UiO : Department of Informatics
University of Oslo

Improving the performance of Web Services in Disconnected, Intermittent and Limited Environments

Joakim Johanson Lindquister

Master's Thesis Autumn 2015

Abstract

Lorem ipsum dolor sit amet, cu sed suas apeirian, decore iudicabit at per, pro ne lorem dicit dictas. Cu quo aeque maiorum gubergren, principes complectitur ei ius, numquam veritus minimum mel id. Ea ius vidit soleat. Mel timeam laoreet tractatos no.Pro an sadipscing efficiantur, esse ludus diceret nam in. Vis percipit probatus in. Est noster moderatius dissentiet te. Eirmod latine dissentias in sea, perfecto omittantur at duo, mea vide exerci ut. Nec euismod vocibus consectetuer eu.

Et fierent delectus sapientem eam, id eum dolore nullam. Cu his quod possit utamur, mel offendit copiosae forensibus ut, ius fabulas fierent sapientem an. Sed at vidit mentitum expetendis, utamur insolens ad cum, dicat dicta salutatus ei duo. Est te numquam explicari posidonium. Vim amet nostrud at, ea nam graece mediocritatem, cu fabulas maiorum nostrum vix. Ius id zril nullam aperiam, at sint corpora repudiandae eam.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Military units may operate under conditions where the reliability of the network connection is low. They can operate far from existing communication infrastructure and rely only on wireless communication. Such networks are often characterized by unreliable connections with low date rate and high error rates making data communication difficult. In a military scenario it is necessary for units at all operational levels to seamlessly exchange information across different types of communication systems. This ranges from foot soldiers with radio equipment operating on the battlefield, to the commanding officer in a far away headquarter full of computers. To North Atlantic Treaty Organization (NATO), this concept is referred to as Network Enabled Capability (NEC). In a feasibility study, NATO identified the Service-Oriented Architecture (SOA) paradigm and the Web Service technology as key enablers[1] for such information exchange.

Web Service technology is well tested and in widespread use in civil applications where the network is stable and the data rate is abundant. However, certain military networks suffer from high error rates and very low date rate, which can leave Web Services built for civilian use unusable. This thesis investigate how these challenges can be overcome by applying optimization techniques at different layers of the protocol stack.

1.1 Background and Motivation

NATO is a military alliance consisting of 28 member countries[2] and which primary goal is to protect the freedom and security of its members through political and military means. In joint military operations the relatively large number of member countries can be a challenge when setting up machine-to machine information exchange. Differences in communication systems and equipment attribute to making the integration of such systems more difficult. In order to address this issue, NATO has chosen the SOA concept[3].

1.1.1 Service-Oriented Architecture

Service-Oriented Architecture (SOA) is an architectural pattern where application components provide services to other components over a network. SOA is built on concepts such as object-orientation and distributed computing and aims to get a loose coupling between clients and services. In their reference model for SOA[4], the Organization for the Advancement of Structured Information Standards (OASIS) define SOA as:

Service Oriented Architecture 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.

In SOA business logic is divided into smaller chunks of logic, referred to as *services*. A service can be business related, e.g a patient register service, or a infrastructure service used by other services and not by a user application. OASIS define a service as:

A service is a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description

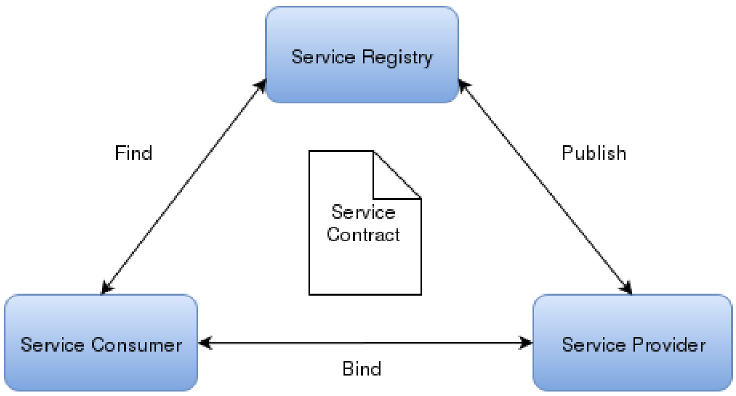

Figure 1.1: The three roles in SOA(from [3])

Following the SOA principles dictates a very loose coupling between services and the consumers of those. This allows software systems to be more flexible, as new components can be integrated with minimal impact on the existing system. Another aspect of loose coupling is with regard to time, which enable services and its consumers to not be available at the same instance of time. This enables asynchronous communication. Loose coupling with regards to location allows the location of an service to be changed without needing to reprogram, reconfigure, or restart the service consumers. This is possible through the usage of service discovery, which is dynamically retrieval of the new location of the service.

