NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-109)TP/618

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-109**

Use Cases for Dynamic Secure Wireless Networking in Coalition Environments

(Cas d'utilisation de réseau sans fil dynamique et sécurisé dans des environnements de coalition)

This Report documents the findings of Task Group IST-109/RTG-054.

Published May 2015

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-109)TP/618

www.sto.nato.int

STO TECHNICAL REPORT **TR-IST-109**

Use Cases for Dynamic Secure Wireless Networking in Coalition Environments

(Cas d'utilisation de réseau sans fil dynamique et sécurisé dans des environnements de coalition)

This Report documents the findings of Task Group IST-109/RTG-054.

The NATO Science and Technology Organization

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

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

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

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

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

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

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

Published May 2015

ISBN 978-92-837-2010-2

Table of Contents

List of Figures/Tables

List of Acronyms

CC	Coloured Cloud
CoI	Community of Interest
CoT	Communities of Trust
DNS	Domain Name Service
ET	Exploratory Team
FOB	Forward Operating Base
HF	High Frequency
IDS	Intrusion Detection Systems
IPsec	Internet Protocol Security
MAC	Media Access Control
MANETs	Mobile Ad hoc Networks
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NII	Networking and Information Infrastructure
NINE	NATO NII IP Network Encryption
NMCD	Network Management and Cyber Defence
NNEC	NATO Network-Enabled Capability
NRF	NATO Response Force
NTK	Need-To-Know
PCN	Protected Core Networking
PCS	Protected Core Segments
PHY	Physical layer
PKI	Public Key Infrastructure
PTT	Push-To-Talk
RF	Radio Frequency
RTARA	Real-Time Automated Risk Assessment
RTG	Research Task Group
SA	Situational Awareness
SCIP	Secure Communications Interoperability Protocols
SLA	Service-Level Agreement
UHF	Ultra High Frequency
VHF	Very High Frequency
WCT	Wireless Coalition Tactical

Acknowledgements

We wish to thank the contributions of the following co-authors to this report:

- Peter C. Mason, Defence R&D Canada
- Helen Tang, Defence R&D Canada
- Ronggong Song, Defence R&D Canada
- Darcy Simmelink, Defence R&D Canada

IST-109 Membership List

J. David BROWN
Defence R&D Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
CANADA
Email: david.brown@drdc-rddc.gc.ca

Anders FONGEN
Norwegian Defence Research Establishment (FFI)
P.O. Box 25
Instituttveien 20
N-2027 Kjeller
NORWAY
Email: anders.fongen@ffi.no

Simon HUNKE
Fraunhofer (FKIE)
Research Group Cyber Defense
Neuenahrer Strasse, 20
D-53343 Wachtberg
GERMANY
Email: simon.hunke@fkie.fraunhofer.de

Mazda SALMANIAN (Chair)
Defence R&D Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
CANADA
Email: mazda.salmanian@drdc-rddc.gc.ca

Use Cases for Dynamic Secure Wireless Networking in Coalition Environments

(STO-TR-IST-109)

Executive Summary

Dynamic, mobile wireless networks use transformative technologies that promise to deliver significant communication capabilities to military forces, such as full networking functions at the soldier level, including routing. These networks are wireless, self-forming, and self-managing, offering the additional benefit of reducing the required deployment and management resources compared to those of fixed networks. However, the very properties that make these networks attractive in the first place – their open medium, flexible topology, dynamic membership rules, simple network-formation algorithms, and the routing capabilities afforded to each node – raise security concerns, in addition to those of wired networks.

The security of these networks for national defence usage is being addressed by national defence research programs. However, multi-national forces could also reap the benefits facilitated by these networks – improved connectivity and information sharing capabilities – by allowing for some co-operation and interconnectivity among national tactical edge forces. Such interconnectivity presents a host of architectural and security challenges, adding to the security challenges faced by individual Nations. Coalition communication interoperability and information sharing – already challenges themselves – will make deployment of dynamic wireless networks even more difficult. It is important to ensure that national programs recognize the constraints of these networks and endorse compatible security solutions for support of the NATO Response Force (NRF), adhering to the NATO Network-Enabled Capability (NNEC) vision.

In order to advance the technology in dynamic secure wireless networking, this Task Group (IST-109/ RTG-054) has focused its research to first develop a number of use case scenarios in a deployed, coalition context. The sample mission scenarios in this report are approached with the assumption that a suite of wireless communications equipment is available to coalition members – i.e., connected national tactical forces. To that end, related characteristics of a coalition tactical network are summarised. Various network topologies and interfaces among national networks are laid out; these were developed in consultation with members of IST-103/RTG-049 (Protected Core Networks) and IST-ET-069 (Heterogeneous Networks). Policies on offering graded services for connectivity and for security are discussed in coalition scenarios for tactical deployments. A capability for identifying Communities of Trust (CoT) is proposed along with appropriate security requirements.

It is believed that the resulting architectures, policy models, and future experimental results from these scenarios will have a high impact in this domain – dynamic secure wireless networking – which we believe has high value for NATO.

Cas d'utilisation de réseau sans fil dynamique et sécurisé dans des environnements de coalition

(STO-TR-IST-109)

Synthèse

Les réseaux sans fil mobiles et dynamiques utilisent des technologies adaptives qui promettent de fournir des capacités de communication importantes aux forces militaires, par exemple des fonctions de mise en réseau complètes au niveau du soldat, incluant l'acheminement. Ces réseaux sans fil, se constituent et se gèrent eux-mêmes, offrant l'avantage supplémentaire de nécessiter moins de déploiement et de ressources de gestion que les réseaux fixes. Néanmoins, les propriétés qui, précisément, rendent ces réseaux séduisants de prime abord – support ouvert, topologie souple, règles d'adhésion dynamiques, algorithmes simples de formation du réseau et capacités d'acheminement attribuées à chaque nœud – soulèvent des problèmes de sécurité, qui s'ajoutent à ceux des réseaux câblés.

La sécurité de ces réseaux dans l'optique de la défense nationale fait l'objet de programmes de recherche de défense nationale. Cependant, des forces multinationales pourraient également profiter des avantages induits par ces réseaux – amélioration de la connectivité et des capacités de partage d'information – en autorisant une certaine coopération et une certaine interconnectivité entre les forces tactiques nationales. Une telle interconnectivité pose de nombreux problèmes architecturaux et de sécurité, qui s'ajoutent aux défis de la sécurité auxquels chaque pays doit faire face. L'interopérabilité de la communication et le partage des informations en coalition – qui sont en soi des défis – compliqueront encore le déploiement de réseaux sans fils dynamiques. Il est important de veiller à ce que les programmes nationaux tiennent compte des contraintes de ces réseaux et mettent en oeuvre des solutions de sécurité compatibles en appui de la Force de Réaction de l'OTAN (NRF), et conforme à la vision de la capacité réseau-centrique de l'OTAN (NNEC).

Afin de faire progresser la technologie de la mise en réseau sans fil sécurisé et dynamique, le groupe de travail (IST-109/RTG-054) s'est concentré en premier lieu sur l'élaboration d'un certain nombre de scénarios d'utilisation dans un contexte de déploiement en coalition. Les scénarios de mission proposés dans ce rapport partent de l'hypothèse qu'une suite de matériels de communication sans fil est à la disposition des membres de la coalition, autrement dit des forces tactiques nationales interconnectées. Dans ce but, une synthèse des caractéristiques correspondantes d'un réseau tactique de la coalition a été réalisée. Diverses interfaces et topologies de réseau parmi celles des réseaux nationaux sont exposées. Elles ont été développées en consultation avec les membres de l'IST-103/RTG-049 (Réseau central protégé) et de l'IST-ET-069 (Réseaux hétérogènes). Les politiques relatives à la fourniture de services gradués de connectivité et de sécurité sont discutées dans des scénarios de déploiement tactique de la coalition. Une capacité d'identification de communautés de confiance est proposée et ses besoins en matière de sécurité sont exposés.

Nous sommes convaincus que les architectures, modèles de politique et résultats expérimentaux futurs issus de ces scénarios auront une grande influence dans le domaine de la mise en réseau sans fil sécurisé et dynamique, domaine de grande valeur pour l'OTAN.

USE CASES FOR DYNAMIC SECURE WIRELESS NETWORKING IN COALITION ENVIRONMENTS

1.0 INTRODUCTION

Allied Nations are beginning to embrace dynamic, mobile wireless networks that promise to deliver significant communication capabilities to tactical military forces. Such capabilities will allow for full networking function at the (dismounted) soldier level and enable a cost-effective way to gather information about environments in which Allied forces are deployed. Mobile Ad hoc Networks (MANETs) – in which each node can perform routing functions – are a particularly suitable wireless networking technology for military deployments, because these networks are wireless, self-forming, and self-managing; MANETs offer the additional benefit of reducing the required deployment and management resources compared to those of fixed networks.

