Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Military Wireless Network Information Operation Scenarios

Mazda Salmanian

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2003-241
December 2003

Canada

Military Wireless Network Information Operation Scenarios

Mazda Salmanian
Defence R&D Canada – Ottawa

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2003-241

December 2003

Abstract

Wireless technology is often an integral part of military scenarios. Military scenarios are narratives that describe situations within which the military may need to operate. Military personnel, including military network operators, use these scenarios to practice their duties in those situations. The scenarios also provide military network designers with a context in which to identify specific products that meet the requirements of the specific situation. This context is especially important for wireless network designers, who must build military mobile ad hoc networks that are interoperable, manageable, and secure.

Wireless networking concepts, such as mobility, network size, and quality of service, are important considerations when designing military ad hoc network information operation scenarios. Until now, the combination of scenario and concepts has produced a wireless architecture that may not be suitable. This was the result of the scenario being fully defined before dealing with the relevant concepts. This report proposes a process whereby scenarios and concepts are evaluated together, iteratively, to progressively produce a wireless network architecture that better supports the military's needs.

This report gives a general overview of wireless networking concepts. Their role in military ad hoc network information operation scenarios is highlighted. Strategic, operational, and tactical scenarios are established for secure mobile ad hoc networking. Concept constraints are discussed for each scenario, as well as potential network vulnerabilities. Finally, the iterative, cyclical approach to network architecture design is introduced, where the concepts not only assist in defining the background assumptions of the design, but also the architecture's suitability for each scenario.

Résumé

Les scénarios militaires ont pour but de fournir une image complète aux opérateurs de réseaux afin de les aider dans l'exercice de leurs fonctions. Du même égard, les scénarios fournies aux architectes de réseaux une plate-forme qui assiste a déterminer la position de certains produits dans une architecture désignée de réseau quelconque. Ceci dit, l'utilisation de scénarios bénéficie aux architectes de réseaux en réduisant d'une façon concrète le temps qui doit être consacre a la création d'un réseau mobile protégé a des fins militaires et aussi y donnant un cachet plus maniable tout en offrant une maintenance plus aisée.

Les concepts de communication pour ce qui a trait aux réseaux sans fil jouent un rôle très important dans l'architecture de scénarios d'opérations d'information afin de créer des réseaux ad hoc a buts militaires. En plus, les concepts appliqués dans une architecture quelconque et le scénario même, sont ensemble impliques dans un cycle itératif ou l'évaluation de l'architecture mène a la modification des concepts qui eux-mêmes sont des critères dans l'évaluation de l'architecture. Cette approche cyclique itérative assure la pertinence des architectures de réseaux ad hoc sans fil dans les scénarios militaires.

Dans ce rapport, un apercu général est donné des concepts de communication des réseaux sans fil et leurs rôles dans la création de scénarios d'opérations d'information en réseau, ad hoc, dans un contexte d'utilisation a buts militaires y sont soulignées. Trois types de scénarios militaires y sont contemplé, stratégique, opérationnel et tactique qui seront créés pour les communications mobiles ad hoc protégés. Les attributs des concepts pour les communications sans fil y sont soulignes pour chaque type de scénario ainsi que leurs vulnérabilités propres. L'approche itérative et cyclique qui a pour but de déterminer l'architecture du réseau base sur les scénarios y est illustrée, ou les concepts ne servent non seulement a assister a la détermination de l'architecture convenant mais aussi ils sont aussi d'aide a évaluer la pertinence de l'architecture dans un scénario donné.

Executive summary

Wireless technology is often an integral part of military scenarios. Military scenarios are narratives that describe situations within which the military may need to operate. Military personnel, including military network operators, use these scenarios to practice their duties in those situations. The scenarios also provide military network designers with a context in which to identify specific products that meet the requirements of the specific situation. This context is especially important for wireless network designers, who must build military mobile ad hoc networks that are interoperable, manageable, and secure.

Wireless networking concepts, such as mobility, network size, and quality of service, are important considerations when designing military ad hoc network information operation scenarios. Until now, the combination of scenario and concepts has produced a wireless architecture that may not be suitable. This was the result of the scenario being fully defined before dealing with the relevant concepts. This report proposes a process whereby scenarios and concepts are evaluated together, iteratively, to progressively produce a wireless network architecture that better supports the military's needs.

This report gives a general overview of wireless networking concepts. Their role in military ad hoc network information operation scenarios is highlighted. Strategic, operational, and tactical scenarios are established for secure mobile ad hoc networking. Concept constraints are discussed for each scenario, as well as potential network vulnerabilities. Finally, the iterative, cyclical approach to network architecture design is introduced, where the concepts not only assist in defining the background assumptions of the design, but also the architecture's suitability for each scenario.

Of the three scenarios presented, the tactical scenario has already been adopted by a group of scientists from three countries in order to provide a framework in which a secure mobile ad hoc network could be developed. Secure mobile ad hoc networking is part of a research collaboration between Canada, the Netherlands, and Sweden. It was formed in order to combine the partner's expertise in Information Operations to find better solutions that will, in turn, directly benefit all partners. One such solution is the architecture of an interoperable, manageable, and secure military mobile ad hoc network based on existing and emerging commercial off-the-shelf (COTS) products, services, and standards.

Salmanian, M. 2003. Military Wireless Network Information Operation Scenarios.
DRDC Ottawa TM 2003-241, Defence R&D Canada - Ottawa.

Sommaire

Les scénarios militaires ont pour but de fournir une image complète aux opérateurs de réseaux afin de les aider dans l'exercice de leurs fonctions. Du même égard, les scénarios fournies aux architectes de réseaux une plate-forme qui assiste a déterminer la position de certains produits dans une architecture désignée de réseau quelconque. Ceci dit, l'utilisation de scénarios bénéficie aux architectes de réseaux en réduisant d'une façon concrète le temps qui doit être consacre a la création d'un réseau mobile protégé a des fins militaires et aussi y donnant un cachet plus maniable tout en offrant une maintenance plus aisée.

Les concepts de communication pour ce qui a trait aux réseaux sans fil jouent un rôle très important dans l'architecture de scénarios d'opérations d'information afin de créer des réseaux ad hoc a buts militaires. En plus, les concepts appliqués dans une architecture quelconque et le scénario même, sont ensemble impliques dans un cycle itératif ou l'évaluation de l'architecture mène a la modification des concepts qui eux-mêmes sont des critères dans l'évaluation de l'architecture. Cette approche cyclique itérative assure la pertinence des architectures de réseaux ad hoc sans fil dans les scénarios militaires.

Dans ce rapport, un apercu général est donné des concepts de communication des réseaux sans fil et leurs rôles dans la création de scénarios d'opérations d'information en réseau, ad hoc, dans un contexte d'utilisation a buts militaires y sont soulignées. Trois types de scénarios militaires y sont contemplé, stratégique, opérationnel et tactique qui seront créés pour les communications mobiles ad hoc protégés. Les attributs des concepts pour les communications sans fil y sont soulignes pour chaque type de scénario ainsi que leurs vulnérabilités propres. L'approche itérative et cyclique qui a pour but de déterminer l'architecture du réseau base sur les scénarios y est illustrée, ou les concepts ne servent non seulement a assister a la détermination de l'architecture convenant mais aussi ils sont aussi d'aide a évaluer la pertinence de l'architecture dans un scénario donné.

Les scientifiques qui participent dans le programme de collaboration tri-national ont adopte le scénario tactique pour effectuer l'évaluation de l'architecture de réseau mobile sécurise ad hoc. Ce dernier étant donc le sujet majeur faisant parti du projet de collaboration avec les Pays-bas et la Suède dans l'espoir d'utiliser l'expertise tri-nationale au sujet des opérations d'information afin d'en arriver à des solutions a hautes impactes, qui effectivement seront directement de bénéfice aux nations impliquées. Une de ces solutions est l'architecture d'un réseau ad hoc militaire mobile sécurise qui est interoperationnel et a gestion simple base sur des produits, services et standards commerciaux sur étagère existants qui sont à la fine pointe de la technologie.

Salmanian, M. 2003. Military Wireless Network Information Operation Scenarios. DRDC Ottawa TM 2003-241, R & D pour la défense Canada - Ottawa.

Table of contents

List of figures

List of tables

Acknowledgements

Many sincere thanks to Mr. Kellett, Ms. Genik, Mr. Montreuil, and Dr. McIntyre for their comments and suggestions on the ideas presented in this report.

