Coalition Networks for Secure Information Sharing

CoNSIS

FINAL REPORT

VERSION 1.0

<22 August 2013>

The CONSIS Steering Committee

Chairman Albert Legaspi, SPAWAR, USA

Official Members:
Deniau, Noel, DGA, France
Eggen, Anders, FFI, Norway
Odgen, Roger, SPAWAR, USA
Staufenbiel, Detlef, Bundeswehr, Germany

Task Leaders

Task 1 - Communication Services: Seifert, Hartmut
Task 2 - Information and Integration Services (SOA): Lund, Ketil
Task 3 – Security: Hedenstad, Ole Erik
Task 4 – Management: Sevenich, Peter
Task 5 - Architecture, Test & Demonstration Coordination: Odgen, Roger:

Executive Summary

CONSIS (Coalition Network for Secure Information Sharing) is a multilateral cooperation project based on a signed Memorandum of Understanding (MoU) between the Ministries of Defence of France, Germany, Norway and the United States of America. The objectives of this project has been to develop, implement, test, and demonstrate technologies and methods that will facilitate the participants abilities to share information and services securely in ad-hoc coalitions, and between military and civil communication systems, within the communications constraints of mobile tactical forces.

The project is in step with the migration towards Network Enabled Capabilities (NEC) in the participating countries. As such, CoNSIS aligns with the overarching objective of the NATO NEC (NNEC) to enhance the Alliance’s ability to federate various capabilities at all levels, military (strategic to tactical) and civilian through networking and information infrastructure. In essence, CoNSIS strives to enable collaboration and secure information sharing among users that reduce the decision-cycle time. In terms of technology, the intention of the participating nations has been to utilize, to the maximum extent possible, commercial standards to minimize interoperability difficulties. Only those elements of the technical architecture which are not available from the open market have been investigated, and developed.

The work performed under this project, has been conducted in five tasks focusing on architectures – the overall to-be system architecture and test-and-demonstration architecture (Task 5), networks and radios (Task 1), information infrastructure (Task 2), security (Task 3) and management (Task 5). Phase 1 of CoNSIS concluded with two-week field experimentation in Greding, Germany in June 2012.

While the project has provided technical results and insights in areas of communication services, information and integration services, security, and management through laboratory testing and field experimentation, lessons learned call for further development and refinement. Potential future work in each task area has been identified. In particular, future activities of Task 1 will focus on multicast, quality of service (QoS) in conjunction with integration of operational considerations into policy-based routing and optimization of cross-layer communication technologies. For Task 2, use of service notification and service discovery standards in tactical (radio) networks are two key activities. Since security is an ever-present thrust, Task 3 will focus on its areas of interest with individual and joint experiments supplemented by theoretical studies. Finally, future work of Task 4 will include activities in network performance management as well as network configuration. These proposed research and test-and-experimentation topics are well aligned with NATO activities, regarding the draft STANAG 4711 Internet Protocol (IP) QoS, in addressing many requirements for later deployment phases.

Contents

1 Introduction

CONSIS is a multilateral cooperation project based on a signed Memorandum of Understanding (MoU) between the Ministries of Defense of France, Germany, Norway and the United States of America. The objectives of this project has been to develop, implement, test, and demonstrate technologies and methods that will facilitate the participants abilities to share information and services securely in ad-hoc coalitions, and between military and civil communication systems, within the communications constraints of mobile tactical forces.

The project is related to the migration towards Network Enabled Capabilities (NEC) in the participating countries. The intention of the participating nations has been to utilize, to the maximum extent possible, commercial standards to minimize interoperability difficulties. Only those elements of the technical architecture which are not available from the open market have been investigated, and developed. The work performed under this project has been conducted in five tasks focusing on architectures, networks and radios, information infrastructure, security and management respectively.

The project concluded its work with a field experiment, which took place in Greding, Germany over two weeks in June 2012. In order to obtain realistic hands-on experience with the integrated solutions, during the experimentation, technologies were assembled and deployed in the fields in conjunction with a military scenario created to put the use technologies in a meaningful operational context. This report presents an overview of the CONSIS project and its deliveries. More detailed results can be found in the individual task reports.

2 Technology areas and organization

2.1 Technology areas

The CONSIS areas of work were broken down into five major tasks as follows:

Task 1 - Communication Services
Task 2 - Information and Integration Services (SOA)
Task 3 - Security
Task 4 - Management
Task 5 - Architecture, Test & Demonstration Coordination

The main goal for Task 1 is to provide a transparent network connection between end systems within a tactical environment, independent of whether these end systems are located in deployed headquarters (fixed network part) or in mobile nodes. This transparency has to be realized independent of any transmission technologies (e.g., different radio system vendors) and any network connection condition.

Task 1 also experiments with QoS mechanisms in flexible mobile ad hoc networks in a coalition environment, based on heterogeneous radio systems using different waveforms. This scenario clearly reflects the reality in NATO nations where interoperable radio systems using common waveforms (such as the Software Defined Radio (SDR) approach) will not be available for a long time to come.

The main focus of Task 2 is to verify whether Service Oriented Architecture (SOA)-based infrastructures can be efficiently used and interconnected in tactical domains during coalition operations. In particular, Task 2 aims to verify if the SOA Baseline provided by NATO is sufficient for interoperability for ad-hoc combined elements of coalition partners in various scenarios. In addition to inherent challenges of tactical mobile networks such as low bandwidths, high delays, and frequent disruptions, the integration of coalition nodes in a common operation requires a model which allows for ad-hoc organization and provision and usage of services across various domain boundaries.

Task 3 investigates, develops, tests, and demonstrates security mechanisms for use for integration and interoperability of heterogeneous coalition networks. Key management, cross domain solutions, protected and control communications between civilian and military networks together with confidentiality, authenticity and integrity protection of user traffic between colored enclaves are addressed.

