Data Centric Resource and Capability Management in Modern Network Enabled Vehicle Fleets

GREGOR THOMECZEK

A thesis submitted in fulfilment of the requirements
of the University of Brighton for the degree of
Doctor of Philosophy

August 2015

Vetronics Research Centre,
School of Computing, Engineering and Mathematics
The University of Brighton, UK

Declaration

I declare that the research contained in this thesis, unless otherwise formally indicated within the text, is the original work of the author. The thesis has not been previously submitted to this or any other university for a degree and does not incorporate any material already submitted for a degree.

Gregor Thomeczek 17-08-2015

Abstract

The objective of this thesis is to improve battlefield communications capability through improved management of existing platform and fleet level resources.

Communication is a critical capability for any platform node deployed on a modern battlefield and enables vital Network Enabled Capabilities (NEC). However, the dynamicity and unpredictability of wireless battlefield networks, as well as the constant threat of equipment damage make wireless battlefield networks inherently unreliable and as such the provision of a stable communication represents a significant technology management challenge.

Fulfilling increasingly complex communications requirements of diverse platform types in a chaotic and changing battlefield environment requires the use of novel Resource and Capability Management Algorithms (RCMA) informed by application level context data to manage limited heterogeneous resources at the platform and the fleet level while fulfilling current mission goals.

To address platform level communications resource management, this thesis presents High Availability Wireless Communications (HAWC), a novel platform architecture which enables RCMA to take maximum advantage of current platform resources. Compared to existing approaches, which are often hard wired, inflexible and lack context awareness, HAWC's modular and highly integrated approach facilitates platform repair, upgrade and reroll with minimum integration cost by performing equipment management to detect damaged, replaced and upgraded communications hardware and making it available to platform RCMA seamlessly. HAWC also provides access to fleet wide application layer contextual information such as mission, situational and platform data using a Shared Data Model (SDM) approach and thus better enables RCMAs to fulfil current mission goals.

To significantly improve fleet level communications resource and capability management, this thesis presents three novel fleet level RCMA that optimise and protect communications capability across diverse vehicle platforms using topology management techniques: I) Mission Aware Topology Healing (MATH) is a context aware topology management algorithm which reintegrates disjointed network segments whilst avoiding geographic danger zones, thereby significantly reducing node loss and network reconnection time compared to similar existing approaches; II) Group Capability Integrity Management (GCIM) performs context aware node selection to preserve mission critical group capabilities during network topology repair; III) Coordinated Node Selection (CNS) coordinates network repair efforts between disjointed network segments by predicting node selection decisions, thereby preserving group capabilities and reducing network downtime compared to existing approaches.

To enable the development, testing and performance assessment of the proposed algorithms as well as future algorithms in a realistic battlefield network context, this thesis presents a novel Battlefield Network Simulation Tool. The tool is validated by accurately reproducing experiments with publically available stimulus and result sets.

List of Publications

Gregor Thomeczek, Ian Colwill and Elias Stipidis “Resource Dependent Radio Allocation For Battlefield Communications - A Data Model Approach”, International Journal of Engineering Research and Applications (IJERA), ISSN : 2248-9622, Vol. 4, Issue 10(Part - 2), October 2014.

Gregor Thomeczek, Ian Colwill and Elias Stipidis “Mission Aware Topology Healing for Battlefield MANET” Journal of Battlefield Technology Vol 17, No 3, November 2014.

Gregor Thomeczek, Ian Colwill and Elias Stipidis “Group Capability Integrity Management (GCIM)” Journal of Battlefield Technology Vol 18, No 1, March 2015.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AFV	Armoured Fighting Vehicle
AHP	Analytic Hierarchy Process
C2AM	Connectivity with application level Constraints on Actor Mobility
C4I	Command, Control, Communications, Computers and Intelligence
CAHN	Cellular Assisted Heterogeneous Networking
CNS	Coordinated Node Selection
COTS	Commercial off-the-Shelf
CPH	Context Profile Handler
CSMA	Carrier Sense Multiple Access
DDS	Data Distribution Service
DLEP	Dynamic Link Exchange Protocol
DS	Dismounted Soldier
DSTL	Defence Science and Technology Laboratory
DZ	Danger Zone
ECM	Electronic Counter Measures
EPM	Electronic Protection Measures
FANET	Flying Ad-Hoc Networks
FIST	Future Integrated Soldier Technology
GAN	Generic Access Networks
GCIM	Group Capability Integrity Management
GPS	Global Positioning System
GRA	Grey Relational Analysis
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
GVA	Generic Vehicle Architecture
HAWC	High Availability Wireless Communication
HID	Human Interface Device
HUMS	Health and Usage Monitoring System
ICS	Interface Control Document
IDE	Integrated Development Environment
IED	Improvised Explosive Devices