1. Introduction

Network centric warfare is mostly associated with wireless networks. The Canadian Forces are interested in it because they must protect mobile military networks from intrusions and attacks. Increasingly, military operations require wireless network connectivity for the flow of command and control information from the central command to the deployed field units. Since the military is a highly mobile entity, it requires networks that can be set up and configured in an ad hoc fashion. Moreover, since security and mobility are critical factors to the military, securing mobile ad hoc networks is an area worthy of focus.

As such, wireless technology is often an integral part of military scenarios. Military scenarios are narratives that describe situations within which the military may need to operate. Military personnel, including military network operators, use these scenarios to practice their duties in those situations. The scenarios also provide military network designers with a context in which to identify specific products that meet the requirements of the specific situation. This context is especially important for wireless network designers, who must build military mobile ad hoc networks that are interoperable, manageable, and secure.

Network architectures for operational scenarios must be evaluated against design criteria to ensure they are suitable for the mission or the purpose for which they are designed. This is especially important for military scenarios that are derived around network architectures based on existing and emerging commercial off-the-shelf (COTS) products, services, and standards. Suitability of commercial products, services, and standards must be evaluated for military purposes. The evaluation criteria are the concepts that form the basis on which the architecture was designed. In other words, the concepts not only assist in the background assumptions of the design of an architecture, but are also used for the evaluation of the architecture's suitability for a scenario. The outcome is a set of concepts with which one can design and evaluate the make-up of an architecture for a scenario. In turn, modifications of the concepts result in fine-tuning a suitable architecture for the scenario.

Wireless networking concepts, such as mobility, network size, and quality of service, are important considerations when designing military ad hoc network information operation scenarios. Until now, the combination of scenario and concepts has produced a wireless architecture that may not be suitable. This was the result of the scenario being fully defined before dealing with the relevant concepts. This report proposes a process whereby scenarios and concepts are evaluated together, iteratively, to progressively produce a wireless network architecture that better supports the military's needs.

Following this introduction, a general overview of wireless communication networking concepts is provided in Section 2, where the concepts' roles in the make-up of military, ad hoc, network information operation scenarios are highlighted. In Section 3, three types of military scenarios are established for secure mobile ad hoc networking. The attributes of wireless networking concepts are highlighted for each scenario type and the network vulnerabilities are discussed for each scenario. The iterative, cyclical approach to network architecture design within the confines of a scenario is illustrated in Section 4. The conclusions and recommendations for future activities are provided in Section 5.

2. Concepts for Consideration

Wireless communications networking concepts, such as mobility, network size, and quality of service, are integral factors in limiting the scope of a networking demonstration for a particular scenario. The concepts form the assumptions for network design, and the connection integrity in a network depends on these concepts and their respective parameters. Military scenarios that involve wireless networks provide for an environment that stretches the integrity of network connectivity. Thus, before the scenario exercise, these networking concepts must be analyzed and evaluated during the scenario design phase. Mobility, network size, and quality of service are a few of these concepts. A secure mobile ad hoc network must also be designed to be robust, have adaptive routing, and manage mobility with control protocols. These concepts and their corresponding relation to an applied military scenario are explained in further detail in this section.

2.1 Mobility

Mobility is a basic necessity in military operations. A military team is given a mission that may start at one coordinate and end at another. While moving, the forces require connectivity for voice, data, and perhaps video. Therefore, mobility is a basic assumption in military network design. The network should be autonomous, capable of self-forming, and self-maintaining so that it can be deployed anywhere without the need for infrastructure. Thus, the network itself should be mobile and “ad hoc”. The nodes within a military network are also mobile. These nodes consist of soldiers with PDAs, armoured vehicles, tanks, unmanned aerial vehicles (UAVs), and even helicopters and fighter jets.

An important parameter to consider for mobility is speed. Doppler effects, fading, and shadowing are among the impairments of the received signal that are directly related to mobility and the speed of a node. A wireless receiver in a mobile ad hoc network should be designed to adapt to the changes in conditions of the radio channel being used. Nodes may be stationary sensors, as slow as soldiers on foot, or as fast as ground vehicles, helicopters, UAVs, or supersonic fighter jets.

2.2 Network size

Network size may be determined as a measure of the number of nodes in a network, the coverage (range) of the network, or both. For the purpose of this document, range is defined as the radius of omni directional coverage, or the maximum distance that the signal may travel in one dimension with reasonable reception. Although used intermittently, range and coverage are not the same. Directional antennas provide poor coverage with very short range in all directions except for those designated by design. Reasonable reception means sufficient signal strength for the receiver to obtain an acceptable error rate. Both range and coverage are

specified as averaged measurements of sufficient signal strength in different environments and terrains.

A large number of nodes may be densely populated in a command centre, or may be sparsely distributed in the mountains. In both cases, the size of the network is an important design consideration. It affects the integrity of network connectivity not only through capacity impairments due to high traffic, but also through distance (range) effects on signal strength. If the network is too densely populated with active nodes, the generated traffic limits network availability by exceeding the network's capacity. If the network is too sparse, parts of the network may be left without radio coverage due to insufficient signal strength.

The number of nodes and their coverage play an important role in determining and narrowing the choices of wireless standards and their respective hardware terminals in a scenario. For example, cellular systems operate in urban environments, have a moderate capacity for low data-rate (<10Kbps) users, and with tall antennas offer a large coverage area (2 Km radius). On the other hand, Wireless LAN technology (IEEE 802.11) can be deployed anywhere, has high capacity (5Mbps to 20Mbps) for up to 10 users, and can provide coverage for up to a 30-metre radius. For longer distances, either directional antennas have to be used to direct the signal to the receiver, or other technologies should be considered.

Free Space Optical (FSO) devices can provide point-to-point connectivity between two clusters of nodes, up to 2 Km apart, with a high capacity data-rate (up to 2.5 Gbps). Wireless devices are power limited and this limitation introduces a compromise between the range of coverage and available bandwidth. The further a transmitter is required to serve a receiver the more its signal power must be increased and adjusted for that distance. At the same time, transmitters of high capacity communication links must distribute their signal power over a large number of bits per unit time. Given limited power, capacity and range can only go so far. Systems are generally optimized for a range of coverage and capacity with some adaptability via power control. The capacity is in turn optimized to "number of nodes" for specific multiple access schemes.

Multiple users may gain access to a wireless channel through various technology dependent techniques, such as having a time-slot reservation (TDMA), code assignment (CDMA), frequency reservation (FDMA), or a sophisticated mixture of all three (OFDM). There are also protocols where the users do not transmit when others are using the channel: Carrier Sense Multiple Access (CSMA). These techniques and protocols also limit the type of hardware terminals used in a scenario. Not all are implemented by a manufacturer on the same device (PDA, laptops, phones) and the choices must be carefully analyzed for use in a scenario. Thus, it is important to look at network size, and its parameters, range and capacity, as a concept whose analysis provides much input to designing a network for a military scenario.

2.3 Quality of Service

Networks are not just about connectivity. The Quality of Service (QoS) provided by a network is important and can be measured using several parameters. As shown in Figure 1, QoS parameters for wireless networks include delay, capacity, range, and the bit error rate (BER). It is essential that a service provided through the wireless medium has a low latency and arrives reliably at its destination. The tolerances for each of the QoS parameters needed to assure the quality of the service vary depending on the application. For example, tolerance for delay is on the order of 10^{-3} seconds for real-time voice traffic [1]. The majority of the delay comes from the wireless device's processing power and available bandwidth. Propagation delay in this application tends to be minimal because radio waves travel at the speed of light. Capacity poses a problem when too many users are competing for limited resources or high-bandwidth applications are utilized on low-bandwidth connections. Range becomes important in the example above when the wireless voice user reaches the edge of the radius of coverage. Generally, delay is measured in seconds, capacity in bits per second and range/coverage in metres. The bit error rate (BER) is a measure of noise or interference in the communications channel. As we will see in the next section, it can also be used as a measure of the integrity of the connection. The BER tolerance for data and voice are on the order of 10^{-6} and 10^{-3} respectively [1]. It is understood that communication services in a military context should be held to even higher standards than those mentioned here. Just like range, capacity, delay, and BER, security should also be considered a measurement of QoS, as it has been in a previous study [2].