To facilitate network management for delivering end-to-end QoS across multiple domains, Task 4 uses a well established framework called PerfSONAR (Performance focused Service Oriented Network monitoring Architecture) for network performance monitoring in a federated environment. Developed by an international consortium with members from research and education organizations, PerfSONAR framework provides an infrastructure for federated sharing of network management data via its web services.

Task 5 has developed an overall Experimentation Architecture for CoNSIS. This architecture defined the way in which the deliveries of Tasks 1 to 4 have been integrated. Task 5 has also carried out the overall co-ordination and planning of the CoNSIS project. It has provided reporting and dissemination of the results of CoNSIS during and upon completion of the project. The intent is to generate technical results that will be applicable to operational scenarios outside of this project.

2.2 Organization

The CoNSIS project has been directed and administered on behalf of the participants by an organization consisting of a Steering Committee (SC) and Task Leaders (TLs). The SC has had the responsibility for effective implementation, efficient management, and direction of the Project in accordance with the agreed MOU.

The SC has consisted of one voting representative designated by each participant. The meetings of the SC have been facilitated by the elected Chairman Albert Legaspi from SPAWAR, USA. The chairman has not voted and has not been an SC representative.

3 Deliverables and Results

Deliverables and results of the CoNSIS project are summarized in the following table. Detailed results can be found in individual deliverables.

Table 3-1: List of Deliverables and Summary of Results

Responsible Task	**Summary of Deliverable**
5	Describe the to-be system architecture and test-and-experimentation architecture for use in the CoNSIS project [1]
5	Describe an effort to design, develop, test and demonstrate an interoperable coalition interface for a Naval Task Force for CoNSIS [2]
1	Provide an overview of studies and results from activities performed in Task 1 "Communication Services", as well as analysis of Task1's results from the CoNSIS field experiment in Greding, Germany in June 2012 [3]
1	Explore implementation of RFC 5578 Point-to-Point Protocol over Ethernet (PPPoE) Extensions for Credit Flow and link Metrics [4]
1	Show how Multi-Topology routing is used to support differentiated QoS and maintain different network topologies in the heterogeneous land mobile network architecture used in CoNSIS field experiment [5][35]
1	Demonstrate an inter-domain QoS mechanism that uses Technical Profiles and User Profiles to set up the best path for the user traffic in the network. This technique also allows traffic to be adapted to best suit the current network conditions [6][7][8][9][10][11]
1	Describe SCIP-enabled gateway that is based on IP as the transport medium and uses SIP for session instantiation [12]
1	Describe a reliable UDP using the WAP Session Protocol to support longer SOAP PDUs in a narrow band radio network [13]
1	Describe Multi Link Processor Services for connecting Link-11, Link-16, and Link-22 systems [14]
2	Provide an overview of concepts and results related to Service-Oriented Architectures, as well as analysis of results from the CoNSIS field experiment in Greding, Germany in June 2012 [22]
2	Describe the elements necessary to allow SOA based Command, Control and Intelligence Systems to operate in a mobile tactical environment

	[24]
2	Describe challenges and lessons learned from the field experiment in Greding, Germany in June 2012 in terms of SOA interoperability in a large scale heterogeneous tactical network [23]
3	Provide an overview of Task 3 work on security; field experimentation and theoretical studies [25]
3	Identify threats to national networks and propose mechanisms and procedures to thwart them [26]
3	Describe the implementation of the Network Authentication Header (NetAH), a modified version of the standard IPsec AH [27]
3	Provide overhead evaluations and optimization methods in three PKI scenarios [28]
3	Address different optimization strategies for PKI operations [29]
3	Provide an assessment of MIKE for its use in tactical Ad Hoc networks and a number of suggested enhancements of MIKE [30]
3	Show the use of a guard to provide interconnection between two different security domains in a service-oriented environment [31]
3	Describe filtering of messages sent from a classified to an unclassified network using a cross-domain guard [32]
3	Propose a framework that protects communications and controls access to information resources. A prototype based on the framework has been built and was evaluated during the CoNSIS field experiment in Greding, Germany in June 2012 [33]
4	Provide an overview of concepts and results related to network management as well as detailed analysis of results from the CoNSIS field experiment in Greding, Germany in June 2012 [34]
4	Discuss the goals of measurements in a CoNSIS-type architecture, specific measurements in a tactical environment, and propose generic solutions and operating principles[15]
4	Outline a configuration management architecture [16][17]
4	Describe ways to perform measurements with active test flows despite the bias that may be introduced by routers implementing fair queuing techniques [18]
4	Provide an overview of Multilevel Security and discuss approach to exchange data between domains and security implications [19]

4	Provide an overview of indicators suggesting the presence of a jamming attack in a wireless network [20]
4	Address network management challenges and lessons learned from the CoNSIS field experiment in Greding, Germany in June 2012 [21]

4 The Distributed Joint Experiment

The CONSIS project concluded its work with a field experiment, which took place in Greding, Germany over two weeks in June 2012. In this experimentation, technologies were put together and deployed in the fields to get realistic hands-on experience with the integrated solutions. A military scenario was created in order to put the use of technologies into an operational context.

The main venue was at the "Bundeswehr Technical Center for Information Technology and Electronics" in Greding demonstrated with interconnections with the French laboratory at CELAR in Rennes, and the US laboratory at SPAWAR in San Diego.

In Greding, Germany provided the lab facilities, network infrastructure in addition tovehicles in which the Norwegian and German systems, networks and radios were installed.