ILS	Integrated Logistics Support
ISM	Industrial Scientific and Medical
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
LOSA	Land Open Systems Architectures
LRU	Line Replaceable Unit
LSA	Local Situational Awareness
MADM	Multiple Attribute Decision Making
MANET	Mobile Ad-Hoc Network
MATH	Mission Aware Topology Healing
MCC	Mission Critical Capabilities
MEW	Multiplicative Exponent Weighting
MIMO	Multiple Input Multiple Output
MOD	Ministry of Defence
MP	Mobility Potential
MRI	Mobility Readiness Index
NATO	North Atlantic Treaty Organization
NEC	Network Enabled Capability
OMG	Object Management Group
OSI	Open Systems Interconnection
PBDM	Policy Based Decision Making
PC	Personal Computer
PDR	Packet Delivery Ratio
QoS	Quality of Service
RAT	Radio Access Technology
RCM	Resource and Capability Management
RCMA	Resource and Capability Management Algorithm
RN	Repair Node
RPH	RAT Profile Handler
SAW	Simple Additive Weighting
SC	Secondary Capability
SDM	Shared Data Model
SDR	Software Defined Radio
SNR	Signal to Noise Ratio

TDMA	Time Division Multiple Access
TMA	Topology Management Algorithm
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution
TPH	Traffic Profile Handler
UAV	Unmanned Aerial Vehicles
UGV	Unmanned Ground Vehicle
UK	United Kingdom
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
VICTORY	Vehicle Integration for C4ISR/EW Interoperability
VRC	Vetronics Research Centre
VSI	Vehicle Systems Integration
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networks
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network

Acknowledgements

I would like to express my sincere gratitude to my supervisor Elias Stipidis and to my friend Ian Colwill, whose advice and support was essential during my research and the writing of this thesis.

I will be eternally grateful to my parents, my sister and my friends for supporting me and without whom I am certain I would not have been able to complete this thesis.

Thank you all for your support and your friendship.

Chapter 1 Introduction

Reliable communications is an essential capability of mobile assets in the battlefield [1]. Seamless information exchange between vehicle platforms enables mission critical capabilities, such as improved situational awareness and survivability by being able to disseminate information gathered through advanced Command, Control, Communications, Computers and Intelligence (C4I) [2] technologies by vehicle platforms in the fleet. The importance of communications capability throughout a fleet of manned and autonomous unmanned assets has also been highlighted as an outcome of a recent think tank sponsored by the Defence Science and Technology Laboratory (DSTL) [3] and the Vetronics Research Centre (VRC) [4] which concluded that a fleet's communications capability is of critical importance for mission success and mission survivability as it underpins an increasing amount of other capability in the increasingly network centric operational paradigm, and as such should have considerable resources devoted to optimising its performance.

However, battlefield wireless networks are inherently unreliable due to a number of factors, including equipment damage, fading channels, intentional and unintentional interference such as environmental attenuation and intentional disruption such as jamming. Harsh environments with a hostile topology and saturated radio bands create a highly dynamic pattern of network availability, making wireless communications challenging, especially in emergency and military applications [5-8]. In this context, existing battlefield communications systems are insufficient to fulfil the communications requirements of modern vehicle fleets, for example Bowman [9], the communications system used predominantly by the UK MOD in the battlefield today, which is integrated in state-of-the-art battlefield vehicles, such as Foxhound [10], Scout [11]and Warrior [12] has earned the label "Better Off With Map And Nokia" by some of its users [13, 14].

Battlefield technology is constantly improving. Battlefield networks are now comprised of increasingly heterogeneous vehicle platforms including different classes of manned and unmanned ground and aerial vehicles, dismounted soldiers

and base stations, each equipped with increasingly diverse communications equipment, such as novel Mobile Ad-hoc Network (MANET) technologies and advanced C4I equipment generating communications traffic with an increasing amount of diverse QoS requirements [15, 16]. Novel NECs, such as the use of Shared Data Models (SDM) achieve the fleet wide sharing of this data by improving fleet interoperability through data centric communications. The increased use of Commercial off-the-Shelf (COTS) components in the battlefield results in faster upgrade cycles, greater modularity and a need for management of an increasing range of diverse communications infrastructure [17].

