

Towards Federated Mission Networking in the Tactical Domain

Marianne R. Brannsten, Frank T. Johnsen, Trude H. Bloebaum, Ketil Lund, Norwegian Defence Research Establishment (FFI)

Abstract

NATO is currently working on the Federated Mission Networking (FMN) concept, which will become the foundation for establishing mission networks in the future. The realization of the FMN concept is described in the NATO FMN Implementation Plan (NFIP). The information infrastructure outlined in NFIP today builds on the concept of service-oriented architecture (SOA) in order to achieve interoperability, and bases itself on many of the same standards and specifications as the ones identified through NATO Network Enabled Capabilities (NNEC). The NNEC SOA Baseline [1] identifies a number of Core Enterprise Services (CES) that represent the common functionality needed to build an interoperable service-oriented infrastructure in a federation. A subset of these capabilities includes messaging services, collaboration services, service discovery and security services. It further identifies which standards should be used to realize these core services while ensuring interoperability between the federation members.

This paper looks into each of these foundational core services, and present the challenges related to extending support for these services into the tactical domain and identify potential solutions.

Introduction

NATO is working on the FMN concept to enable efficient establishment of mission networks in the future. FMN consists of three parts; (1) the FMN framework, which serves as a template for how to build mission networks, (2) a number of mission network instances, and (3) a governance structure which oversees both the FMN framework and the specific mission network instances. FMN as a capability will continue to develop over time, and the approved concept¹ uses a spiral approach to the development of FMN.

To realize the FMN concept NATO is working on the NFIP, which is divided into three volumes. Volume I [2] covers the overall concept and governance, Volume II covers the FMN Framework, and Volume III describes the common NATO capabilities. At the time of this writing, the current version of the NFIP is version 3.0, which outlines a spiral approach for FMN Implementation which aims at having an initial capability with limited functionality defined in Spiral 1. The Spiral 1 ambition level is to establish a basic capability, which supports a limited set of mission threads, and enables information exchange down to the deployed headquarters level. Extending the capability to other mission threads and enabling interoperability in the tactical domain is left for future spirals.

The NFIP today consists of many of standards identified in NNEC. Both FMN Spiral 1 and NNEC SOA Baseline focus on interoperability between federation members on the strategic and operational

¹ The Future Mission Network concept was approved by the Military Committee on 16.11.2012, and its name has since changed to Federated Mission Networking.

levels. Neither of these address the additional requirements that arise by including interactions at the tactical level, but later spirals of FMN includes this in their ambition levels. When extending support for the core services into the tactical domain the service implementations need to be adapted to the specific limitations encountered in tactical communications networks. A Disconnected, Intermittent, Limited (DIL) environment is a common description of an environment characterized by the possibility of periodic communication disruptions, bad connectivity, and limitation problems when it comes to both network (e.g., low bandwidth) and node capabilities (e.g., battery life, storage capacity, CPU power).

The CES identified through the NNEC SOA Baseline cover a broad set of capabilities. In the tactical domain, the set of functional services required by the users is smaller than what one would expect to see at higher operational levels [3]. As a consequence of this, the set of CES required at the tactical level is likely to be smaller than what is required in a mission network as a whole.

The NATO RTO/IST-118 working group, titled “SOA Recommendations for Disadvantaged Grids in the Tactical Domain”, has identified a subset of the CES which form a set of foundational core services that should be supported at the tactical level:

- Messaging services – These services enable exchange of messages between systems, and are needed to support basic functions such as Blue Force Tracking, distribution of sensor information and sharing of plans.
- Collaboration services – These services enable communication between humans, and include functionality such as instant messaging, video conferencing and document sharing. Coordination between units involved in the same mission requires that at least a subset of these services is available.
- Service discovery – The inherent limitations of communication resources in the tactical domain means that the availability of services will change over time, and service discovery is needed to handle this dynamicity.
- Security services – Information exchange in the tactical domain must be protected to ensure confidentiality, integrity, availability, authenticity and non-repudiation.

The CES subset listed above are presented in more detail with accompanied tests and evaluations according to our work on the subject in the following sections. We start by looking at messaging services where computer systems on a system level communicate using messages. This fundamental part of information exchange is a first step towards core services on a tactical level.

Messaging between systems

Request/response is a message exchange pattern in which a requestor sends a request message to a service. The service will process the request, and return a response to the requestor. Together with the publish/subscribe message pattern, request/response covers the vast majority of interaction patterns between computers.

Normally, the request/response pattern is implemented in a synchronous fashion, where the connection between the requestor and the service is held open until either the response is returned,

or the request times out. However, it can also be done asynchronously, such that the connection is closed as soon as the request is delivered, and then the response is delivered at some later time, through a callback function. The latter is especially useful when the processing time of the service can be long.

In addition, the request/response pattern can be used for a push-based message delivery pattern, where the data is delivered in the request message, and the recipient only responds with an acknowledgement message.