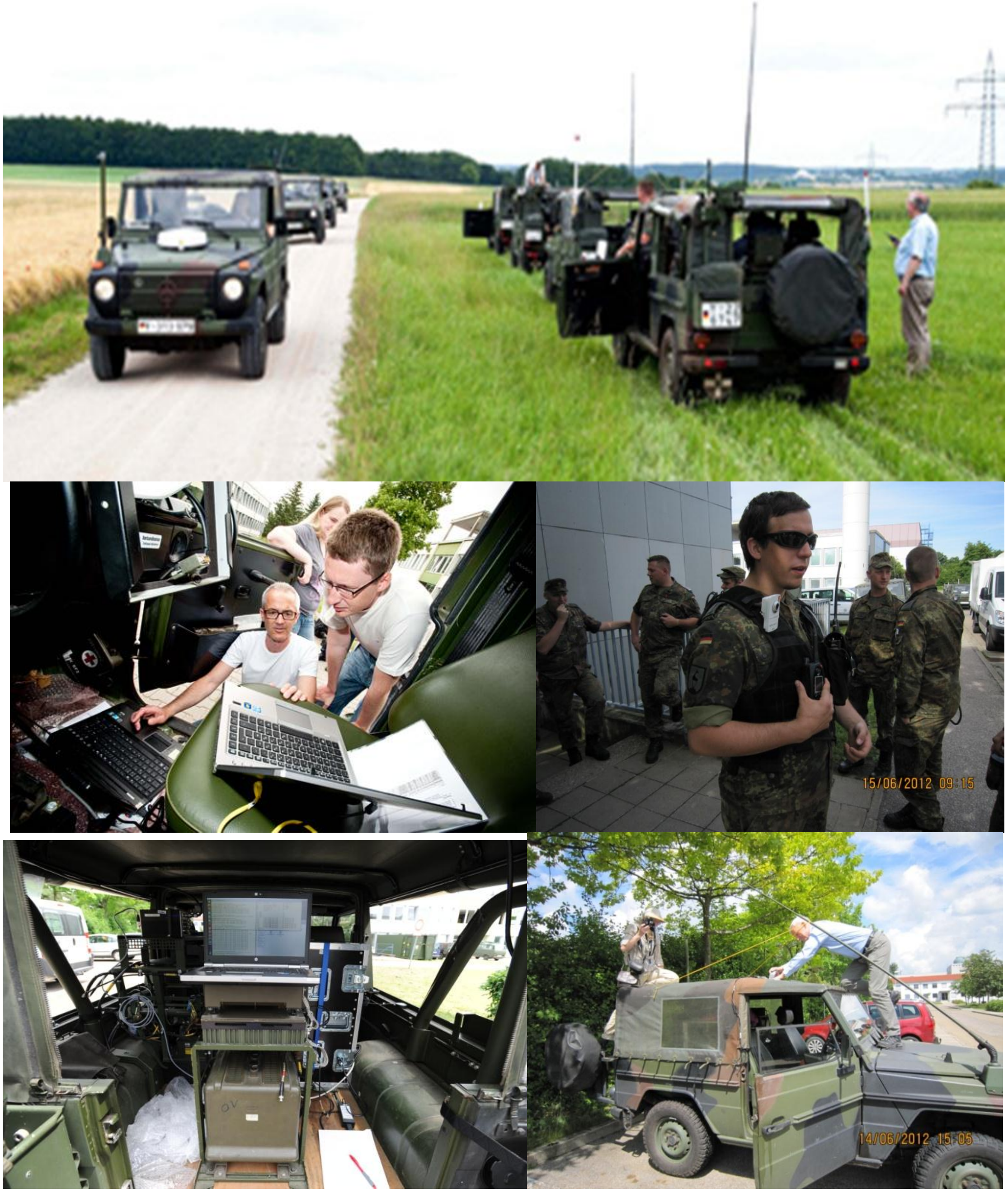

Figure 4-1: Some pictures from the joint experiment in Greding

The scenario and experimentation architecture are described in section 4.1 and 4.2, respectively. Detailed task experiments and corresponding results and analyses can be found in individual task reports and deliverables.

4.1 Scenario

The scenario takes place in a country torn by civil war. An international coalition is involved in this conflict to protect civilians and initiate the peace process.
Main cities are controlled by coalition forces but countryside is not secured. Convoys and advanced posts are regularly attacked by armed groups.

A Navy Task Force, consisting of surface vessels of coalition nations, is deployed in the waters of the Area of Operations. The vessels are deployed for a period of several months in order to patrol the area, control all the vessels that enter and exit the area, and execute search and rescue operations. The navy Task Force is establishing an ad hoc network. Vessels equipped with satellite links are providing high capacity reach-back capabilities to the rest of the Task Force. Traditional low throughput reach-back can be established via long range HF links.

4.1.1 #0 Initial situation

A natural disaster occurs in an area not controlled by the coalition. This area is far away from the nearest coalition headquarters. Additionally, in the area there are civilian organizations (non-governmental organizations (NGOs), etc.) that already help the displaced population. There is a danger that enemy forces may take advantage of the situation to infiltrate the area.

