the recommendations. The recommendations are primarily presented per service, but as the cross-layer optimizations we have considered can be applied to any service, we will cover that first before considering the service specific optimizations.

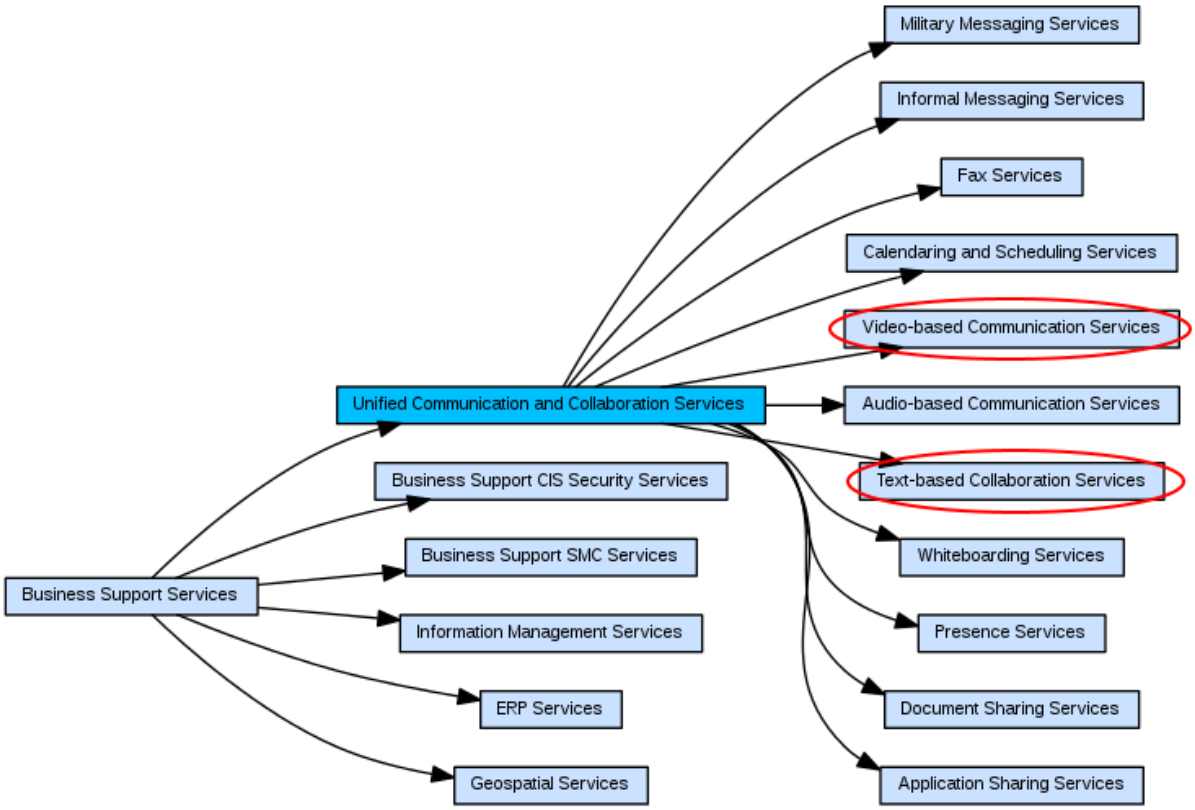


Figure 4: Selected Services Under the Business Support Services Umbrella (Excerpt from the C3 Taxonomy Wiki).

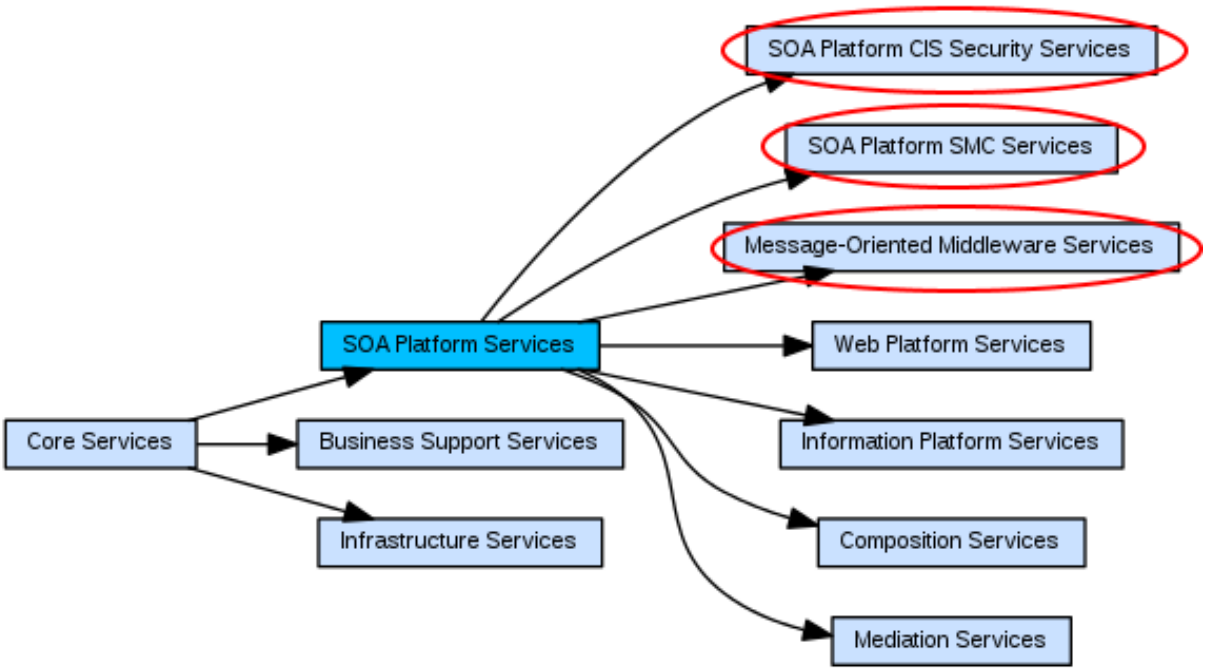


Figure 5: Selected Services Under the SOA Platform Services Umbrella (Excerpt from the C3 Taxonomy Wiki).

4.1 Cross-Layer Adaptations

The objective of IST-118 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 the following subsections, a better coordination between services of Command and Control Information Systems (C2IS) and network protocol layers is useful to increase the overall system performance. This can be achieved by the use of a cross-layer middleware, which allows for an adaptation of the services' communication behavior to the special needs of tactical networks and parameterization of the network to fulfill the communication requirements of the services. For this purpose, the middleware should pass down the services' communication and Quality of Service (QoS) requirements and provide the services with well-adjusted information about the network environment. This can be used by the services to adapt their functionality according to the available communication resources. Furthermore, the middleware should be informed about application knowledge (e.g., mission information about the planned movement of troops). This enables the middleware to account for this additional information when configuring the network layers.

4.1.1 Which Optimizations Are Possible?

This approach allows for a multitude of optimizations: On the one hand, services can adapt their communication behavior to the currently available communications resources by dynamically adjusting the amount of information to be exchanged (e.g., by aggregation of information) or adapting the frequency of information exchanges. On the other hand, the network layers can route and prioritize data flows of services according to their current QoS requirements or to operational requirements. For an overview of possible applications of cross-layer mechanisms, see Ref. [12].

4.1.2 IST-118 Contributions in the Field of Cross-Layer Adaptations

In Ref. [13] an architectural cross-layer concept for the adaptation of SOA technology (in particular, Web Services) in order to enable operational use in the tactical domain is introduced. For this purpose, an Enterprise Service Bus (ESB) specially tailored for the tactical domain (a "tactical ESB") is used as a technical infrastructure for the SOA.

On the network side, a "tactical router" provides connections to different radio technologies (e.g., VHF- and HF-based radios, SATCOM, etc.). A specially tailored cross-layer middleware is introduced to coordinate ESB (infrastructure) services with the tactical router via explicit cross-layer interfaces. The middleware uses a specific state exchange mechanism in order to increase the efficiency of the overall system. Therefore, it obtains characteristics of the network environment and takes advantage of them in order to improve the quality of data transfers.

The architectural concept was prototypically implemented. In this implementation, the designed middleware components and interfaces were coupled with RuDi (an Apache CXF-based ESB by IABG [14]) and an in-house-developed prototype of a tactical router. To realize the intended cross-layer coordination, a concept for distributing the available data rates between different services that are based on a publish/subscribe communication model according to the WS-* specification, WS-Notification was developed (see Section 4.2.2 for a discussion about the WS-Notification standard).

In the concept, the available data rate in the tactical network is dynamically distributed between different message topics. The distribution is done by the middleware. Therefore, the middleware receives network information from the tactical router and calculates distinct transmission frequencies (i.e., messages per second) for different topics sent from this network node. The calculation is based on a given strategy which distributes the currently available communications resources assigned to the network node between the different topics (which correspond to services since every service uses a different topic in this case). This strategy takes the importance of different topics according to the current military order and the count of nodes in radio range into

account. The transmission frequencies are then forwarded by the middleware to an extension of the "Notification Broker" (Notification Broker Interceptor) via interfaces of the middleware. The Notification Broker Interceptor is responsible for compliance with the received transmission frequencies.

The prototypical implementation described above was shown during the demonstration session at the ICMCIS conference in Brussels in May 2016 (see Appendix 2 for further details about this demonstration).

4.1.3 What Is the Way Forward?

The main purpose of the described cross-layer middleware for military networks is, on the one hand, to provide mechanisms for adapting the service behavior to the currently available communications resources and, on the other hand, to provide mechanisms for adapting the network behavior to operational requirements. The introduction of the middleware and its new mechanisms require the introduction of new interfaces between services, the network, and the middleware. We are quite optimistic that this additional investment will lead to a much better performance of the overall system (i.e., distributed C2IS services on top of tactical communication services) and thus will stimulate the development of network-sensitive C2IS services for the tactical level in the long term.

4.2 Messaging Services

Messaging services are the services that support the basic information exchange between entities in a service-oriented system. They can be implemented using a number of different technologies, and different message exchange patterns can be supported. In this section, we summarize the work done by the IST-118 group in support of both request/response services and publish/subscribe services.

4.2.1 Request/Response Services

Request/response is a messaging pattern in which the entity seeking information, the client, sends a request message to the information source, and gets a response back. This basic messaging pattern is also known as client-server.

4.2.1.1 Which Standards Are Used?

In Web Services, as defined by the W3C, request/response messaging is done using the SOAP protocol, which exchanges XML-formatted messages between entities in a transport-agnostic manner. The SOA Baseline [11] points to these same standards, along with the WS-I Basic Profile for interoperability. The current version of the TTB does not address request/response messaging, but the in-progress version 4.0 includes profiles for both SOAP-based messaging and RESTful Web Services. In IST-118 we have primarily focused on SOAP-based request/response services, though we have also performed some early performance comparisons between SOAP- and REST-based services.

4.2.1.2 What Are the Main Challenges for This Service in the Tactical Domain?

In Web Services based on SOAP, all messages follow the XML standard, which is text-based, and messages are formatted so that they are easily readable both for machines and humans. This makes XML fairly verbose, with a significant message overhead.

The SOAP standard is transport agnostic, meaning that its messages can be transmitted using any transport protocol. However, the vast majority of Web service implementations use HTTP over TCP as their transport mechanism. This is partly due to the fact that many development tools only support this standardized SOAP binding. TCP is a connection-oriented protocol, and relying on this as the transport mechanism means that services and clients must be available at the same time, and that a connection between them must be

established and maintained. In networks where both disruptions and long delays are common, relying on such end-to-end connections is a limiting factor.

4.2.1.3 Which Optimizations Are Possible?

In order to overcome the issue of XML messaging overhead, the XML messages can be compacted using either a generic loss-free compression mechanism or a binary XML encoding that also reduces the message size. Using alternate data models, which express the same information more compactly is also possible, but might lead to information loss.

The issues stemming from the use of HTTP over TCP as the transport mechanism for SOAP can be addressed in several ways. This includes tuning the performance of the HTTP and TCP protocols, replacing the standard TCP implementation with other TCP flavors, or replacing the transport mechanism with one that is more suitable for use in tactical networks.

4.2.1.4 IST-118 Contributions in the Field of Request/Response Services

The work done on request/response services in IST-118 is based on the work done by the predecessor group, IST-090, which recommended that the services optimizations should be done in proxies in order to retain interoperability with standard commercial off-the-shelf (COTS) services. Then, we investigated both the edge proxy concept with AFRO [15] as well as proxy pairs / network of proxies with DSProxy [16].

In IST-118 we implemented a proxy pair adhering to the recommendations from IST-090. This proxy pair ensured that COTS services could function in DIL environments. The novel part for the sake of IST-118, was that in this proxy version the delay and disruption tolerance was implemented supporting HTTP rather than SOAP. This meant that the proxy approach was shown to function for both SOAP and REST services, which typically both use HTTP for transport. The proxy implementation and evaluation are further described in Ref. [17].