Furthermore SOA enables service implementation neutrality. The implementation of service is completely separated from the service description. This allows re-implementation and alteration of a service without affecting the service consumers. Thus this can attribute to keep development costs low and avoiding proprietary solutions and vendor lock-in. Another benefit with SOA is re-usability by dividing common business processes into services, which may help cost reduction and avoids duplication. SOA is only a pattern and the concepts can be realized by a range of technologies. The most common used approach is the Web service familiy of standards, using the SOAP messaging protocol. To achieve interoperability between systems from different nations and vendors, NATO has chosen the Web Service technology in order to realize the SOA principles[5]. This allows member nations to implement their own technology as long as they adhere to the standards. The Web service technology is discussed in detail in section 2.4. Another approach to SOA is Representational State Transfer (REST), which use HTTP over TCP. REST has gained a lot of traction in the civil industry and is discussed in section section 2.4.4.

1.1.2 Military Networks

Web services are in widespread use both in civilian and military applications. Military networks are complex and consist of many different heterogeneous network technologies. We can group them into layers which have different chararistics as can been seen in fig. 1.2. At the highest level, there is fixed infrastructure and relatively static users, meaning that they seldome move around or disconnects. At the lower levels, there are fewer units, but they are much more dynamic. The lower level is called tactical networks which is discussed in the next paragraph.

Tactical Networks

Tactical networks are characterized by that the units are deployed to operate in a battlefield, which means there is no existing communication infrastructure. They use tactical communication equipment which includes technologies like VHF, UHF, HF, tactical broadband and satellites[3].

Examples of such units are mobile units like vehicles, foot soldiers and field headquarters. The tactical network connects deployed headquarters with mobile units. These types of networks are unpredictable and may have very low date rate, possibly high delay, high error rates and frequent disconnections. They are often called disadvantaged grids or Disconnected, Intermittent and Limited (DIL), which is the term used in this thesis. DIL is discussed in section 2.1.

NATO studies[7] have identified such networks to have the following characteristics:

Disadvantaged grids are characterized by low bandwidth,variable

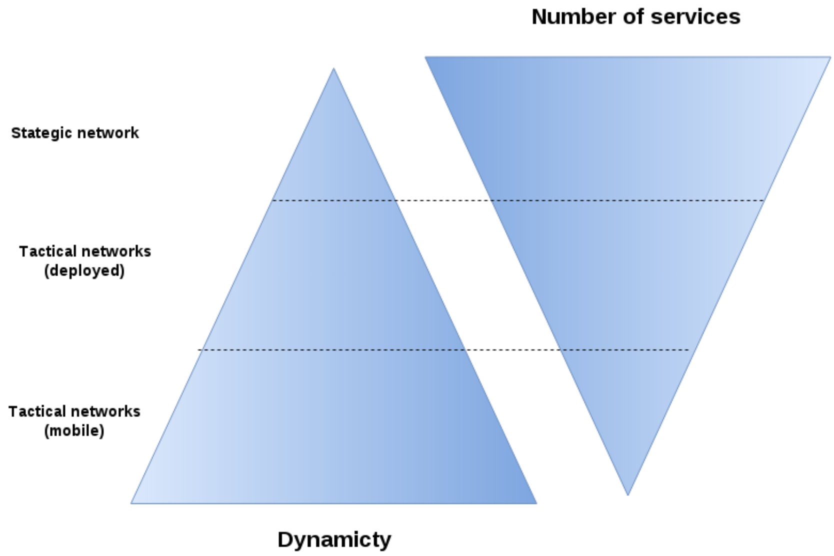

Figure 1.2: Complexity of military networks(from [6])

throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that link the nodes.

The characteristics of these networks and what challenges they impose are discussed in detail in section 2.1.

1.2 Example scenario

Tenkte her å introdusere et scenario som illusterer problemer og utfordringer med DIL nettverk.