Security in dynamic wireless networks is of fundamental concern. These networks face a number of risks and vulnerabilities (in addition to those of wired networks), most of which can be associated with the very properties that make the networks attractive in the first place – their open medium, flexible topology, dynamic membership rules, simple network-formation algorithms, and the routing capabilities afforded to each node. Moreover, secure coalition communication information sharing and communication interoperability are already challenging in traditional networks; these challenges will increase with the deployment of dynamic wireless networks. It is important at this early stage of research and development to ensure that any security solutions and approaches developed by national programs are compatible with the principles of coalition deployment and recognize the constraints of these networks. Distributed wireless network defence can be more effective when information from multiple sources is fused. In coalition environments, establishing a security information sharing architecture and a data model for sharing that information are problems that need to be considered from a deployed, coalition context.

The overall objective of this Research Task Group (IST-109/RTG-054, Dynamic Wireless Network Security) is to advance research and technology in coalition tactical network security architectures and security awareness as contributions towards the NATO Network-Enabled Capability (NNEC) for support of the NATO Response Force (NRF). Ultimately the resulting architectures, policy models, and experimental results will have a high impact in this domain and could be used to influence future standards and policies, which we believe has high value for NATO. To serve this objective, we developed three scenarios for wireless coalition tactical networking in consultation with members of NATO IST-103/RTG-049 (Protected Core Networks) and NATO IST-ET-069 (Heterogeneous Networks), whose summary is also published in Ref. [1].

The rest of this report is organised as follows. Characteristics of a wireless coalition tactical network are summarized in Section 2. In Section 3 we describe the first scenario, where Nation-B provides several different levels of network connectivity to Nation-A to allow it a means of communicating to a trans-national Forward Operating Base (FOB) in the case where Nation-A tactical forces are out of range. In Section 4, we describe the second scenario, where Nation-B provides different grades of security services to Nation-A to enhance the security posture of Nation-A's tactical network (and ultimately the coalition network). Finally in Section 5, we describe the third scenario, where Nation-A establishes cross-network Communities of Trust (CoT) for special roles with appropriate security requirements. In each scenario, security concerns of special consideration are highlighted, various network topologies with national network interfaces are described, and policy models on offering graded services are discussed.

2.0 CHARACTERISTICS OF A WIRELESS COALITION TACTICAL NETWORK

We present our assumptions regarding the characteristics of a Wireless Coalition Tactical (WCT) network in this section. These characteristics should be considered when threat analyses and protection mechanisms are formulated for MANETs. This section serves as a definition and threat analysis overview for the sections that follow which describe scenarios that incorporate MANETs, which are a specialized extension to WCT networks[1].

2.1 Wireless

In a wireless network, the physical media is not as safeguarded as cables are in wired networks. A detected intrusion in a wireless network is generally an indication that the intruder is within radio range, possibly armed and prepared to engage in a kinetic attack. An intrusion alarm in a WCT network merits different types of responses than those in a wide-area wired network.

2.2 Coalition

This term is used for a network whose elements are governed by different bodies. As result, different policies may apply for procurement, use, and protection of the network. In coalition networks, there is a need for carefully specified and controlled information exchange between the different coalition network elements. In practice, the trust between coalition governing parties is limited and network traffic is generally not exchanged freely.

2.3 Tactical

Information flowing in WCT network is typically related to an operation in progress; the value of the information may decrease rapidly with time. The confidentiality requirements of data are likely to be of short duration. Since messages could be commands to soldiers to undertake joint fires, their integrity and authenticity are of great importance, and the network should be protected from injected messages, replay attacks, and message modifications.

2.4 Connectivity

Tactical wireless networks are limited by low bandwidth and noise. The radios that operate on military VHF/UHF bands provide only few kHz of bandwidth (resulting in 16 to 150 kb/sec), roughly half of which is used to mitigate the high error rates and multiple user access to the radio channel. These tactical radios support robust long-range connections of 5 to 30 km through complex terrains while providing jamming resistance, using anti-jamming techniques such as channel frequency hopping. Tactical networks have requirements to support bandwidth-intensive one-to-many and many-to-many real-time group communications such as all-informed voice, group push-to-talk, and situational information sharing, despite their limited available spectrum.

In future WCT networks, responsiveness, reliability, and robustness will be paramount; supporting these message and process-intensive capabilities makes scalability a challenge. The network size is foreseen to be equivalent to a military platoon (of a few sections) size, in the order of 20 – 60 nodes or even fewer for

[1] Wireless Coalition Tactical (WCT) networks provide tactical networking capabilities to a deployed force in a mission which may include a Forward Operating Base (FOB), mobile and stationary nodes, as well as network formations aided by base-stations and peer-to-peer ad hoc nodes.

operations on the move. Even if a tactical network scales up to 100 nodes in the future, it will remain smaller than most (wired) networks.

Tactical wireless networks tend to be mission oriented, require preparation, and their node movements are in (hierarchical) groups [2]. Node mobility tends to be on foot (5 km/h) or in vehicles (100 km/h). Most nodes tend to maintain network connectivity. While the long-distance radio range and short hops are good for network connectivity, they could also hinder it by considerable interference if efficient multiple access techniques (in Media Access Control – MAC – layer) are not used. In addition to multiple access techniques, performance in WCT networks may be improved by cross-layer network optimization as well as traffic and flow control techniques to reduce the overhead and improve throughput.

2.5 Threat Analysis

A sophisticated attacker could use several techniques to study the network, its protocols and messages, and even inject traffic into the network; he/she may weigh the risks of being detected to possible outcomes for each step in an attack. A passive attacker could breach the link security to eavesdrop on the traffic without further actions.

A sample of possible attacks on the WCT network is presented below, in ascending order of difficulty and descending likelihood of implementation:

1) **Attack on the Radio Spectrum** – Emitting radio energy into the frequency band used by the network may disrupt network traffic. A radio jammer can be inexpensive. Some jammers can be detected and located easily. Sophisticated jammers can be very difficult to detect and locate [3].
2) **Attack Using Stolen/Found Friendly Radios** – A radio loaded with crypto keys in the hands of an adversary could disrupt the network by traffic injection, e.g., holding the Push-To-Talk (PTT) button. This attack is more difficult to detect since this behaviour may appear to be caused by a friendly, but unskilled, operator.
3) **Attack Using Link Crypto Keys** – An attacker could inject forged messages using friendly link crypto keys on the same radio frequency band as the friendly operation. The attacker could also eavesdrop on friendly traffic or even disrupt the routing protocol. These attacks could be detected by Intrusion Detection Systems (IDS) because they generate abnormal and suspicious traffic.
4) **Attacks Using Compromised Services** – An attacker with advanced reverse engineering and laboratory resources could compromise existing services, such as a Discovery Service or a Domain Name Service (DNS), or could set up rogue services, spoof data, or use "man-in-the-middle" strategies for modification of messages. An IDS may have difficulties detecting these sophisticated attacks, which require knowledge from key services, protocol specifications, network architectures, and crypto keys.

2.6 Attacker's Assets

The attacker is likely to keep its capabilities hidden for as long as possible. Capabilities could involve material or immaterial assets. Material assets could consist of money or equipment while immaterial assets could include proximity or secrecy and knowledge.

2.7 Summary

The characteristics of wireless coalition tactical networks differ from those of conventional wide-area networks; some of these characteristics affect the threat model and the protection requirements of WCT networks.

The limitations and threats to WCT networks are kept in consideration in the next three sections where we present extensions to connectivity, security services, and establishing CoTs in coalition scenarios for tactical deployments.

3.0 CONNECTIVITY SERVICE

Distributed wireless network defence may be performed more effectively when information from multiple MANETs can be shared and fused. Therefore, providing connectivity to another MANET can be considered as the first step in securing dynamic wireless networks in coalition environments, which is of fundamental concern. In this section we describe a scenario where MANET-B (MANET of Nation-B) provides network connectivity to MANET-A (MANET of Nation-A) to communicate to the trans-national Forward Operating Base (FOB), as depicted in Figure 1. By design, MANETs help facilitate range extension to mobile nodes where all nodes operate under a common security and network management policy. However, the security and policy complexities for two MANETs from different Nations (with different internal policies) to co-operate to provide range extension to one another is a fundamental challenge explored by this scenario.

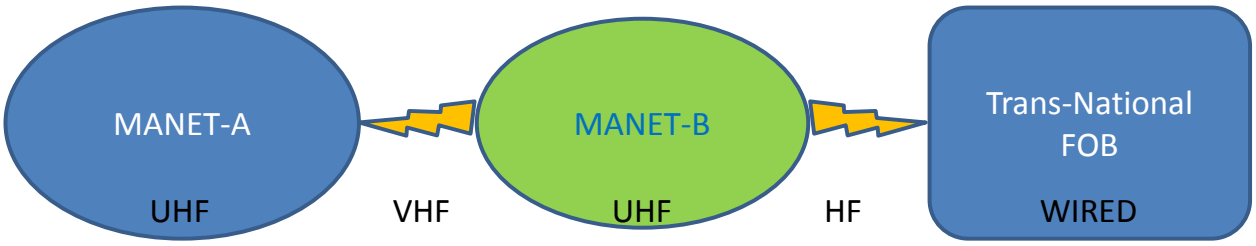

Figure 1: Nation-B Provides Network Connectivity to Nation-A to Communicate to the FOB.