Performance tests involving SOAP Web Services (which use XML), compared to REST with XML and REST with JSON show that REST is preferable from a pure performance point of view, whereas SOAP's strong points are standardization and interoperability [18].

Follow-up work evaluating SOAP and REST on the Android platform showed similar results, in that consuming REST services consumed less power (leading to increased battery life) than consuming SOAP services [19].

4.2.1.5 Recommendations for Request/Response Services

General recommendations include using filtering and compression to reduce overhead, and tuning transport protocols and application servers to better fit the underlying transport medium. In order to retain COTS compatibility in both clients and services, we recommend putting proprietary optimizations in proxies between said clients and services.

With respect to which implementation technology to use where, recommendations from our study on Android [19] are summarized in Table 1.

4.2.1.6 What Is the Way Forward?

The work of IST-090 and now IST-118 has thoroughly studied optimizations for SOAP request/response services. Our recommendations can be used to help deploy systems involving this technology. However, with the increasing popularity of REST services it would make sense to study these further in a similar manner as we have done for SOAP services.

Table 1: SOAP vs. REST Recommendations.

Overall Goal	Recommendation
NATO interoperability	SOAP
Machine-to-machine infrastructure services	SOAP (or REST, maybe wrapping the SOAP service)
Functional area services	SOAP (or REST, maybe wrapping the SOAP service)
Smart device clients	REST
Non-smart device clients	SOAP (or REST, if the client is written in JavaScript)

4.2.2 Publish/Subscribe Services

Publish/subscribe is a term used to describe a communication pattern in which clients that are interested in a certain type of information subscribe to information of this type. The clients indicate what type of information they are interested in either by using topics (or keywords), content filters or both. When new information becomes available the new information is sent to the interested clients based on the subscriptions. The information is sent either directly by an information producer, or via a broker, which can offload producers from the task of doing both subscription management and notification dissemination.

4.2.2.1 Which Standards Are Used?

The SOA Baseline points to the standard WS-Notification from OASIS for publish/subscribe between Web Services, and a SIP has been written for this standard. There is also ongoing work within the TIDE community related to producing a WS-Notification-based profile as part of the TTB. In IST-118 we have thus focused primarily on WS-Notification in our optimization work – note that the implementations used have not been tested for full compliancy with the TTB specification as that profile is currently awaiting verification through CWIX testing.

4.2.2.2 What Are the Main Challenges for This Service in the Tactical Domain?

When using a broker-based approach to publish/subscribe, all information will go via the broker(s), which means that the availability of the brokers might be a bottleneck. The impact of the non-availability of a broker depends on the broker deployment topology used; whether one has a single-broker deployment or a multi-broker deployment. In a multi-broker deployment, there are different possible topologies, but deploying brokers close to clients and services might help alleviate the issue of broker availability.

The WS-Notification standard specifies that notifications are to be delivered unicast to each client. When multiple clients, connected through the same broadcast-based communications medium, are interested in the same information, this means the several copies of the same notification are sent over the same network, which leads to suboptimal use of the often-limited network resources.

In many cases, the information producer will be located in a non-resource-constrained network, and might not be aware of the network constraints between it and the client. Using publish/subscribe means that the transmission of notifications is initiated by the information producer (or broker) rather than by the client. This means that the client has no way of controlling when its communication resources are being used, and how often it receives updates.

4.2.2.3 Which Optimizations Are Possible?

The message exchange between the consumers, brokers and producers is done using standard SOAP messages. The registration of publishers and the creation and management of subscriptions are similar to the

request/response message exchange, while the distribution of notification messages can be seen as a one-way service call. This means that the SOAP message optimizations recommended for request/response services also can and should be applied to the publish/subscribe message exchanges.

In addition to the optimizations that can be applied to request/response services, there are a number of optimizations that can be done by the publish/subscribe middleware. Some optimizations done at this level are non-intrusive, i.e., they do not change either the content of notifications or which notifications are delivered to the client. This includes changing the behavior of WS-Notification to use multicast delivery of notifications where applicable and replacement of the transport mechanisms used.

In addition to these non-intrusive adaptations it is also possible to use optimizations that alter some aspect of the message flow between the information producer and consumer. This includes altering the content of the message (for instance, through filtering or transcoding of information), altering how notifications are distributed (for instance, aggregating many smaller notification messages into one larger message, and thus altering the timeliness of the delivery of information) and also selective dropping of notifications (also known as frequency filtering) to limit how many messages are transmitted over the network. All of these intrusive adaptations require knowledge of how the information is used by consumers, and must be applied selectively.

4.2.2.4 IST-118 Contributions in the Field of Publish/Subscribe Services

The optimizations of publish/subscribe services have been addressed by IST-118 in a number of experiments, publications, presentations and demonstrations.

We first tested standard WS-Notification without any optimizations in a wireless broadband radio network. The purpose of this test was to determine whether WS-Notification can be used in such networks without any optimizations, and to measure how much resources this consumes. These tests are documented in Ref. [20] and show that while WS-Notification functions in these network types without modification, simple transport optimizations should be used to limit the amount of network resources consumed.

Retaining interoperability while performing tactical optimizations is important, and in Ref. [21] we combined our work on WS-Notification in wireless broadband radio networks with an interoperability test. Two independent implementations of WS-Notification were used to transfer information through a network that included a wireless broadband radio network where we performed transport-level adaptations. This experiment showed that performing these optimizations did not negatively impact interoperability.

An alternative to performing tactical optimizations of the WS-Notification standard is to replace the standard with a publish/subscribe protocol that is more suited to the constraints of tactical networks. In Ref. [22] we performed a comparative performance evaluation of three publish/subscribe protocols.

The different types of networking technologies that are used in tactical networks have very different characteristics. In order to be able to give recommendations for more than one networking technology, we performed experiments with WS-Notification in all five network configurations as described in Section 2.4 Network Types. These experiments [23] were performed in an emulated environment based on the CORE network emulator.

In Appendix 1, we describe a demonstration and experiment where we combine all our previous efforts on WS-Notification into one larger experiment. Two different implementations of WS-Notification were connected in order to show interoperability, while running over a network consisting of both an emulated tactical network and a real wireless broadband radio network.

In addition to the experiments described in the publications referenced above, IST-118 group members have experimented with combining publish/subscribe with cross-layer mechanisms, where each WS-Notification

topic was allocated a given amount of resources it was allowed to consume based on the currently available resources. These optimizations were shown during the demonstration session at ICMCIS conference in Brussels in May 2016. For further details on this demonstration see Appendix 2.

4.2.2.5 Recommendations for Publish/Subscribe Services

A publish/subscribe service can, simply put, be seen as a reverse request/response service. As such, publish/subscribe services can benefit from the same optimizations as request/response services: Using compression, filtering, etc. In addition, several optimizations can be made specifically for publish/subscribe services. For example, the group has, through demonstrations and experiments, shown that the family of WS-Notification standards can benefit from applying cross-layer optimizations, message aggregation, and multicast distribution of notifications.

4.2.2.6 What Is the Way Forward?

NATO has chosen WS-Notification for publish/subscribe, hence we focused mostly on that standard in IST-118. The WS-Notification standard is intended for use both in the NATO enterprise and in federated networks. That being said, WS-Notification may not be the best choice for use in tactical networks even though we have shown the feasibility of applying it to such networks in some of our experiments and demonstrations. Also, WS-Notification is not used much in civilian systems, which means that there are few implementations of the standard out there. Hence, we suggest investigating also other approaches to publish/subscribe (e.g., AMQP and MQTT) for which there exists many different implementations. If some other solution than WS-Notification proves more efficient in certain tactical networks then it could be suggested for use there, but then one also needs to look into making said protocol interoperable with WS-Notification when such networks need to share information with NATO.

4.3 CIS Security Services

Security properties, such as confidentiality, integrity, and availability (CIA) must be supported in order to handle security requirements of services running in the tactical environment. In particular, they need to manage the security requirements of all relevant security levels, and information flow between security domains. CIS Security Services encompass all communication layers, but here we focus on the security aspects related to protecting core services.

4.3.1 Which Standards Are Used?

There are many standards that can be used for securing core services, as Figure 6 shows.

CIS security is a vast field, but in IST-118 we have focused on a small subset of standards related to identity management and access control. As the figure shows, there are three standards for identity management, of which two are currently considered by NATO: WS-Federation and SAML 2.0. These tie together with the other standards to provide a complete infrastructure for security management, message security, reliable messaging, policies and access control. SOAP is the common protocol and XML the common data format. For an elaborate explanation of how the standards work and tie together, see Ref. [24]. We have not considered non-SOAP-related standards, and we have not looked into issues with SSL/TLS or IPSec. Also, NATO has recently started looking into securing REST-based services using the Oauth and OpenIDConnect standards, but neither of these have been addressed in IST-118.

It must be emphasized that the current standardization in the area of access control relates only to the request/response message exchange pattern. It is assumed that after the user subscribes to a topic, he is entitled to receive notifications. The messages themselves can be labeled or encrypted, being subject to border protection.

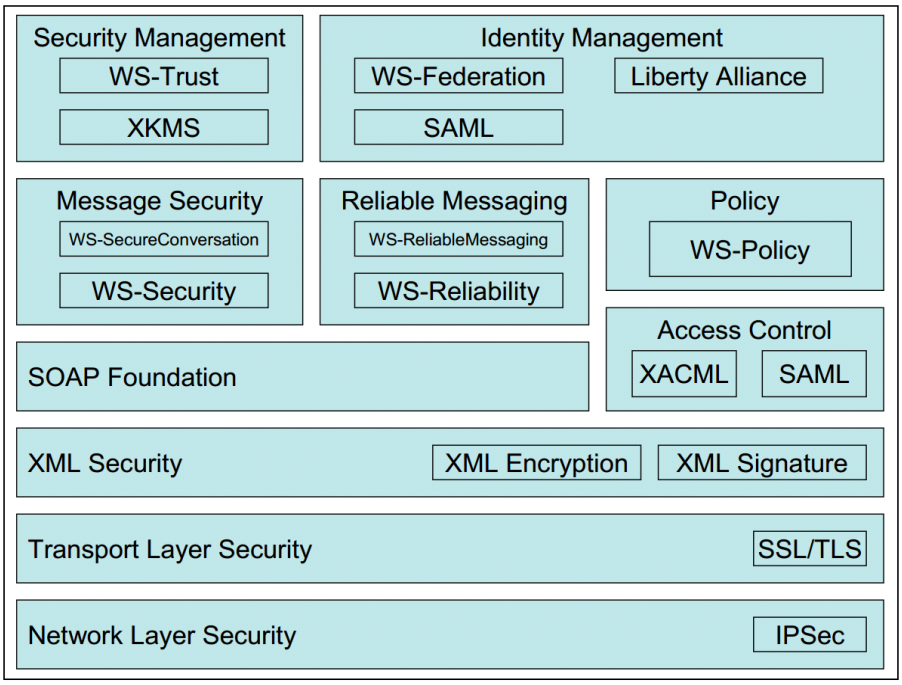


Figure 6: Security Standards (from Ref. [24]).

4.3.2 What Are the Main Challenges for This Service in the Tactical Domain?

The main challenges include using a Public Key Infrastructure (PKI) in DIL environments (certificate distribution, revocation lists, etc.) and the general overhead introduced by adding digital signatures, encryption, and identity management to services.

The distributed nature of the security services' architecture results in the necessity to realize several exchanges of messages during the authentication and authorization process before the access is granted. Thus, the complex call chains requiring many subsequent synchronous connections to be successful limit the usability in DIL environments.

4.3.3 Which Optimizations Are Possible?

So far, we have only investigated the overhead of security services, which can be deemed considerable. However, we have some suggestions for optimizations that should be pursued: The need for synchronous calls needs to be reduced to a minimum, so one should consider pre-distribution of assets where possible (e.g., certificates), longer timeouts would also help mitigate part of the problem (e.g., increase token validity time [26]). As for the issues of message overhead, one should leverage compression prior to encryption. Also, more compact XML representations of assets that must be distributed (e.g., a more compact signature representation or using an identifier for a certificate that has been pre-distributed rather than including said certificate within every SOAP message) would increase the usability of the security solutions in tactical networks.

4.3.4 IST-118 Contributions in the Field of CIS Security Services

IST-118 has focused on a subset of the CIS security services, namely aspects related to Single Sign On. Both the SAML 2.0 [27] and WS-Federation [28] protocols have been investigated, and we found that there are issues related to reliance on several synchronous service calls for either protocol to work, and also that there is extra overhead associated with the solutions.