As opposed to request/response, the publish/subscribe paradigm relieves the client from having to check for new data. Instead, the node simply sends a subscription request to the information provider, asking to be notified whenever new information is available. This has several advantages: The network traffic is reduced, since the client doesn't have to send periodic requests; the server load is reduced, since there are fewer requests to process; and the client will potentially receive new data sooner, although this is dependent on the request frequency in a Request/Response setting (which in turn will affect network and server load). For a given subscription, the notifications are normally always of the same type, independent of the actual information that is delivered (i.e., the payload of the notification). When a client wants to subscribe to a specific type of data, it therefore expresses the type of information it is interested in by including a topic in the subscription request.

Web services

Web services are based on loose coupling between client and server, and instead of having to rely on Application Programming Interfaces (APIs), the focus is on message formats. Thus, a Web service can be used by any platform that supports exchange of messages that conform to the format used by the service interface. Web services often use the XML-based SOAP protocol for information exchange, and are in widespread use on the Internet today, with civil, commercial products and development tools readily available. Both request/response and publish/subscribe are supported.

In a NATO context, there are two general requirements that must be met by any message exchange mechanism, namely interoperability and ability to function in DIL environments.

For publish/subscribe, the use of WS-Notification is specified, including all sub-specifications (WS-BaseNotification, WS-BrokeredNotification and WS-Topics).

Web services in DIL networking environments

Web services in general focus on environments with static networks and abundant data rates, which in a military context typically means strategic, operational, and deployed tactical levels. Consequently, the overhead associated with Web services is not a problem in such environments.

However, in NNEC the challenge is to enable users to exchange information with each other at *all* operational levels. This includes users in the field who may only communicate with others over radio systems with DIL characteristics. Radio systems such as HF or VHF may have a very low data transfer rate, due to the need for long range signals and jamming resistance. In addition, some radio systems suffer from long turn times for directional changes, plus long setup times for connections.

Reducing the traffic generated is thus necessary. This can be done both by the application itself, and by the platform/communication system [4]. Filtering done by the application will typically be based on message content (e.g. only send tracks within a certain radius from the user. On the platform

level, filtering will typically be based on criteria like importance of the message, type of data (e.g. text or video), or priority.

In addition, a common way of reducing network traffic is through compression. Although verbose, XML-based messages are compression friendly, and the size can be reduced significantly, even with standard compression mechanisms like gzip [5].

As mentioned above, NATO has chosen the WS-Notification standard for publish/subscribe. This standard is well-suited to strategic networks, but may require some adaptation for deployment in tactical networks. We have attempted to use WS-Notification over tactical broadband radios and our results show that it functions, but that loss of messages must be expected under poor networking conditions. Figure 1 illustrates this using actual radios. On the X-axis the interval 1-100 is the total message count for the first half of both runs from publisher to broker. The interval 101-200 on the X-axis shows the second half of the experiment runs from broker to subscriber. The Y-axis shows the packet count, thus, the fluctuation illustrates poor conditions leading to retransmissions. In good conditions 12 packets constitute a message sent, and at times more packets are sent in retransmission in order to try delivering the packets and other times the message is lost.

We performed two experiments, using Wm600 Kongsberg radios and a network degradation tool (a matrix of attenuators) for emulation of poor link conditions, using NATO Friendly Force Information (NFFI) [6] over WS-Notification. Note that figure 1 shows some fluctuations in traffic, this can be attributed to signal loss and routing changes. If we were to simulate this, instead of using actual hardware, these results would have looked “cleaner”. The scenario is simple; a deployed user periodically reports his position to a broker, which relays the information back to the tactical forward deployed HQ. In the first run (depicted by the blue line), the radios are well within range and fully connected. 100 messages consisting of multiple NFFI messages were sent, and all were received by the HQ. In the second run (depicted by the red line), the conditions are good between publisher and broker, but poor on the link between broker and subscriber (i.e., HQ). HQ only received 85% of the issued messages due to packet loss and the fluctuation in the packet count resulting in retransmissions.