In the following scenarios presented below, we describe situations where one or a combination of radios (UHF, VHF, and HF) may be used to provide connectivity service to MANET-A for communication with the FOB. Note that while Figure 1 depicts national MANETs as enclosed entities, the descriptions of the scenario use cases assume a more practical, non-uniform shape, more reflective of military formations of a section or platoon in tactical operations. As depicted in the figure, we assume that each nation has radio connectivity within its MANET and that the connectivity range of the wide-band radios within a national MANET with UHF is shorter than the narrow-band VHF radios available for longer range communication between nations. In HF radios, yet more bandwidth is traded for longer range connectivity.

We have divided the scenario into several use cases by considering the degree of exposure of MANET-A's messages to MANET-B as they are delivered back to the FOB; specifically, we examine to what degree should the messages of MANET-A be readable by MANET-B so that MANET-B can first learn of the need for service (discovery) and then provide the service (routing/connectivity). Cases for discovery could range from a direct order from the FOB, to a sophisticated and secure NATO protocol for service request, service discovery, and node authentication. In the former, there is no message exposure; whereas in the latter, secure messages are shared openly by a well-defined protocol. Cases for routing could range from static gateways tunneling MANET-A's messages (least exposure) to a full merge of both MANETs sharing the same routing protocol (most exposure). In all, message exposure itself could also be considered in different grades:

- At the header only with encrypted payloads, where MANET-B would be able to distinguish broadcast and unicast messages;

- At the header and certain payloads, where MANET-B would be able to recognize Situational Awareness (SA) data, signaling messages, routing messages, but not other payloads; and
- At the header and all payloads, where complete sharing of encrypted messages with a common key management system and security policy is certified and permitted.

In discussions with IST-103 – Protected Core Networking (PCN) – we explored how, or if, PCN concepts could be applied to the MANET connectivity scenario. In PCN terminology [4][2], an E-node[3] advertises guarantees of bandwidth and other services of its Coloured Cloud[4] (CC). It will be equipped with Service-Level Agreement (SLA) management functions, including support for security and risk. In consideration of E-node functions, a MANET node can only partially benefit from the PCN concept because under PCN guidelines, a MANET node cannot (should not) connect Protected Core Segments (PCSs), because it cannot advertise bandwidth guarantees [7]. The PCN-1 interface limits MANETs from PCS interconnections, because it is defined only for connecting two E-nodes of distinct PCSs, and MANETs cannot be distinct PCSs. A MANET can be an E-node only when paired with the Narrow-Band Waveform Radio[5] – see Figure 2 (left); otherwise a MANET would be treated as a CC. There is, however, partial benefit from the PCN concept for providing a connectivity service; it may be explained by the PCN2 interface requirements which include management functions such as:

- Network Management and Cyber Defence (NMCD):
  - Authentication, authorisation and accounting;
  - SLA management;
  - Sensor fusion;
  - Network and security analysis (incl. Real-Time Automated Risk Assessment – RTARA);
  - Decision support;
  - Network control; and
  - Situational awareness.
- Public Key Infrastructure (PKI):
  - Management of PCN credentials; and
  - Used for PCN-1, PCN-2.

[2] FKIE is developing a first draft requirements overview for federated networking for the 2005 NATO Network-Enabled Capability (NNEC) [5]; this draft document is prepared on behalf of NCIA based on the work of IST-069.

[3] An E-node is a "logical component in the Protected Core Segment (PCS) that supports the interface with the other PCN components": PCN-1 (for connecting to an E-node of another PCS), PCN-2 (for connecting to a Coloured Cloud), and Internal Connections (for connecting to an E-node of the same PCS). No specific assumptions have been made concerning the internal architecture of the E-node; its functional characteristics are described in [6].

[4] Coloured Clouds are external networks that connect to a Protected Core Segment (PCS) and use its services.

[5] As shown in Figure 2 (right), the logical representation of a national LAN may be with a Coloured Cloud. However, the physical implementation of a MANET node, Figure 2 (left), may span a CC and a PCS. For example, a Narrow-Band Waveform Radio – a low capacity, long-distance VHF radio for voice and Situational Awareness (SA) data meant for use as gateways interconnecting two MANETs of other waveforms – could support NINE (a NATO IPsec implementation) and SCIP (an application encryption – Secure Communications Interoperability Protocols) crypto modes for secure and agile interconnectivity. In this example, the interconnection between NINE and SCIP would follow the PCN-2 interface requirements, making NINE as part of the PCS, an E-node. Unlike an E-node that connects to other E-nodes with a PCN-1 interface, a MANET node adheres to the PCN-2 interface to connect to an E-node; the E-node itself doesn't have to be mobile. Though, a PCN-1 interface is not permitted on NINE, or other MANET-type radios, such limitations within the PCN concept are outside the scope of this report.

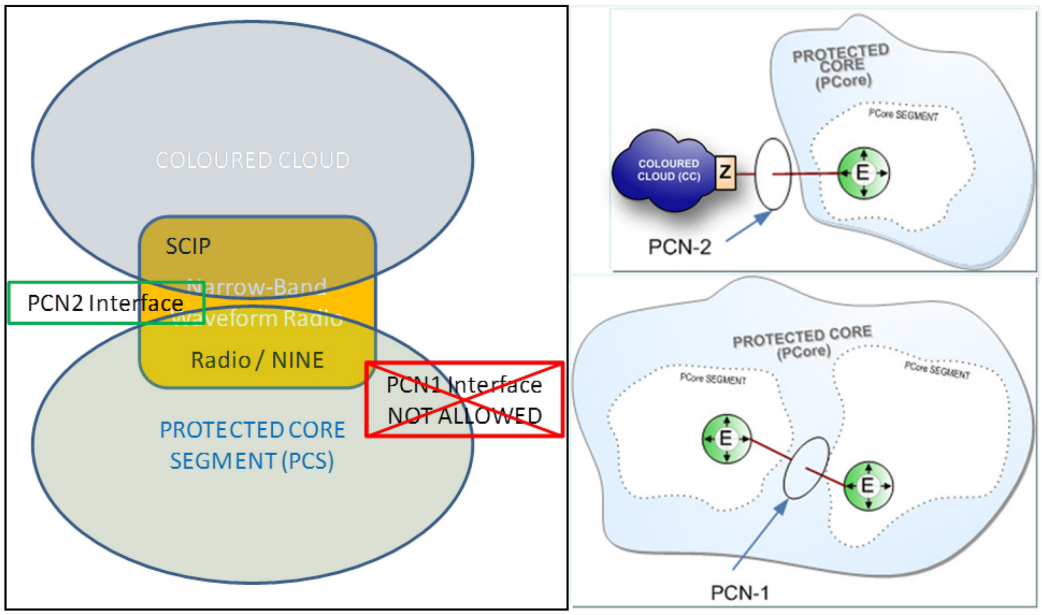

Figure 2: The Physical Implementation of a PCN (left for Narrow-Band Waveform Radio) may be Different from its Logical/Functional View (right) [7]. A PCN-1 interface connects E-nodes to PCSs. A PCN-2 interface connects E-nodes to Coloured Clouds [4].

A MANET node should be able to benefit from those management functions for the purposes of our set of scenarios (providing a connectivity service) if the PCN concept were applied to MANETs.

With the above management functions (for discovery and routing) in mind, MANET-B could either fully merge with MANET-A forming a larger MANET-AB, or it could provide a forwarding tunnel service to MANET-A. Supplementary use cases would fall within special circumstances of these two. The full merge use case would allow for complete sharing of information between the two MANETs. This use case requires security policy, key management, and routing protocols to be compatible (common) to both MANETs A and B so that node discovery or need-for-service discovery could trigger full merge procedures. These common algorithms, procedures, and processes will have to be pre-set in the mission planning stage by NATO force Commanders. On the other hand, a forwarding tunnel service would only allow for limited sharing of information between the two MANETs. Limited sharing may or may not require the above concepts, algorithms, procedures, or processes. Depending on the availability of any of them, one could produce several use cases, a sample of which we have listed below in ascending order of complexity.

We consider five sub-scenarios that offer trade-offs between message exposure and flexibility / automation / management overhead. These sub-scenarios are depicted in Figure 3 to Figure 7, where the “stars” in each MANET represent gateway nodes capable of communicating with peer-level gateway nodes in the other MANET.

3.1 Use Case 1: MANET-B Gateway is Directed to Establish a Tunnel with MANET-A Gateway

The first connectivity sub-scenario minimizes the exposure of information between the two MANETs, but offers the least automation and configuration flexibility. In the absence of any automated node discovery or need-for-

service discovery algorithms operating between MANETs A and B, a connectivity service could be initiated and managed by the FOB. The FOB can direct MANET-B to provide connectivity services to MANET-A, assuming the FOB possesses knowledge of MANET-B's location and has observed a loss of connectivity with MANET-A. In this case, MANET-B could establish at least two static gateways (under the direction of the FOB):

- One gateway to connect to a designated gateway node in MANET-A; and
- One gateway to connect to the FOB.