4.3.5 Recommendations for CIS Security Services

SAML 2.0 seems to be the standard for identity management with best vendor support these days. Hence, we suggest to focus efforts on researching this, as this is most likely to be the standard of choice for SSO for NATO in the future based on results from e.g., CWIX 2014 and 2015 [29], [30]. Also, we suggest pursuing message-level security in addition to transport or network layer security despite the overhead due to the benefit of achieving multi-hop message-level security and border protection.

4.3.6 What Is the Way Forward?

An important aspect is the timeframe a security token is valid ("liveness" of the tokens). There needs to be an evaluation of the trade-off between usability, trust and SSO token liveness. How long should the token be valid? If the token lives forever the risk of a security breach is increasing as time goes by, and if the token has a time to live through liveness data there has to be an evaluation on how long time it should be valid. Too short gives more overhead as the user might have to re-authenticate often and by this adding traffic and overhead. Other, "classic" challenges of CIS security also remain unsolved, like PKI (with aforementioned distribution and revocation of certificates) in DIL environments.

4.4 Service Discovery

Before a potential consumer of a service can use the service, it needs to be able to find the services that are available to it, and also discover how to use those services. In Web Services, this translates into the consumer needing to find the machine-readable service description, which describes the interface of the service, and also contains the endpoint address of the service. The process of finding this description is called service discovery. Service discovery can be performed either in design-time, run-time or both. In IST-118 we have focused on run-time discovery, which targets finding available services and consuming them in run-time.

4.4.1 Which Standards Are Used?

There are three SOAP Web Services discovery standards, all by OASIS:

- Universal Description, Discovery and Integration (UDDI);
- Electronic business using XML (ebXML); and
- WS-Dynamic Discovery (WS-Discovery).

Of these, UDDI is mentioned in the SOA baseline and current FMN instructions. Both UDDI and ebXML are registries, suitable for use in stable environment. Of the three, only WS-Discovery targets run-time discovery in dynamic networks. Hence, we have focused on that standard in IST-118. WS-Discovery offers a multicast-based approach to discovery. The protocol has both a proactive and a reactive mode (the latter is necessary to give an up-to-date view of services in a dynamic environment). The reactive mode allows you to actively probe the network for services and use the result, which mirrors the current network state.

4.4.2 What Are the Main Challenges for This Service in the Tactical Domain?

Using a registry is not a good option because it constitutes a single point of failure. In addition, registries rely on services being registered and explicitly deregistered, which is not always feasible in a dynamic environment. Hence, stale data can occur in a registry under such conditions. Broadcast/multicast-based solutions like WS-Discovery overcomes these challenges but introduce new ones: A decentralized protocol consumes more network resources than a centralized registry. It is necessary to limit this overhead for WS-Discovery to be usable (to keep the discovery overhead low in order to maximize the amount of useful payload traffic).

4.4.3 Which Optimizations Are Possible?

Many approaches are possible to optimize service discovery for a given network. Examples here include the usual approaches like enabling compression and using filtering to reduce overhead. Further, it is possible to replace the mechanism itself to a protocol better suited to a certain network's characteristics. For example, using UDDI is fine in an enterprise, but it is ill-suited for use in a tactical network. For WS-Discovery, the protocol offers both so-called generic and specific probing of the network. By using specific probes one can search for only the services the client actually needs to know about (limit by scope and port type) so that only information that is useful for the client will traverse the network. As different protocols solve different needs, we will need to bridge protocols somehow. We have considered different approaches to this, like adaptive protocols, using an abstraction layer, and introducing service discovery gateways.

4.4.4 IST-118 Contributions in the Field of Service Discovery

In the predecessor to IST-118, IST-090, we performed several experiments on service discovery. Our findings from that work, and the recommendation to use service discovery gateways remain valid also at the conclusion of IST-118. In IST-118 we have focused mainly on WS-Discovery, and experimented with ways to extend the reach of WS-Discovery using peer-to-peer networking [31].

4.4.5 Recommendations for Service Discovery Services

Use service discovery gateways to translate between different protocols to bridge different ownership domains. This approach limits the impact on deployments by keeping the need for mutual agreement to the interoperability points in a federated system. Different networks have different characteristics and need discovery solutions that take the limitations into account. For example, using WS-Discovery instead of UDDI in dynamic networks, such as mobile ad hoc networks, allows us to discover services without the problems of a registry (stale data in the registry and/or unavailability of the registry itself as it constitutes a single point of failure).

4.4.6 What Is the Way Forward?

In IST-118 we have focused only on discovering SOAP services. As times change, we see an increased use of other technologies and deployment strategies that need addressing. So, for the follow-on group we think that discovery in hybrid environments should be pursued in further experimentation. In this sense, we mean "hybrid" in the broadest sense of the word, i.e., encompassing different service technologies (notably both REST and SOAP), different networks (narrowband and broadband tactical networks, etc.) and different deployment strategies (your service-hosted stand-alone, in an ESB, in a tactical cloud, etc.).

4.5 Collaboration Services

Collaboration services (known in the C3 Taxonomy as Unified Collaboration and Communication Services) is a group of services that support human-to-human communications, such as email, audio and video-based conferencing and instant messaging. Common for all of these services is that while they are indeed services, they are not realized using Web Services technology.

In IST-118 we primarily address the adaptation of traditional SOA technologies such as Web Services, but we also consider some non-SOA services such as instant messaging and video teleconferencing (VTC). These services have been included, as supporting them is of great importance also in the tactical domain.

4.5.1 Text-Based Collaboration Services

Text-based collaboration services, often called chat, allow users to exchange relatively brief text-based messages in near real-time. The messages can be delivered either between two participants (instant messaging), or between several participants (chat room).

4.5.1.1 Which Standards Are Used?

One of the most prominent solutions in recent years is the XMPP protocol, which is implemented in several instant messaging products, both servers and clients. This protocol has also been chosen for chat by NATO, as it is mentioned in the SOA baseline as one of the protocols to use when implementing the collaboration core services. NATO's JChat client implements XMPP, which has been used with success in many missions. XMPP also supports presence, which is a collaboration service that has not been considered by IST-118.

4.5.1.2 What Are the Main Challenges for This Service in the Tactical Domain?

XMPP is server-based making it ill-suited for use in disadvantaged grids where a central server constitutes a single point of failure. Also, there is potential overhead of the presence mechanism, and overhead from the fact that the messages are XML.

4.5.1.3 Which Optimizations Are Possible?

Multicast is an efficient means of distributing one message to many recipients. This can be leveraged in order to decentralize a chat application and do away with the central server. By using gateways and proxies, such a chat solution can be compatible with XMPP clients. We have identified three approaches that are commonly used when attempting to realize chat in tactical networks.

Figure 7 illustrates these three approaches, from left to right:

- Attempting to use XMPP directly, but with certain optimizations;
- Using a proprietary solution in the dynamic environment, but using gateways to achieve interoperability with COTS XMPP clients and servers; and
- Proprietary client and optimizations but using a gateway for interoperability with an XMPP server in the backbone network.

4.5.1.4 IST-118 Contributions in the Field of Text-Based Collaboration Services

In IST-118 we have made a prototype solution that we call P_MUL Chat. The motivation for creating this chat solution was to be able to leverage the key properties of ACP142 [32] for instant messaging in disadvantaged grids. The key properties are:

- Reliable multicast messaging;
- Designed for bandwidth-constrained networks; and
- Delayed acknowledgement for EMCON environments.

Both our ACP142 Java implementation and the P_MUL Chat were released as open source and provided to the NATO STO/IST-ET-070 exploratory team for tactical chat for evaluation. For more information on our work on chat, see Ref. [33].

4.5.1.5 Recommendations for Text-Based Collaboration Services

The outcome of the NATO STO/IST-ET-070 evaluation was that there is no particular need to investigate tactical chat further. Proprietary enhancements that function well in the tactical domain now exist, and can be used together with corresponding proprietary gateways translating to the XMPP protocol. In this way, interoperability with NATO can also be achieved. The IST-118 group supports the conclusions of the STO/IST-ET-070 team.

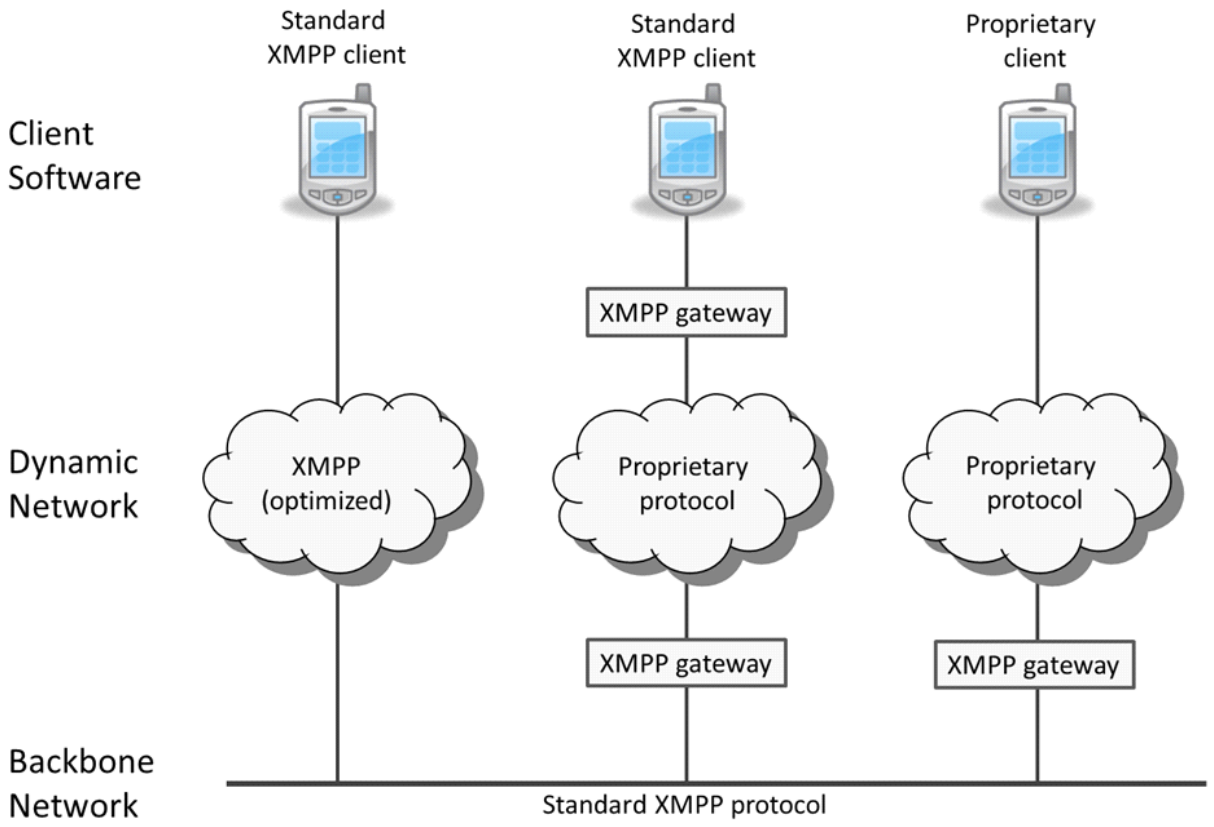


Figure 7: Three Approaches to Implementing Chat Solutions.

4.5.1.6 What Is the Way Forward?

As mentioned above, there exists proprietary solutions for supporting chat in tactical networks, so little new research is required for this service. By using these proprietary optimizations, according to recommendation from the exploratory team on tactical chat, one can remain interoperability with XMPP using gateways. Achieving interoperable configurations of XMPP can be achieved by following the SIP or FMN Service Instructions for this service.

4.5.2 Video-Based Collaboration Services

Video-based collaboration services may provide two-way video communication between two or more participants, so-called VTC. VTC normally also includes audio communication. VTC services are similar to audio conferencing services in many respects: Users expect real-time behavior, the service must provide an application allowing users to connect to a video conference, and all or only some participants could be allowed to speak and send video. Another use case for video services is one-way streaming, which can also be used for other services, such as getting information from video-based sensors. Full motion video (FMV), either for surveillance and intelligence gathering purposes or to provide immediate situational awareness, is becoming an increasingly important part of NATO's collaboration services selection. This latter case has been the focus of IST-118.

4.5.2.1 Which Standards Are Used?

STANAG 4609 specifies that all motion imagery in the visible light and infrared spectrums must be contained in MPEG-2 transport streams and, if compression is used, should be employed in one of three

commercial formats. Of these three the most commonly used is the H.264 advanced video coding standard first introduced in 2003. This standard is also in the NATO Interoperability Standards and Profiles (NISP). For civilian application the more recent H.265 standard is becoming increasingly abundant.

4.5.2.2 What Are the Main Challenges for This Service in the Tactical Domain?

The bandwidth-intensive, delay- and loss-intolerant nature of high-resolution FMV transmission means that there are still challenges in transmitting over DIL networks such as those often found in tactical-edge radio networks.