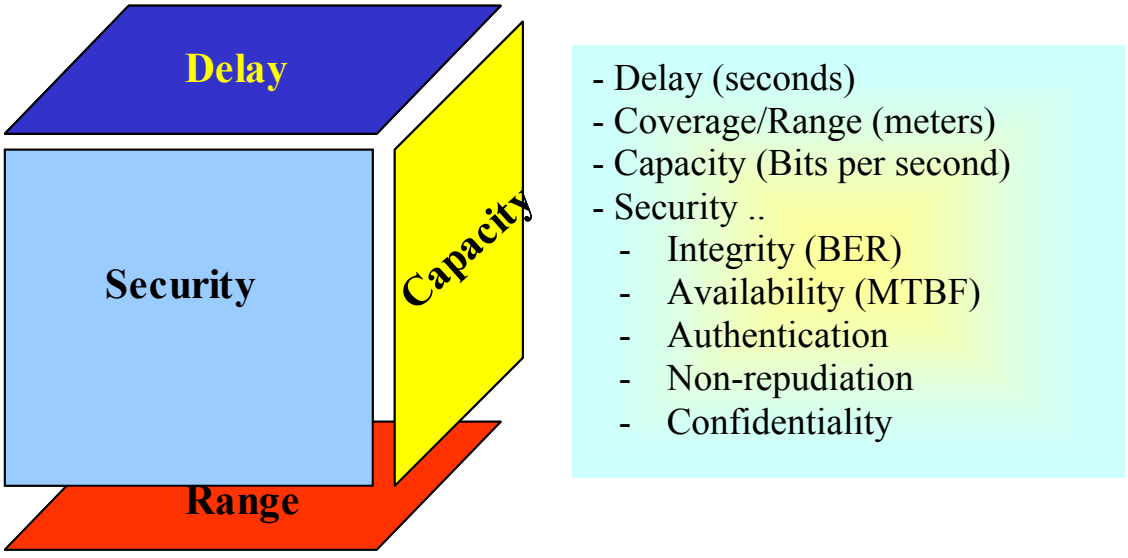

Figure 1. *Security as a QoS parameter*

2.4 Security

Network security is characterized by the following attributes as shown in Figure 1: authentication, non-repudiation, confidentiality, data integrity, and availability. As mentioned in the previous section, integrity may be measured in terms of errors that are introduced into the data. Error correction and error checking methods can also highlight if the data has been tampered with or spoofed. Availability is often measured in units of time. Mean Time Between Failure (MTBF) of a network is a statistical indication of how long the network was disconnected and inaccessible to the users.

Unfortunately, unlike integrity and availability, there are no clear, standardized ways to measure the other security attributes: authentication, non-repudiation, and confidentiality. Scientifically, the methods and algorithms applied to these concepts are only as good as the last person who attempted to break them. For example, confidentiality can be mitigated with encryption. The quality of cryptographic algorithms is statistically measured as a function of the time: how long would it take someone to break them? More often than it is publicized, encrypted data is deciphered by ingenious techniques that are unrelated to the statistical approaches used to determine the encryption algorithm's quality and which generally take a fraction of the time predicted.

Authentication is the verification of the identity of users in a communication network. It is a key network security concept because it is the first step towards the prevention of unauthorized access to network resources and sensitive information. As opposed to commercial networks where authentication is secondary to system discovery and routing, this concept is primary to military environments. As an added layer of protection, mutual authentication verifies the network to the user as well as the user to the network. This guards against a user giving his or her credentials to network that only appears legitimate. Authentication requires key management for the secure creation and distribution of the cipher keys that allow the users access to the network.

Non-repudiation provides proof that a particular user performed a particular action at a particular time. It is used to record the origin and date of information so that the communicated facts cannot be disputed at a later date. Non-repudiation is essential in military environments where national security is at stake. Moreover, the enabling technologies for this concept may be used as proof in courts for judicial law enforcement.

Security may be applied at different layers of a wireless network. At the physical layer, certain techniques such as Time division (TDMA), code division (CDMA), frequency division (FDMA), or a sophisticated mixture of all three - orthogonal frequency division (OFDM) multiplexing, add a certain amount of cipher to the wireless network. Link layer algorithms like Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) provide protection against eavesdroppers. IPSec, Layer-2 Tunneling Protocol (L2TP), and secure routing algorithms for Mobile Ad hoc NETworks (MANET) [3] are all candidates for network layer security. Transport Layer Security (TLS) and Secure Socket Layer (SSL) are generally used for security at the transport layer. The remaining layers are protected by application level security such as Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).

Given the nature of military information in a coalition environment, data should be transferred within a common security architecture to allow secure, seamless communication across different wired and wireless network technologies, devices, and applications. COTS products can make this commonality possible so that the networks of different coalition partners can interoperate with one another. The additional overhead on network bandwidth and device resources, such as processing power, imposed by security requirements should be balanced against the applications and services of the network for QoS management. In a wireless context, QoS must include detection and protection against unauthorized access and the protection of authorized access.

2.5 Stealth

Control of the emitted electro-magnetic energy from wireless devices is important to the military in order to avoid detection. Emission control on wireless devices is not a trivial task because emissions are used to connect devices. However, there may be scenarios under which a device may take a stealth role in the network and become receive-only. In such modes, authentication and key management become challenging.

There are no known stealth technologies available for wireless devices. TEMPEST is the only publicly known, documented standard for stealth operations on wired networks. TEMPEST stands for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions and includes technical security countermeasures, standards, and instrumentation, which prevent (or minimize) the exploitation of security vulnerabilities by technical means. TEMPEST protects against technical surveillance or eavesdropping of equipment emanations, which means that it would be problematic to apply it as a standard to a device that is design for such emissions.

2.6 Robustness

A military wireless network should provide sufficient connectivity under harsh conditions for command and control communications (C^3) services. Network nodes may be destroyed or compromised by the enemy. Jamming techniques may reduce connectivity and hinder QoS. A distributed network topology, as opposed to a centralized one, increases the availability of the network by reducing the probability of having one point of failure for the entire network. Distributed ad hoc networks, on the other hand, are difficult to manage. Routing and security implications such as key management are quite challenging in these networks.

A network should also be able to adapt its Quality of Service (QoS) to the demands of the military scenario. Commercial networks are designed to track the harsh conditions of the wireless medium and to provide a steady predictable QoS over time. However, it is crucial for a military network to also adapt to the demands of the situation. Functions such as point-to-point, multicast, and broadcast are critical to military scenarios and must remain operational. The integrity of the connection with these functions may come at a cost to QoS. A military network should be able to dynamically compromise certain attributes in favour of others in

order to maintain the integrity of the connection. For example, it is common in short-lived ad hoc networks under severe conditions to sacrifice certain security attributes in order to gain the benefit of higher bandwidth and lower delay.

2.7 Network Location

A secure mobile ad hoc network may be placed on either hostile or friendly ground to provide connectivity for strategic, operational, or tactical purposes. It may be on dry land or a maritime environment. On dry land, building density may be classified as downtown, urban, or suburban on terrain that can be either flat or mountainous. In maritime environments, the sea conditions and the weather should be taken into considerations for network design. These concepts directly affect the wireless channel conditions. Consideration of the concepts and parameters shown in Figure 2 allows the network architect to not only account for connectivity of the network, but also assess its security risk.

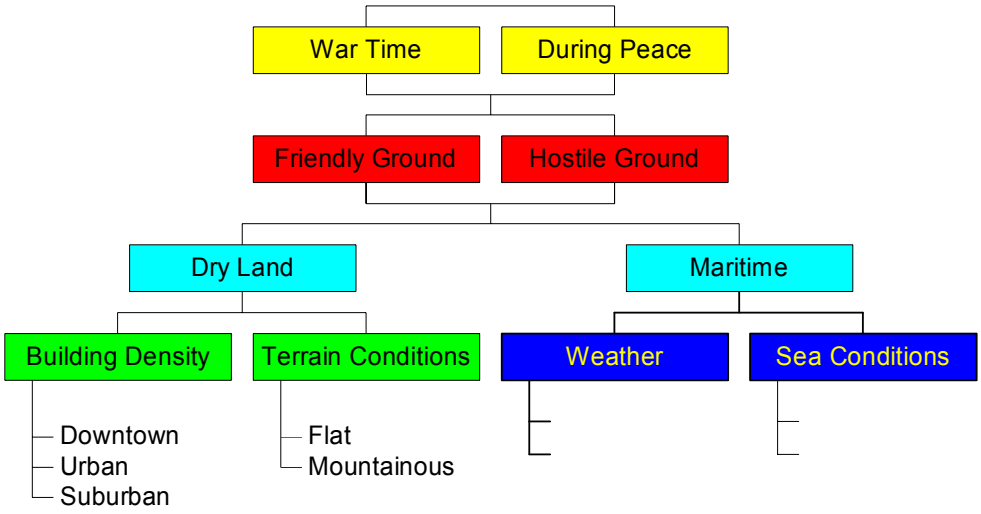

Figure 2. Network Locations' Criteria

In [4], cyber security risk was logically defined as a function of threat, vulnerability, and impact.

$$Cyber\ Security\ Risk = f\left\{\begin{array}{c} External\ Threats \\ Internal\ Vulnerabilities \\ Potential\ Impacts \end{array}\right\}$$

It is interesting that security risk is described as a function of the external parameters to the network (threats), internal parameters of the network (vulnerability), and the potential aftermath of the damage to the network (impact). The deployed location of a wireless network directly affects its internal and external vulnerabilities and threats. Network architects should consider these in their design and assess the potential risks to the network.