1.3 Problem Statement

Most of the Web Service solutions used today are aimed for civilian use and do not necessarily perform well in military environments. In contrast to civilian networks where the date rate is abundant, mobile tactical networks may suffer from high error rates and low date rate. Adapting Web service solutions meant for civil networks directly for military purposes may not be possible. Therefore, Web services needs to be adapted in order to handle network challenges. However, it can be very expensive to alter existing Web service technology and incorporate proprietary solutions. A NATO research task group has previously identified the foundation on open standards to avoid tighter coupling between service providers and consumers[3]. It is much better to use Commercial off-the-shelf (COTS) software. By placing the optimization in proxies, the Web Services can remain unchanged.

The goal of this thesis is to investigate different optimization techniques that can be applied in order to improve Web service performance in DIL networks. In order for the clients and services to remain interoperable the optimization techniques will be placed in proxies. The Web Services will communicate as normal, while all network traffic is tunneled through a proxy. The Web Service itself does not need to pay attention to the bad connectivity, the proxy will choose the appropriate protocol and configuration.

1.4 Premises

The Web services and clients do not need to be changed.

1.5 Scope and Limitations

Sikkerhet er ikke adressert i denne oppgaven(skal kanskje se på IPsec).

SOAP over HTTP klart det mest brukte, samt rest er utelukkende på HTTP. Derfor støtter proxien kun HTTP ut og inn.

1.6 Research Methodology

Denning.

1.7 Contribution

The outcome of this thesis is a recommendation regarding which optimizations techniques which can be used in DIL to enhance the performance of Web services. Aswell as a prototype implementation of a DIL proxy.

1.8 Outline

Hvordan er resten av oppgaven strukturert.

Chapter 2

Background

2.1 Disconnected, Intermittent and Limited

The DIL concept refers to three characteristics of a network. As we discussed in the introduction, military tactical networks may suffer from these constraints.

Disconnected Military units that participating in a tactical network are highly mobile and may disconnect from a network either voluntarily or not. This causes topology changes. Unplanned loss of connectivity can be due to various reasons, such as loss of signal or equipment malfunction. The disconnected term refers to that nodes in the network may be disconnected for a long time, possibly for multiple days.

Intermittent Nodes in a DIL may loose connection temporarily before reconnecting. The duration range from seconds to minutes.

Limited The Date rate, how many bits that are sent per second, is limited in DIL networks. Various aspects that affects the date rate are discussed in the next section.

2.1.1 Network metrics

Link throughput The link throughput is influenced by how large distance there is between the units communicating.

Link reliability How much of the arriving data that is correct. This is called *bit error rate* or *packet error rate*. With high error rates, more data to be transmitted again due to the data arriving being incorrect. This contributes to longer transmission time. In a military setting, an enemy may deliberate sabotage the network with jamming, causing higher error rates.

Link latency The communication technology in use influences how fast data transmission can be done. Long delay may cause that the application sending data timing out.

2.1.2 Other constraints

Energy constraints imposed by the wireless communication grid. The battery capacity and the transmission range of the communication equipment for mobile units may be limited. Another issue is that in some cases military units are required to enter radio silence in order to avoid being detected by the enemy. During radio silence units may only receive data and not send any.

2.2 Related Work

IST-090 ser på muligheten av å bruke SOA på taktisk nivå, med spesielt fokus på disadvantged grids. Fokuserer på mulighet for Web services across disadvantaged networks. Samt Data Distribution Service(DDS) på taktisk nivå.

In the report IST-090, a task group investigated solutions for making SOA applicable at the tactical level. Three key issues that needs to be addressed in order to apply Web Services in tactical networks was identified[8][3]:

End-to-end connections

Web Services depend on a direct, end-to-end connection between the client and the service. Attempting to establish and maintaining connections in DIL environments can lead to increased communication overhead and possible complete breakdown of communication. Most Web Services use TCP as the transport protcol, which is a connection-oriented protocol designed for wired networks. In DIL environments with high error rates and high latencies, the congestion control of TCP will cause sub-optimal utilization of the network due to frequent connection timeouts. Simmilar, HTTP, which is the application layer protocol most often used together with TCP, struggeles in such enviroments. HTTP is a synchronous protocol which means that the HTTP connection is kept open until a response is received. Long response time cause timeouts. IST-090 points out the obivious solution to replace HTTP and TCP with other, more suitable protocols.

The report mentions two approaches to replace HTTP/TCP. The clients and services itself can be modified to support other protocols, or proxies which support alternative protocols can be used. With employing a proxy solution, standards complience can be retained.

Network heterogeneity

Another issue is when heterogenous networks are interconnected. Different performance in networks may lead to buildup of data in buffers, risking loss of information. A proposed solution to this is to have store-and-forward support which can support that messages are not dropped, but stored and forwarded when possible.