Messages and data from MANET-A would be tunneled through MANET-B to the FOB using security policy, key management, and routing protocols proprietary to MANET-B. The data from MANET-A would remain encrypted as per protocols in place by MANET-A and it is this encrypted data that would be tunnelled through MANET-B. In this scenario, MANET-A would have no insight into the networking/routing in MANET-B taking place to provide the service. In this scenario, MANETs A and B could remain non-compatible in terms of network management, internal key management, and routing protocols. While this scenario minimizes information exposure between the two MANETs, it requires manual intervention by the FOB even to the point of identifying gateways to provide the connectivity service.

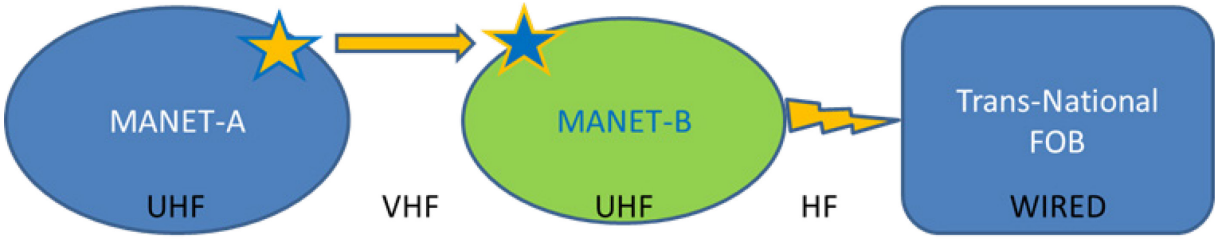

Figure 3: A Depiction of Use Case 1 Showing Limited and Pre-Arranged Information Sharing Between MANETs A and B.

3.2 Use Case 2: MANET-B Gateway Discovers a Compatible MANET-A Gateway and Establishes a Tunnel

The second connectivity sub-scenario presumes the existence of a single gateway in each MANET that supports service discovery from the other Nation's MANET (whereas the first scenario presumed no such service discovery existed). Such a scenario would require that gateway nodes be capable of communicating securely with a (potentially NATO-provisioned) radio. If MANET-A lost connectivity with the FOB, then Gateway-A could automatically discover Gateway-B and request a connectivity service, assuming these gateways were in range of one another. In this case, MANET-B could connect MANET-A to the FOB, once again with messages of MANET-A tunneled through MANET-B to the FOB using security policy, key management, and routing protocols proprietary to MANET-B. This case is more difficult to implement than "Case-1" because MANETs A and B now have at least two compatible nodes that require mission planning for a common NATO security policy, key management scheme, and routing protocol to discover one another and allow service discovery. Exposure between the two MANETs is still minimal in this scenario, although it does require the exchange of service discovery messages between the gateways. It allows an increased flexibility compared to the first case, however, since the FOB is no longer required to be involved in service discovery and management.

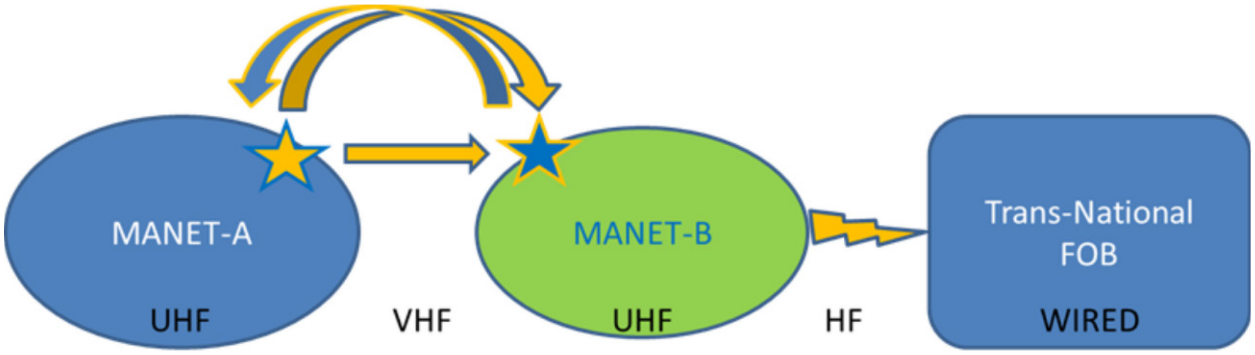

Figure 4: A Depiction of Use Case 2 Showing Limited but Self-Organized Information Sharing Between MANETs A and B.

3.3 Use Case 3: MANET-B Mobile Gateways Discover Compatible MANET-A Mobile Gateways and Establish Tunnels

In the third connectivity sub-scenario, we consider the case where several nodes in MANETs A and B are capable of functioning as gateways, in contrast to the previous scenario where each MANET had only one Gateway node. In this case, gateway nodes in both MANETs must have access to common algorithms, procedures, and processes to exchange request and response messages for services. Any gateway node in MANET-A would be able (through discovery) to select the most appropriate gateway node in MANET-B from which to request connectivity services. Nodes in MANET-A would forward data to the FOB via a path from Gateway-A to Gateway-B and then through a tunnel in MANET-B, once again using protocols proprietary to MANET-B. This case is more complex than the preceding one because MANETs A and B now require compatible algorithms, procedures, and processes necessitating NATO mission planning for (at a minimum) node/service discovery, and perhaps basic situational awareness sharing (at least between the gateways). Exposure between the MANETs is increased compared to the previous two scenarios since gateway nodes share discovery information; however, the flexibility of this scenario is considerably greater than "Use Case 2", since more nodes can operate as gateways, removing the requirement that the single designated gateways remain in close proximity to one another.

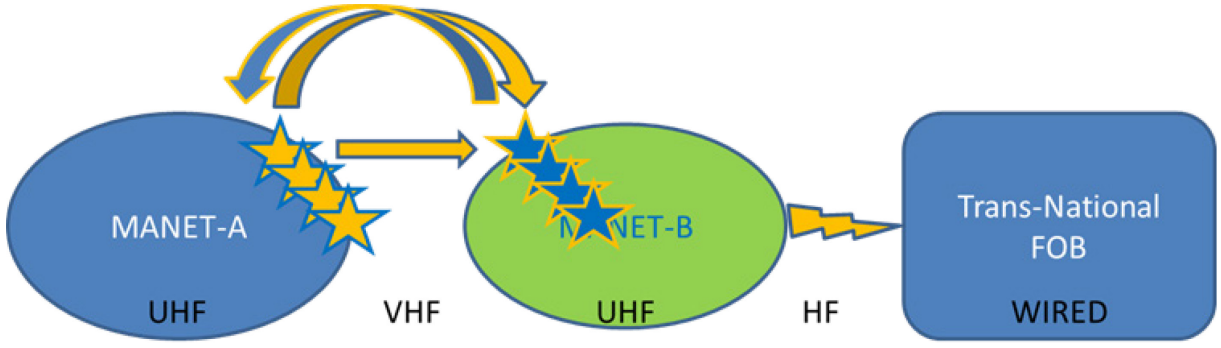

Figure 5: A Depiction of Use Case 3 Showing Limited NATO-Organized Information Sharing Between MANETs A and B.

3.4 Use Case 4: MANET-B Mobile Nodes Discover and Establish Routes to Compatible MANET-A Mobile Nodes

In the fourth connectivity sub-scenario, we consider the case in which MANET-A's requirement for connectivity service is not limited to a connection back to the FOB. If some of the nodes in MANET-A are out of range from one another (e.g., in the simple case where the MANET is divided into two disconnected groups), then MANET-A could benefit from a service offered by MANET-B nodes to provide connectivity between the separated MANET-A nodes, as well as connectivity back to the FOB. In this case, every node in MANET-A and MANET-B would be capable of serving as a gateway to connect to nodes from the other MANET. This case is more complex than the preceding one because not only would all nodes in MANETs A and B require gateway functionality (including compatible algorithms, procedures, and processes for sharing basic situational awareness and node/service discovery), but also MANET-B nodes would need to maintain sufficient awareness of the connectivity of the nodes in MANET-A in order to adequately advertise the connectivity services that MANET-B can provide. This scenario further increases the exposure of information between the two MANETs, as they are required to share more information to support the increase in services. As before, messages of MANET-A nodes would be routed through MANET-B to other MANET-A nodes or to the FOB using security policy, key management, and routing protocols proprietary to MANET-B.