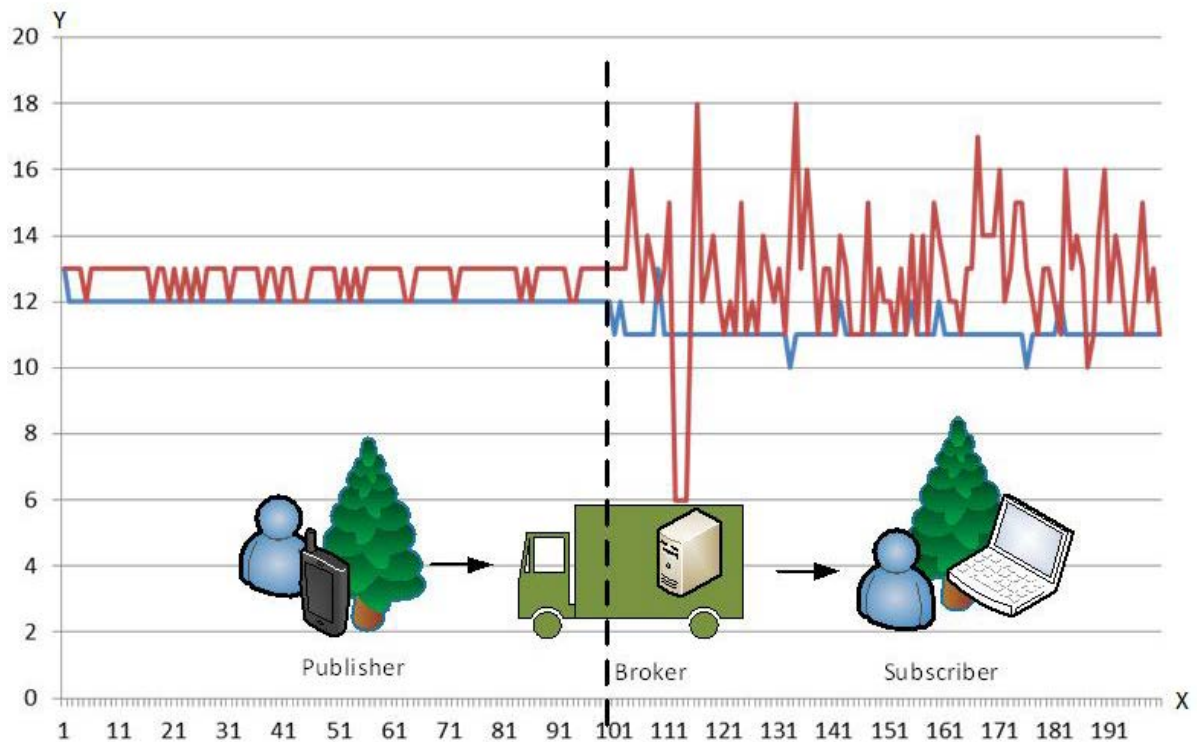


Figure 1 Publish/Subscribe over tactical radio

It should be noted that WS-Notification is a relatively simple standard. In principle, it is a reversed request/response service, in the sense that the server invokes a Web service at the client side when delivering a notification (in other words, it follows the publish/subscribe pattern). In addition, the standard is based on unicast message transmission only, which may have implications in limited capacity networks; even when multiple nodes in the same network want the same information, a WS-Notification broker will send one unicast message to each recipient rather than send one multicast message that reaches all recipients. When subscribers unexpectedly leave the network, permanently or temporarily, WS-Notification is unable to deliver messages to them. NATO has created an add-on to the WS-Notification standard that opens up for caching of messages so that messages can be saved for later delivery [7]. In radio based networks, where the transmission medium is shared, there is a potential for a significant reduction in network load by switching from unicast to multicast. In this case, a reliable multicast mechanism would seem necessary. Note that making such a switch will require further functionality to be implemented into WS-Notification, namely the ability to manage multicast group memberships.

Messaging services as described above enable information exchange between systems. At the next level we need to facilitate collaboration between humans. The following section discusses the parameters for enabling functionality like chat and video conferencing.

Collaboration

Collaboration services are part of the NATO CES, but differ from other services in that they are not pure middleware services as such, but provide functionality directly to the user. Examples of typical collaboration services include audio, video, and chat. The SOA Baseline [1] talks of collaboration

services, but only points to a standard to use for Chat (i.e., XMPP – the Extensible Messaging and Presence Protocol). In this section we summarize available collaboration services and their suitability for the tactical domain.

Commercially available collaboration services can enable collaboration between soldiers in different physical locations. Most current technologies are geared towards use across the Internet or within an enterprise network. The common denominator here is high bandwidth and fairly stable network connections. We have identified three main challenges of using collaboration services in the tactical domain: 1) How applicable are the collaboration services to DIL environments, and to what extent can they be adapted to the tactical domain? 2) Interoperability is of paramount importance. The services must be able to interoperate with other systems. 3) Security must be upheld and compatible with the direction NATO is taking with FMN and the NFIP.

By collaboration services, we mean services related to

- Text, audio and video based collaboration,
- Application sharing, and
- Data sharing

Text based collaboration

Text based collaboration services, often called chat, allow users to exchange text messages. The messages can be delivered either directly between two participants (instant messaging), or between several participants (chat room). In NATO, the XMPP-based JChat is being used. XMPP functions very well in stable, infrastructure based networks. However, as our previous research has shown [8], it is not a protocol directly applicable in the tactical domain. When we talk about increased mobility here, we mean that the nodes' velocity (in meters per second) increases. The mobility model used was random waypoint. As mobility increases, XMPP gradually delivers fewer chat messages, our bespoke solution, Mist [9], delivers more than 99.5% of the messages in all experiments. Mist is an experimental middleware that implements application layer multicast. It is especially designed for use in mobile DIL environments. We use this middleware as a foundation for both experimental chat and service discovery applications. The bandwidth consumed by XMPP is approximately double that of Mist. For complete experiment details, see [8]. These aspects indicate that XMPP is best used in infrastructure-based static networks, whereas other solutions should be employed in the tactical domain where resources are scarce and nodes are mobile. Note that all communication with the XMPP server was compressed using zlib compression, and that we used a single multi-user chat room.

Audio, video, application, and data sharing collaboration

These kinds of services are well understood and much used in the civil domain, and can also be used in infrastructure-based networks. However, they are to a lesser degree employed in tactical networks (particularly those with high mobility and low bandwidth) where conventional solutions do not function.

For all of the above areas, the current state of the collaboration services is shown in Table 1. There, the colors of the cells indicate the state of available solutions and products. The green area in the

table indicates that, even though there may still be open issues, this area is well covered by current solutions. The yellow areas indicate that there are known solutions, but there are still some open issues. The red areas indicate that more research is needed. For further details, see the survey of existing applicable technologies given in [10].