Web Service overhead

Web services generate overhead as the Web Service technology is based on SOAP, which use XML-based messages. It is a textual data format and produce much larger messages than binary formats. Optimization approaches should seek to reduce the network traffic generated by Web services by using techniques as compression to reduce the size of messages. Another approach is to reduce the number of messages being sent, which was looked into in IST-090[3]. In their work they investigated three different ways to do this:

1. Employing caching near the client in order to reuse older messages.
2. Using publish/subscribe paradigm, which allows clients to subscribe to information instad of requesting it. This allows the same message to be sent to multiple clients.
3. Employing content filtering, which filters out uneccessary data.

2.2.1 Proxies

This section lists previous implementations of proxies designed to work in DIL environments.

DSProxy

DSProxy is a proxy solution developed by Forsvarets forskningsinstitutt (FFI) which transports SOAP messages over DIL networks. It reduces bandwidth needs by employing different optimization techniques such as compression. It also provides delay tolerance which allows COTS clients to function in DIL networks.

AFRO

Adaption Framework foR Web Services prOvision (AFRO) is an edge proxy which offers different levels of Quality of Service (QoS) to Web Services through performance monitoring and application of the context-aware service provision paradigm. It perform so called adaption actions, which modifies the SOAP XML messages by changing their encoding to more efficient data representation. It also cuts out information that are accepted to be removed by the service requester. However, since the proxy modifies the data being sent, the checksum of the data is also changed. In applications where we want to be sure that no one has tempered with the data before arriving, checksums is often used. Therefor this solution would not work for such applications.

Suri?

Finn ut mer.

2.2.2 Evaluation of Transport Protocols

Previous studies have investigated potential gains from replacing HTTP/TCP with alternative transport protocols [9]. They looked into how TCP, UDP, SCTP and AMQP for conveying Web services traffic under typical military networking conditions.

- Stream Control Transmission Protocol (SCTP) has the highest success rate in military tactical communication. However, on the lower bandwidth links the protocols tends to generate more overhead than TCP. Due to SCTP has a more complex connection handshake procedure and in addition use heartbeat packets.

2.2.3 Configuration

IST-90: Configure HTTP on the application server or ESP to prevent time-outs. Anbefaler at hvis man trenger å gjøre propetiære optimaliseringer, så burde de plasseres i proxier.

2.2.4 Compression

Extensible Markup Language (XML) is the data format used by Web Services and has a significant overhead. Previous studies have evaluated different compressions algorithms for Web services.

2.3 Service-Oriented Architecture

Services are provided by *service providers* and are consumed by *service consumers*. The service provider is responsible for creating a service description, making the service available to others and implementing the service according to the service description. Services are made available to service consumers through a form of *service discovery*. This can be a static configuration, or more dynamic with a central *service registry*, where service providers publish service descriptions. Service consumers find the services they need by contacting the service registry. The communication between services occur through the exchange of standardized messages.

2.4 Web services

Web Services are client and server applications that communicate over a network and can be used to implement a service-oriented architecture. All communication is based on sending XML-based SOAP messages. There exists many definitions of Web services where the core principles are the same, but the finer details may vary. The World Wide Web Consortium has defined Web Services as[10]:

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

This definition points out a set of standards that enables machine-to-machine interactions. These standards are discussed in the following sections. The Web Service technology, following the SOA principles, provides loouse coupling and ease integration beteween systems. Figur her.

2.4.1 XML

XML is a markup language and is considered as the base standard for Web services. An XML document consist of data surrounded by tags and is designed to be both machine and user readable. Tags describe the data they enclose. The tags can be standarized, which allows exchange and understanding of data in a standarized, machine-readable way.

2.4.2 Service descriptions: WSDL

Web Services Description Language (WSDL) is an interface definition language that using XML describes functionality offered by a Web Service. The interface describes available functions, data types for message requests and responses and binding information about the transport protocol, as well as address information for locating the service. This enables a formal, machine-readable description of Web Service which clients can invoke.

2.4.3 SOAP

SOAP (SOAP) is an application level XML-based protocol specification for information exchange in the implementation of Web services. It is transport protocol agnostic and can be carried over various protocols. The far most transport protocol used is HTTP over TCP, but other protocols such as UDP and SMTP can be used as well. A SOAP message is an "envelope" consisting of an optional header and a required body. The header can contain information not directly related to the message such as routing information for the message and security information. The body contains the data being sent, known as the payload.