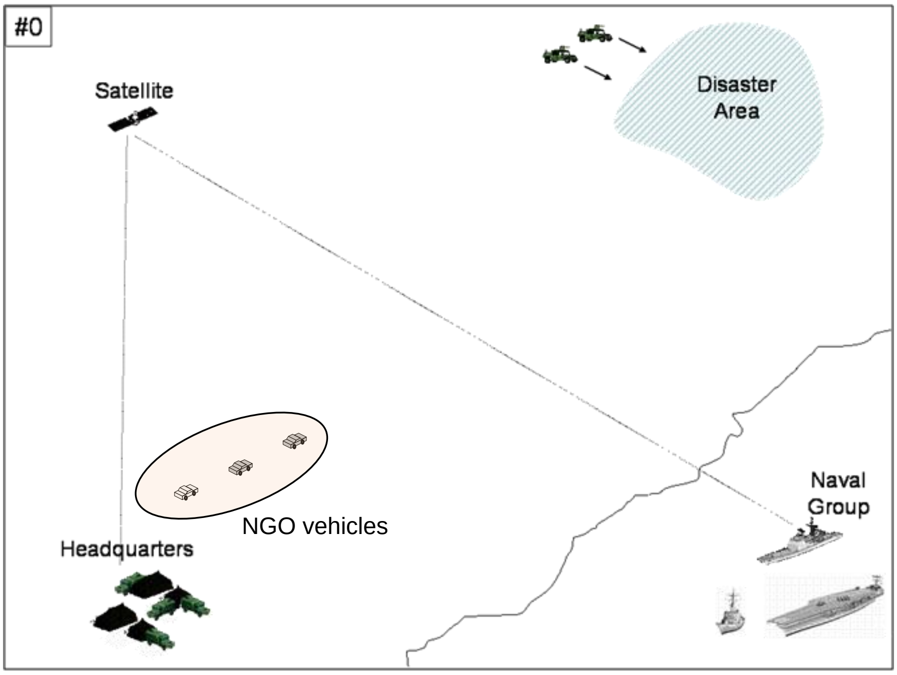

Figure 4-2: Initial situation

4.1.2 #1a Convoy setting up

The coalition headquarters decides to escort an NGO convoy to the disaster area. A battalion of coalition forces has been assigned to protect this convoy, to set up a security perimeter to protect the NGOs when building temporary camps to host the displaced population, and to facilitate the NGO activities providing coordination and security. The convoy consists of NGO vehicles and coalition armored cars. The convoy military vehicles are connected together in an ad hoc manner through a series of short hops. The convoy leaves the HQ.

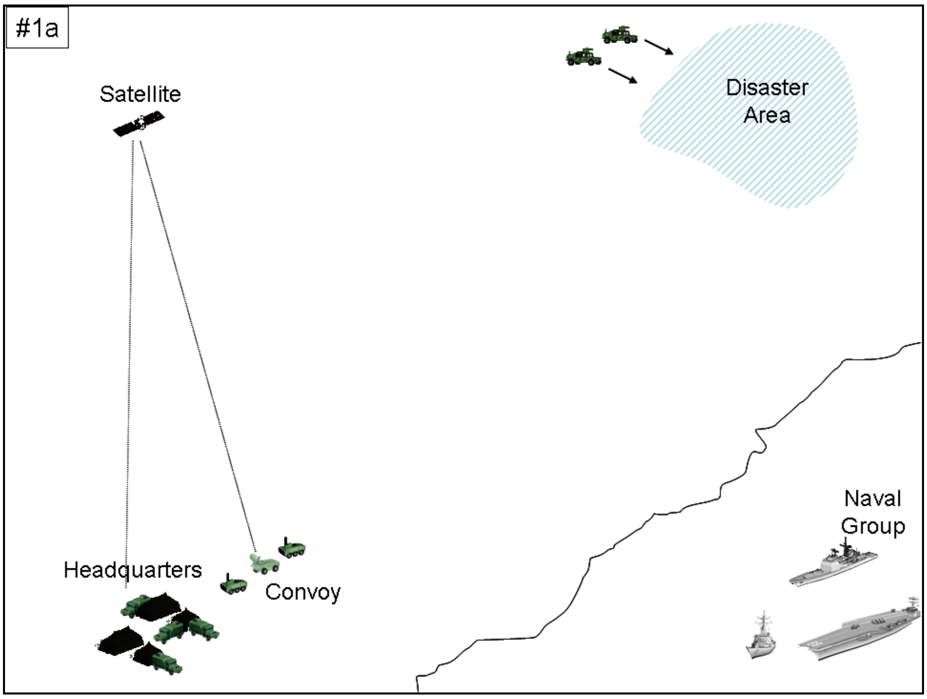

Figure 4-3: Convoy setting up

4.1.3 #1b Convoy merging

Sometime after the convoy has left the HQ, it is joined by a second squad of military vehicles. This second squad is from a different nation and may use different radios internally. Communication between the convoys and between the convoys and the HQ is either done by satellite or by using radios compatible on the air. Some of the vehicles in the different convoys are equipped with these compatible radios, and the remaining vehicles communicate via the links set up by the compatible radios. These radios automatically discover each other.

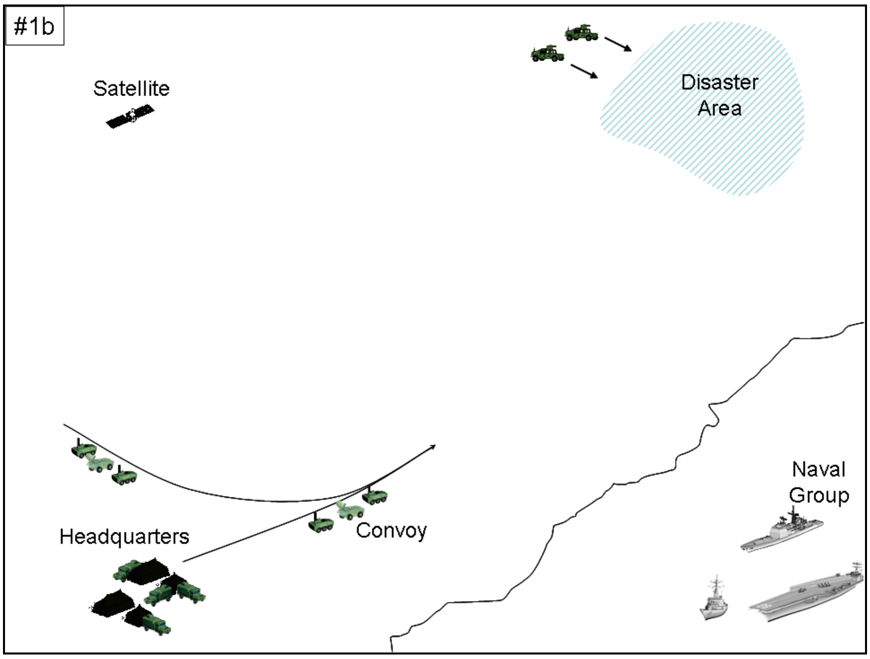

Figure 4-4: Convoy merging

4.1.4 #2 UAV launching

In order to protect the convoy, a UAV is launched from the HQ the to collect up-to-date intelligence information and to provide live surveillance. The UAV squadron has established a ground station that enables communication with the UAV, typically using CDL (Common Data Link). The ground station forwards the collected surveillance/intelligence data to the HQ for analysis and storage. The ground station also forwards remote control data to the UAV. The HQ staff analyses collected source data and provides information products on intelligence and surveillance. The operation is supported by an AWACS aircraft that performs tactical air control.