2.8 Ad Hoc Architecture

A military wireless network should have a distributed topology. Non-centralized architectures eliminate single points of failure. The network should also be self-organizing and dynamically hierarchical in order to function autonomously with little or no preparation time for set up. Self-organization methods consist of routing algorithms that adapt to the dynamic changes and movements of the network nodes. However, in fast-changing networks, updates to the routing tables may leave little or no bandwidth for users to utilize the services of the network.

The dynamic, hierarchical aspects of ad hoc networking avoid the routing table problems by enabling group-wise peer management. This in turn allows the nodes to save power and allows the (sub)networks to manage their bandwidth better. For example, there is no reason for foot soldiers near a tank to be connected to a base-station on an Unmanned Aerial Vehicle (UAV) for network access. The tank's battery power and carrying power is far greater than that of the soldiers or the UAV. Instead, the UAV can provide point-to-point connectivity to the tank, and the tank can act as the central distributor to the soldiers. The network size, however, may dictate certain hierarchies that may be required for the management of these pseudo peer-to-peer networks, especially when the hierarchical military command is considered. Pure peer-to-peer or pseudo peer-to-peer topologies require robust routing protocols. The security implications, such as key management, are even more challenging to implement and manage in these types of topologies.

2.9 Routing Protocols

Wireless military ad hoc networks require routing protocols that can dynamically adapt to the topology and hierarchical changes of the network nodes. Much of the research in this area is documented and criticized in IETF's MANET Working Group [3]. Many routing algorithms are adapted from wired networks for the purposes of wireless ad hoc networking. However, the most interesting concept, which is unique to this field, is multi-hop routing capability.

This concept was developed for nodes or servers that have little or no access to the network. In such cases, access is made possible via other nodes in the vicinity. There are cases where the lack of signal coverage dictates the forwarding of packets through several nodes. This multi-hop routing requires local routing table maintenance to include routing to all the nodes within a node's coverage area, and the sharing of updates periodically with them. The frequency of updates must match the node's coverage and environment, taking into consideration mobility and signal impairments. The method of updates, whether it is by

broadcast or request, must match the network size and the intended QoS of the network. The overhead of the system is a compromise between channel resources and the routing protocol's efficiency.

2.10 Traffic Type

Voice, data, and video are the types of traffic most often found on today's networks. Each traffic type has distinguishing factors. Real-time traffic, like voice and video, is delay sensitive and error tolerant within statistical limits. For example, the human ear's BER tolerance for voice communications is on the order of 10^{-3} [1]. Traditionally, real-time traffic transmission only used circuit-switched networks. A circuit would be set up and dedicated to one communication, which would be terminated upon completion. This technique does not use resources efficiently because it requires large amounts of bandwidth to be dedicated for 100% of the communication session, while the actual activity is on the order of 40%.

On the other hand, data, which is traditionally carried on packet-switched networks, is less delay sensitive and much more error sensitive. For example, the integrity of a short classified message carrying target GPS locations is of utmost importance to a network architect. The BER tolerance of packet-switched data is on the order 10^{-6} [1]. More advanced networks, like third generation cellular, take advantage of the low activity factor of data applications to dynamically perform radio resource management with the remaining bandwidth.

In fact, modelling the statistical characteristics of data sources for modelling and simulation tools has pushed the need to classify packet generation behaviours. Capacity planning on the network requires statistical traffic modeling. For example, assuming the traditional circuit-switched telephony Erlang models - of Poisson distributed connection arrivals based on human behaviour - one may plan for other parameters of interest in network traffic modeling such as connection duration and, ultimately, network capacity.

2.11 Applications

The bearer (application) traffic supported on the network dictates the types of devices that need to be used in the network. For example, if voice were the only service needed for a mission, a laptop capable of running NetMeeting with full video would be excessive. Support of multimedia traffic requires high bandwidth channels and high processing power devices. Traffic types, as shown in Table 1, may be voice, video, and data with sub-types varied by speed and other QoS parameters. For example, the control information for a UAV camera would be very low bandwidth, especially in comparison to the bandwidth required to transmit the UAV video stream.

The type of application on a network dictates the bandwidth of connectivity that is required in the network architecture. Applications such as situational awareness within a group may require low bandwidth connections, or applications such as reconnaissance video may require

high-speed connections. A particular scenario may only need connections within a group, or it may need Internet and PSTN (Public Switched Telephone Network) access to a core network.

As mentioned in the previous sections, dynamic adaptability in military wireless ad hoc networks is very important; and this includes traffic management. The application type and the grade of connectivity may have to be prioritized to allow for QoS degradation under severe conditions. For example, collaborative planning tools may allow multiple attendees at various locations to share multimedia traffic. Clearly, if this were an important application starting on a connection with limited bandwidth, certain QoS attributes must change dynamically in order for the service to remain useful. This might mean blocking all low priority (Table 1) traffic in order to make the required bandwidth available for high priority data.

Table 1. *Traffic Types*

APPLICATION	**SPEED**	ENCRYPTION	**PRIORITY**
ALARMS	Low	Needed	1
UAV CONTROL	Low	Needed	1
COMMAND VOICE	Low	Needed	1
PLATFORM SENSOR CONTROL: POSITION, SPEED, DIRECTION	Low	Needed	2
VIDEO, IR VIDEO	High	Not needed	1
COLLABORATIVE PLANNING	High	Needed	1

2.12 Evaluation Criteria

Like other networks, secure mobile ad hoc networks should be evaluated using a list of criteria. Commercial networks are generally classified based on cost and the QoS parameters presented in the previous sections: capacity (number of connections or active users), error rate, outage rate (probability of blocking), etc. In addition to these, military wireless networks should also be rated on (currently) non-quantifiable vulnerabilities such as performance under jamming, probability of physical damage, and the security attributes presented in Section 2.4: authentication, non-repudiation, and confidentiality.

Networks should be established and tested based on military scenarios so that they can be rated and "tagged" as being available tools under those conditions. The military is usually called to aid in situations where there is little time for preparations. The military maintains its

readiness with its physical assets and machinery; and networks should be treated as assets [5], be tested in war-games, and maintained as deployable-ready.

3. Military MANET Scenarios

Military scenarios are classified by their geographical coverage and the vastness of the mission. They are presented, in descending order of size, as strategic, operational, and tactical scenarios. The Canadian Forces and the Department of National Defence have 11 Force Planning Scenarios [6]. Almost none of them involve technology or its related concepts as tools that will evolve with the scenarios. Just recently, an addendum to Scenario 10, Defence of North America, was published to include "a cyber attack component"[7], but it lacked any technical aspect or conceptual references. The intent of this section is to provide scenario examples that are complementary to those presented in [6]. They are complementary in the sense that they involve technology in the scenario planning phase.

The wireless networking concepts that were presented in the previous section play important roles in the creation of these scenarios. In this section, the context (storyline) of the scenarios is presented and the attributes of wireless networking concepts are highlighted for each scenario type, followed by a short discussion on network vulnerabilities. The strategic scenario is very similar to the cyber attack addendum of Force Planning Scenario 10, but its emphasis is on recovery. The operational scenario is also similar to the Force Planning Scenario 10, but its emphasis is on the required technologies that enable a cross-border ISR mission. The tactical scenario is targeted and explained further because of its immediate fit in applying secure, mobile, ad hoc networking. It is very similar to the Force Planning Scenarios 6 and 11. In Section 4, an iterative, cyclical approach to network architecture design within the confines of a scenario is illustrated in order to highlight the importance of combining the technology with the military scenario's story. This process also encourages researchers to take heed of the technical needs of the Canadian Forces in such scenarios.