4.5.2.3 IST-118 Contributions in the Field of Video-Based Collaboration Services

We have proposed a novel H.265-based video service for use as part of a SOA framework for services in DIL tactical networks. The service aims to provide a robust unidirectional video service for FMV for tasks such as video surveillance or provision of real-time situational awareness. The service has been designed to operate effectively in disadvantaged tactical networks by providing error protection and selective dropping mechanism that ensure that delivered video content can be both decoded and interpreted. Results of an empirical investigation show that video quality is maintained despite bandwidth fluctuations and packet loss. This work is described further in Ref. [34].

4.5.2.4 Recommendations for Video-Based Collaboration Services

For high-bandwidth networks and interoperability with current systems, we recommend using H.264 SVC. For the future, we recommend that NATO considers H.265 HEVC for certain applications – it can achieve less network load by trading it for more intensive processing, which in many cases can make it preferable for use in resource-constrained networks where the throughput is the main limiting factor.

4.5.2.5 What Is the Way Forward?

Suggested future work for the IST-118 follow-on group in this area is to concentrate on developing a fully functional Web service for video surveillance over DIL tactical networks that can be used for further experiments and evaluation.

5.0 ACTIVITIES

In addition to performing technical work, IST-118 has also focused on creating awareness for the problem space and the results generated by the group. This has been done through a number of different channels, including hosting workshops, giving presentations and publishing the results of the work at relevant peer reviewed conferences. This section gives an overview of all the activities in IST-118, including work meetings, workshops, publications and presentations.

5.1 Workshops and Demonstrations

IST-118 has hosted four workshops of two types – in two of the workshops IST-118 members presented the work done by the group to the audience, while in the other two workshops we invited others to submit papers, and got input on our problem space through these papers and the following discussions:

1) Enabling SOA in the tactical domain, workshop in conjunction with Mobile Deployable Communications (MDC) in 2015;
2) International Workshop on Service-Oriented Computing in Disconnected, Intermittent and Limited (DIL) Networks (SOC-DIL), workshop at IEEE VTC Spring 2015;

3) Self-hosted event at the Defence Science and Technology Laboratory (DSTL), Porton Down 2015; and
4) Workshop on "Tactical domain SOA", in conjunction with IEEE ICMCIS 2016.

5.1.1 Enabling SOA in the Tactical Domain, Workshop at MDC 2015

MDC is an annual event where registered conference participant can attend presentations and engage in discussions on many aspects of mobile communications. Every year, the conference also hosts one or more in-depth workshops on selected topics. During the 2015 conference, members of IST-118 hosted a workshop, named "Enabling SOA in the tactical domain", detailing the problem space and early results of the group. The workshop was a half-day event where we gave a number of presentations and engaged the audience in discussion related to the use of service-oriented technologies in tactical network.

5.1.2 International Workshop on Service-Oriented Computing in Disconnected, Intermittent and Limited (DIL) Networks (SOC-DIL), Workshop at IEEE VTC Spring 2015

The SOC-DIL workshop was hosted in conjunction with the 2015 spring edition of the IEEE Vehicular Technology Conference (VTC), as this event is attended by a community that faces many of the same challenges as those addressed by IST-118. This was the first academic workshop arranged by IST-118 members, where we invited the larger academic community to submit papers related to the IST-118 topics. The workshop had its own technical program committee, and the submitted papers were reviewed by at least two TPC members. The selected papers were then presented by the authors at the workshop. The papers, and the following panel discussion, served as valuable input to the work done further in IST-118.

5.1.3 Self-Hosted Demonstration at DSTL, Porton Down 2015

In November 2015, IST-118 hosted a presentation and demonstration event at the DSTL facilities in Porton Down, UK. The initiative for this event was taken by the GBR representative to IST-118, in order to engage the DSTL community in the IST-118 work. As the event was held at a closed facility, participation was by invite only. The event was attended primarily by representatives from the UK, but NATO was also represented.

During the event IST-118 members gave presentations on the various core services, and our experiences with adapting these to the tactical domain. This included ample time for discussions, and we received valuable feedback for participants with operational experience. The event concluded with a demonstration, where the participants were shown services running a number of different optimizations.

5.1.4 Workshop on "Tactical Domain SOA", in Conjunction with IEEE ICMCIS 2016

IST-118 hosted a workshop and demonstration at the IEEE ICMCIS in Brussels, Belgium, in 2016. This event served at the closing event for the group and was open both to the conference participants and to the IST-panel members that were attending the co-located IST-panel business meeting.

The workshop consisted of a keynote given by the IST-118 chairman, followed by a half-day session in which a number of academic papers were presented. These papers had been submitted to the workshop, and been peer reviewed as a part of the IEEE ICMCIS review process. After the workshop concluded IST-118 members also gave a demonstration as part of the IEEE ICMCIS demonstration session, which is further described in Appendix 2.

5.2 Publications

Most of the technical results that the IST-118 members have contributed have been documented in the form of technical papers. These papers have primarily been published as peer-reviewed conference papers, though some journal papers are included as well. All the IST-118 relevant papers are listed below:

- Johnsen, F.T., Bloebaum, T.H., Meiler, P.-P., Owens, I., Barz, C., and Jansen, N., "IST-118 – SOA recommendations for disadvantaged grids in the tactical domain", 18th ICCRTS, Alexandria, VA, USA, June 2013.
- Johnsen, F.T., Bloebaum, T.H., Avlesen, M., Spjelkavik, S., and Vik, B., "Evaluation of transport protocols for web services", Military Communications and Information Systems Conference (MCC) 2013, Saint-Malo, France, October 7 – 8, 2013.
- Johnsen, F.T., Bloebaum, T.H., Cetusic, L., Flaatten, H.K., Kjensmo, K., Lothe, E., Pettersen, O.J., Schmid, T.M., and Tungesvik, B., "Collaboration services: Enabling chat in disadvantaged grids", 19th ICCRTS, Alexandria, VA, USA, June 16 – 19, 2014.
- Bloebaum, T.H., and Johnsen, F.T., "Enabling service discovery in a federation of systems: WS-Discovery case study", 19th ICCRTS, Alexandria, VA, USA, June 16 – 19, 2014.
- Johnsen, F.T., Bloebaum, T.H., and Eggum, D.O., "Efficient SOAP messaging for Android", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Krakow, Poland, May 18 – 19, 2015.
- Johnsen, F.T., Bloebaum, T.H., and Karud, K.R., "Recommendations for increased efficiency of Web services in the tactical domain", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Krakow, Poland, May 18 – 19, 2015.
- Jansen, N., Krämer, D., Barz, C., Niewiejska, J., and Spielmann, M., "Middleware for Coordinating a Tactical Router with SOA Services", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Krakow, Poland, May 18 – 19, 2015.
- Sliwa, J., et al., "Efficiency of the single sign on mechanism in a tactical network environment", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Krakow, Poland, May 18 – 19, 2015.
- Barz, C., Jansen, N., Alcaraz-Calero, J.-M., Manso, M., Markarian, G., Owens, I., Wang, Q., Meiler, P.-P., Bloebaum, T.H., Johnsen, F.T., Sliwa, J., and Chan, K., "IST-118 SOA recommendations for disadvantaged grids in the tactical domain – SOA experiments on wireless broadband mobile networks in the tactical domain", International Command and Control Research and Technology Symposium (ICCRTS), CCRP publication, USA, 2015.
- Manso, M., Alcaraz-Calero, J.-M., Meiler, P.-P., Chan, K.S., Barz, C., Owens, I., Sliwa, J., Jansen, N., Wang, Q., Bloebaum, T.H., Markarian, G., and Johnsen, F.T., "SOA and wireless mobile networks in the tactical domain: results from experiments", IEEE MILCOM 2015.
- Bloebaum, T.H., and Johnsen, F.T., "Evaluating publish/subscribe approaches for use in tactical broadband networks", IEEE MILCOM 2015.
- Bloebaum, T.H., and Johnsen, F.T., "Exploring SOAP and REST communication on the Android platform", IEEE MILCOM 2015.
- Brannsten, M.R., Johnsen, F.T., Bloebaum, T.H., and Lund, K., "Towards federated mission networking in the tactical domain", IEEE Communications Magazine, Special edition on Military Communications, October 2015.
- Nightingale, J., Wang, Q., Alcaraz-Calero, J.-M., Owens, I., Johnsen, F.T., Bloebaum, T.H., and Manso, M., "Reliable FMV services in disadvantaged tactical radio networks", IEEE International Conference on Military Communications and Information Systems (ICMCIS) 2016.
- Bloebaum, T.H., Johnsen, F.T., Brannsten, M.R., Alcaraz-Calero, J.-M., Wang, Q., Nightingale, J., "Recommendations for realizing SOAP publish/subscribe in tactical networks", IEEE International Conference on Military Communications and Information Systems (ICMCIS) 2016.

5.3 Presentations

In addition to presentations given at the conferences where we have published papers and at the workshops we have hosted, IST-118 members have also given presentations at other events in order to share information with other communities and create awareness for the problem space. Presentations included:

1) Presentation to SCI-254 Architecture Assessment for NEC, Peter-Paul Meiler, 2013;
2) Keynote at Military Communications and Information Systems Conference (MCC), Peter-Paul Meiler, 2013;
3) Presentation at IQPC Interoperable Open Architecture, Peter-Paul Meiler, 2013;
4) Presentation to MSG-136 Modeling and Simulation as a Service (MSaaS), Frank T. Johnsen, 2014;
5) A second presentation to MSG-136, at their request, Peter-Paul Meiler, 2015;
6) Presentation at IQPC Mobile MILSATCOM, Peter-Paul Meiler, 2015;
7) Presentation at IQPC Interoperable Open Architecture, Jose Alcaraz-Calero, 2015;
8) Presentation at the Mobile Deployable Communications main conference, Joanna Sliwa, 2015; and
9) Presentation to the TIDE Technology Track at the Spring TIDE Sprint, Trude H. Bloebaum, 2016.

5.4 Work Meetings

IST-118 has had regular work meetings two to three times each year, where the entire IST-118 team has participated, when possible. We have also arranged a few smaller meetings in order to prepare for common activities such as the demonstrations. During these smaller meetings only the members that were contributing with technical solutions participated. Meetings included:

1) Kick-off meeting in March 2013, hosted at Shrivenham DCC, Swindon, UK;
2) Group meeting co-located with IEEE MCC 2013, in St. Malo, France;
3) Group meeting in January 2014, hosted at TNO, The Hague, the Netherlands;
4) Group meeting in August 2014, hosted at UWS, Glasgow, Scotland;
5) Group meeting in conjunction with MDC 2015, Prague, Czech Republic;
6) Group meeting in May 2015, hosted at UWS, Glasgow, Scotland;
7) Integration meeting (preparations for the upcoming demonstration) in September 2015, hosted by Rinicom in Lancaster, UK;
8) Demonstration event and group meeting in November 2015, hosted at DSTL Porton Down, UK;
9) Integration meeting (preparations for the IEEE ICMCIS demonstration) in May 2016, hosted by Fraunhofer FKIE in Bonn, Germany; and
10) Demonstration event and workshop at IEEE ICMCIS 2016, hosted in Brussels, Belgium.

6.0 CONCLUSIONS

The main goal of IST-118 has been to provide research-based recommendations for how to support foundational core services in the tactical domain. Our work was performed in synergy with SOA-related specification and profiling work done as part of other NATO efforts such as NNEC and FMN.

IST-118 used a spiral approach to structure the work and chose a continuous approach to sharing results by publishing papers and organizing events. This approach generated some additional workload, but it allowed us to continuously get feedback from both the NATO and academic research communities and incorporate that feedback into our work. In our experience, the benefits from this approach are significant enough to offset the added workload, and we recommend following a similar approach in the continuation of this work.

In IST-118 we have investigated selected core services, attempted to bring them into the tactical domain, and have found several optimizations and recommendations to give for anyone undertaking such an endeavor. We focused on generating concrete recommendations for a subset of the core services from the NATO C3 Taxonomy, based on systematic testing and evaluation, rather than providing higher-level recommendations for a wider set of services. This ensured that our work could have a direct impact on NATO operations.

Table 2 summarizes our findings, and indicates the maturity of our recommendations for the different core services we have addressed.

Table 2: Service Recommendations Maturity. Green = mature, yellow = further work recommended, red = further work required.

Service	Recommendation Maturity
SOAP Request/Response	Recommendations are mature and tested
REST Request/Response	No recommendations yet; further work needed
SOAP Publish/Subscribe	Mature recommendations exist, but we suggest exploring further optimizations
CIS Security	Challenges identified; further work needed
Service Discovery	Mature recommendations exist, but we suggest exploring further optimizations
Text-Based Collaboration (Chat)	Recommendations are mature and tested
Video-Based Collaboration	Some recommendations exist, further work needed

For the SOAP request/response services we can give several recommendations: Compression of XML-formatted data should be used in any disadvantaged network to reduce overhead. Compression may reduce message size significantly. In networks with disruptions or high delays, we suggest to use a transport binding that does not require end-to-end connectivity. For example, replace TCP with an alternative transport protocol and consider using store-and-forward. Also, keep in mind that the application server configuration can be optimized as well. By introducing the optimizations in proxies, it is feasible to continue using COTS clients and services even in DIL environments.