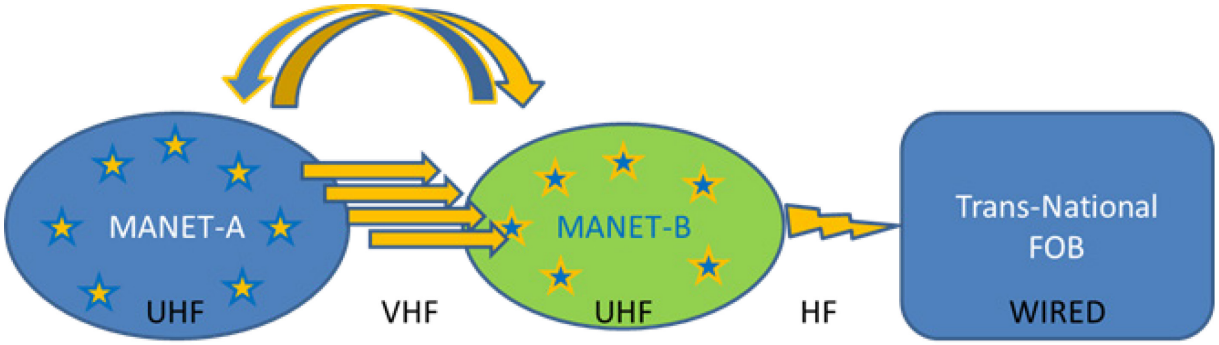

Figure 6: A Depiction of Use Case 4 Showing Less Stringent Information Sharing Between MANETs A and B.

3.5 Use Case 5: MANET-B Performs a Full Network Merge with MANET-A

The final connectivity sub-scenario examines the case where the two coalition networks, MANET-A and MANET-B, operate using a common set of routing algorithms and network policies such that – for routing and connectivity purposes – they "functionally" merge into the single network MANET-AB. In this case, MANET-AB nodes would effectively obtain interconnection with the FOB if either MANET-A or MANET-B were connected to the FOB. Some MANET-A data could still be encrypted (at the application layer) to preserve confidentiality from MANET-B, but lower layer information would be shared. This case is considered the most complex because MANETs A and B now must have compatible algorithms, procedures, and processes that require NATO mission planning for all communications applications. This case also leads to the most exposure between the two MANETs, but provides the greatest level of service with all A and B nodes connected to a larger MANET covering a larger area with an efficient use of routing algorithms. Messages of MANET-A would be relayed (as opposed to tunnelled) by MANET-AB nodes to the FOB using security policy, key management, and routing protocols common (or interoperable) to both MANETs A and B.

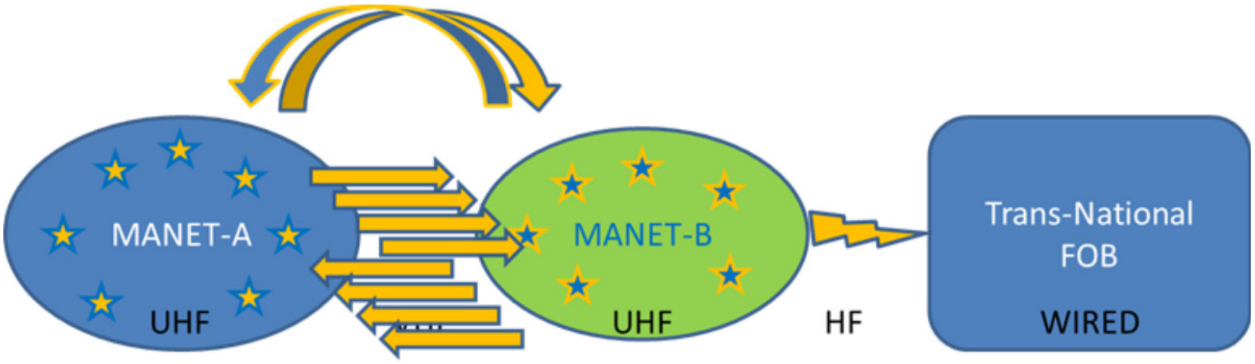

Figure 7: A Depiction of Use Case 5 Showing Unlimited Information Sharing Between MANETs A and B.

3.6 Summary

Distributed wireless network defence for coalition tactical networks may be performed more effectively when information from multiple MANETs can be shared and fused. While connectivity service is important on its own, providing connectivity services between two MANETs can be considered as a first step in securing dynamic wireless networks in coalition environments. In this chapter, we have discussed five connectivity sub-scenarios where one MANET (MANET-B) provided different levels of connectivity services to a second MANET (MANET-A). The scenarios demonstrate a trade-off between the level of exposure of data between the two MANETs and the automation / level of connectivity services offered. Table 1 summarizes this trade-off for the five sub-scenarios considered.

Table 1: A Summary of Sub-Scenarios with Respect to Service Discovery, Routing, Connectivity Service, and Degree of Exposure.

Sub-Scenario Number	Service Discovery	Routing	Connectivity Service	Degree of Exposure
1	Manual by the FOB	Tunneled	Manually configured two static gateways	Low
2	Manual by (potentially) NATO provisioned radios	Tunneled	Pre-configured two static gateways	Low
3	Automatic by (potentially) NATO provisioned radios	Tunneled	On-the-fly configured static gateways	Medium
4	Compatible algorithms, procedures, and processes for sharing basic situational awareness and node/ service discovery	MANET-B routing protocol	Mobile gateways	Med – High
5	Common algorithms, procedures, and processes for sharing basic situational awareness and node service discovery	Common routing protocol	Relayed by MANET-AB nodes	High

The use cases vary based on the level of exposure of messages MANET-A requires to exchange to first be discovered with a need-for-service and then receive the routing service. Ultimately, both service discovery and routing depend on the compatibility of the MANETs' algorithms, procedures, and processes that require NATO mission planning for applications such as, situational awareness, node discovery, and voice/data communication.

4.0 SECURITY SERVICE

In military coalition environments, national MANETs may be interconnected for information sharing by means of a common coalition waveform. In this setting, each Nation is responsible for protecting its networks against cyber-attacks and for implementing adequate security measures. The coalition partners may also provide security services to one another, i.e., sharing security related information and enhancing situational awareness. In this section, we describe a set of scenarios where MANET-B provides varying levels of security services to MANET-A, ranging from monitor-and-alerting to a collaborative security posture. We discuss how the level of service provided influences how much information must be shared between the two nations. The considered network setup is depicted in Figure 8.

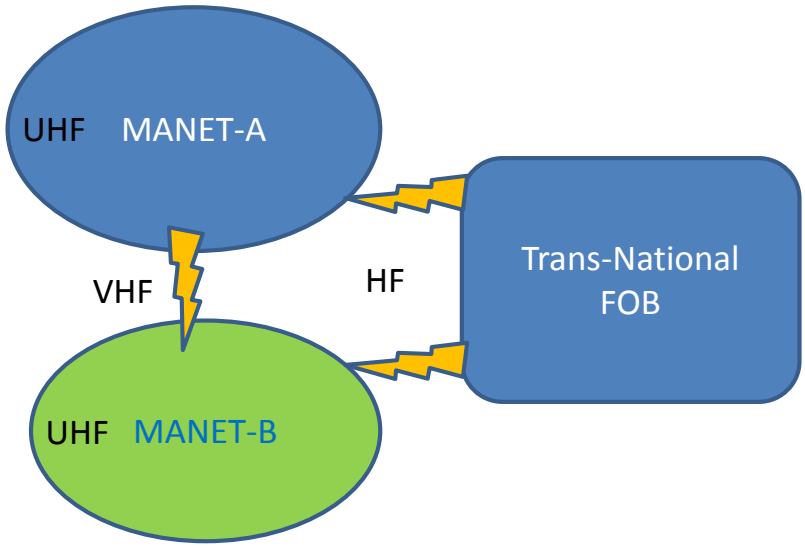

Figure 8: Nation-B Provides a Security Service to Nation-A.

Sharing security-related information in a coalition could provide complementary benefits to the participating Nations, but it will depend on the capabilities and the disposition of the Nations. Information shared by MANET-B (operated by Nation-B) about network events may constitute a new source of information for MANET-A (operated by Nation-A) which it could use as an extension of its sensor coverage or fuse with its own observations. This complementary monitoring may relieve MANET-A from deploying a comprehensive set of sensors – which can be a cost saving for coalition deployments.

The knowledge of security incidents anywhere inside and outside a coalition network may help MANET-A to decide on counter measures or security posture. For example, a map of all observed actions of external attackers, conceivably provided by MANET-B, may reveal a level of awareness about the tactical situation of the adversary forces; this map could allow the commander of MANET-A to refine its mission planning. Such indicators (e.g., of adversary nodes) could allow MANET-A to adapt its routes and security policies from

blocking the access to internal resources for certain nodes, up to a complete isolation of designate nodes, or avoiding routes through specific networks.

In order to provide a security service, MANET-B has to overcome several challenges related to monitoring the network events in the wireless domain. The assumed UHF radios for communication within a single MANET are typically short range, which limits the spatial distribution and the distances for monitoring coverage. Another challenge or a limiting factor in this case, is that information at the network layer (of MANET-A) and above could be obfuscated to MANET-B – by MAC layer encryption. Even worse, the perceived communication behaviour of monitored nodes may be altered by an attacker node outside MANET-B's sensing range targeting the MAC processes. These challenges could make monitoring data difficult, unreliable, or incomplete for MANET-B.