To mitigate the challenges of the battlefield environment given the increased resource diversity, advanced platform Resource and Capability Management Algorithms (RCMA) are required to manage resources at the platform level and the fleet level to create capabilities and improve network reliability [18, 19].

At the platform level, RCMA must manage the existing set of heterogeneous communications hardware in an effort to be always best connected. To mitigate equipment damage and to facilitate rapid upgradability and vehicle re-roll, replaced and upgraded equipment must be detected seamlessly and made available to these RCMA with minimum configuration. At the fleet level, RCMA must manage physically dispersed network capability actively by exploiting platform mobility and relocating specific nodes in the network in an effort maximise QoS, mitigate damage, and reconnect disjointed clusters.

However, due to the aforementioned diversity of fleet resources and capabilities, it is not always appropriate to manage the whole network homogeneously. In a battlefield context, the ability to fulfil current mission goals depends critically on sufficient and appropriate resources being available in the right location, to the right vehicle platforms and at the right time.

Therefore modern vehicle fleets must take advantage of novel NECs such as fleet wide Shared Data Models (SDMs) to manage resources and capabilities in a data centric fashion. Modern RCMA must be application and context aware, i.e. must account for mission goals, situational awareness data and platform diversity to mitigate damage and allocate resources appropriately within current mission

parameters. These RCMA must be highly integrated, modular and flexible and be able to adapt to the context of a dynamic environment.

1.1 Thesis Objectives

The main objective of this thesis is to improve battlefield communications capability through improved management of existing platform and fleet level resources. In order to achieve this objective, the thesis has two main goals:

1. To develop a platform level communication management framework that improves battlefield communications capability by enabling application layer Resource and Capability Management (RCM) within current mission goals. The Communications Management Framework needs to satisfy the following top level requirements:
   - Manage equipment to mitigate failures.
   - Enable current and future application level resource management algorithms by providing access to a Shared Data Model (SDM).
   - Enable flexible and reconfigurable resource management behaviour to react to current context and goals.
   - Be flexible and reconfigurable to allow for future modifications.
   - Comply with current technology integration guidelines.

2. To develop a set of fleet level topology management algorithms to regain communications capability in case of damage and degradation while accounting for hostile agents and mission goals.

Due to the unique problem space of battlefield networks, to develop and to assess the behaviour and performance of the developed management framework and proposed algorithms in a realistic battlefield environment, a new modelling and simulation tool must also be developed.

1.2 Thesis Structure

The remainder of the thesis is structured as follows:

Chapter 2 is the first background chapter.

It provides an introduction to Battlefield Communication Networks and an overview of the range of platforms and equipment deployed in the battlefield. Chapter 2 also examines related emerging technology management approaches in military and related fields. The approaches aim to manage an increasing range of diverse communications equipment through integration and interoperation of resources.

Chapter 3 is the second background and related work chapter.

It discusses platform level and fleet level Resource and Capability Management (RCM) approaches and explores ways in which they can be used to leverage existing battlefield equipment to more effectively to fulfil mission goals through provision of increased capability such as increased situational awareness. The theme developed in this chapter is the Platform vs. Fleet dichotomy of RCM approaches. This theme provides a platform level vs. fleet level communications management approach that prevails throughout the thesis.

Chapter 4 is the methodology and tools chapter and the first contribution chapter.

It presents a novel Battlefield Network Simulation Tool, developed to provide the facilities to investigate the behaviour and measure the performance of the proposed algorithms at the platform and fleet level. The simulation tool is built in a modular and flexible manner in order to make it easily expandable and allow the modelling of heterogeneous networks in a realistic battlefield context. It allows for the modelling of a wide range of platforms equipped with heterogeneous communications technologies within a dynamic and hostile environment. The tool is validated by replicating experiments using publically available input stimuli and results.

Chapter 5 is the second contribution chapter.

It presents High Availability Wireless Communications (HAWC), a flexible and integrated framework to improve platform level communications resource management. The chapter details how HAWC enables state-of-the-art RCMAs with fleet level context information to act as a broker between communications data and a heterogeneous suite of wireless communications resources while recognising overall mission goals. Experiments that demonstrate the functionality of HAWC are presented and a discussion of the results and their implications for battlefield communications is provided.