REST is seeing an increased use for both civilian and military applications. We have seen that for Android using REST rather than SOAP has a positive effect on device battery life. Apart from this, REST was not much studied in IST-118 and should be investigated further.

SOAP publish/subscribe, i.e., using the WS-Notification family of standards, is feasible on the tactical level using some proprietary extensions like cross-layer optimizations and switching from unicast to multicast communication. In addition, message aggregation and frequency filtering at the application level should be used. Finally, the same optimizations as for request/response apply here (using compression, etc.).

CIS Security remains an open issue. In IST-118 we focused on a subset of such services, namely single sign on. Issues that we identified with the protocols SAML 2.0 and WS-Federation include the challenge of providing a public key infrastructure in an ad hoc network and that the protocols rely on long synchronous service call chains, which means that the service is not disruption tolerant. Also, security as prescribed by WS-Security and related standards introduce a lot of additional overhead.

Service discovery, which in IST-118 was limited to run-time discovery of SOAP services implementing known interfaces, is a challenge in tactical networks. We have found that one solution cannot accommodate all needs. Hence, we suggest to use standardized solutions when possible, and proprietary solutions only where needed. For example, we had success using WS-Discovery in ad hoc networks that support multicast routing. For interoperability between protocols we considered several approaches, of which the gateway approach seems best and is the approach we recommend.

Text-based collaboration, which in IST-118 was limited to investigating chat solutions, showed that using plain XMPP is not necessarily feasible at the tactical domain. As the protocol is client/server-based, the server constitutes a single point of failure, and hence it is not well suited for use in DIL environments. In addition, the presence functionality generates background traffic. Therefore, our recommendation here is to use bespoke chat solutions in the tactical domain that are particularly suited to the specific networks, and then implement a gateway to standard XMPP for when interoperability is needed.

Video-based collaboration, in IST-118 limited to streaming video, is viable in tactical networks when scalable video streaming is used. H.264/SVC is a well-established scalable video coding standard, and can be utilized for this purpose. For approximately double the processing power one can further cut throughput requirements in half by leveraging H.265/HEVC, which is a promising new solution in this area. For maximum interoperability one currently needs H.264/SVC as that standard is in the NISP.

In addition to the service specific recommendations summarized above, we also recommend to look further into cross-layer adaptations. The tactical level comprises heterogeneous communication technologies, and the services running across these networks have different QoS requirements. In order to be able to meet all these requirements, a tighter coordination between applications and the network is necessary. A cross-layer-based middleware design can serve as a basis for cross-layer optimizations such as optimizing the frequency of publish/subscribe message exchanges to match networking conditions.

In addition to the recommendations given in this document, there is still need for further work: In IST-118 our real-life deployments have only leveraged tactical broadband radios. Though we have emulated narrowband links, it would be preferable to perform further experiments using actual radios. In addition, experiments in hybrid networks consisting of both broadband and narrowband radios would give an extra dimension to any recommendations given. Finally, we have focused on SOAP services in IST-118. Though we had some minor efforts related to REST, such services need further scrutiny in the tactical domain. Consequently, we have proposed a follow-on group to IST-118 that should delve into the realm of both SOAP and REST services in hybrid tactical networks. At the time of finalizing this report, said proposal has been accepted, and the follow-on has been approved as IST-150.

7.0 REFERENCES

[1] C4ISR Technology and Human Factors (THF) Branch, Allied Command Transformation (ACT), “The C3 Taxonomy”, Technical report, 2016. Document generated from the ACT Enterprise Mapping Wiki in November 2016.

[2] Coalition Network for Secure Information Sharing, “Final Report Version 1.0”, 22 August 2013 http://www.consis.info/content/dam/fkie/consis/en/documents/CONSIS%20Final%20report%20v%201%200.pdf.

[3] Bloebaum, T., and Lund, K., "CoNSIS: Demonstration of SOA Interoperability in Heterogeneous Tactical Networks", Military Communications and Information Systems Conference (MCC), 2012.

[4] The Linux Foundation. NETEM. http://www.linuxfoundation.org/collaborate/workgroups/networking/netem. Retrieved 12 Dec 2019.

[5] Home Networks and Communication Systems Branch, U.S. Naval Research Laboratory, "Common Open Research Emulator (CORE)", http://www.nrl.navy.mil/itd/ncs/products/core. Retrieved 12 Dec 2019.

[6] OASIS, "Reference Model for Service Oriented Architecture 1.0", OASIS Standard, 12 October 2006, http://docs.oasis-open.org/soa-rm/v1.0/.

[7] Bartolomasi, P., Buckman, T., Campbell, A., Grainger, J., Mahaffey, J., Marchand, R., Kruidhof, O., Shawcross, C., and Veum, K., "NATO Network Enabled Capability Feasibility Study", version 2.0, October 2005.

[8] World Wide Web Consortium, "Simple Object Access Protocol (SOAP) 1.1", May 2008, http://www.w3.org/TR/2000/NOTE-SOAP-20000508/.

[9] Haas, H., and Brown, A., (eds.), "Web Services Glossary", W3C working group note, http://www.w3.org/TR/ws-gloss/, 11 February 2004.

[10] Fielding, R.T., "Architectural Styles and the Design of Network-Based Software Architectures.", Doctoral dissertation, University of California, Irvine, CA, 2000.

[11] Consultation, Command and Control Board (C3B), "Core Enterprise Services Standards Recommendations: The SOA Baseline Profile Version 1.7.", Enclosure 1 to AC/322-N(2011)0205, NATO Unclassified releasable to EAPC/PFP, 11 November 2011.

[12] Johnsen, F.T., Flathagen, J., Hauge, M., Gjørven, E., Mjelde, T.M., and Lillevold, F., "Cross-Layer Design and Optimizations", FFI-report 2014/00985, http://rapporter.ffi.no/rapporter/2014/00985.pdf.

[13] Jansen, N., Krämer, D., Barz, C., Niewiejska, J., Spielmann, M., "Middleware for Coordinating a Tactical Router with SOA Services", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Krakow, May 2015.

[14] Seifert, H., Franke, M., Diefenbach, A., and Sevenich, P., "SOA in the CoNSIS Coalition Environment: Extending the WS-I Basic Profile for Using SOA in a Tactical Environment", Military Communications and Information Systems Conference (MCC), 2012, p. 1, p. 6, pp. 8-9.

[15] Sliwa, J., and Jasiul, B., "Efficiency of Dynamic Content Adaptation Based on Semantic Description of Web Service Call Context", IEEE MILCOM 2012.

[16] Lund K., Skjervold, E., Johnsen, F.T., and Eggen, A., "Robust Web Services in Heterogeneous Military Networks", IEEE Communications Magazine, Special issue on military communications, October 2010.

[17] Johanson-Lindquister, J., "Improving the Performance of Web Services in Disconnected, Intermittent and Limited Environments", Master's Thesis, University of Oslo, Norway, Spring 2016, http://urn.nb.no/URN:NBN:no-54571.

[18] Johnsen, F.T., Bloebaum, T.H., and Karud, K.R., "Recommendations for Increased Efficiency of Web Services in the Tactical Domain", IEEE ICMCIS 2015.

[19] Bloebaum, T.H., and Johnsen, F.T., "Exploring SOAP and REST Communication on the Android Platform", IEEE MILCOM 2015.

[20] Barz, C., Jansen, N., Alcaraz-Calero, J.-M., Manso, M., Markarian, G., Owens, I., Wang, Q., Meiler, P.-P., Bloebaum, T.H., Johnsen, F.T., Sliwa, J., and Chan, K., "IST-118 SOA Recommendations for Disadvantaged Grids in the Tactical Domain – SOA Experiments on Wireless Broadband Mobile Networks in the Tactical Domain", International Command and Control Research and Technology Symposium (ICCRTS), CCRP publication, USA, 2015.

[21] Manso, M., Alcaraz-Calero, J.-M., Meiler, P.-P., Chan, K.S., Barz, C., Owens, I., Sliwa, J., Jansen, N., Wang, Q., Bloebaum, T.H., Markarian, G., and Johnsen, F.T., "SOA and Wireless Mobile Networks in the Tactical Domain: Results from Experiments", IEEE MILCOM 2015.

[22] Bloebaum, T.H., and Johnsen, F.T., "Evaluating Publish/Subscribe Approaches for Use in Tactical Broadband Networks", IEEE MILCOM 2015.

[23] Bloebaum, T.H., Johnsen, F.T., Brannsten, M.R., Alcaraz-Calero, J.-M., Wang, Q., Nightingale, J., "Recommendations for Realizing SOAP Publish/Subscribe in Tactical Networks", IEEE International Conference on Military Communications and Information Systems (ICMCIS) 2016.

[24] Singhal, A., Winograd T., and Scarfone, K., "Guide to Secure Web Services", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-95, August 2007.

[25] Nordbotten, N.A., "XML and Web Services Security Standards", IEEE Communications Surveys and Tutorials, Vol. 11, no. 3, Third Quarter 2009.

[26] Sliwa, J., Jasiul, B., Podlasek, T., and Matyszkiel, R., "Security Services Efficiency in Disadvantaged Networks", in Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st, pp. 1-5, Glasgow, May 11 – 14, 2015.

[27] Brannsten, M.R., "Federated Single Sign on in Disconnected, Intermittent and Limited (DIL) Networks", IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, May 2015.

[28] Sliwa J., et al., "Efficiency of the Single Sign-On Mechanism in a Tactical Network Environment", Military Communications and Information Systems (ICMCIS), Krakow, May 2015.

[29] Allied Command Transformation (ACT), "CWIX 2015 Final Report Volume I", 18 August 2015.

[30] Allied Command Transformation (ACT), "CWIX 2015 Final Report Volume II", 20 August 2015.

[31] Bloebaum, T.H., and Johnsen, F.T., "Enabling Service Discovery in a Federation of Systems: WS-Discovery Case Study", 19th ICCRTS, Alexandria, VA, 2014.

[32] The Combined Communications-Electronics Board (CCEB), ACP142, "P_MUL – A Protocol for Reliable Multicast Messaging in Bandwidth Constrained and Delayed Acknowledgement (EMCON) Environments", June 16 – 19, 2014. http://jcs.dtic.mil/j6/cceb/acps/acp142/ACP142.pdf.

[33] Johnsen, F.T., Bloebaum, T.H., Kittilsen, K.M., Cetusic, L., Flaatten, H.K., Kjensmo, K., Lothe, E., Pettersen, O.J., Schmid, T.M., and Tungesvik, B., "Collaboration Services: Enabling Chat in Disadvantaged Grids", 19th International Command and Control Research and Technology Symposium (ICCRTS), Alexandria, VA, 2014.

[34] Nightingale, J., Wang, Q., Alcaraz-Calero, J.-M., Owens, I., Johnsen, F.T., Bloebaum, T.H., and Manso, M., "Reliable Full Motion Video Services in Disadvantaged Tactical Radio Networks", IEEE International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016.

[35] Rinicom Ltd., "PodComm", http://www.rinicom.com/products/software-solutions/podcomm/ accessed 7 November 2016.

Appendix 1: COMMON EXPERIMENTS

The recommendations given in the main body of this report are based on a large number of experimental activities, some of which were conducted by one nation alone while other experiments were performed as joint efforts between multiple partners. In these common experiment efforts, multiple partners contributed with service implementations, communications equipment and synthetic experimentation frameworks. The main purpose of these common experiment activities was to test interoperability between components and collect data in order to gain further insights related to overall performance of the optimizations used in different configurations.

Note that the content of this appendix is based on our published papers presented in international peer reviewed conferences. We provide references to those papers, which contain information about the experiments where relevant.

A1.1 WS-NOTIFICATION IN WIRELESS BROADBAND MOBILE NETWORKS

In these experiments [20] [21], we applied SOA Web Services, in the form of WS-Notification, to a Wireless Broadband Mobile Network (WBMN) in the tactical domain. The experiments involved components provided by two different nations, including radio hardware equipment, the publish/subscribe messaging service and NATO Friendly Force Information (NFFI) (as our functional service). We measured the system performance at service and physical (radio) levels in the presence of network disruptions.

As opposed to traditional military networks that are predominantly narrowband, WBMNs provide high data throughput (above 1Mbps). They are, however, still prone to latency and connectivity issues resulting from mobility. As such, the application of SOA-based services in these networks is not straightforward and needs to be assessed.

A1.1.1 WBMN Use Case: Small-Size Tactical Unit

We deployed a small-size tactical unit connected via a WBMN with mesh networking capabilities using Rinicom PodNodes. The unit is constituted by three deployed nodes (representing soldiers, each carrying a wireless broadband radio) operating over an area of 1 km. They report their location and receive each other's location periodically (in real-time).