3.1 Strategic Scenario

This scenario describes a soft attack against a national or international information infrastructure. The goal is to recover from a coordinated national level Distributed Denial of Service (DDOS) attack on Transnational Defence Headquarter (TNDHQ) servers.

The recovery from such an attack requires a communications network that is not connected to the public network (i.e. the Internet) where the attack started. Under such an attack, a secure mobile ad hoc network offers sufficient connectivity, quick setup, and reliable links during the recovery period. This scenario is similar to the cyber attack addendum to the Force Planning Scenario 10, but its emphasis is on the recovery. As shown in Figure 3, the backbone of the WAN must be replaced with satellite links for individual key national headquarter locations. Every location that is (pre)-identified as critical becomes a node on the WAN, and that location itself becomes an ad hoc LAN.

Such networks demand very low scale mobility (pedestrian). The network size consists of scattered single buildings that are inter-connected via satellite. Each has approximately 10 floors and 10 nodes per floor (WLAN). The QoS parameters should be configured to provide

high bandwidth for interactive voice and data exchange. The security level needs to be top secret because national security is at risk. Stealth operations are not required. There is little or no threat of signals being jammed because the network is located in friendly territory, during peacetime, and in downtown environments. The network architecture consists of Access Points (AP) on each floor that connect and route to APs on other floors. The routing protocols are centralized for each floor's wireless nodes, with token passing between APs of different floors. The supported traffic types are voice and data. Video signals for a network of such a large size may diminish QoS especially on the satellite communication links. The primary applications are interactive voice and data exchange and there is no connection to the public network.

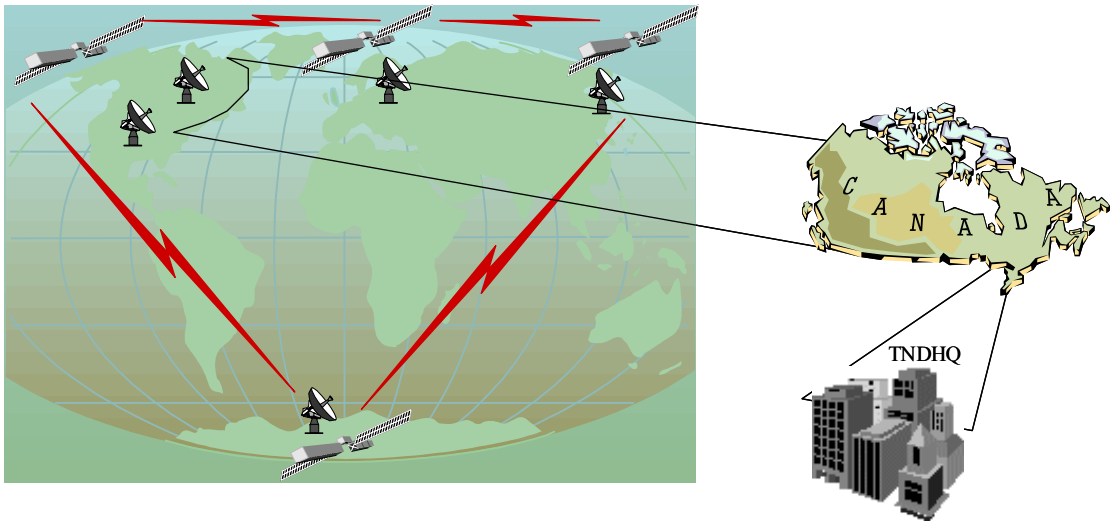

Figure 3. Strategic Theatre

3.2 Operational Scenario

This scenario describes a coordinated physical terrorist attack that uses a cyber attack for diversion. The goal is to identify a suspected ship with a biological weapon cargo aboard.

An unknown commercial ship is suspected of carrying biological weapons and is heading towards the North American continent. The warhead / missile can be armed remotely when it is within range. Intranet cyber attacks have impaired detection of the ship and its cargo.

The DDOS attack on the US and Canadian Coast Guard's radar systems suggests the possibility of a physical attack on the coast. In such a case, re-establishing communication (esp. data) links quickly, and launching a more detailed Intelligence Surveillance & Reconnaissance (ISR) mission to look for suspected intruders could prevent widespread loss of lives and properties. A secure mobile ad hoc network offers sufficient connectivity, quick

setup, and reliable links to replace the affected infrastructure, and to proactively deal with the threat. As illustrated in Figure 4, this scenario is similar to the Force Planning Scenario 10, but its emphasis is on the technologies required for the cross-border ISR mission.

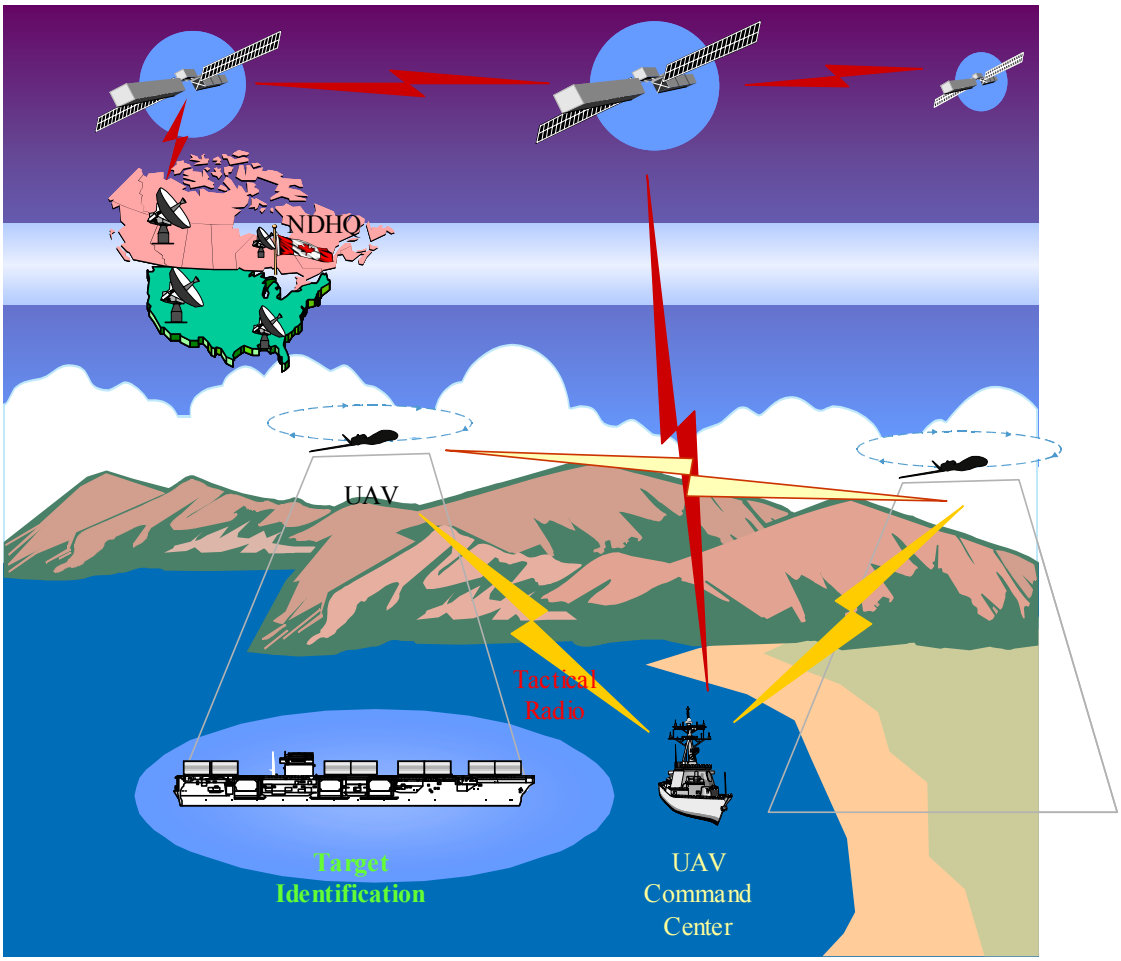

Figure 4. Operational Theatre

The mission requires 24 hour a day surveillance of the coast within 50Km by unoccupied marine and aerial vehicles (UXVs) armed with sensors for ship identification and for missile-arming signal detection and jamming. The surveillance areas served by the UXVs overlap, and each has an autonomous command and control center with secure links to/from the UAVs and the TNDHQ. The continent's critical infrastructure and this ad hoc network are isolated from the public network.