Chapter 6 is the third contribution chapter.

It describes novel context aware methods of managing communications resources at the fleet level, that is the technology and communications capability that exists across groups of military platforms. It presents the Mission Aware Topology Healing (MATH) algorithm which protects battlefield assets in the event of an attack by enabling them to avoid Danger Zones (DZ). Chapter 6 also presents the Group Capability Integrity Management (GCIM) algorithm which preserves mission critical group capabilities and the Coordinated Node Selection (CNS) algorithm which coordinates node movements to minimise wasted resources during node relocation events.

Chapter 7 discusses and concludes the thesis and recommends future work which would build on the achievements of the thesis.

Chapter 2 Battlefield Networks

2.1 Introduction

Battlefield communications are an essential requirement in modern armed forces. “The need for seamless information exchange is apparent, shared situational awareness among military units is essential for NEC operations.” [20]. Military and disaster relief assets benefit greatly from the capacity to communicate wirelessly, enabling myriad capabilities critical to operations in otherwise infrastructure-less environments.

Network Enabled Capabilities (NEC) such as intelligence gathering for the purposes of gaining greater Local Situational Awareness (LSA) are now a critical part of any mission and are therefore a highly researched topic [21]. Since the ability to communicate between different vehicles and equipment is a fundamental requirement to achieving LSA, communications suites are often considered mission critical systems.

However, Battlefield networks face significant challenges and are typically characterised by unreliable connectivity due to damage, interference and a saturated wireless spectrum [22]. Although the military is increasingly utilising wireless communications, the North Atlantic Treaty Organization (NATO) sites mobile tactical communications as “increasingly the weakest link when conducting effective NATO and coalition operations“ [1].

Increasing mission complexity is met with a growing range of platforms and capabilities and accordingly an increasing range of vehicle platform equipment that generates more data with diverse and dynamic priorities and security levels. The network itself can range from a few nodes with point to point communications up to vast mesh networks consisting of numerous passive sensor nodes dispersed over a wide area [23].

For these reasons Battlefield networks are subject to stringent requirements. They are required to be highly reliable, resilient, scalable, secure and rugged communications

networks with inherent anti-jamming properties while simultaneously delivering high throughput to mobile nodes at long range even in the face of a constant threat of attack. To fulfil these stringent requirements in a cost effective manner, inspiration is taken from the commercial sector. An increasing number of military systems are designed using Commercial off-the-Shelf (COTS) equipment in order to facilitate upgradeability and to take advantage of economies of scale [22]. Continuous advances in commercial sector technologies result in improved wireless communications with enhanced Quality of Service (QoS) and faster upgrade cycles. These improvements have the potential to directly translate into enhanced battlefield capabilities, increased situational awareness and improved survivability.

2.2 Battlefield Environment

Battlefield equipment is required to operate in a large variety of environments, ranging from open landscape with low interference, line-of-sight communication to environments which significantly impede the use of wireless communications, such as mountainous terrain, dense vegetation, and weather conditions ranging from mild to extreme. Some of the most challenging environments for land forces using tactical wireless networks are urban areas. Scenarios involving tall buildings and subterranean tunnels produce three dimensional network topologies which result in non-line-of-sight communications and therefore suffer from signal attenuation, making the wireless network particularly unreliable [24]. Further challenge is presented by increasingly diverse mission types involving an increasing range of heterogeneous battlefield equipment including many different types of mobile node ranging from manned and unmanned aerial and ground vehicles to handheld devices and man packs. The resulting diversity in wireless capability makes interoperability a challenge [1].

In recent years, with the commercialisation of mobile broadband, tremendous advances have been made in terms of transmission speed and power efficiency that allows handheld mobile devices to communicate with each other at high speed. Although continuous improvement of modern high performance communications equipment results in improved performance under ideal conditions, the medium over

which they communicate remains unreliable and hence the reliability and availability of wireless communications in battlefield applications remains a challenge.

For this reason wireless networks, especially ad-hoc networks are said to be inherently unreliable. Obstacles to reliable networks include fading channels, noise and an implicitly unpredictable and time varying nature of the transmission medium [5, 25, 26] as well as jamming and attenuation due to physical obstructions [27], changes in the environment such as weather [8], node compromisation, hardware failure and resource depletion, such as battery drain [6]. In some cases traditional wireless networks can be made highly reliable, but at the cost of high latency and low throughput [28]; but in general, network reliability is a quality which is not directly proportional to either throughput or latency [26] and hence must be addressed independently.