Depicted in Figure A1-1 are four key locations (labeled as A, B, C and D) defined for the experiments. Node 1 is located in Point A, Node 2 is located in Point C and Node 3 is located in Point B. Only Node 3 will be moving (from B via C to D; and back from D via C to B). The distances between the points varied from 215 meters between Points A and B, to 960 meters between Points A and D.

A1.1.2 Experiment Setup

As part of our experiments, we used components provided by two different nations:

- Publish/Subscribe CES (WS-Notification Broker), provided by FFI (NOR);
- NATO Friendly Force Information (NFFI) FAS provided by FFI (NOR);
- NFFI Subscriber FAS provided by FFI (NOR); and
- PodNode – Mobile Broadband Radio provided by Rinicom (UK).

Openly available network monitoring tools were used in the experiments to collect measurements at physical (radio) and services levels.

Figure A1-1: Small-Size Tactical Unit Use Case (Map Source: OpenStreetMap).

The nodes were setup with Nodes 1 to 3 being mobile and representing deployed soldiers. Each node has the following configuration:

- One PodNode radio;
- One portable computer running an operating system supporting Java Runtime Environment (required to run our service implementations);
- NFFI FAS;
- NFFI Subscriber FAS; and
- Network monitoring and logging tools.

In addition, Node 1 has a special role in the network since it hosts the WS-Notification Broker, which is the service that deals with message subscriptions and exchange.

Figure A1-2 depicts the system architecture used. The services used in the first experiments were not bandwidth-intensive (they only require exchanging a few KBs of data periodically across all nodes) and thus stayed within the capacity of the WBMN.

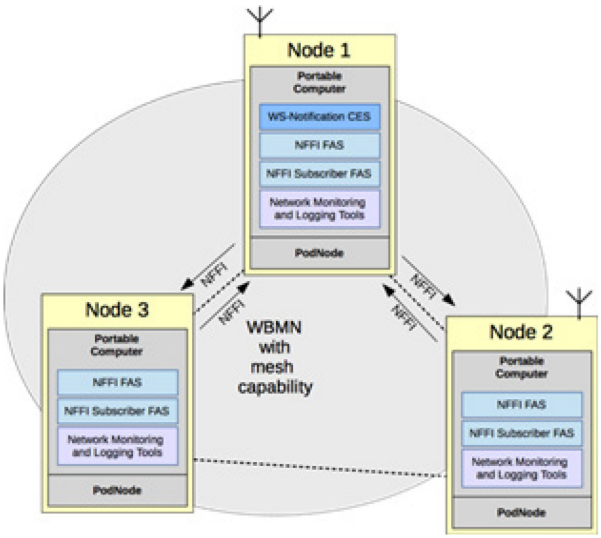


Figure A1-2: System Architecture for Experiments.

A1.1.3 Radio-Level Measurements

We measured the transmission (Tx) and reception (Rx) throughput (in Mbps) over time (each 10 seconds) calculated per link at Node 1 and Node 2.

Results are presented in Figure A1-3, where the experiment timeline is represented on the x axis. Key points in the timeline are marked with vertical dotted lines. The figure contained three different measurements:

- The top chart presents the throughput between Nodes 1 and 2, as measured by Node 1;
- The middle chart presents the throughput between Node 1 and 3 measured at Node 3; and
- The bottom chart presents the throughput between Node 2 and 3 measured at Node 2.

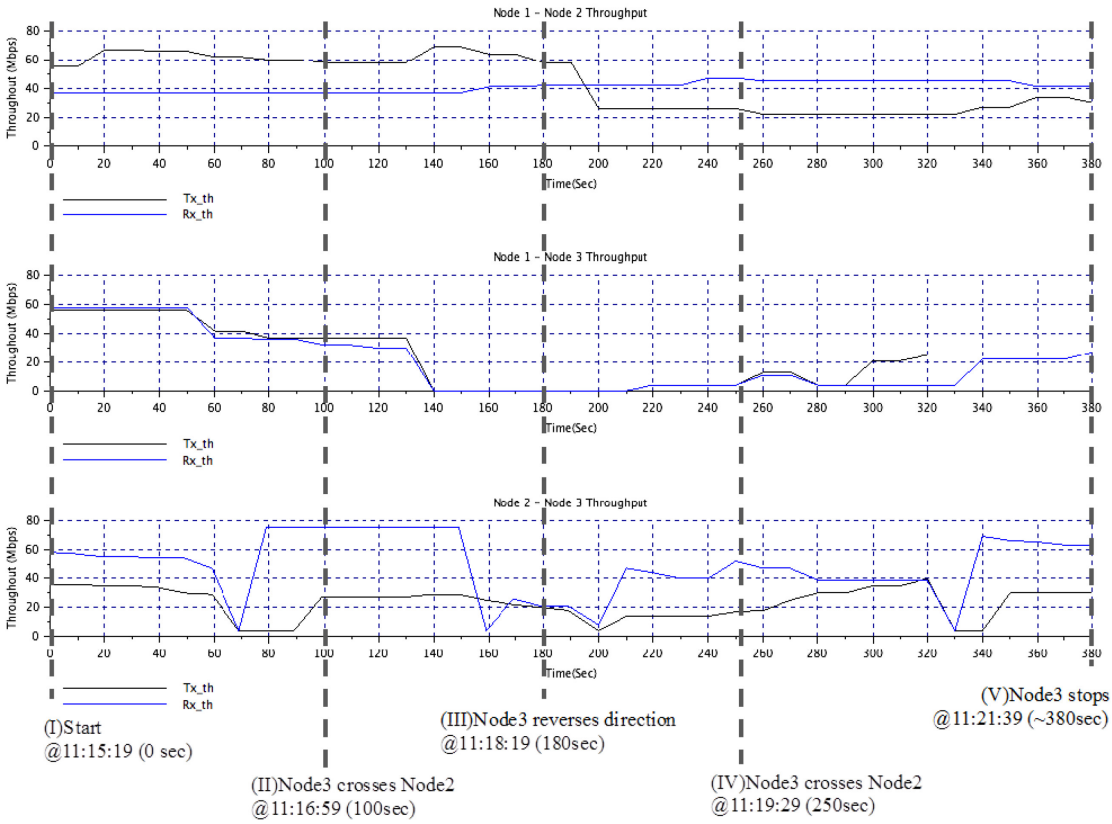


Figure A1-3: Radio-Level Measurements.

For all three charts, the black line and the blue line represent the Tx and the Rx throughput respectively.

We outline the following:

- Node 1 and Node 2 are placed at fixed locations and in line-of-sight. Thus, there is always connectivity between them during the whole experiment.
- Node 1 and Node 3, initially connected, are temporarily disconnected as Node 1 moves further away from Point C.
- Node 2 and Node 3 throughput varies over time as a result of movement and several moments with non-line-of-sight. However, a connection is always present.

A1.1.4 Service-Level Measurements

To assess performance at services level, we measured the number of NFFI messages received by nodes. The results are presented in Table A1-1, which has one row of results per NFFI publisher. The messages from each of these nodes are first sent to the WS-Notification Broker, residing in Node 1, which in turn distributes the messages to the consumers running in all three nodes. Note that the second column displays the number of NFFI messages received at Node 1 (which is also hosting the WS-Notification Broker). As no messages are assumed lost between the broker and the Node 1 consumer (as they are running on the same physical machine), this number functions as the baseline reference.

Table A1-1: Service-Level Measurements: Number of Messages Received.

	@Node 1 Subscriber	@Node 2 Subscriber	@Node 3 Subscriber
Node 1 NFFI Msg	68 (baseline reference)	68 (assumed 0 lost)	66 (assumed 2 lost)
Node 2 NFFI Msg	58 (baseline reference)	58 (assumed 0 lost)	58 (assumed 0 lost)
Node 3 NFFI Msg	51 (baseline reference)	50 (assumed 1 lost)	50 (assumed 1 lost)
TOTAL	**177 (none lost)**	**176 (1 lost)**	**174 (3 lost)**

The third and fourth columns display the number of NFFI messages received by Nodes 2 and 3 respectively. Note that each node receives back the NFFI messages that it produces since the WSN sends all messages received to those that subscribed to the applicable topic(s). The last row displays the total number of NFFI messages received by each node.

A1.1.5 Conclusions

The deployed WBMN proved to be sufficiently robust to support the use case without needing additional optimizations on the service level. The mesh networking features provided by the PodNodes compensated for the network dynamics: most of the time, all nodes were connected either directly or via other nodes.

The NFFI FAS functioned as expected, and the WS-Notification-based distribution proved to be effective. In addition, the transport mechanism used, which was standard TCP, performed reasonably well for this use case. It could be optimized to improve the performance of tactical services, in particular for mobile users.

A1.2 WS-NOTIFICATION CONVOY CASE STUDY AND EXPERIMENT

In these experiments, we applied WS-Notification-based publish/subscribe services to mobile nodes in the tactical domain involving two convoys that exchange information using NATO standards in order to achieve Friendly Force Tracking between different nations. The scenario used in this experiment was the CoNSIS-inspired scenario described in Section 2.3, and we used a hybrid setup consisting of real nodes using WBMN for one convoy and emulated nodes using CORE for the second convoy. This is the same configuration as we showcased during the demonstration event in Porton Down, which is described in further detail in Appendix 2.

The goal of this experiment was to the WS-Notification standard for use in the tactical domain. We applied optimizations (i.e., compression) and measured outcomes related to network performance, such as bandwidth, percentage of packet loss and network delay.

A1.2.1 Experiment Setup

Figure A1-4 shows how the experiment network was set up. On the left side, we used a WBMN formed by Rinicom PodNodes, whereas on the right side we had the emulated tactical network using CORE.

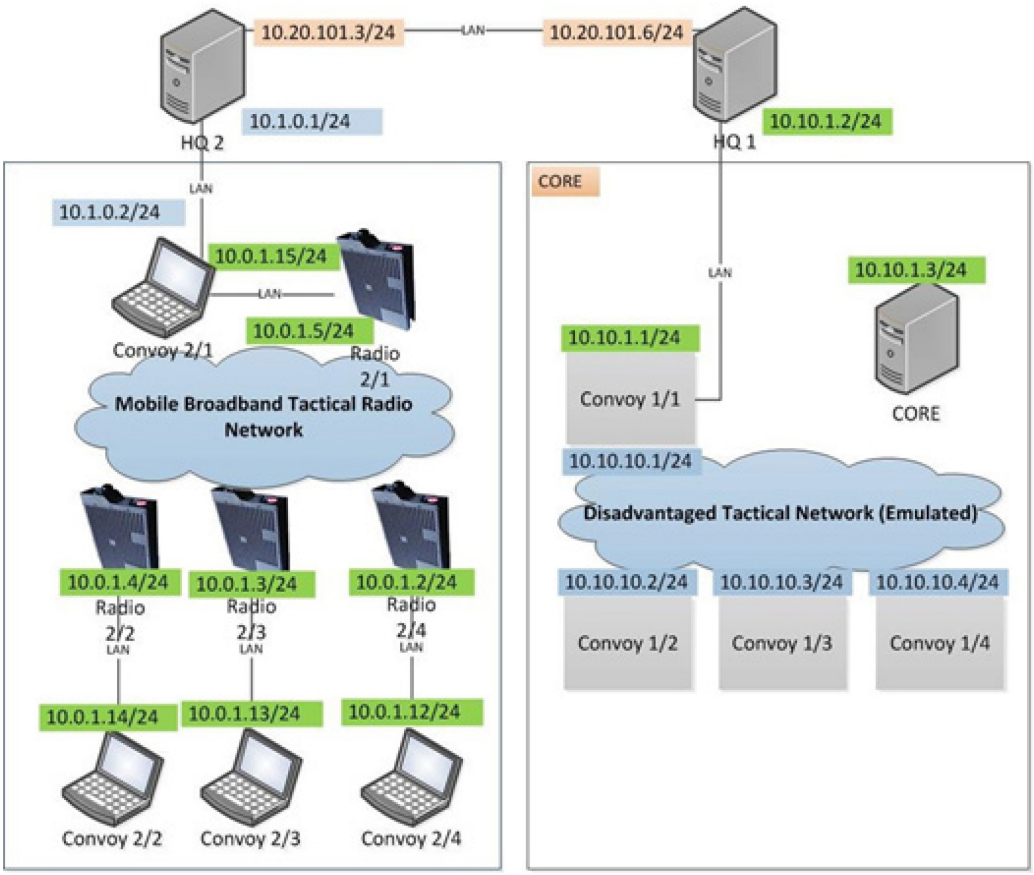


Figure A1-4: Network Diagram.