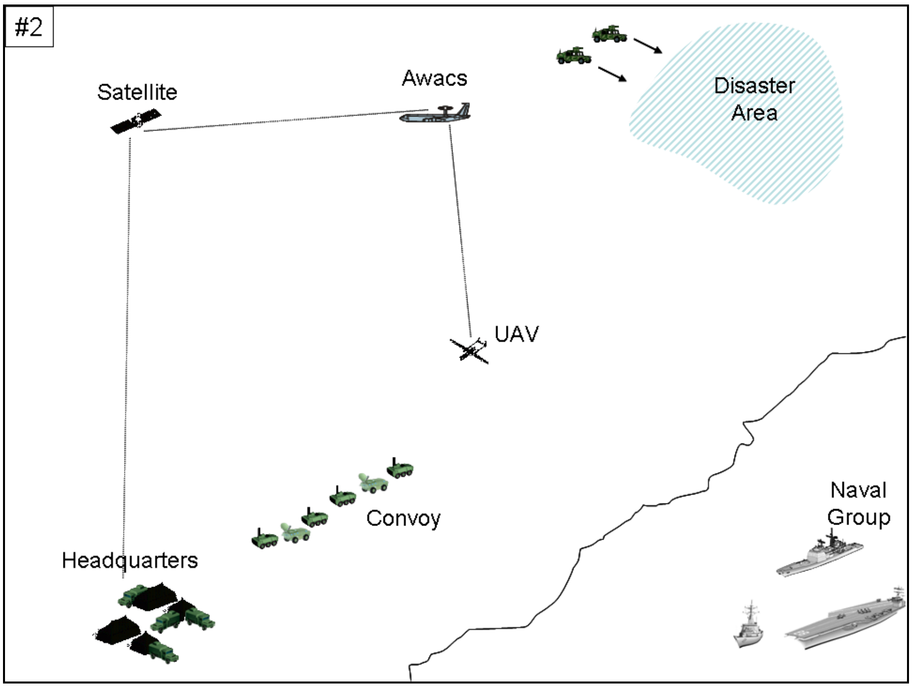

Figure 4-5: UAV launching

4.1.5 #3 Jammer attack

During the journey, the convoy radio communications are suddenly severely degraded due to jamming. The convoy informs the headquarters through the satellite link that is not affected by the jammer.

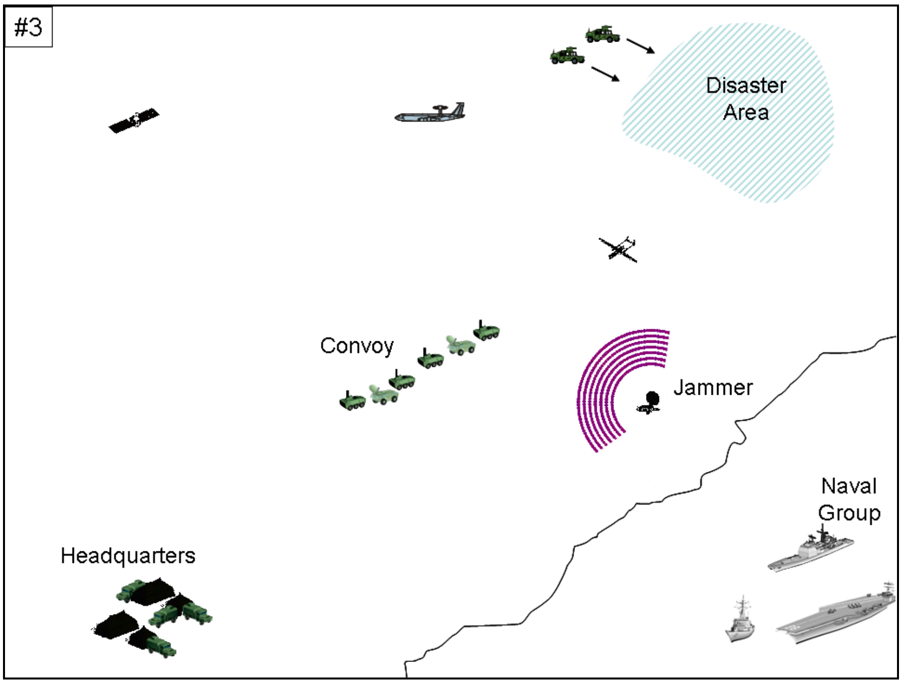

Figure 4-6: Jammer attack

4.1.6 # 4 Jammer neutralization

The UAV detects and localizes the communication jammer. It gathers various types of information about the jammer (e.g. snapshots, geographic location) and sends them to the Headquarters. The headquarters send a request for air support to the naval group using an available network link/path. Two aircrafts are launched from the carrier. Their mission is to destroy the jammer located by the UAV. The jammer is destroyed.