2.2.1 Internal Interference

Internal interference is a threat to reliability of any radio transmission. It occurs when a communication signal is itself the source of distortion or interference. There are several causes of internal interference. Particularly wireless networks in urban and indoor environments are susceptible to internal interference due to signal reflections which can cause significant packet loss [5]. In some cases simply the resulting added distance the signal has to travel due to several reflections off of surfaces can weaken the transmission enough to result in a lower signal to noise ratio. Signal reflections can also create several distinct waveforms; when the original and the reflections reach the receiver they can cause multipath fading [25]. Another source for interference is signal collision, which can occur when two or more nodes attempt to transmit simultaneously. Various techniques exist to avoid signal collisions; examples include Carrier Sense Multiple Access (CSMA) which determines if the physical medium is available before transmitting, or Time Division Multiple Access (TDMA) [26] which assigns predefined transmission slots to each transceiver.

The increasing need for higher bandwidth communications has prompted much research to better utilise the wireless spectrum. While multiple radio transceivers of

the same type operating on different channels have been shown to deliver significantly higher throughput than single transceiver communications by enabling nodes to transmit and receive simultaneously and utilize more of the frequency spectrum [29], internal interference between the radios can be a problem [30]. This effect can be reduced with the use of spatial multiplexing [26], or the use of heterogeneous transceivers which solve this problem by operating on completely separate frequency bands, thus improving robustness, reliability, connectivity and performance.

2.2.2 External Interference

External interference is another common threat to reliability; it is the interference caused by signal sources that are not part of the network [31]. There are two types of external interference, unintentional and intentional. Unintentional external interference can be caused by any type of radio emitter, such as wireless phones and microwave ovens as well as terrain, foliage and weather. Intentional external interference is caused by deliberate and hostile attempts to block, distort or overpower a radio signal, e.g. with electronic countermeasures. External interference can be overcome in a number of technical and physical ways. Frequency diversity such as orthogonal frequency-division multiplexing [32] and frequency hopping can be used in an effort to occupy a part of the spectrum with less interference [33]. Diverse transceivers can be used to occupy multiple bands, transmitting redundant data can be used to recover information from a distorted signal [34] and time diversity can be used in an effort to transmit during times when external interference is not present [35].

2.2.3 Equipment Damage and Degradation

Damage to communications equipment can degrade or defeat a vehicle's communications capabilities, possibly jeopardising mission success and vehicle survivability. Equipment degradation can occur for several reasons, such as damage to the vehicle platform and failure of components critical to the communications capability of the vehicle, such as antennas. Harsh environments with great temperature differentials, moisture and dust in addition to the constant risk of node

damage resulting from an attack, make node failure a common scenario in the battlefield.

2.3 Range of Platforms

A vehicle platform describes any type of asset deployed in the battlefield. In a battlefield networks context, a vehicle platform may represent nodes in multiple overlapping heterogeneous networks, depending on the radio equipment it is carrying (see section 2.4 for more information about different platform equipment). The increased variety of missions combined with the continuous development of new technology has resulted in an increased number of vehicle platform types in use by modern armed forces, each with different capabilities and applications [36]. The availability of COTS technology has enabled the use of a wide range of specialised unmanned vehicles, some controlled by a dismounted soldier from a few metres away, and some from communications base stations on a different continent. Modern vehicle fleets are highly integrated; to manage their resources and capabilities effectively, it is important to recognise their diverse requirements. As nodes in a common network, each platform's mission goals include facilitating an effective communications capability for the fleet.

2.3.1 Dismounted Soldiers

Dismounted Soldiers (DS) play a significant role in modern military operations and often cannot be replaced by manned or unmanned vehicles. Technology in the battlefield is often built around the requirements and capabilities of DS in the battlefield. In addition to the large number of vehicle platforms developed solely to deliver dismounted soldiers into theatre, many unmanned vehicles are designed for the sole purpose of aiding DS; logistics, such as carrying soldier equipment over long distances, or provide improved LSA.