Nevertheless, MANET-B could attempt to provide graded security services to MANET-A in a spectrum that could range from monitoring and alerting to a collaborative security posture. The former service, would require little interaction between the MANETs other than the communication of alarms and alerts, because the monitoring could transpire with little input from MANET-A. In this approach, while MANET-B performs the analysis just once and distributes the results efficiently with condensed alert messages, it could also lose details of the original data and might therefore reduce the options of identifying correlations in the data. In contrast, in a collaborative approach, the two MANETs could exchange sensor data, cover a wider range (area), and act as one (joint) MANET. This approach would consume more bandwidth and requires MANET-A to spend resources analysing the received raw data. This trade-off (of bandwidth efficiency and resolution to potential security issues) should be considered carefully for use case development. With this in mind, we assume an information sharing method where either one of these two approaches may be applied. The decision of whether to share alert messages or the raw (monitored) data should take into consideration the willingness of the service provider to share information in the first place. In the context of network security in a coalition environment, this willingness could be impeded by one's exposure.

The willingness of coalition partners to share or expose internal networking information to Allies may vary between Nations. This willingness will restrict the extent of the security services a Nation may provide. Just as MANET-A would assess the trustworthiness of shared tactical data and services, MANET-B could be cognisant of its own exposure as a consequence of the data it shares, the services it provides, and ultimately the traffic it monitors in a coalition. It is assumed that the less reflexive the exposed information, the higher the willingness for providing the service. With this consideration, we present four security service sub-scenarios in decreasing level of information that is disclosed to other Nations about the internal security state of the service provider, MANET-B. The use cases highlight the trade-off between the type of information disclosed amongst partners and the security services that can be offered from one MANET to another.

Figure 9 provides an overview of the four use cases which are described in more detail below. In all cases, MANET-B captures information from a variety of sources (i.e., by monitoring different locations of the network topology) and shares the information (either pre- or post-analysis) with MANET-A. In each case, MANET-B inspects a different information source and a different part of the network topology; in descending order, it exposes less of its own internal security state and thus, addresses diverse threats.

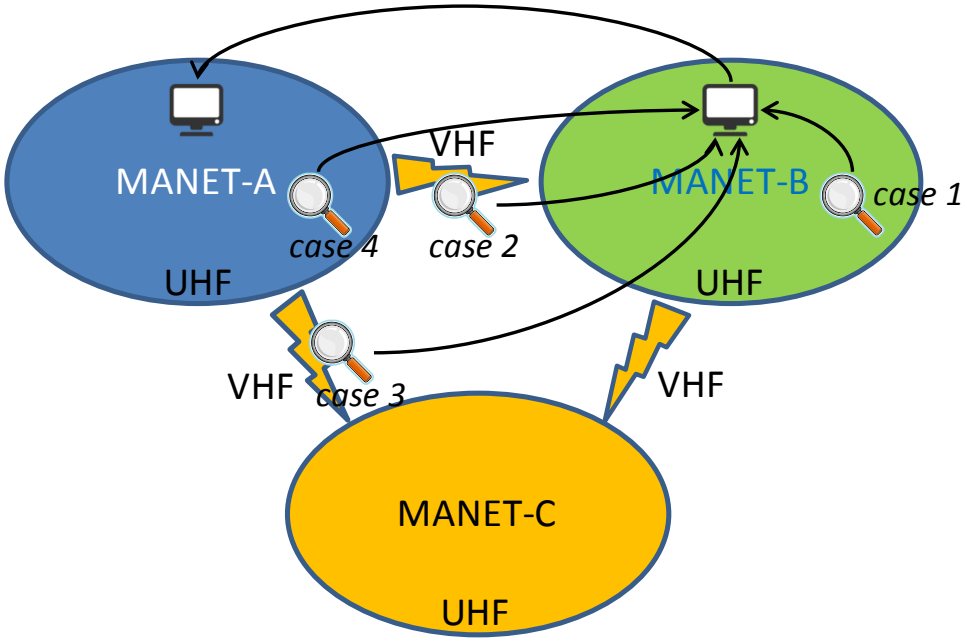

Figure 9: A Depiction of Four Security Service Sub-Scenarios, Which Show Nation-B Monitoring Network Traffic from Different Locations in the Network Topology and Providing Security Services to Nation-A.

4.1 Use Case 1: MANET-B Monitors Intra-MANET-B Traffic

In the first sub-scenario, MANET-B could monitor its own internal activities (i.e., control and application data and traffic flows) and potentially apply intrusion detection techniques for analysing the captured data. By sharing the corresponding results of the intrusion detection analysis with MANET-A, MANET-B could enhance the security awareness across the boundaries of both MANETs[6]. However, at the same time, MANET-B could risk exposing certain capabilities and vulnerabilities of its own network, as well as its own internal security state.

Since MANET-B limits its security monitoring scope to its own network, this provides for accurate traffic observation since all monitored nodes are controlled by the same authority and can actively and willingly participate in the monitoring process. In this sub-scenario, the data shared by MANET-B might reveal compromised nodes in, or adversaries near, MANET-B. Regardless of where the data is analysed (in MANET A or B), the shared information allows MANET-A to assess the capabilities and trustworthiness of MANET-B and to decide whether to restrict interaction with MANET-B, (e.g., remove routes that involve MANET-B nodes as relays). This case poses the most exposure to MANET-B's information.

4.2 Use Case 2: MANET-B Monitors Inter-MANET-AB Traffic

In contrast to focusing only on its own internally generated traffic, in the second sub-scenario, sensors deployed in MANET-B could capture and inspect all traffic exchanged between MANET-A and MANET-B, including

[6] Note that instead of sharing the results of the intrusion detection analysis with MANET-A, MANET-B could instead share the "inputs" to the intrusion detection sensors and allow MANET-A to perform its own analysis, coupled with any data independently gathered by MANET-A. In this case, the shared information could consist of traffic statistics related to the exchange of control data (e.g., routing traffic statistics) and traffic statistics related to the exchange of tactical data.

management and control data. These data (or the analysis thereof) could be shared with MANET-A, and could provide the basis for uncovering suspicious node behaviour without directly involving the corresponding source and destination devices. The interconnection of MANETs A and B by means of a coalition waveform could give nodes from both networks the opportunity to access information and services on nodes of the other network.

In comparison to Use Case 1, the exposed information about capabilities, vulnerabilities, or the internal security state of MANET-B is reduced; this is a consequence of the fact that MANET-B is reporting only on inter-MANET traffic as opposed to on events occurring in (and limited to) its own network. Here, the data shared by MANET-B might reveal compromised nodes in, or adversaries near, either network. Regardless of where the monitored data is analysed (in MANET A or B), the shared information allows both MANETs to assess their joint capabilities and to decide how to react to a network event.

4.3 Use Case 3: MANET-B Monitors Inter-MANET-AC Traffic

In the third security service sub-scenario, we consider the case where MANET-A interacts with the network of another coalition Nation, MANET-C, where MANET-A and MANET-C use a common NATO coalition waveform. If a common group key were used for encryption of the coalition radio links, then MANET-B would be able to monitor the traffic flows between MANETs A and C; MANET-B could analyse the traffic flows to potentially detect adversaries, intrusions, or suspicious node behaviour of either MANET without directly interacting with them. The monitored traffic flows by MANET-B (the security service provider) to MANET-A (the security service recipient) could include management and control data targeted to, coming from, or just relayed by MANET-A. The information shared by MANET-B to MANET-A could comprise of MANET-B's analysis of these data if MANET-A is not equipped with proper analysis tools.

Because MANET-B only monitors the coalition-wide traffic flows and is not a participant in the application layer communication in these monitored flows, MANET-B reveals much less information about its own capabilities, vulnerabilities, or internal security state in comparison to Use Case 2. The data shared by MANET-B may reveal compromised nodes in MANET A or C (with respect to all monitored traffic, i.e., coalition-wide traffic and application layer traffic) and in MANET-B, but only with respect to the coalition-wide traffic in which it participates.

4.4 Use Case 4: MANET-B Monitors Intra-MANET-A Traffic

In the final security service sub-scenario, MANET-B monitors the internal traffic of MANET-A, and applies intrusion detection techniques to analyse the captured data. The analysed data shared by MANET-B may reveal compromised nodes in MANET-A. In contrast to the previous cases, the information shared by MANET-B is completely unrelated to its own security state; therefore, it may be most willing to provide this service from an exposure point of view[7]. The effective accuracy of intrusion detection, however, is limited because the traffic of monitored nodes (MANET-A) may be encrypted with keys unknown to MANET-B.

[7] We note, however, that this service requires MANET-B to perform additional work that it would not otherwise be doing. Thus, from the point of view of MANET-B's power usage and general network efficiency this is the least desirable service for it to provide. There is a trade-off here between analysis effort that MANET-B was going to undertake in any case (e.g., in Use Case 1, where MANET-B analyses its own traffic) and exposure of MANET-B's internal state. Use Case 4 provides the least exposure of MANET-B, but requires the most additional analysis effort.