2.4.4 Representational State Transfer

There also exist other types of Web services which does not follow the previously discussed standards. REST is an architectural style which let users manipulate data using a set of stateless operations. It is based on a client-server model where a client requests data from a server when needed.

It is closely associated with HTTP and use HTTP verbs(e.g GET, POST, DELETE) to operate on resources on a server.

REST is easy to understand and has gained a lot of traction in the civil industry in the latest years. REST uses exclusively HTTP over TCP. However, TCP does not necessarily perform satisfactorily in DIL environments, which limits the usability in tactical networks(trenger kilde?). It also lack standardization, which may have interoperability issues.

2.5 Optimization techniques

The Web service technology enable interoperability between systems, but also increase the information overhead, requiring higher data rate demands. Employing Web Services developed for use in civilian networks directly into a DIL environment may not perform satisfactorily. To increase the performance we can apply optimalization techniques. There are many approaches and optimalization techniques which can be applied at different levels of the protocol stack. In the coming sections the different optimization techniques are presented and a overview is presented in Table 2.1. Another issue that needs to be addressed is, when we have identified optimization techniques, where do we place them? In the application itself or in a proxy? This is discussed in the next section.

2.5.1 Where to place the optimalization?

One approach is to modify the Web service application itself. However, this would mean that every application that is used in a tactical network would require modification. This would require a lot of resources and severely limit the flexibility of using Web services. Another solution is, by using proxies, we can place the optimization there without altering the Web Services themselves. The only thing required to do is to setup the application to send and receive data through the proxy. The proxy will take care of the optimization for tactical networks. This seems like a more reasonable approach and is explored in this thesis.

Protocol Stack	**optimization possibilities**
The application	Optimize the application
Web service messaging: SOAP	Optimize SOAP, e.g XML compression
HTTP/TCP, UDP or other transport protocols	SOAP is transport agnostic. Other protocols can be used.
IP	NATO NEC feasibility study states that all protocols should be over IP.
Lower layers	Not in the scope of this thesis.

Table 2.1: Optimization possibilities.

2.5.2 Compressing the payload

The first optimization techniques deals with the optimization of the encoding. By compressing the Web service payload, we can reduce the amount of data that need to be sent. This optimization technique addresses one of the many challenges of tactical networks, namely the bandwidth consumption due to large message sizes.

- GZIP
- EFX(Efficient XML). XML spesefikt, får ikke brukt på REST når vi har andre payloads..

Previous experiments shows EFX has the compression results with GZIP as the second best alternative[11].

2.5.3 Reducing overhead of SOAP

HTTP/TCP is the most used transport protocol for SOAP messages, but since SOAP is transport protocol agnostic different protocols can be used. Experiments show that this is possible.

Transport Protocol	**Summary**
HTTP over TCP	Widely used. Breaks down in DIL environments.
MQTT	Summary here
Stream Control Transmission Protocol(SCTP)	Features multihoming.
Advanced Message Queuing Protocol(AMPQ)	Application level protocol. Employs a broker architecture with store-and-forward capabilities.
SOAP directly on TCP	Its possible

Table 2.2: Transport protocols

2.6 Transport Protocols

2.6.1 The Constrained Application Protocol

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol designed for use with constrained nodes and constrained networks in the Internet of Things. It is based on the REST model, where the server makes resources available under a URL. Clients access these resources using the HTTP-verbs GET, PUT, POST and DELETE. Designed to use minimal resources, both on the device and on the network.

- Application level protocol.
- Can carry any data format.

- UDP on IP.
- Standardized in RFC 7252.
- Simple binary base header format

2.6.2 Advanced Message Queuing Protocol

Advanced Message Queuing Protocol (AMQP) is a messaging middleware that can utilize different transport protocols.

- Support both request/response and publish/subscribe communication paradigms.
- Reliable when facing network disruptions, since it employs a broker-based architecture with store-and-forward capabilities.

2.6.3 MQTT

MQTT is

2.6.4 Stream Control Transmission Protocol

SCTP is transport-layer protocol which offers functionallity from both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

- Message-oriented like UDP.
- Ensure reliable, in sequence transport of messages with congestion control like TCP.
- Multi-homing and multi-streaming.

2.6.5 Transmission Control Protocol

TCP is one of the core transport protocol of the Internet Protocol Suite.

- Connection-oriented.
- End-to-end reliability.

2.6.6 UDP

WSReliability? For rest må det da bygges inn støtte i proxien. Reliable UDP. Implmentasjon av UDP som er reliable. En gammel protokoll?