This network requires moderate scale mobility because of the UXVs. The network size consists of approximately 50 nodes across the eastern seaboard, including UXVs and their command and control centers. The expected QoS is to have high bandwidth for interactive video and data exchange. The security level needs to be top secret because the continent's critical infrastructure and security are at risk. Stealth operations are not required; however, there may be a signal jamming threat. Although the network locations are located in friendly territory, this is a suspected terrorist attack with sophisticated technology. The network architecture consists of 12 Marine and aerial UXVs. All are individually controlled & monitored and the coverage of control centers overlap for signalling and handoff. The routing protocol is peer-to-peer for UXV control stations (CS). Inter-CSs' connectivity is through dedicated optical fibre and SATCOM links. Support for multimedia traffic is required, especially streaming video. The primary application is streaming video and data exchange from the UXVs to the CSs, where the information is processed. The UXVs and the CSs have access to NDHQ via satellite communications and there is no connection to the public network.

3.3 Tactical Scenario

This scenario describes a reconnaissance mission requiring special communication tools. The goal is to identify and secure a suspected biological weapons chemical factory for disarmament by United Nations (UN) weapons inspectors.

Tactical scenarios are smaller than strategic and operational scenarios and are extremely relevant for the application of secure mobile ad hoc networks (S-MANETs). This tactical scenario is highlighted and explained in detail because secure, mobile, ad hoc networking is relevant and immediately applicable to this scenario. The scenario includes land, air, and marine forces operating at a multi-national coalition MAN/LAN level. Illustrated in Figure 4, this scenario is similar to the Force Planning Scenarios 6 and 11. This scenario allows a communication network architecture to be designed that provides a tactical team with sufficient connectivity to carry out a short mission.

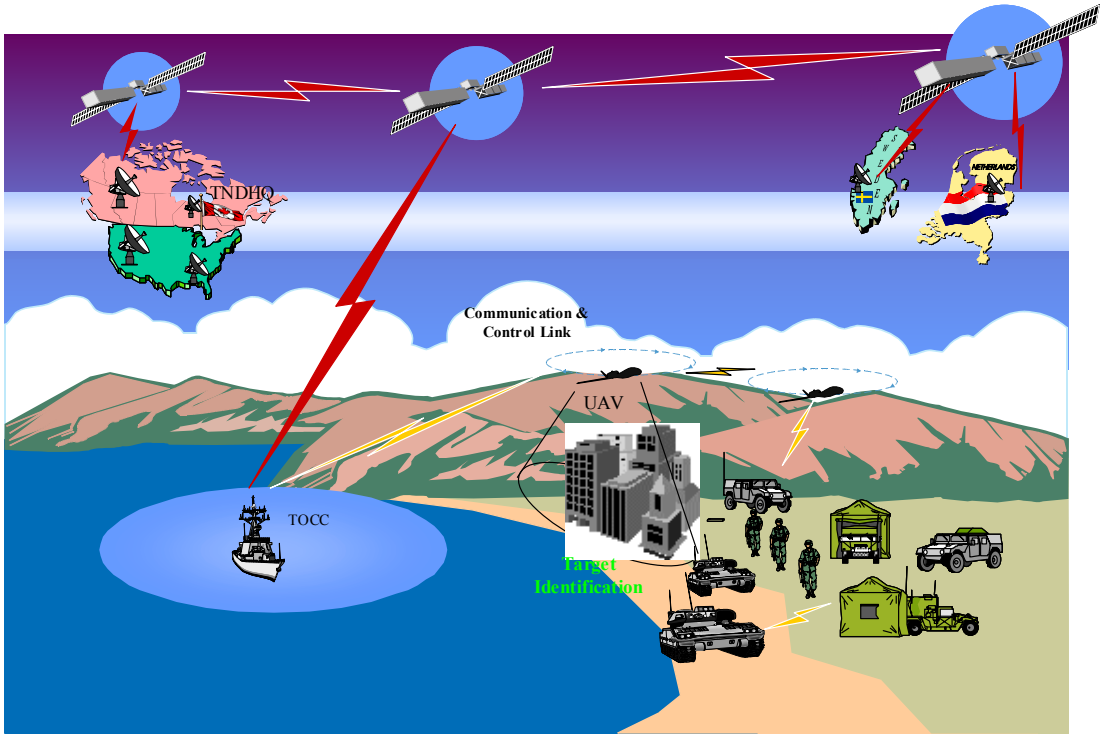

Figure 5. *Tactical Theatre*

The scenario consists of an Intelligence Surveillance & Reconnaissance (ISR) mission to identify and inspect suspected biochemical manufacturing facilities. The scenario also incorporates the post-ISR ad hoc communication that will be required to maintain the security of the manufacturing area. The participating forces and platforms are

- Transnational Operational Command Centre (TOCC) aboard a ship with links back to national strategic command centers and to the Transnational Defence Headquarters (TNDHQ),
- UAVs equipped to conduct wide-area surveillance,
  - <1500 ft altitude / 2 hrs endurance for reconnaissance,
  - <15000 ft altitude / 24 hrs endurance for communications access point,
- Tanks and Armoured Personnel Vehicles (APVs), and
- Ground troops for reconnaissance and control of suspected sites.

The required network connection types include troop-troop, troop-APV, APV-TOCC, UAV-TOC, UAV-APV, and others as shown in Figure 6.

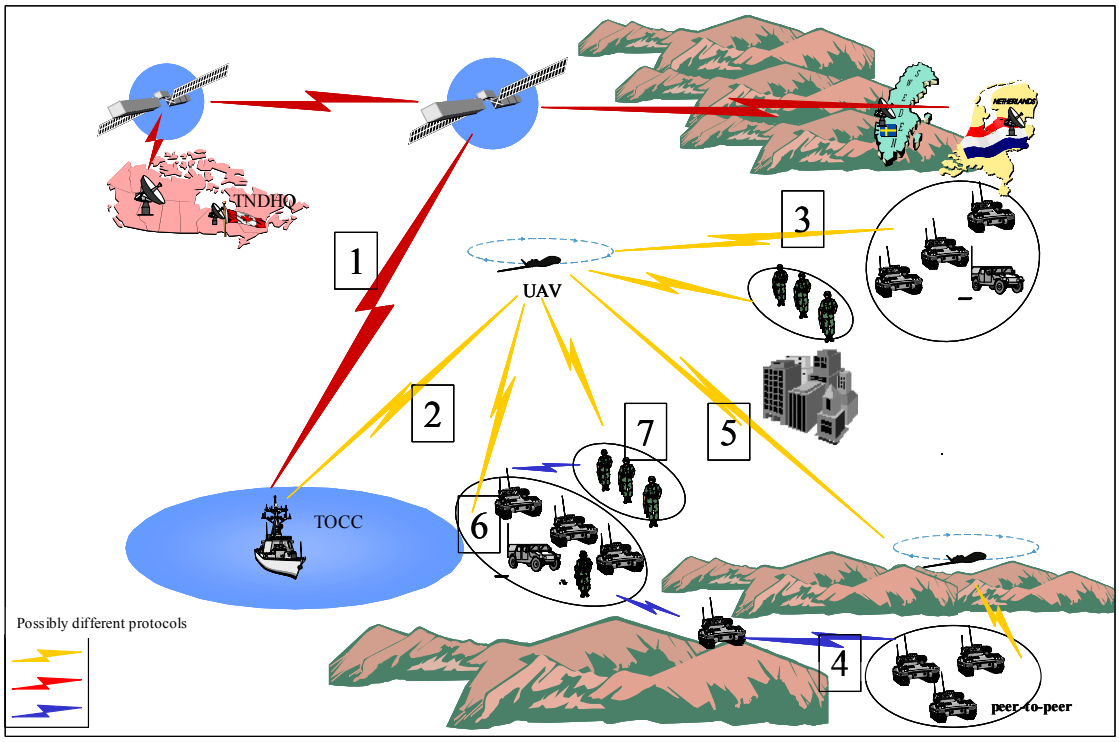

Figure 6. Network Associations

The applications that require security are primarily:

- Collaborative planning,
- Data transmission,
- UAV control,
- Situation awareness,
- Battlefield managements systems, and
- Messaging.

The scenario is a tactical peacekeeping mission undertaken by a coalition of forces from Canada, the Netherlands, and Sweden. The coalition peacekeeping forces are called to surround the building and control the area until the UN Weapons Inspectors arrive and complete their disarmaments. In the first phase of the mission, ISR, an army-controlled UAV equipped with an infrared camera, gas sensors, and wireless communication links is remotely operated to obtain surveillance information from the suspected factory at night. The

information is relayed by secure link to the TOCC where an executive officer verifies the target. The information is then processed and sent to the TNDHQ via a secure satellite link.