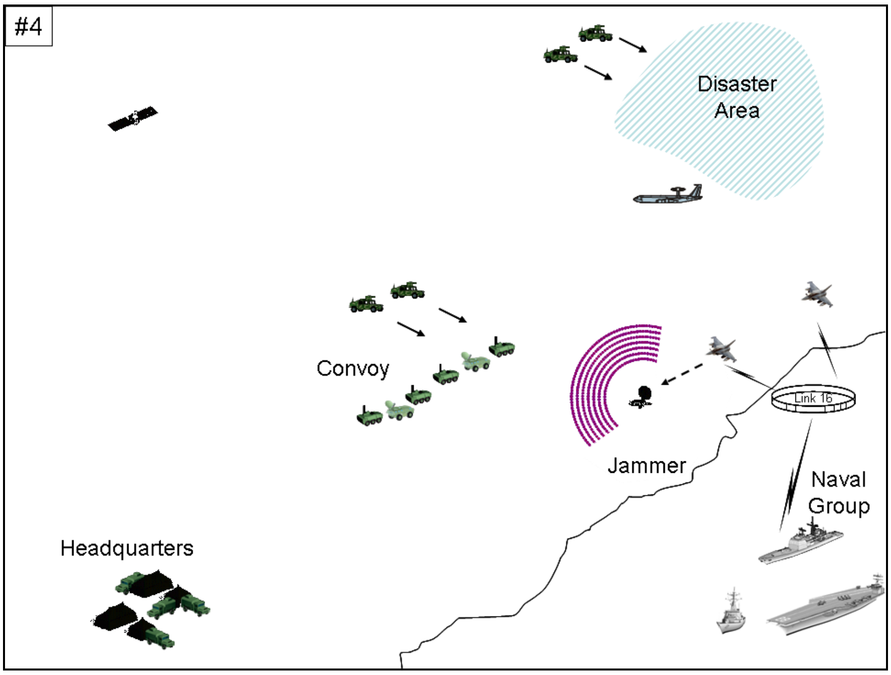

Figure 4-7: Jammer neutralization

4.1.7 #5 Ambush

A short while after the jamming starts, the convoy is ambushed. The Coalition Forces convoy is stopped by the detonation of a remote-controlled IED. The blast hit the first armored vehicle. Simultaneously, insurgents equipped with fast moving vehicles open fire on the convoy. In the fire one NGO truck is destroyed and several NGO members are wounded. Coalition forces riposte but their situation is not favorable. The coalition forces inform the headquarters using an available network link/path. Air support from the Naval Group is requested by the HQ.

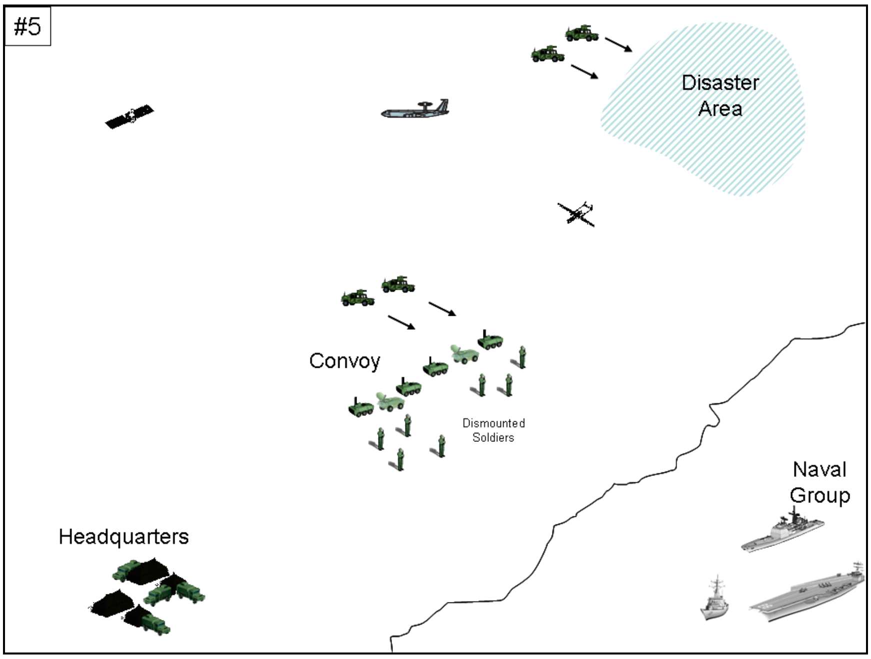

Figure 4-8: Ambush

4.1.8 #6 Attackers neutralization

The Headquarter requests additional air support to help the convoy. The aircrafts in-flight are re-assigned with a new target. Two more aircrafts are launched from the carrier. The Insurgents are defeated and escape; several of their vehicles are destroyed.

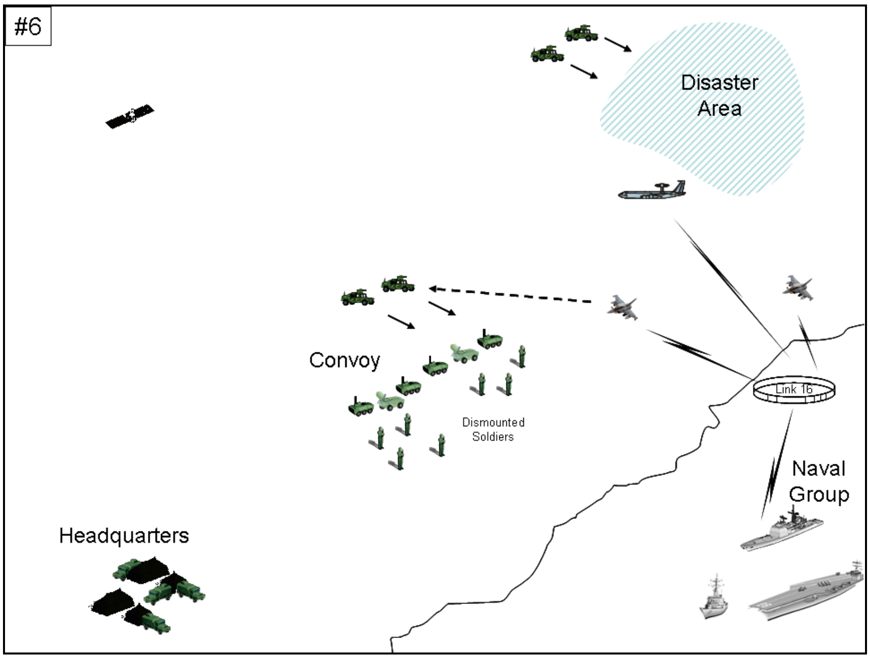

Figure 4-9: Attackers neutralization

4.2 The Experimentation Architecture

The experimentation architecture is a subset of the system architecture chosen for test and demonstration purposes. The test and demonstration architecture involves phase 0, phase 1a, phase 1b, phase 3 and phase 4. The overall challenge is to share information in order to build a common operating picture (COP) for common situation awareness. Each of the enclaves (i.e. inside the convoys and the HQs) has services that the other enclaves need to use in order to maintain the COP.