Table 1 Current state of collaboration services (adapted from [10]).

	Chat	Audio and video	Data-centric collaboration services
Adaptation to the tactical domain	Solutions are known and tested.	Known solutions work well in the civil domain, but must be tested in the tactical domain. A specific implementation must be explicitly tested for compliance.	New trends in the civil domain barely introduced in the military domain.
Interoperability	Agreement on XMPP, but tactical adaptations and security protocols are not standardized. Requires a gateway between proprietary solution and standardized XMPP to function seamlessly.	Several standards exist, but in practice interoperability is not always achievable.	Well established standards in the civil domain, but these have to be adapted to the tactical domain.
Security	Known mechanisms can be applied, but open issues exist related to tactical adaptations and interoperability.	Interoperability issues related to streaming and many-to-many communication.	No support for classified information. Largely based on network and transport layer security.

Messaging and collaboration both play an important part towards FMN. In addition to these services, as we discuss in the next section, service discovery is important to facilitate an up-to-date view of the available services (e.g. weather, chat, email).

Service discovery

Operating in a DIL environment puts an additional demand on service discovery. Services will change over time and the dynamicity has to be handled accordingly.

A strategic level fixed network can employ civilian standard service registries for discovery like UDDI or ebXML. UDDI and ebXML are central registries, constituting a single-point-of-failure. The further one moves from fixed networks, the more one needs an interoperability gateway to mediate service discovery between levels [3].

Web Service Discovery in DIL networking environments

Deploying technology designed for fixed-infrastructure networks on tactical networks might not be feasible as resources can be scarce and there are no guarantees for connectivity at any given time. Web service discovery is an important part of the Web service scheme, and in [11] we evaluate Web service discovery in military tactical networks. Important criteria for service discovery in such environments are that discovery needs to be distributed and robust. All participants in an operation need to be able to both use and potentially share their services.

As mentioned above, standard Web service registries are not suitable for DIL environments. WS-Discovery is somewhat better as it is a distributed solution, eliminating the problem of “single point of failure,” but it still is designed for an office environment and does not take into consideration the specific challenges of a DIL environment.

Another service discovery parameter to consider is if the service discovery solution is reactive, where the client probes for updates; proactive, where updates are sent automatically at given time periods; or user-initiated. A client will include a cache of discovered services, and either the client regularly probes to see what services are available at the moment and eliminates cache entries that are no longer responding to probes (reactive), or the services regularly issue advertisements and the client adds advertised services to the cache and declares services that are no longer being advertised to be stale (proactive). More frequent probing consumes more bandwidth, but allows clients' caches to be more accurate to conditions. Each client probing the network individually consumes more bandwidth than each service issuing regular advertisements. However, clients would need to time-out stale cache entries quickly if they don't hear an advertisement in a while. Less frequent probing or advertising-and-staling saves bandwidth at the cost of client cache accuracy.

To evaluate Web service discovery solutions in DIL environments we considered both reactive and proactive discovery protocols. Protocols designed for DIL environments are SAM and Mist. SAM is short for Service advertisements in MANETs [3]. It is an experimental service discovery protocol developed especially for use in DIL environments. SAM Service advertisements are sent at regular time periods using IP-multicast. Mist, on the other hand, does not rely on IP-multicast. The last solutions to be evaluated are the Service Location Protocol (SLP) originally designed for other purposes, but with some adaptation enabled to be used for Web service Discovery, and finally WS-Discovery.

Testing and evaluation of DIL Web service Discovery

In order to illustrate the usefulness of different Web service discovery protocols in DIL environments, we have evaluated them in specific node configurations according to bandwidth usage. The result shows there is a need for specialized protocols to efficiently operate in DIL environments.

The participating nodes are configured in different types of topologies during a mission. As shown in figure 2. there are in some cases several smaller groups where the physical topology of the groups vary from a cluster topology, where the nodes all are in reach of each other, to a fan-out topology, where the nodes form a line and there might not be connectivity between all the nodes, but only between direct neighbors.

The first part of Table 2 describes the results of evaluating a fan-out topology. WS-Discovery and SLP are reactive protocols. They use the most bandwidth in contrast to Mist and SAM. This is true for

both central and edge nodes. In a fan-out topology it is important to notice the difference between average bandwidth of the central node of the topology and the nodes residing at the edge of the topology because the central nodes are responsible for forwarding on behalf of other nodes.

The second part of Table 2 describes the average bandwidth results for a cluster-topology. In a cluster all the nodes are within reach of each other. If you look at the “Per node” result it is approximately the same as for the “Edge” nodes in the fan-out-topology as the topology enables direct requests to all nodes. The bandwidth per query is a calculation of bandwidth divided on queries per second, whilst the proactive have a constant usage of bandwidth to maintain state.