In the second phase of the mission, securing the theatre, the ground troops, including tanks and APVs, move in and secure the identified target. At least one (army/navy-controlled) UAV continues to perform “lookout tasks” and acts as a communication relay between the theatre and the ship. The tanks/APVs use peer-to-peer communication. One tank secures the area between the two mountains and provides multi-hop routing from the theatre to the troops on the other side of the mountain. Some tanks/APVs and soldiers may have dedicated satellite links to connect directly to the TNDHQ. The soldiers maintain site security and keep the public away from the factory. They are equipped with secure PDAs that, based on solicited messaging, reply with their location, status, and meta information (type of artillery, rank, etc.). This system links to a situational awareness picture accessible to all PDAs. If the soldier is within range of a tank, then the tank acts as the relay point within the architectural hierarchy (saving battery power, and allowing for the cheapest possible signalling route). Otherwise, the soldier relays through the UAV. A back-up HF radio link provides diversity for the connectivity of the (low bandwidth) voice network.

4. Iterative Evaluation Process

To design a wireless network, a network architect must consider the wireless networking concepts presented in Section 2. To establish a scenario that involves wireless networking, a military network operator must also consider these concepts. However, it is unusual to find network operators who are also network architects and therefore are equipped to consider these concepts fully. Furthermore, the scenarios are fully developed before the wireless networking concepts are applied, as shown in Figure 7. This serial application of military and technical input produces networks that are sub-optimal for the needs of the scenario. The intent of this section is to highlight the need and importance of combining the technology with the story behind a military scenario, concurrently. This joint process not only enables a military scenario to become more effective, but also encourages researchers to note the technical needs of the Canadian Forces in such scenarios.

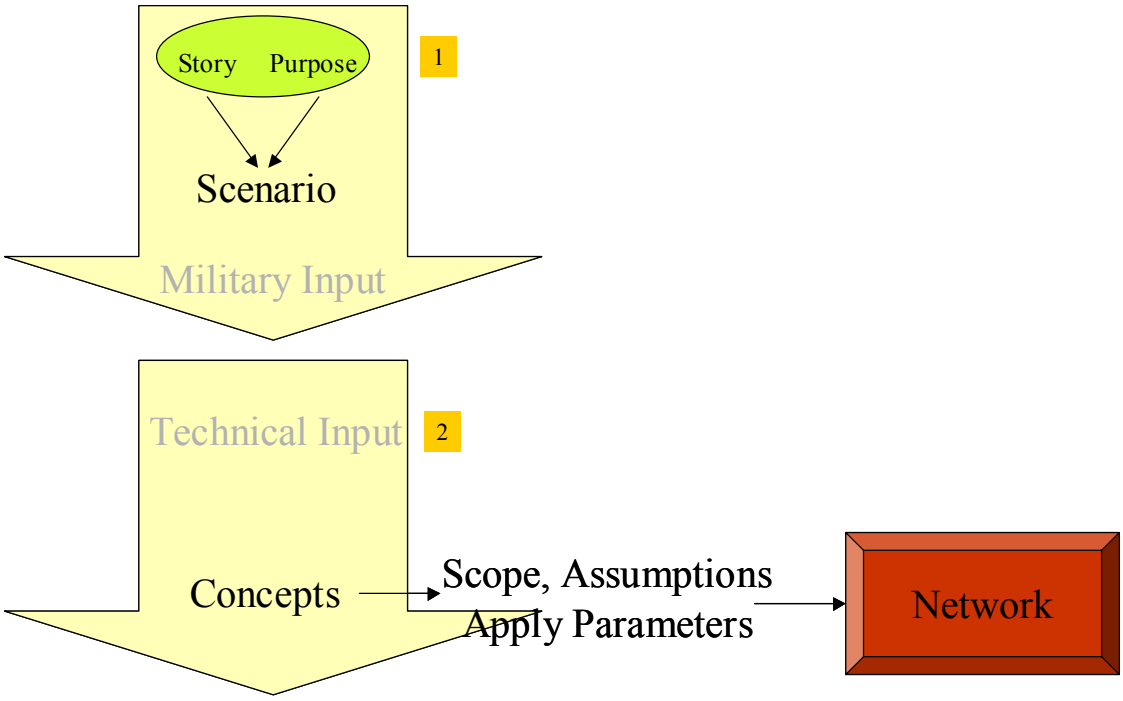

Figure 7. Scenario Creation

An architect's wireless network design would be more applicable if he or she had prior knowledge of the story and its requirements. This knowledge would assist him or her in fine-tuning the architecture to better apply and satisfy the scenario's requirements. At the same time, the military network operator's knowledge of the wireless networking concepts would

aid the writers of the scenario in establishing a story that can better satisfy their military requirements. Thus, a military scenario is more than just a story, and more than just a network as shown in Figure 7. It is written for specific purposes, and its requirements must be met. The requirements of a scenario with wireless networking must be evaluated and considered with the concepts presented in Section 2.

While the sequential approach is sub-optimal and does not allow for flexibility and change, the cyclical process proposed in Figure 8 offers the right fit. An architect's technical knowledge and an operator's military experience are combined in an iterative cycle of evaluation and assignment of parameters for the fine-tuning of a scenario's network. The story is analyzed and a straw-man network is established. Related technical concepts are chosen, analyzed, and assigned parameters. The network is evaluated against the purpose of the mission. New concepts and parameters may be added or deleted in order to have a network that satisfies the mission requirements best. These iterations end when both the technical architect and the military operator agree that the network fits the scenario.

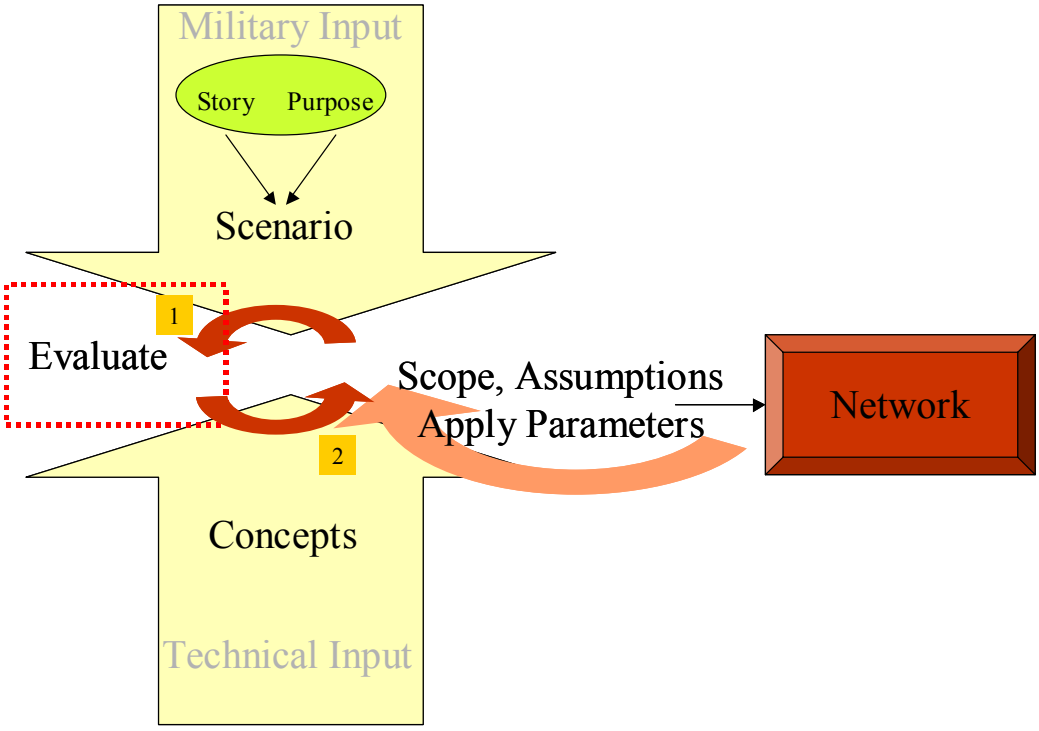

Figure 8. Iterative Scenario Evaluation Process

An applied example of this process may offer more clarity. The storyline of the tactical scenario is a peacekeeping mission to secure a chemical factory on hostile ground, with the purpose of protecting international security against possible terrorism. The area is mountainous and provides harsh conditions for a large deployment of military vehicles. The

network architect, with little or no knowledge of the storyline, travels the Concepts → Parameters → Network path for designing a network that fits (to his/her knowledge) best for a military operation. At the first glance, any wireless device, including cellular phones, might be a fit for a military application.