The convoys and the HQ are “played” by different nations taking part in the test and demonstration. The convoy is created by a DEU and a NOR part, the coalition HQ is provided by FRA and an additional Maritime HQ is provided by the USA.

The laboratories of the nations involved in the test and demonstration are connected using the Internet.

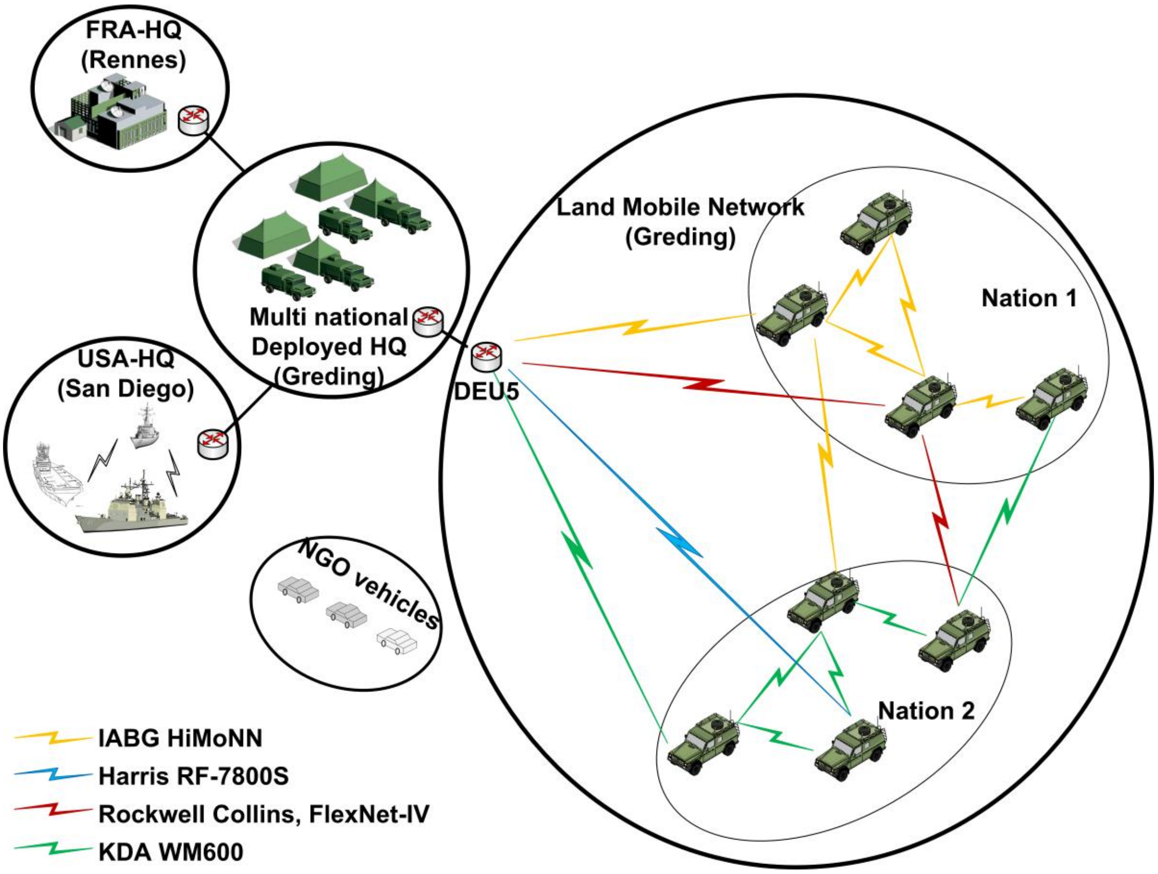

Figure 4-10: Joint Experimentation Setup

5 Lessons Learned and Future Work

Laboratory testing and field experimentation performed by Task 1 for communication services within a tactical environment have identified two fundamental gaps in current technologies and implementations. First, most military radios are designed for building a large homogenous radio network and without technical consideration for connection between the radio network and an external router. With the introduction of external routers interfacing radio networks, Task 1 implemented routing overlay to ease routing efficiency and end-to-end quality of service; however, this approach is complex to configure and does not scale well. Secondly, multicast, the heart of information sharing, also poses problems. Essentially, multicast protocols in commercial routers and those available for military radios are not ready for interaction.

Task 2, with focus on information and integration services, conducted testing and experiments on technologies to ensure interoperability in operational environments. Task 2 found that Web services can serve as an interoperability enabler not only in large complex networks, but also in limited capacity tactical networks. By following the SOA Baseline specifications from NATO, nations will be able to interconnect their systems with relatively low effort. However, the experiments showed that there is a need for further development and profiling of the standards in order to fully meet interoperability challenges facing participating nations.

Task 3 addressed three security areas, namely, transport network protection, key management, and protection of user traffic, in addition to aspects of confidentiality, integrity, authenticity, and availability. Experimentation has been conducted with security as individual topics and in a comprehensive joint experiment scenario. Task 3 found that comprehensive joint experimentation is needed to bring new security solutions into operational systems. Furthermore, theoretical studies performed in conjunction with experimentation are necessary to provide insights into complexity of security issues.

Focused on federated network management, Task 4 took into considerations requirements of security and information hiding, as well as wireless and core enterprise domains. Experimentation showed that the overhead of active probing and passive monitoring were small relative to the overall network traffic in a typical convoy scenario. During the CoNSIS field experiment, Task 4 found that probes had parameter areas for valid results such that results became unreliable outside the areas. Moreover, experiment indicated that cross-layer solutions could optimize network and operational performance.