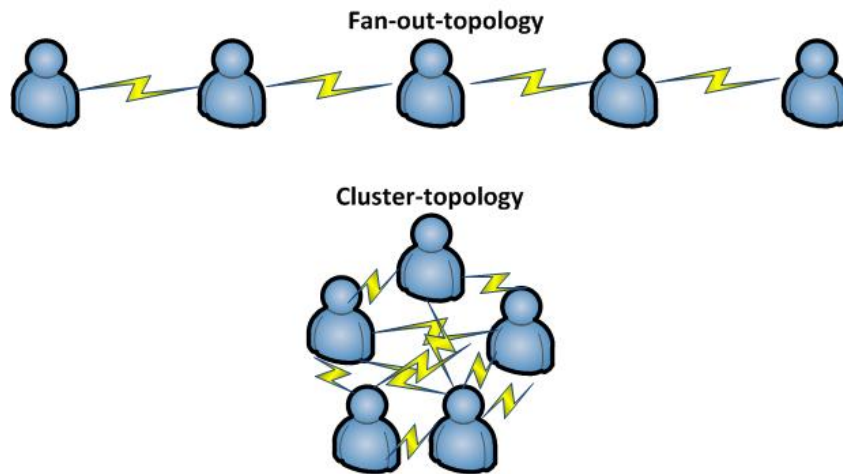


Figure 2 Fan-out-topology vs. cluster-topology

Table 2 Average bandwidth for cluster- and fan-out- topology (from [11])

<i>Average bandwidth for fan-out-topology</i>				
<i>Protocol</i>	Mist	WS-Discovery	SAM	SLP
<i>Central</i>	0.06 KB/s	14.90 KB/s	0.28 KB/s	7.12 KB/s
<i>Edge</i>	0.05 KB/s	2.28 KB/s	0.02 KB/s	1.05 KB/s
<i>Average bandwidth for cluster-topology</i>				
<i>Protocol</i>	Mist	WS-Discovery	SAM	SLP
<i>Total</i>	0.62 KB/s	27.30 KB/s	0.27 KB/s	12.57 KB/s
<i>Per node</i>	0.05 KB/s	2.27 KB/s	0.02 KB/s	1.05 KB/s
<i>Per query</i>	N/A	27.08 KB/q	N/A	12.59 KB/q
<i>Per query/node</i>	N/A	2.26 KB/q/n	N/A	1.05 KB/q/n

The result of testing Web service discovery in different military squad topologies revealed that WS-Discovery and SLP should not be used if bandwidth is a concern. The experimental solutions Mist and SAM showed a much more efficient solution in DIL environments.

Handling service discovery in a DIL environment is a challenge. Another challenge is to ensure the security of services. In the next section securing Web resources is discussed.

Security

In FMN, information exchange and collaboration between nations span more than one security domain. Inside a security domain the Web resources are often guarded with security solutions, such

as Web authentication where participants are granted and denied access based on e.g. username and password. In a federated scenario we manage such authentication with setting up trust relations between the different systems enabling participants to access several security domains authenticating only to their local authentication authority in a Single Sign On (SSO) scheme.

However, in a military setting there are some potential limitations to take into consideration. In the civil arena there are more than enough bandwidth and stable connections, but in DIL environments the overhead created by the security solutions might be costly for the network and influence the stability of the resources available.

Web Authentication

Users often have to authenticate before they are granted access to a Web resource, and it is the site owner that handles the authentication scheme, e.g. username and password. More and more sites collaborate in order to give the users a complete solution to their specific problem. As an example, consider that a user is going on a trip and needs a flight and a hotel. The airline and car service might be separate sites, and if the user had to authenticate at both sites this can become troublesome and time consuming. Remembering several passwords is a challenge in itself. But if the airline and car service collaborate, and they agree on trusting each other to authenticate users in an SSO setting they allow a user to authenticate at one site and get access to the other site automatically.

In [12] we study the cost of adding an SSO solution using SAML 2.0 in a federated environment. These results are complimentary to the work done in [13] where we measured and evaluated overhead of SOAP security and showed that the SOAP messages increased in size by a factor of five when compared to running with no security. The study exposed a potential problem of bringing such solutions to DIL environments. Traditionally SSO is handled in browser cookies, where the cookies store access information. When an SSO solution is to include more than one Domain Name System (DNS), the cookie solution will not work as a cookie may not be shared between DNS domains. The SSO scheme adopted in our experiments are the use of a central service handling Web authentication. The entities handling security are an Identity Provider (IdP) and a Service Provider (SP). Digital certificates form the basis for trust between IdP and SP, so a functioning Public Key Infrastructure (PKI) is a prerequisite for SSO.

SP is the security lock on the resource that can be opened by the security tokens. The security tokens are the responsibility of the IdP which produces and distributes security tokens when the identity of a user is established.

Enterprise vs. Federated SSO

In a military setting a Web resource federation scenario is very important as it enables collaboration between coalition partners, enabling them to easily share Web resources. But while bringing SSO into a federated scenario there are even more challenges implementing a SSO solution in a federated DIL environment.

The enterprise scenario requires all the participants to belong to the same enterprise, and Figure 3 depicts two enterprises in a federation. The Consumer has a direct trust relationship to the local IdP, and the IdPs of the different enterprises forms a trust relation across enterprise borders. The SP secures a Web resource. When the Consumer, in the remote domain, requests access to the Web resource without an authentication token, the SP redirects the Consumer to acquire one from the local domain's IdP. If the Consumer successfully authenticates to the local domain's IdP, the IdP further requests a token from the remote domain's IdP authorizing access to the Web resource.