4.5 Summary

In this section, we discussed four security service scenarios in which one MANET provides security services to another MANET by monitoring and analysing traffic and traffic flows at different points in a network topology. We have shown how different grades of service may be afforded by a provider and that these different grades of service will require the provider to risk exposing its own security state to a greater or lesser degree. Throughout the sub-scenarios, we assumed the availability of a common NATO coalition waveform (for PHY and MAC layer communication for applications such as situational awareness, node discovery, and voice/data communication), which would facilitate coalition participation for provisioning security services at the tactical edge.

Table 2: A Summary of Sub-Scenarios with Respect to Service Provider Willingness and Degree of Exposure.

Sub-Scenario Number	Monitored Traffic	Service Provider (MANET-B) Willingness	Degree of Exposure
1	Intra-MANET-B	Low	High
2	Inter-MANET-AB	Medium	Medium
3	Inter-MANET-AC	High	Low
4	Intra-MANET-A	Highest	Lowest

5.0 COMMUNITIES OF TRUST

In this final scenario, we introduce the concepts of a Community of Trust (CoT) and a Community of Interest (CoI); we describe how these concepts can be applied in a coalition MANET and highlight the difference between the two concepts. Specifically, we discuss how MANET-B sensor nodes could share data with MANET-A nodes as part of a CoI, although the nodes from A and B are not members of the same Community of Trust.

A CoT describes a group of networked nodes that have established trust relationships such that they allow a less restricted flow of information between one another, e.g., a group of soldiers belonging to the same platoon or nodes operating at the same security classification level in a national strategic network could be considered a single CoT. The CoT concept is useful, since it allows the individual nodes within the CoT to implement relaxed protection mechanisms for intra-CoT communications, assuming the existence of adequate perimeter security / border control[8]. We use the term Community of Interest (CoI) to denote a group of nodes – within the same CoT or across multiple CoTs – who share a common interest in certain information and who wish to securely share that information (e.g., a group of intelligence community nodes within MANETs A and B who wish to securely share intelligence data may constitute a CoI). As shown in Figure 10, while two nodes belonging to two separate Nations may share interests in a common information domain and form a CoI, the trust that they share inside

[8] We acknowledge that it is difficult to have border control in a wireless network in the physical sense. However, border control in a networking sense is a feasible concept via firewalls and MAC address filtering.

their respective Nations (inside the CoT) is not extended to the nodes of other Nations. The CoTs may restrict or even hide system details, identity credentials, and information metadata from each other. To support the concept of a CoI, however, we submit that the exchange mechanisms between communities are subject to far more flexible authorization arrangements than a simple 'guard' between two hierarchical security domains.

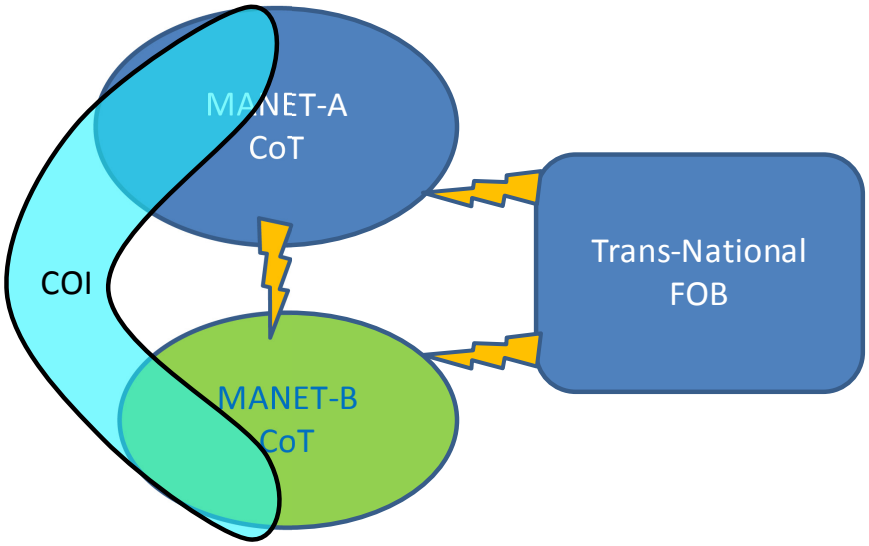

Figure 10: A Depiction of Two CoTs Communicating Across Nation-A and Nation-B for a Specific CoI. A CoT describes a group of networked nodes that have established trust relationships with one another such that they allow a less restricted flow of information. Nodes that belong to a CoI share a common interest in information and may communicate across national boundaries.

In the remainder of this section, we first provide a general introduction to the problem of information exchange in the coalition context, addressing the following concepts important to information exchange across security domains: *Access Regime, Relay of Information Across CoTs,* and *Authorization Requirements.* With an operational example for each concept, we will highlight the relevance of the CoT to information exchange. We will then present a scenario incorporating and illustrating all of these concepts working together.

5.1 Access Regime

By definition, a user with the required clearance level gets access to all the information in a CoT; the user may only be restricted by the required Need-To-Know (NTK) authorization principles, where applicable. The 'System High' security mode of operation (e.g., using a style of Mandatory Access Control policies) facilitates the exchange of information in accordance to security policy, allowing the "free" flow of information between peer classification levels or to higher security levels. Sending information opposite to this policy requires an assurance that the actual information item not be classified higher than the classification of the target CoT [8] (or have release terms counter to the policy).

One technique to obtain such assurance is to attach trusted (e.g., cryptographically bound) *security labels* to all information objects, which can be inspected by a *guard*. A guard is a non-by-passable unit in the connection point between two CoTs. The guard implements an access regime where it verifies security labels attached to information objects and enforces policies before allowing the information to pass through. Guards and security labels are well researched in the literature [9],[10]; a Common Criteria Protection Profile allows guards to be

evaluated for high assurance [11]. However, it is plausible that information exchange may take place between two CoTs that do not align with one single hierarchical classification regime. Thus, there is a requirement for a more flexible representation of security policies and a more flexible framework for policy enforcement than guards which assume a 'System High' mode of operation, incapable of handling different security hierarchies.

5.2 Transit CoTs

Ordinary information exchange among CoTs may cause information destined from CoT-1 to CoT-2 to be passed on to CoT-3. This situation brings about a decision question whether or not the exchange policies from CoT-1 to CoT-2 should be applied to the exchange from CoT-2 to CoT-3. This reasonable demand requires the exchange point between CoT-2 and CoT-3 to be able to interpret the corresponding security related meta data **of the information** and to make transfer decisions accordingly. In a *guard centric exchange,* the policies are **attached to the guards**, where CoT-2 will not be able to observe CoT-1's policies regarding the transfer of its information to CoT-3. Therefore, it is necessary to implement enforcement precautions so that the CoT-1's policies are both observed at CoT-2 and enforced by CoT-2.

In a data-centric security model, in contrast to the guard-centric model, the policy is attached[9] to the information by the authorized originator and that same policy is enforced by intermediate relay nodes[10], regardless of their access regimes. The data-centric security model seems to be better suited for the required flexibilities of information exchange in collation operations at the tactical edge.

5.3 Authorization to Exchange

Only authorized subjects should be allowed to initiate exchange of information between CoTs. The authorization should be checked prior to the transfer process and (optionally) validated by the receiver to ensure that the information came from an authorized entity. The intention of this arrangement is to prevent mislabelling and intentional compromise of sensitive information.

In light of these concepts, we now present a coalition scenario in which national wireless networks form individual CoTs.

5.4 Use Case: Sensor Network

A platoon from Nation-A (MANET-A) deploys a number of sensors in an area to monitor RF activity and to detect potential adversaries. The sensor network is self-organized and is not necessarily connected to any backbone network; but it is an extension of MANET-A (as intelligence nodes) and part of the same CoT. It collects information and, upon authorised solicitation from the platoon that deployed it, the sensors provide access for a data download. At a later time, a unit from Nation-B (MANET-B) intends to enter into this area and requires access to the observations made by the sensor network to learn of any potential adversarial RF activity.

Nations A and B constitute different CoTs and will not share information openly with one another. The CoTs may restrict or even hide system details, identity credentials, and information metadata from each other. However, the intelligence members within MANETs A and B have agreed to share sensor information; they have formed a CoI. In this case, only select aggregate packages of data are designated (and labeled) for download;

[9] In a data-centric solution, the label is the policy attached to the information object with enough resolution to remove ambiguities; e.g., CANADA SECRET releasable to NORWAY SECRET.

[10] Relay nodes are interface (gateway) nodes between CoTs.

the raw individual sensor readings will not be shared. At the time of MANET-B's request for access, the platoon that comprises MANET-A may or may not be physically co-located with the sensors. An interface node – either from the sensor network itself or from the intelligence members of platoon-A – will be the gateway for this CoI from MANET-A to communicate with the gateway node of MANET-B.