While CoNSIS results and findings have advanced the understanding of the networking and information infrastructure, the 'physical reality" of NNEC, as an enabler of secure information sharing, more work is needed to keep the progress on a steady path. Potential future work in each task area has been identified. In particular, for Task 1, future activities include multicast specification and testing, generation of automatic report of quality of service (QoS) parameters at Link Layer and consumption at Network Layer, integration of operational considerations into policy-based routing, and optimization of cross-layer communication technologies. For Task 2, use of the WS-Notification standard for service notification and that of the WS-Discovery standard for service discovery in tactical (radio) networks are two key proposed activities. Since security is an ever-present thrust, Task 3 will focus on its technology area with experiments (individual and joint) supplemented by theoretical studies. Finally, future work of Task 4 includes both network performance management (passive measurement techniques, tighter integration of measurement services into Service Oriented Architectures (SOA), and network monitoring services with a high level of abstraction) and network configuration management (dynamic service level agreements (SLAs), mapping of SLAs to network/device configurations, and standardized interfaces for network configuration.) Regarding STANAG 4711 IP QoS, these proposed research and test-and-experimentation topics are well aligned with NATO activities in addressing many requirements for later deployment phases.

Bibliography

[1] "System and Experimentation Architectures - Version 1.0", CoNSIS/Task 5/DL/002, September 2011

[2] N. Tuan, S. Lam, C. Castro, R. Ogden, T. Cam, and A. Legaspi, "Naval Task Force interface for Coalition Networks for Secure Information Sharing (CoNSIS)," MILCOM 2012, October 2012

[3] “CoNSIS Final Report – Task 1”, Document CoNSIS/Task 1/DU/001, ver. 1.0.3 24th January, 2013

[4] “RFC 5578 Implementation”, Document CoNSIS/DEU/Task1/DU/001, Sept. 2010

[5] “Multi-Topology Routing – QoS functionality and results from field experiment”, CoNSIS/NOR/Task1/DU/002/, ver. 1.1, Jan. 2013

[6] "Technical Profiles – Definition and Associated Processes", CG/UM-ESIO/IDRE/10.099/V2.0, Dec. 2012

[7] "Technical Profiles and Communication Chains", CG/UM-ESIO/IDRE/10.100/V2.0, Dec. 2012

[8] "Technical Profiles and User Services", CG/UM-ESIO/IDRE/10.101/V2.0, Dec. 2012

[9] "Relationships between End-to-end QoS, Technical Profile and user Profile", CG/UM-ESIO/IDRE/10.096/V2.0, Dec. 2012

[10] "Application and Network-level QoS", CG/UM-ESIO/IDRE/10.097/V2.0, Dec. 2012

[11] "Differentiated QoS in Networks of Different Operational Levels", CG/UM-ESIO/IDRE/10.098/V2.0, Dec. 2012

[12] “SCIP-enabled Gateway – v1”, CoNSIS/DEU/Task1/DL/002, Sept. 2010

[13] “Reliable UDP”, CoNSIS/DEU/Task1/DU/002, Nov. 2010

[14] “MLP Services”, CoNSIS/DEU/Task1/DU/004, Nov. 2011

[15] “IP Network Metrology –Architectures and Tools applicable in a coalition network”, Document CoNSIS CG/UM-ESIO/IDRE/10.107/V1.1, July 2010

[16] “Coalition Management Philosophy”, CG/UM-ESIO/IDRE/11.029/V1.0, January 2011

[17] “Management Organisation in a C-TNS”, CG/UM-ESIO/IDRE/11.062/V1.0, March 2011

[18] “Fair Queuing and active Measurement Methods”, CG/UM-ESIO/IDRE/11.260/V1.0, November 2011

[19] P. Steinmetz, “Multilevel Security and network management in CoNSIS”, Fraunhofer FKIE Technical Report, 2012

[20] Fatih Abut, “Jamming Indicators in Wireless Networks” – CoNSIS Task 4, Nov. 2012

[21] C. Barz et.al., “The CoNSIS Approaches to Network Management and Monitoring,” IEEE MCC, Gdansk, Poland, October 2012

[22] "CoNSIS Task 2 - Final Report", December 2012

[23] T. H. Bloebaum, K. Lund, “CoNSIS: Demonstration of SOA Interoperability in Heterogeneous Tactical Networks,” IEEE MCC, Gdansk, Poland, October 2012

[24] H. Seifert and M. Franke, "SOA in the CoNSIS coalition environment", IEEE MCC, Gdansk, Poland, 2012, in press.

[25] "CoNSIS Task 3 Final Report", Version 1.0, December 2012

[26] Simone P. (2010), "Core Network Protection", CG/UM-ESIO/IDRE/10.109/V1.1, Cogisys

[27] Kongsberg Defence & Aerospace AS (2011), "Implementation of the NetAH (Military Authentication Header / AH*/QAH), Technical Report", 2/1559/2-FCPR10127 Rev A

[28] Engohan E. and Simone P. (2010), "Scalability of a Tactical PKI", CG/UM-ESIO/IDRE/10.110/V1.1, Cogisys

[29] Fongen A. (2010), "Optimization of protocol operations in a Public Key Infrastructure", FFI-rapport 2010/02499

[30] Hegland A. M. and Ellingsrud H.-A. (2012), "The Multicast Internet Key Exchange (MIKE) in tactical Ad Hoc Networks", *IST-111 Symposium on Information Assurance and Cyber Defense*

[31] Haakseth R. (2012), "SOA Pilot 2011 – demonstrating secure exchange of information between security domains", FFI-report 2012/00117

[32] Steinmetz P. (2012), "Use of Cross Domain Guards for CoNSIS network management", *IEEE MCC,* Gdansk, Poland, 2012

[33] Fongen A. (2012), "Protected and Controlled Communication Between Military and Civilian Networks", *IEEE MCC,* Gdansk, Poland, 2012

[34] “CoNSIS Final Report – Task 4”, Document CoNSIS/Task 4/D/003. 26th November 2012

[35] M. Hauge, J. Andersson, M. Brose, J. Sander, “Multi-topology routing for QoS support in the CoNSIS convoy MANET”, IEEE MCC, Gdansk, Poland, 2012, in press