Security Overhead in DIL

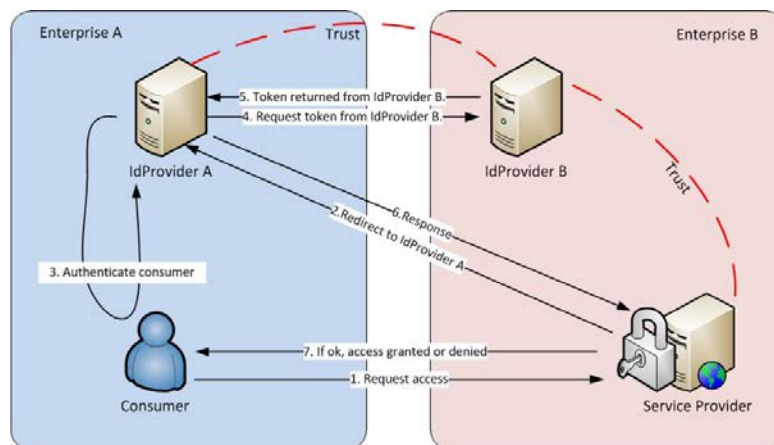


Figure 3 Federated Web authentication

There are two ways of initiating Web authentication, SP-initiated or IdP-initiated. This is defined as to where the user goes first. A user can start by going to SP, getting redirected to IdP, and then directed back after authentication, or the user can go to the IdP first, authenticate and then manually go to the SP to request access.

Table 3 shows the measured results of SP initiated SSO and IdP initiated SSO. The overhead ranges from 5233bytes to 7252bytes. If the user already has a valid token the overhead only diminishes between 165 bytes and 370 bytes. This tells us that the evaluation of how long a token is to be valid is not that important when considering overhead. The result is rather that adding security is costly, but at the same time it is a necessity.

Table 3 Federated Web authentication [12]

Federated SSO	Network traffic in bytes		
	Network traffic	Payload	Overhead
SP-initiated SSO (not logged in)	7459	207	7252
SP-initiated SSO (logged in)	7089	207	6882
IdP-initiated SSO (not logged in)	5505	207	5298
IdP-initiated SSO (logged in)	5340	207	5133





There are experimental approaches to supporting SSO in DIL environments with low overhead, an example being [14]. However, interoperability has largely been neglected in such experimental solutions. Hence, further research is necessary in order to bring interoperable SSO to the tactical domain.

Summary

The realization of the FMN concept rests on NATO's work on the NFIP. Future NFIP spirals include work on enabling interoperability in the tactical domain. NNEC also focuses on interoperability and points to SOA and Web services as an enabling technology. CES identified for this enablement are amongst others: messaging, collaboration, discovery and security. These CES were evaluated on the tactical level in this paper. We found that further research is still needed in different areas in pursuit of fully realizing FMN in the tactical domain.

References

- [1] 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.
- [2] North Atlantic Council. NFIP Volume I. Approved 29.01.2015
- [3] Frank T. Johnsen, Trude Hafsv e, Anders Eggen, Carsten Griwodz, P al Halvorsen , *Web Services Discovery across Heterogenous Military Networks*, *IEEE Communications Magazine*, October 2010, pp. 84-90
- [4] NATO Science and Technology Organization. *STO-TR-IST-090 - SOA Challenges for Real-Time and Disadvantaged Grids*. STO-TR-IST-090 AC/323(IST-090)TP/520. Final Report of TR-IST-090. ISBN 978-92-837-0195-8. April 2014.
- [5] Teixeira, M.A., et al., *New Approaches for XML Data Compression*. In proceedings of International Conference on Web Information Systems and Technologies (WEBIST 2012), pp.233–237., 2012.
- [6] NC3B Information Systems SC, *Interim NFFI Standard For Interoperability of FTS*, AC322(SC5)N(2006)0025, 16 (Approved on 16 December 2006)
- [7] NCI Agency. TTB Notification Cache V1.1.0.
http://tide.act.nato.int/tidepedia/index.php?title=TTB_Notification_Cache_V1.1.0 (Access requires a Tidepedia account), 26 March 2013.
- [8] Magnus Skjegstad, Ketil Lund, Espen Skjervold, and Frank T. Johnsen. *Distributed chat in dynamic networks*. IEEE Military Communications Conference (MILCOM) 2011, pp.1651-1657, 7-10 Nov. 2011, Baltimore, MD, USA.
- [9] Magnus Skjegstad et.al., *Mist: A Reliable and Delay-Tolerant Publish/Subscribe Solution for Dynamic Networks, New Technologies, Mobility and Security (NTMS), 2012 5th International Conference, 2012*
- [10] Eli Gjørven et al., *Towards NNEC – breaking the interaction barrier with collaboration services*, FFI-Report 2014/00943, <http://rapporter.ffi.no/rapporter/2014/00943.pdf>
- [11] Magnus Skjegstad, Frank T. Johnsen, Trude Hafsv e, *An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield*, Military Communications and Information Systems Conference (MCC) 2011, Amsterdam, Netherlands, 17-18 October 2011
- [12] Marianne R. Brannsten, *Federated Single Sign On in Disconnected Intermittent and Limited (DIL) Networks*, IEEE VTC2015-Spring International Workshop on Service-Oriented Computing (SOC) in Disconnected, Intermittent and Limited (DIL) Networks (SOC-DIL), Glasgow, Scotland, May 2015.
- [13] Trude Hafsv e et al., *Using Web Services and XML Security to Increase Agility in an Operational Experiment Featuring Cooperative ESM Operations*, 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington DC, USA, June 2009.
- [14] Anders Fongen. *Federated identity management in a tactical multi-domain network*. International Journal on Advances in Systems and Measurements, vol 4, no 3&4, 2011