DS are being equipped and interfaced with more and more information generating equipment which requires each DS deployed in a modern battlefield to represent a node in a wireless network. Head mounted, gun mounted and handheld sensors and devices generate an increasing amount of data that must be shared over this network

[16]. DS need to control and share data with many types of unmanned vehicles. While this often occurs with dedicated hardware, future dismounted soldiers will be more integrated with all types of wireless platform.

2.3.2 Unmanned Vehicles

2.3.2.1 Unmanned Aerial Vehicles

There exist a wide variety of Unmanned Aerial Vehicles (UAV) in the battlefield, with wingspans ranging from several centimetres to over ten metres, fulfilling a range of activities involving critical support missions such as reconnaissance and gathering enhanced targeting data to aid land forces, as well as engaging targets actively using a variety of weaponry.

Advances in microelectronics, battery, motor and communications technology and the resulting higher availability of compact UAV means that small UAV are becoming more widespread in the battlefield especially for reconnaissance missions. These small UAV can be carried by a dismounted soldier and can be used to significantly enhance LSA by giving land forces a bird's eye view of a large area very quickly. Several types of these small UAV exist; most currently in use, are either in the form of a miniature fixed wing electric aircraft, or a quadcopter design while significantly smaller designs the size of a bee [37] or a hummingbird [38] are in development, but still in their infancy.

Advances in computer algorithms and swarm behaviour are being developed to enable fully autonomous activities, such as the fully autonomous mapping of urban scenarios [39] as well as agile [40] and formation flight [41] where small UAV are able to carry out tasks as a group, such as lift heavy objects using multiple quadcopters cooperatively. To enable communications between these swarms of UAV, Mobile Ad-Hoc Networks (MANETS) are being developed which account for the specific requirements of Flying Ad-Hoc Networks (FANET) [42].

While the power constraints of smaller UAV significantly limit communications capabilities, larger UAV are typically equipped with multiple wireless links, for

command and control from the base station and to feed information to DS and Manned Vehicles on the ground.

2.3.2.2 Unmanned Ground Vehicles

Unmanned Ground Vehicles (UGVs) are widely used in the military. Their use has gained popularity because they allow personnel to remotely carry out otherwise dangerous tasks, such as Improvised Explosive Device (IED) detection and disposal, while remaining at a safe distance. Continuous technological advances enable UGVs to perform increasingly complex tasks making UGVs a more and more indispensable tool thin the arsenal of moderns land forces.

UGVs are being used in a wide range of sizes and weight classes. UGVs, such as the "Throwbot" [43] are small enough to be carried by a dismounted soldier, while large UGV, such as the Abrams Panther mine clearing vehicle can have a mass of over forty tons. Different UGVs are equipped with several types of propulsion. While most UGVs mirror manned vehicle design and use wheels or tracks, some types of UGV are developed to use two [44] or four legs [45] to be able to traverse difficult terrain.

UGVs can be used to carry out a wide range of critical support missions. Enhanced local situational awareness through reconnaissance by UGVs, particularly in urban scenarios can significantly improve survivability for dismounted soldiers. UGVs can also be used for the detection and disposal Nuclear, Biological and Chemical threats. While most UGVs in use today fulfil a supporting role, such as detailed above, some varieties, such as the SWORDS can be equipped with weapons, including grenade launchers and automatic rifles and can be used to actively engage threats from a distance. In addition to remotely controlled UGVs, advances in computer algorithms give rise to UGVs capable of performing a growing number of tasks autonomously, such as patrolling a perimeter or take part in a supply convoy.

Due to these diverse capabilities and safety requirements, a UGV may be equipped with a variety of Radio Access Technologies (RATs). Typically, communication between a UGV and the operator occurs via a point to point connection to a specialised terminal; however, more widespread use and the necessary reduction of

efficiency bottlenecks will result in UGV communications becoming increasingly integrated with other battlefield systems. Due to battery power limitations of smaller UGVs, transmission power may be limited and advanced resource management may be necessary.

The highly versatile nature of UGVs combined with the reduced risk for the operator are clear advantages which will only result in an increased number of UGVs being employed in the battlefield. The resulting increased variety and number of nodes in a wireless network brings stringent QoS requirements in an increasingly larger network which must be fulfilled in order to support the inevitable growth of UGV missions.