- No mechanisms for flow control, packet ordering or integrity of messages.

2.7 Requirement Analysis

A discussed in section 2.2, the dependency on end-to-end connections needs to be removed. This can be done by adding proxies to the network. Mobile units have to carry batteries with them and the capacity is therefore limited. Advanced compression techniques may reduce the overhead, but also requires more battery. This trade-off needs to be considered.

Requirement	**Priority**
Receive and forward HTTP 1.X requests	1
Allow modifications on the payload	1
Allow configuration of HTTP timeouts	1
Keep HTTP-connection alive	1
Support protocol X and y	2

Table 2.3: Proxy requirements

2.8 Summary

Chapter 3

Design and Implementation

3.1 Overall Design

3.2 Proxy

3.2.1 Apache Camel

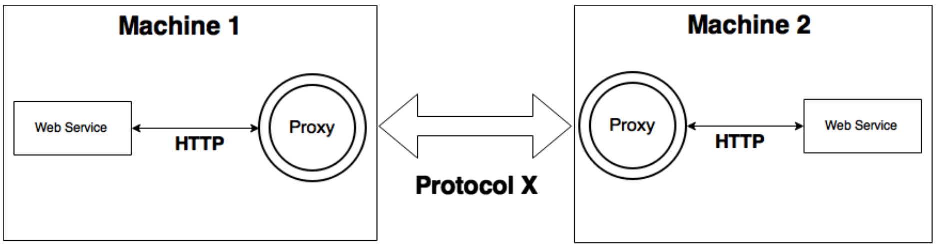

Figure 3.1: Architectural overview of proposed design

3.2.2 Apache Camel

3.2.3 Tuning application server configuration

3.2.4 Alternative transport protocols

3.3 Summary

Chapter 4

Testing and Evaluation

4.1 Evaluation Tools

Chapter 5

Conclusion and Future Work

5.1 Conclusion

5.2 Future Work

Bibliography

[1] P. Bartolomasi et al. *NATO network enabled capability feasibility study*. 2005.

[2] NATO. *NATO - Member Countries*. `http://www.nato.int/cps/en/natohq/nato_countries.htm`. Accessed: 2015-05-04.

[3] F. Annunziata et al. *IST-090 SOA challenges for disadvantaged grids*. `https://www.cso.nato.int/pubs/rdp.asp?RDP=STO-TR-IST-090`. Apr. 2014.

[4] OASIS et al. *Reference Model for Service Oriented Architecture 1.0 OASIS standard*. `http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf`. Accessed: 06. 10. 2015. Oct. 2006.

[5] NATO C3 Board. *Core Enterprise Services Standards Recommendations - The SOA Baseline Profile*. 1.7. 2011.

[6] Frank T. Johnsen. "Pervasive Web Services Discovery and Invocation in Military Networks". In: *FFI-rapport 2011/00257* (2011).

[7] A. Gibb et al. "Information Management over Disadvantaged Grids". In: *Task Group IST-030/ RTG-012, RTO-TR-IST-030* (2007). Final report of the RTO Information Systems Technology Panel.

[8] Frank T. Johnsen et al. "IST-118 - SOA recommendations for Disadvantaged Grids in the Tactical Domain". In: *18th ICCRTS* (2013).

[9] Frank T. Johnsen et al. "Evaluation of Transport Protocols for Web Services". In: *MCC 2013* (2013).

[10] Hugo Haas and Allen Brown. *Web Services Glossary*. `http://www.w3.org/TR/ws-gloss/\#webservice`. Accessed: 2015-05-06.

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

Acronyms

AFRO Adaption Framework foR Web Services prOvision. 19

AMQP Advanced Message Queuing Protocol. 24

CoAP The Constrained Application Protocol. 23

COTS Commercial off-the-shelf. 14, 19

DIL Disconnected, Intermittent and Limited. 13, 15, 17, 19, 22

FFI Forsvarets forskningsinstitutt. 19

NATO North Atlantic Treaty Organization. 11

NEC Network Enabled Capability. 11

OASIS Organization for the Advancement of Structured Information Standards. 12

QoS Quality of Service. 19

REST Representational State Transfer. 13, 21, 22

SCTP Stream Control Transmission Protocol. 20, 24

SOA Service-Oriented Architecture. 11–13, 18, 21

SOAP SOAP. 21

TCP Transmission Control Protocol. 24

UDP User Datagram Protocol. 24

WSDL Web Services Description Language. 21

XML Extensible Markup Language. 20, 21