	<p>MARIANNE R. BRANNSTEN (Marianne-rustad.brannsten@ffi.no) is a research scientist at the Norwegian Defence Research Establishment (FFI), engaged in theoretical research and practical development in areas such as distributed systems and Service Oriented Architecture. She received her Master's degree from the University of Oslo (UiO) in 2006, and has been working at FFI since then.</p>
	<p>FRANK T. JOHNSEN (frank-trethan.johnsen@ffi.no) received his Ph.D. from UiO. He started work as a scientist at the Norwegian Defence Research Establishment (FFI) in 2006. At FFI he is currently working within the area of secure pervasive SOA. His research interests include Web Services, Quality of Service, and middleware. He also holds a position as part-time Associate Professor at UiO.</p>
	<p>TRUDE H. BLOEBAUM (trude-hafsoe.bloebaum@ffi.no) is a scientist at the Norwegian Defence Research Establishment (FFI), where she has been working since 2006. Before coming to FFI she worked with content distribution systems at UiO. She received her Cand.scient. degree from UiO. Her research interests are Web Services, Quality of Service, and network protocols.</p>
	<p>KETIL LUND (ketil.lund@ffi.no) is a scientist at the Norwegian Defence Research Establishment (FFI), where he has been working since 2006. His research interests include Service Oriented Architectures, Web Services, Quality of Service, and middleware. At FFI he is currently working within the area of secure pervasive SOA. He received his Ph.D. in informatics from UiO.</p>