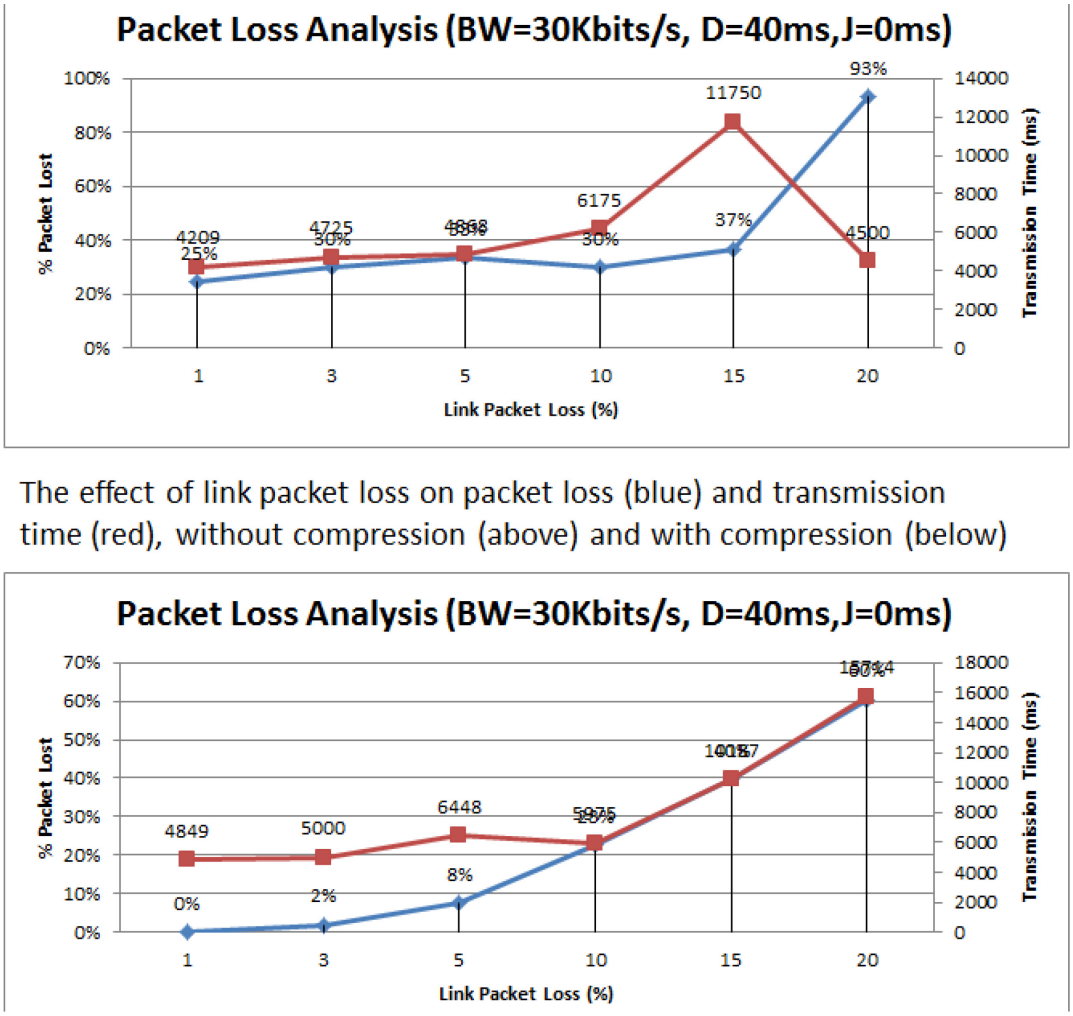
CORE ensured that the communication between the nodes in the convoy had different limitations representing different networking conditions. CORE also simulated node mobility, where disconnections due to nodes being out of radio range were enforced by the link emulation.

Individual position updates were published every five seconds and aggregated positions (the COP) every ten seconds. Statistics were gathered over a course of 30 seconds, and each experiment was run five times. The results shown are averages of these runs. We produced different network aspects using the CORE emulator, namely change throughput from 15 to 1000 Kbit/s, delays ranging from 20 to 320 ms, and packet loss from 0 to 20 %. In addition, we obtained results for both uncompressed and compressed payloads, and we captured three network metrics: packet loss, bandwidth and transmission delay. The results presented herein apply only to the CORE part.

A1.2.2 Packet Loss Measurements

The results pertaining to packet loss are presented in Figure A1-5, which shows the measured packet loss both without (top chart) and with (bottom chart) compression. The throughput was fixed at 30 Kbit/s.

The blue lines, showing the measured packet loss, show that the measured packet loss rate is significantly higher than the configured link level packet loss in both graphs. This means that compressing the message payload not only lowers the number of bytes that needs to be transmitted over the network, but it also reduces the impact of the link loss, as fewer network-level packets need to be successfully transmitted for the middleware-level packet to arrive at the recipient.



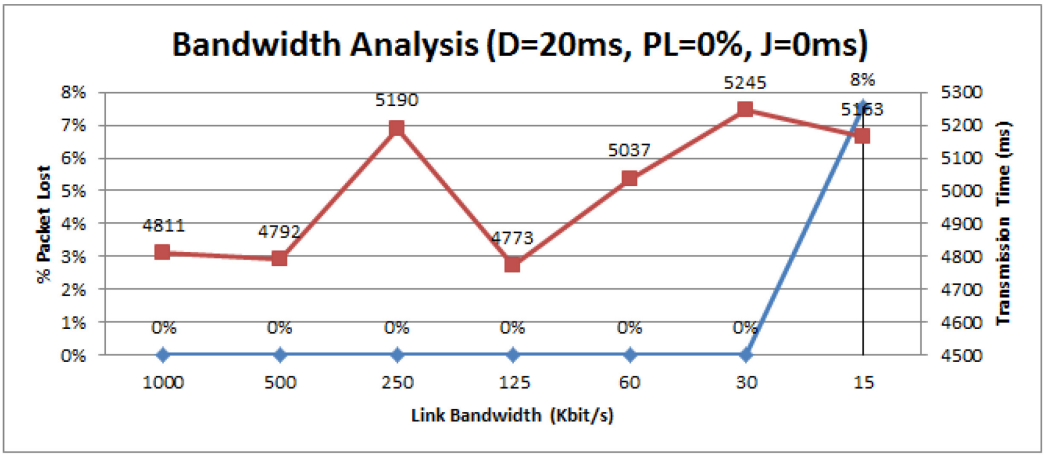
The effect of link packet loss on packet loss (blue) and transmission time (red), without compression (above) and with compression (below)

Figure A1-5: Packet Loss Measurements, Without (Top) and with (Bottom) Compression.

Overall, we see the positive effect of applying compression with respect to the number of packets that are successfully delivered, but the measured results for transmission time (red lines in the graphs) do not show the same improvement. The fact that the total time spent is the same for both compressed and uncompressed data means that the reduction in propagation time achieved by sending smaller messages is offset by the time it takes to perform the compression and decompressing the data.

A1.2.3 Bandwidth Measurements

In the bandwidth (e.g., throughput) analysis, we also tested without compression (see top chart in Figure A1-6) and with compression (see bottom chart in Figure A1-6). The delay was fixed at 20 ms for these tests.



The effect of link bandwidth on packet loss (blue) and transmission time (red), without (above) and with compression (below)

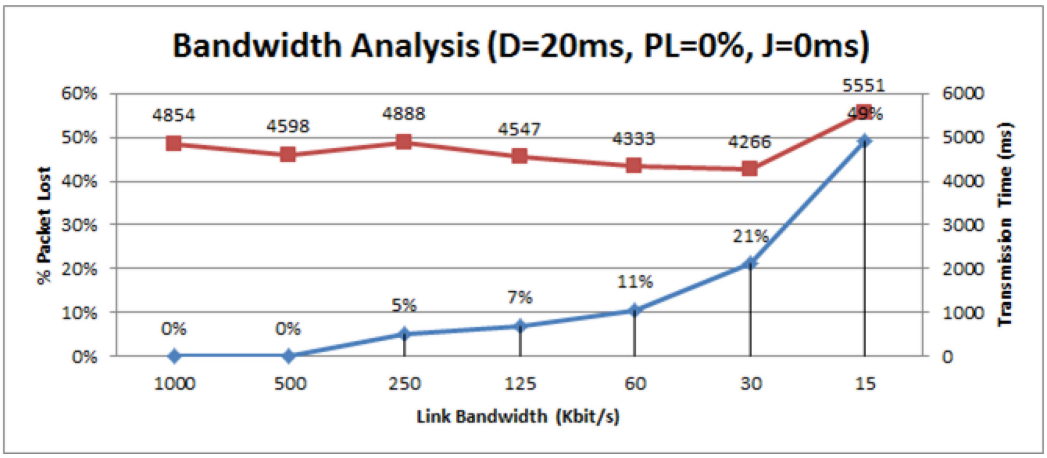


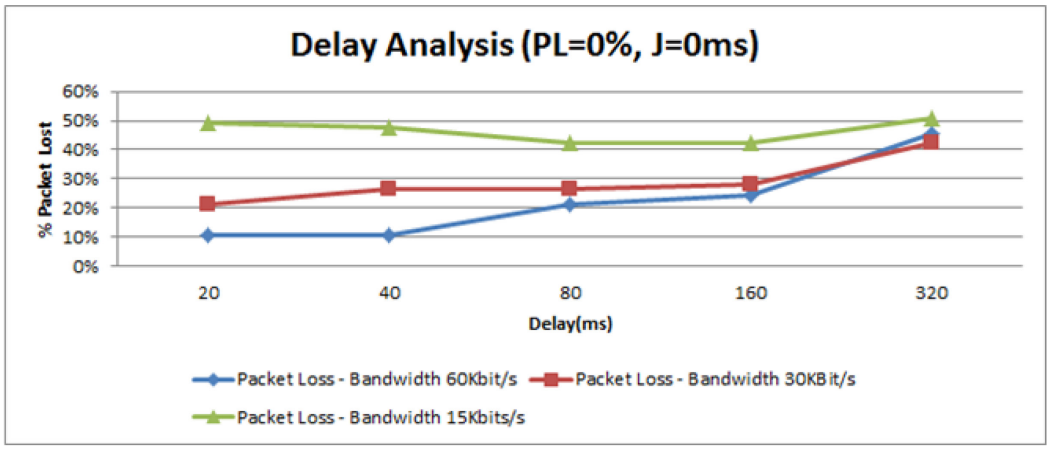
Figure A1-6: Bandwidth Measurements, Without (Top) and with (Bottom) Compression.

For the results without compression enabled, we see that a lower throughput leads to an increase in lost packets.

For the transmission time measurements (red line in the figures), we can see that the measured transmission time when not using compression increases somewhat when the throughput is reduced, but not as much as one might expect. For the results with compression, almost all packets arrived at the recipient, and this leads, as expected, to a larger increase in transmission time as the throughput decreases.

A1.2.4 Transmission Delay Measurements

For the delay analysis we ran the tests with three different bandwidth configurations, namely 15 Kbit/s, 30 Kbit/s, and 60 Kbit/s, and varied the introduced delay between 20 and 320 ms. In Figure A1-7 we show the effect the delay (X-axis) has on the measured packet loss (Y-axis) using no compression (top chart) and compression (bottom chart) respectively.



The effect transmission delay on packet loss, without (above) and with compression (below)

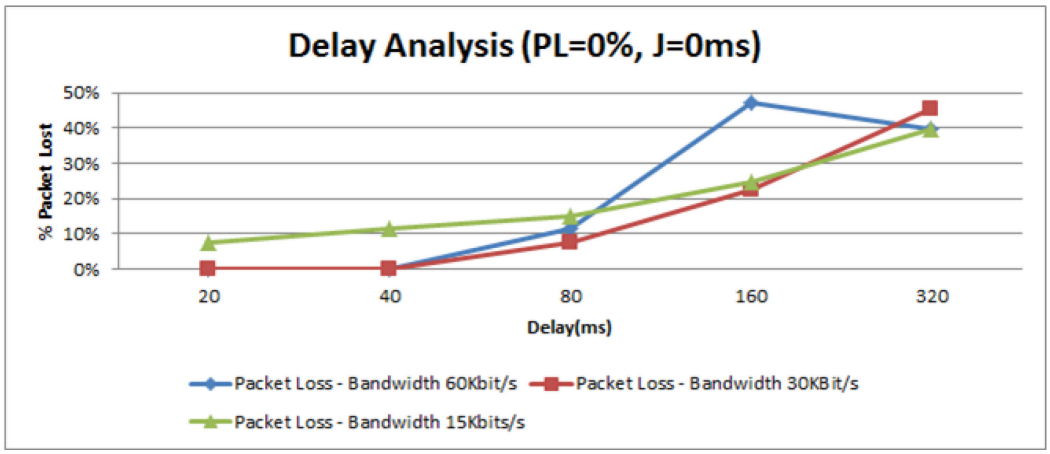


Figure A1-7: Transmission Delay Measurements, Without (Top) and with (Bottom) Compression.