If the story and the purpose are made available to the architect, the design of the network becomes more appropriate. For example, the architecture will match the network to the intended terrain; will propose devices that are ruggedized, will design the network hierarchically to be flexible between peer-to-peer and centralized architectures – all this and more in order to optimize the service to the ground troops.

The first iteration of the cycle clearly specifies the network for the intended purpose. The second and future iterations optimize the network even further. If there are slight changes to the scenario, one can follow this cyclical process to adapt the design to suit those changes.

For example, if there were a possibility to bomb the factory with supersonic fighter planes, then the among the concepts that require consideration are the effects high-speed and Doppler effects on mobility, ground-to-air communications for the sniper laser targeting the factory, and air-to-TOCC communications for command and control. These concepts would in turn translate to parameters such as near mach speed Doppler shift in frequencies used in the ground-to-air link. The longer range of coverage for the communications links would need to be considered to connect the pilot to the laser sniper, as well as the TOCC. There is also the possibility of providing live video transmission of the operation from the snipers' point of views and the airplane's cockpit as a back-up for target authentication. These parameters would be applied to the network architecture, and would enhance operations using the scenario. The feedback from the scenario could optimize the concepts and/or the parameters for the actual operations under scenario conditions.

5. Conclusions

Wireless technology is often an integral part of military scenarios. This report gave a general overview of wireless networking concepts. Their role in military ad hoc network information operation scenarios was highlighted. Strategic, operational, and tactical scenarios were established for secure mobile ad hoc networking.

In the strategic scenario, it was shown that a secure mobile ad hoc network offered sufficient connectivity, quick setup, and reliable links for the recovery period after a massive DDOS attack on the TNDHQ's key servers.

For the operational scenario, a secure mobile ad hoc network was established to perform reliable ISR along the eastern seaboard of North America. The wireless network was established for preparing and defending against a forthcoming physical terrorist attack from a cargo ship sailing towards the continent with suspected biological warheads. The scenario also involved a twist in conjunction with the potential biological threat: a DDOS attack focused on marine defensive networks to hide and divert attention from the real threat.

A tactical scenario was devised within the context of a peacekeeping mission. The tactical scenario involved Intelligence Surveillance & Reconnaissance (ISR), communication, nodal situation awareness, and collaborating planning tools with TNDHQ and the ground forces.

The attributes of wireless networking concepts were discussed for each scenario, as well as potential network vulnerabilities. These building blocks not only assisted in defining the background assumptions of the design, but also the architecture's suitability for each scenario. The iterative, cyclical approach to network architecture design was introduced. The process enables researchers to focus on the technical needs of the Canadian Forces in such scenarios.

The tactical scenario has already been adopted by a group of scientists from three countries in order to provide a framework in which a secure mobile ad hoc network could be developed. The militaries of Canada, the Netherlands, and Sweden have reviewed and approved of the scenario. Secure mobile ad hoc networking is part of a research collaboration between Canada, the Netherlands, and Sweden. It was formed in order to combine the partner's expertise in Information Operations to find better solutions that will, in turn, directly benefit all partners. One such solution is the architecture of an interoperable, manageable, and secure military mobile ad hoc network based on existing and emerging commercial off-the-shelf (COTS) products, services, and standards.

6. References

1. Mike Tzamaloukas, “IEEE 802.11 QoS MAC Enhancements”, tutorial notes, IEEE Wireless Communications and Networking Conference (WCNC), 2002.

2. Mazda Salmanian, “Secure Mobile Networking, A Look Ahead”, DRDC Ottawa TM 2002-083, Defence R&D Canada - Ottawa.

3. J. Macker and S. Corson, IETF Mobile Ad hoc Networking Working Group Charter, www.ietf.org/html.charters/manet-charter.html.

4. Conversation with Ian Bryant, Head of Research and Technology, National Infrastructure Security Coordination Centre (NISCC), October 2003, www.niscc.gov.uk.

5. Lefebvre J. H. et al, “Joint Network Defence and Management System Concept Document”, DRDC Ottawa TM 2003-230, Defence R&D Canada-Ottawa.

6. Department of National Defence, “Force Planning Scenarios”, www.vcds.forces.gc.ca/dgsp/pubs/rep-pub/dda/scen/intro_e.asp.

7. Dominic Lafleur, “Force Planning Scenario 10: The Case For Including A Cyber-Attack Component”, Department Of National Defence Canada, Operational Research Division, Directorate Of Operational Research (Joint), DOR(Joint) Draft Research Note RN 2003, July 2003.

8. “Initial System Architecture”, Document INSC/Task 1/D/001, Version 1, December 11, 2001.

9. Anders Hansson et al, “Tactical Radio Access Networks – A Comparison of Ad Hoc and Cellular Network Concepts”, Swedish Defence Research Agency, FOI-R--0086—SE, March 2001, ISSN 1650-1942.

10. Conversation with Dr. Mark McIntyre, “Trip Report, Meeting of the CA/NL/SE Information Operations Collaboration Group”, August 2, 2002.

11. Haiying Zhu, “Impact of Wireless Technologies & Wireless IP on Spectrum”, Communication Research Centre (CRC), Wireless and Inter-networking Systems Experimentation LABoratory (WISELab), April 2000.

List of symbols/abbreviations/acronyms/initialisms

AP	Access Point (WLAN term)
APV	Armoured Personnel Vehicles
BER	Bit Error Rate
BW	Bandwidth
CDMA	Code Division Multiple Access
CSMA	Carrier Sense Multiple Access
COTS	Commercial Off-The-Shelf
DDOS	Distributed Denial of Service
FDMA	Frequency Division Multiple Access
FNBDT	Future Narrow Band Digital Terminal
FSO	Free Space Optical
ISR	Intelligence Surveillance & Reconnaissance
L2TP	Layer-2 Tunneling Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MANET	Mobile Ad hoc Networking
MTBF	Mean Time Between Failure
NDHQ	National Defence HeadQuarters
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Data Assistant

PSTN	Public Switched Telephone Network
S-MANET	Secure Mobile Ad hoc Network
SATCOM	Satellite Communications
VHF	Very High Frequency
TDMA	Time Division Multiple Access
TNDHQ	TransNational Defence HeadQuarters
TOCC	Transnational Operational Command Centre
UAV	Unmanned Aerial Vehicle
UN	United Nations
UXV	Unmanned (aerial, marine, land, etc.) Vehicle
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
QoS	Quality of Service

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Military Wireless Network Information Operation Scenarios (U)

4. AUTHORS (Last name, first name, middle initial)

Salmanian, Mazda

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (total cited in document)
December 2003	25	11

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)
5B36	N/A

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)
DRDC Ottawa TM 2003-241	N/A

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

N/A

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Military scenarios are narratives that describe situations within which the military may need to operate. Military personnel, including military network operators, use these scenarios to practice their duties in those situations. The scenarios also provide military network designers with a context in which to identify specific products that meet the requirements of the specific situation. This context is especially important for wireless network designers, who must build military mobile ad hoc networks that are interoperable, manageable, and secure.

Wireless networking concepts, such as mobility, network size, and quality of service, are important considerations when designing military ad hoc network information operation scenarios. Until now, the combination of scenario and concepts has produced a wireless architecture that may not be suitable. This was the result of the scenario being fully defined before dealing with the relevant concepts. This report proposes a process whereby scenarios and concepts are evaluated together, iteratively, to progressively produce a wireless network architecture that better supports the military's needs.

This report gives a general overview of wireless networking concepts. Their role in military ad hoc network information operation scenarios is highlighted. Strategic, operational, and tactical scenarios are established for secure mobile ad hoc networking. Concept constraints are discussed for each scenario, as well as potential network vulnerabilities. Finally, the iterative, cyclical approach to network architecture design is introduced, where the concepts not only assist in defining the background assumptions of the design, but also the architecture's suitability for each scenario.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Military, Wireless, Network, Information Operation, Scenarios, ISR, Tactical, Operational, Strategic, MANET, Ad Hoc

Defence R&D Canada

Canada's leader in defence
and national security R&D

R & D pour la défense Canada

Chef de file au Canada en R & D
pour la défense et la sécurité nationale

www.drdc-rddc.gc.ca