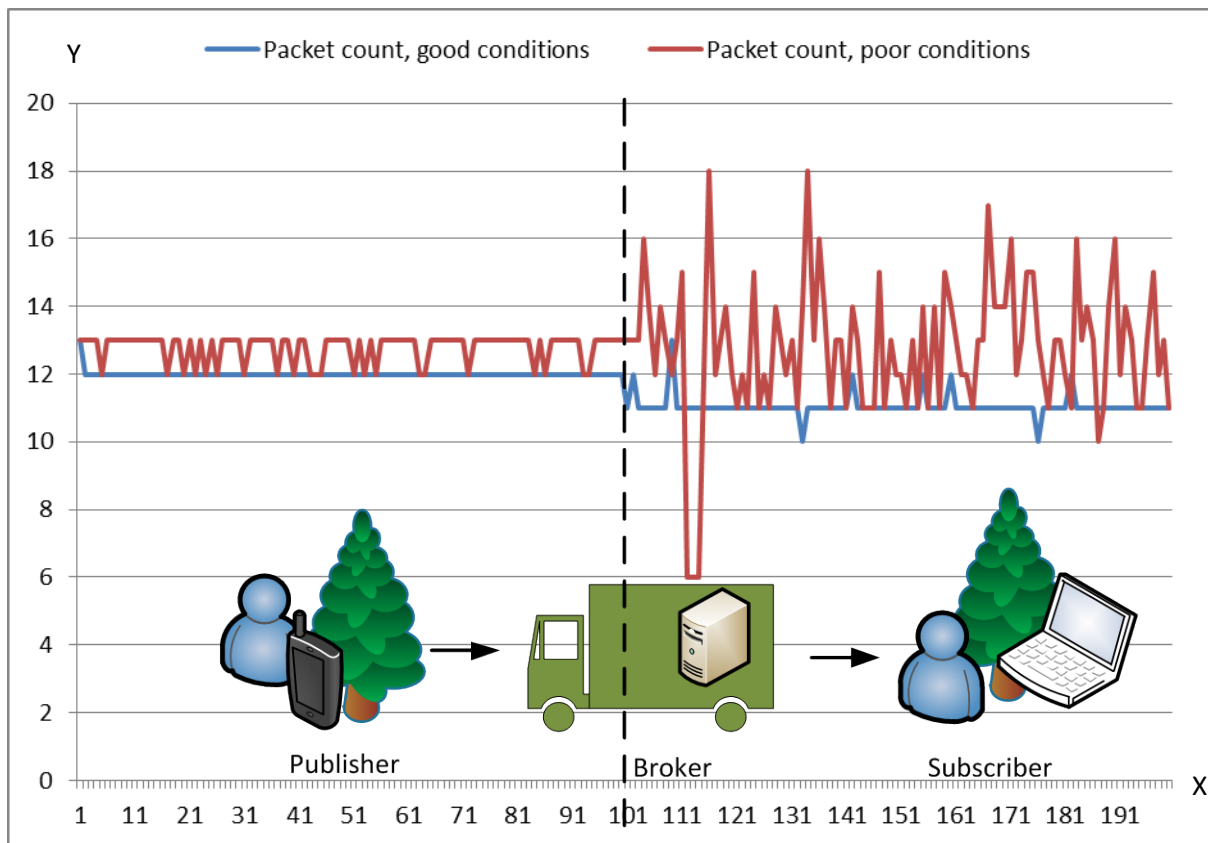


Figure 1 Publish/Subscribe over tactical radio

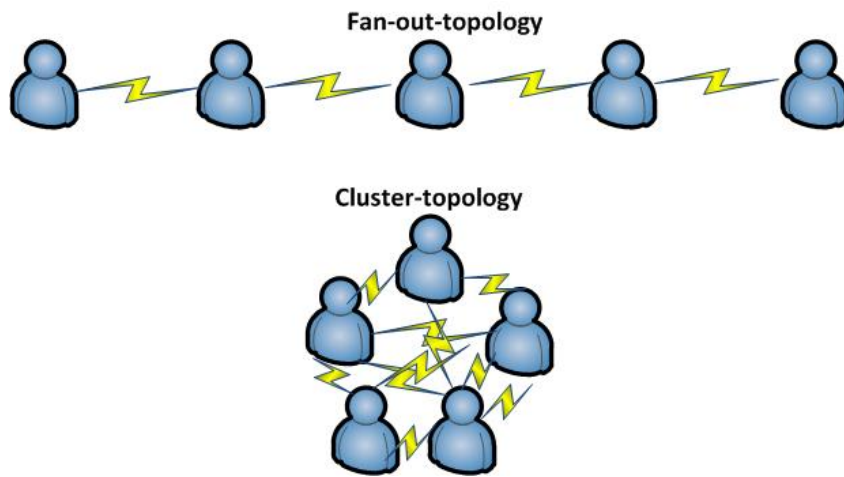


Figure 2 Fan-out-topology vs. cluster-topology

Table 1 Current state of collaboration services (adapted from [10]).

	Chat	Audio and video	Data-centric collaboration services
Adaptation to the tactical domain	Solutions are known and tested.	Known solutions work well in the civil domain, but must be tested in the tactical domain. A specific implementation must be explicitly tested for compliance.	New trends in the civil domain barely introduced in the military domain.
Interoperability	Agreement on XMPP, but tactical adaptations and security protocols are not standardized. Requires a gateway between proprietary solution and standardized XMPP to function seamlessly.	Several standards exist, but in practice interoperability is not always achievable.	Well established standards in the civil domain, but these have to be adapted to the tactical domain.
Security	Known mechanisms can be applied, but open issues exist related to tactical adaptations and interoperability.	Interoperability issues related to streaming and many-to-many communication.	No support for classified information. Largely based on network and transport layer security.

Table 2 Average bandwidth for cluster- and fan-out- topology (from [11])

<i>Average bandwidth for fan-out-topology</i>				
<i>Protocol</i>	Mist	WS-Discovery	SAM	SLP
<i>Central</i>	0.06 KB/s	14.90 KB/s	0.28 KB/s	7.12 KB/s
<i>Edge</i>	0.05 KB/s	2.28 KB/s	0.02 KB/s	1.05 KB/s
<i>Average bandwidth for cluster-topology</i>				
<i>Protocol</i>	Mist	WS-Discovery	SAM	SLP
<i>Total</i>	0.62 KB/s	27.30 KB/s	0.27 KB/s	12.57 KB/s
<i>Per node</i>	0.05 KB/s	2.27 KB/s	0.02 KB/s	1.05 KB/s
<i>Per query</i>	N/A	27.08 KB/q	N/A	12.59 KB/q
<i>Per query/node</i>	N/A	2.26 KB/q/n	N/A	1.05 KB/q/n

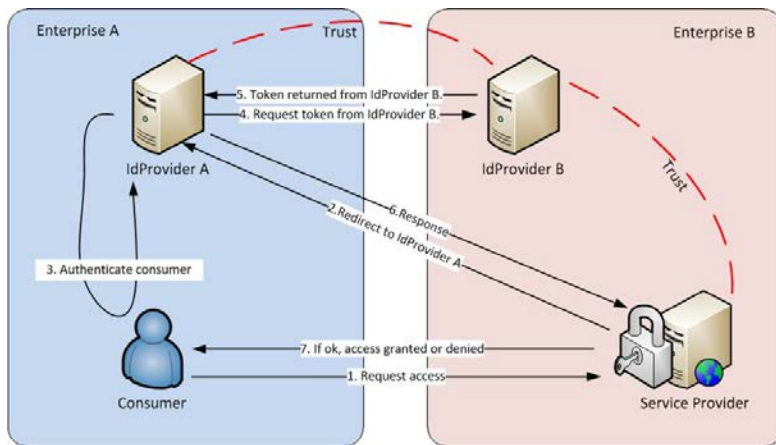


Figure 3 Federated Web authentication

Table 3 Federated Web authentication

Federated SSO	Network traffic in bytes		
	<i>Network traffic</i>	<i>Payload</i>	<i>Overhead</i>
SP-initiated SSO (not logged in)	7459	207	7252
SP-initiated SSO (logged in)	7089	207	6882
IdP-initiated SSO (not logged in)	5505	207	5298
IdP-initiated SSO (logged in)	5340	207	5133