When considering the results without compression, we see that an increase in the introduced delay leads to a higher packet loss percentage. For the measurement with compression, the packet loss is lower than it is when compression is not used, as the smaller amount of data has a lower propagation time, and thus has a better chance of being successfully transmitted. The effect of increasing the delay is however the same as for the uncompressed data – the loss percentage increases as delay increases.

A1.2.5 Conclusions

Based on the results of these experiments, we can conclude that using the WS-Notification standard in the tactical domain is feasible, but that one should consider optimizations (e.g., compression as we used) in an attempt to mitigate the inherent overhead of this XML-based standard.

Appendix 2: DEMONSTRATION EVENTS

As part of IST-118's focus on engaging the wider community, both within NATO and elsewhere, we hosted two different demonstration events for different audiences. This appendix describes the two demonstration events in detail.

A2.1 DEMONSTRATION AT PORTON DOWN 2015

At Porton Down the group organized a demonstration event and gave a status and overview of the group's work up to that point. As such, we gave presentations of the selected core services, our experiments, and our preliminary recommendations for tactical deployment based on our research. Following these presentations, which in effect covered the main matter of this report, we gave a two-part demonstration, where we first showcased WS-Notification in the tactical domain followed by a demonstration of collaboration services using a software called PodComm [35].

The WS-Notification demo was a precursor to the ICMCIS event described in Section A2.2. At Porton Down we focused on tactical broadband (using Rinicom's PodNodes), where bandwidth is abundant when compared to other types of tactical radios.

Starting at the top in Figure A2-1, we have two headquarters (HQ1 and HQ2) that each has one convoy reporting to it. Each HQ node also functions as a router and gateway to each of the convoys. On the left side, all convoy nodes are actual laptops with actual tactical broadband radios connected to them. The radios, Rinicom PodNodes, form their own subnet, and Rinicom's proprietary mesh routing ensures that the radios can exchange information with each other. The convoy lead in this case functions as a router back to HQ2 as well as connecting to the mesh network. With CORE, the situation perceived by the software in each node is that the node is a vehicle in a convoy. However, this is all emulated, and the only physical machine in the CORE convoy is the laptop running CORE itself. This node has a physical link to HQ1, as well as virtual links to the Linux containers inside CORE that represent the vehicles (one container per node). CORE ensures that the communication between the nodes in the convoy have different limitations representing different networking conditions. CORE also simulates node mobility, where disconnections due to nodes being out of radio range will be enforced by the link emulation. At this point, we have the nodes with IP networking and routing fully configured.

Figure A2-1 illustrates the logical information flow (the services and notification subscriptions). Here, we see the logical information flow and the services being provided. Starting with the HQs, both provide a national Common Operational Picture (COP) on NFFI format that is shared among the HQs. Each HQ has a WS-Notification broker, and subscriptions are set from one HQ to the other HQ's broker, so that COP information is published when it becomes available. All vehicles, both nodes connected to actual radios as well as those emulated with CORE are set up with software publishing the vehicle's position (using NFFI) periodically. Each vehicle reports to its convoy lead, which also hosts a WS-Notification broker. The HQ subscribes to its convoy lead's broker, where from which it receives a partial COP (the COP showing the convoy). This partial COP is then merged into the national COP at the HQ level.

The demo was a success, and fruitful discussions followed. During these discussions, we reached the conclusion that using something more disadvantaged than tactical broadband would probably have made a stronger point of the demo. Hence, we started planning for a final event that would take this feedback into account and aptly illustrate our optimizations and suggestions related to publish/subscribe. This final event is described in the next section.

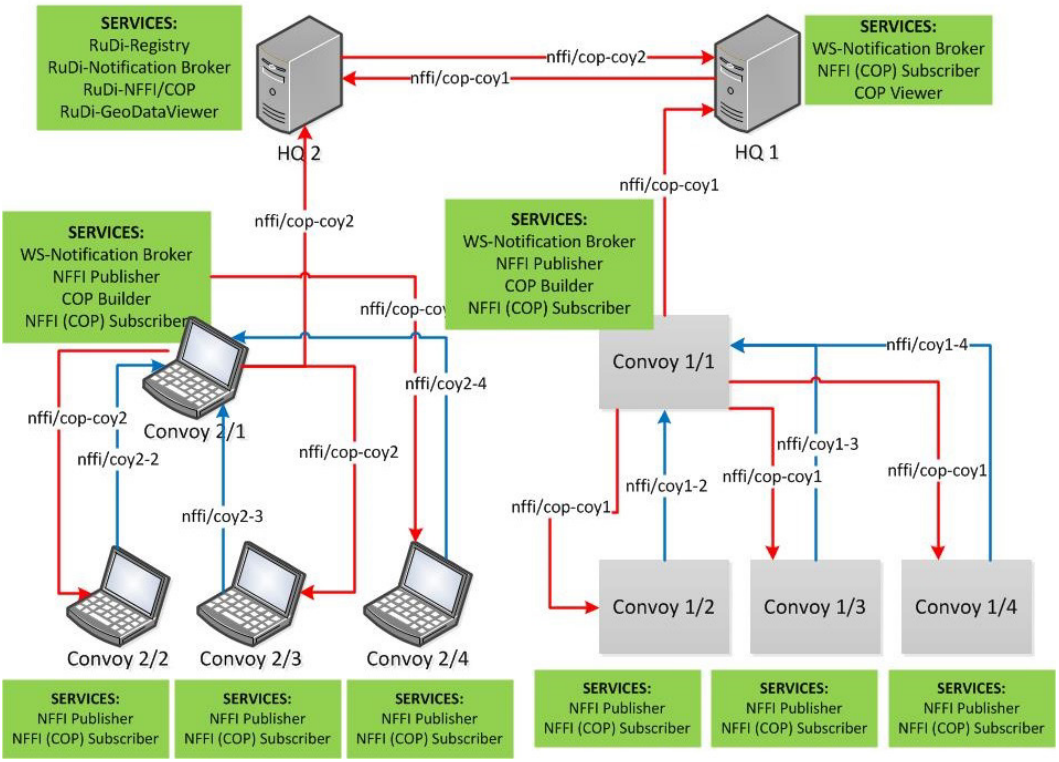


Figure A2-1: Demonstration Setup, Showing the Subscriptions Between Nodes.

A2.2 DEMONSTRATION AT ICMCIS 2016

IST-118 hosted the Tactical SOA workshop during the International Conference on Military Communications and Information Systems (ICMCIS) in May 2016. The workshop was hosted as its own track integrated into the main conference. The workshop, including the keynote given by IST-118 chairman Peter-Paul Meiler, also served as an introduction to the publish/subscribe demonstration that was given after the workshop. In this demonstration two of the IST-118 member nations, Germany and Norway, showed a number of the publish/subscribe optimizations that IST-118 have investigated.

The setup is shown in Figure A2-2, where we had two headquarters, one German (left side) and one Norwegian (right side). Both headquarters had a WS-Notification broker setup, which was used to exchange NFFI tracks between the two nations. At this level, standard WS-Brokered Notification was used to ensure interoperability. Each nation had its own (emulated) convoy that reported positions back to the national headquarters. In these intervehicle networks both nations leveraged their own, proprietary optimizations for WS-Notification.

Germany's setup involved one laptop for the headquarters and for each of their four (emulated) vehicles one laptop and one tactical router. These tactical routers used WiFi-based radio modules to set up an ad hoc network for intervehicle communication. The nodes leveraged cross-layer adaptations where the publication interval of WS-Notification was adjusted to match the available communication resources. So, standard WS-Notification messages were exchanged, but the notification producers had been modified to take the cross-layer information into account before issuing (or choosing not to issue) a given notification. The information was then provided to the German headquarters, where it was also republished as input to Norway's operational picture.

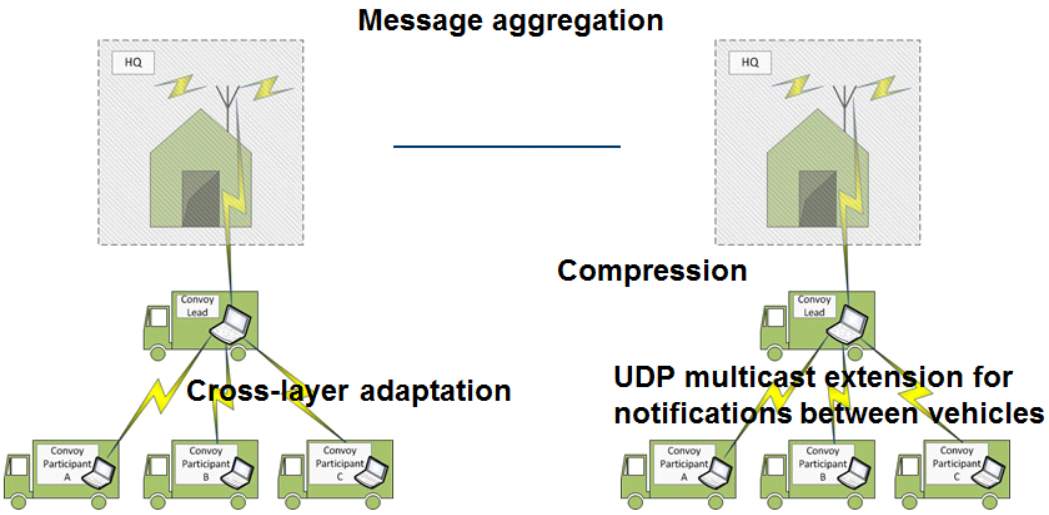


Figure A2-2: Demonstration Setup, Showing Where Different Optimizations Were Utilized.

Norway's setup consisted of just two laptops: one for the headquarters and one for emulating the convoy. The vehicles were represented with virtual machines (VMs), where each VM was equipped with software for blue force tracking. Here, standard WS-Notification messages were exchanged using some proprietary optimizations: First, compression was added to reduce the overhead of XML. Second, the broker (deployed in the lead vehicle) used UDP multicast to disseminate WS-Notification messages in the vehicular network rather than relying on the point-to-point TCP connections that are normally used. Third, the lead vehicle performed aggregation of messages and applied compression before sending the information across the narrow reach-back link to the Norwegian headquarters. There, the messages were uncompressed, and used to visualize the operational picture. The same (uncompressed) information was then republished to Germany for visualization there, as input to the operational picture.

In the demo (see Figure A2-3 for a picture from the event), we successfully showed the exchange of blue force tracking information based on WS-Notification in an efficient and interoperable manner between nations. In addition, we successfully demonstrated the functionality of the tactical level proprietary optimizations and how they could be connected to standards-compliant brokers to ensure interoperability between the nations.

Figure A2-3: Demonstration in Action.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-IST-118 AC/323(IST-118)TP/908	ISBN 978-92-837-2233-5	PUBLIC RELEASE

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

6. Title
SOA Recommendations for Disadvantaged Grids in the Tactical Domain

7. Presented at/Sponsored by
Final Report of RTG IST-118.

8. Author(s)/Editor(s)	9. Date
Editors: Trude H. Bloebaum, Frank T. Johnsen, Peter-Paul Meiler.	May 2020
10. Author's/Editor's Address	**11. Pages**
Multiple	62

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

Analysis	Infrastructure	QoS
Assessment and metrics	Integration	Recommendations
Cross-layer middleware	Interoperability	Service oriented Architecture
Disadvantaged grids	Methodology	Tactical domain
Experimentation	NATO C3 Taxonomy	Video services
Information	NATO Core Services	

14. Abstract

This report provides concrete recommendations, based on systematic testing and evaluation, for Tactical Level application of a subset of the Service Oriented Architecture (SOA) based Head-Quarter (HQ)-level core services from the NATO C3 Taxonomy.

The SOA paradigm is used by NATO for interoperability at (HQ) information infrastructure level. Current technologies (e.g. Web services) are not designed for tactical networks. This frustrates interoperability and integration between tactical and HQ levels and is not cost-effective. IST-118 provides recommendations for the deployment of the core services to the tactical domain, based on experiences and experiments. These recommendations support development of SOA at the tactical level, thus improving integration between tactical and HQ levels. This approach also diminishes the need to develop and implement separate HQ and tactical versions of the same functionalities, thus reducing cost of required materiel, R&D and training.

This report shows the advantage of cross-layer middleware, enabling adaptation of the services' communication behaviour to the special needs of tactical networks and enabling parameterization of the network to fulfil the services' communication requirements, and highlights the contribution of battlefield video- and text-based services. Technology demonstration events show that we reached Technology Readiness Level (TRL) 4 (close to TRL 5).

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

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

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

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

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

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
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

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 Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

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, Ontario 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

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
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 National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

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

GREECE (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
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

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 01 Liptovský Mikuláš 1

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

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

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

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl 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, Ontario 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 978-92-837-2233-5