5.4.1 Access Regime

This scenario contains two different access regimes; the classification systems of Nations A and B are not aligned and the information cannot be exchanged under the policies of one hierarchical security domain. An 'intelligence' node from MANET-B must present a form of identity and authorization credential to an authorised node in MANET-A as a member of the 'intelligence' CoI. Then based on policy decisions in MANET-A, the designated aggregate information may be released for transfer to the intelligence members of MANET-B.

5.4.2 Transit CoTs

MANET-A sensor nodes may aggregate a detailed map (e.g., 1 m resolution) of the observations to be used by MANET-B. A less detailed map (e.g., 10 m resolution) is passed on to the coalition headquarter, which had established another CoI with MANET-A. These policies, on details of the aggregation of information in this case, must accompany the data (i.e., maps) themselves and be represented as meta data by an authorised node in MANET-A. In addition, these attached policies should be observed and enforced by MANET-B. Should Nation-B be tasked to transfer a map to the headquarters through a CoI with MANET-B, then MANET-B must prepare a version with less resolution (e.g., 10 m resolution) before passing it to the headquarters.

5.4.3 Authorization to Exchange

The capabilities of the individual MANET-A nodes and sensors cannot be disclosed to other CoTs because Nation-A uses these nodes for intelligence applications. To ensure that only aggregate sensor readings are exchanged, the exchange operation is subject to special authorization. The interface node of MANET-A that connects to the interface node of MANET-B for the exchange must validate the authorization of the aggregating node in MANET-A (its own intelligence peer in the same CoI and CoT) before allowing the information to be passed to the interface node in MANET-B. The aggregating node is the originator of the information that is exchanged; therefore, its authorization for exchange, its CoI membership, should be verified and validated.

5.5 Summary

With this scenario, we have attempted to show the value of establishing a framework for coalition information exchange in MANETs where nodes from different CoTs belong to a common CoI and have a requirement to share data. We described a use case where certain nodes of MANET-A have legitimate requirements to receive information from select nodes of MANET-B. We discussed the problem in the context of the required flexibilities of information exchange in collation operations at the tactical edge. Specifically, in a data-centric security model, the policy is attached to the information by the authorized originator and that same policy is enforced by intermediate relay nodes; whereas in a 'guard model, the guard verifies security labels attached to the information and enforces policies it (the guard) holds. The data-centric model functions independent of an access regime because the policy is mobile with the information; the guard model only works in a single access regime, where the same hierarchical security standards are shared amongst CoTs.

Based on the scenario presented in this section, we propose that the exchange mechanisms between communities are subject to far more flexible authorization arrangements than a simple guard between two 'System High' hierarchical security domains. Exchange of information should:

- Not assume a 'System High' mode of operation, incapable of handling different security hierarchies;
- Be able to maintain the originator's exchange policy through a chain of exchange operations;
- Separate authorization verification of the exchange from the traditional authorization verification of those accessing, reading, or processing the data; and
- Be supported and adapted by the administration entity in the CoT by including policy enforcement as part of its routine procedures.

6.0 SUMMARY AND FUTURE RESEARCH

In this report, we developed three scenarios for wireless coalition tactical networking. We presented a scenario where Nation-B could provide various levels of network connectivity services to allow Nation-A to communicate to the trans-national Forward Operating Base (FOB). We described a scenario where Nation-B could provide different grades of security services to Nation-A. And finally, we provided a scenario where Nations A and B could establish Communities of Interest (CoI) for special roles with appropriate security requirements. We detailed sample use cases offering graded services for various network topologies and interfaces among national networks. The challenges highlighted by these scenarios are being addressed by the design and development of models, methods, and frameworks for cyber security architectures in coalition MANETs, which are expected to be a part of the NRF at the tactical edge. Specifically, design and development is being conducted within the authors' national research programs in support of (at least one use case from) each of these three scenarios.

7.0 REFERENCES

[1] Salmanian, M., Fongen, A., Hunke, S., Brown, J.D., Mason, P.C., Tang, H., Song, R. and Simmelink, D., Provisioning Graded Services for Dynamic Secure Wireless Networks in Coalition Environments, NATO Symposium STO-IST-122/RSY-030 on "Cyber Security Science and Engineering", October 2014.

[2] Fongen, A., Gjellerud, M. and Winjum, E., A Military Mobility Model for MANET Research, in Proceeding of the Parallel and Distributed Computing and Networks (PDCN), 2009.

[3] Bicakci, K. and Tavli, B., Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, Computer Standards & Interfaces Issue 31, pp. 931-941, 2009.

[4] Bentstuen, I., Overview of PCN, Invited presentation from RTG-103 to NATO IST-109/RTG-054 during the meeting in Oslo, October 30, 2013.

[5] Buckman, T., NATO Network Enabled Capability, Feasibility Study, Executive Summary: Version 2.0, Communications and Information Systems Division, NATO Consultation, Command and Control Agency, 2005.

[6] Lies, M., Dahlberg, D., Steinmetz, P., Hallingstad, G. and Calvez, P., The Protected Core Networking (PCN) Interoperability Specification (ISpec), NATO Communications and Information Agency, Technical Report 2013/SPW008905/13, 2013.

[7] Salmanian, M., Minutes of the NATO IST-109/RTG-054 meeting on 'Dynamic Wireless Network Security in Coalition Environments', Oslo, Norway, October 28 – November 1, 2013.

[8] Bell, D.E. and LaPadula, L.J., Secure Computer Systems: Mathematical Foundations, MITRE Corporation, 1973.

[9] Hvinden, Ø. Murdock, A., Rudack, M., Booth, M., Diepstraten, M., Domingo, A., Kuehne, S. and Schenkels, L., Information Exchange Gateway Roadmap. Technical Report Reference document 2666 Draft Version 1.01, NATO C3 Agency, March 2010.

[10] Wrona, K. and Hallingstad, G., Development of high assurance guards for NATO. In Military Communication and Information Systems Conference (MCC), Gdansk, Poland, 2012.

[11] Wrona, K. and Menz, N., Protection Profile for the NATO High Assurance ABAC Guard (HAAG), NATO C3 Agency, Technical Report TR-2012-SPW008418-13-4, 2013.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-IST-109 AC/323(IST-109)TP/618	ISBN 978-92-837-2010-2	PUBLIC RELEASE

5. Originator

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

6. Title

Use Cases for Dynamic Secure Wireless Networking in Coalition Environments

7. Presented at/Sponsored by

This Report documents the findings of Task Group IST-109/RTG-054.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2015
10. Author's/Editor's Address	**11. Pages**
Multiple	36

12. Distribution Statement

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

13. Keywords/Descriptors

Access	Dynamic	Secure
Ad hoc	Gateway	Tactical
Authorization	Intrusion	Threat
Coalition	MANET	Traffic
Community	Mobile	Trust
Connectivity	Monitor	Use Cases
Detection	Network	Wireless
Discover	Scenario	

14. Abstract

Interconnectivity of coalition dynamic wireless networks presents a host of architectural and security challenges, adding to the security challenges faced by individual Nations. This report highlights the challenges of coalition communication interoperability and information sharing at the tactical edge where dynamic wireless networks offer transformative technologies at the dismounted soldier level. In this context, various mission scenarios are presented, offering tiered services for connectivity and for security, as well as identifying Communities of Trust (CoT) with inherent security requirements. These scenarios provide a framework for policy discussions and exploitation of network topologies for tactical deployments and interfaces among national networks. Adhering to the NATO Network-Enabled Capability (NNEC) vision, it is important to ensure that compatible security solutions from national programs will support the constraints of dynamic wireless networks in coalition deployments where they may be interconnected.

NORTH ATLANTIC TREATY ORGANIZATION

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

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

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

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

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

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

CENTRES DE DIFFUSION NATIONAUX

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

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

BULGARIE
Ministry of Defence
Defence Institute "Prof. Zvetan Lazarov"
Blvd "Totleben" 34
1606 Sofia

CANADA
DGSIST
Recherche et développement pour la défense Canada
101 Colonel By Drive, 6 CBS
Ottawa, Ontario K1A 0K2

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

ESPAGNE
SDGTECIN (DGAM)
C/ Arturo Soria 289
Madrid 28033

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

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

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

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

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

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

LUXEMBOURG
Voir Belgique

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

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

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

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

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

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

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

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

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

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

AGENCES DE VENTE

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

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

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

NORTH ATLANTIC TREATY ORGANIZATION

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

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

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

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

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

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

NATIONAL DISTRIBUTION CENTRES

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

BULGARIA
Ministry of Defence
Defence Institute "Prof. Zvetan Lazarov"
Blvd "Totleben" 34
1606 Sofia

CANADA
DSTKIM
Defence Research and Development Canada
101 Colonel By Drive, 6 CBS
Ottawa, Ontario K1A 0K2

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

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

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

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

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

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

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

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

LUXEMBOURG
See Belgium

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

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

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

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

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

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

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

SPAIN
SDGTECIN (DGAM)
C/ Arturo Soria 289
Madrid 28033

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

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

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

SALES AGENCIES

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

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

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

ISBN 978-92-837-2010-2