2.3.3 Manned Vehicles

Manned vehicles can include ground vehicles, air and water craft. Modern manned ground vehicles such as the Foxhound [10] play an integral role in military operations. Similar to unmanned vehicles, manned vehicles are being equipped with an increasing range of sensors, enabling capabilities such as the streaming of high definition video; however, in addition to the ability to generate an increased amount of data, manned vehicles often represent the command and control station for unmanned vehicles. Future manned vehicles may be equipped to deploy several UAV and UGV to perform a variety of support tasks, such as LSA, mine clearing and reconnaissance.

Manned vehicles tend to be larger in size than unmanned vehicles and have much less stringent power limitations; therefore they are typically capable of more resource intensive tasks. Direct human control of a vehicle still outperforms both autonomous and remotely controlled unmanned vehicles; hence manned vehicles can also carry out more complex tasks.

2.3.4 Command Bases

As the centre for logistics and planning in the battlefield, command bases represent the backbone of the command structure [46]. They interface with all previously discussed node types, acting as the central point of control in the battlefield.

Command bases are typically fortified and hence, represent a more secure node in the network. Because of the stationary nature of a base, power limitations are much less stringent and communications capability is typically the largest of any node in the network.

2.4 Range of Platform Equipment

Assets in the battlefield are becoming increasingly heterogeneous. This results in a wide range of communications equipment deployed in the field.

The range of equipment used in modern vehicle platforms is constantly increasing. Wireless communications equipment has become extremely diverse due to the large range of capabilities and QoS requirements needed to satisfy increasingly diverse mission types. Different types of RATs have different strengths and weaknesses. Modern battlefield vehicle fleets exploit this fact; therefore vehicles with varying communication requirements are equipped with different communications technologies to suit their mission goals. These technologies may be developed entirely for military purposes; however, it is increasingly common for battlefield vehicles to be equipped with technology developed for the commercial sector.

2.4.1 Commercial off-the-shelf Technology

Commercial off-the-Shelf (COTS) equipment includes any generic commercial hardware or software available in the commercial marketplace that can be purchased via government contract. This includes a wide range of products and services including materials and technology used for military vehicle platforms.

Driven by large financial incentives of consumer demand, commercial hardware is being constantly developed resulting in a faster rate of technology evolution compared to government development of custom battlefield technology. COTS devices are typically manufactured in high volumes resulting in a significantly reduced cost and abundance in spare parts. COTS technology requires significantly less training than custom battlefield technology because oftentimes the user is already familiar with a civilian equivalent [47]. Therefore designing a system

utilising mass produced COTS components can result in a more state-of-the-art system, as well as a significant reduction in cost.

The rapid evolution and lower costs mean that it is often inefficient to develop entirely new solutions solely for military application and not to take advantage of the steady evolution COTS technologies. In addition to COTS hardware, when clear advantages can be demonstrated, even COTS *applications* permeate into the battlefield. An example is the increasing importance of text messaging in the battlefield due to its advantages of silence, simplicity and the ability to perform real time translation [1]. For these reasons the military is increasingly adopting a COTS philosophy in regard to their equipment.

Despite these advantages, some inefficiency exists as competing standards and design philosophies of different COTS suppliers struggle to yield the technical coherence necessary to provide the required level of interoperability between different vendors' COTS hardware. Future military vehicles need to have the capability of having any system upgraded or replaced quickly in order to aid mission adaption or in case of damage, any vehicle subsystem needs to be rapidly repaired, or replaced. In order to take advantage of these properties, systems must be designed to seamlessly accommodate and integrate a range of COTS hardware, both by designing the systems in a hardware independent fashion and by defining a clear set of interfaces between the equipment and the rest of the system.

2.4.2 Through-Life Platform Upgrade

Due to a higher required return on investment, battlefield vehicle platforms have longer life cycles [48], thus vehicle platform communications resources may be modified or upgraded during the platform lifetime in order to address changing operational requirements or to take advantage of new technology. To facilitate these modifications, any implementation of communications resources on modern vehicle platforms must facilitate rapid replacement of radio resources, enabling reconfigurability and upgradability at minimum integration cost.

2.4.3 Radio Access Technologies

In order to fulfil more stringent performance requirements, Radio Access Technologies have become increasingly complex. As discussed previously, a clear trend towards the integration of COTS equipment within battlefield equipment means that future battlefield networks will likely use an increasing variety of COTS Radio Access Technologies (RAT) with highly diverse properties, strengths and weaknesses. Used appropriately considering their individual properties and requirements, they have the potential of significantly improving battlefield communications capability. Because they share the same wireless spectrum, their performance always depends on the environment they are being used in.

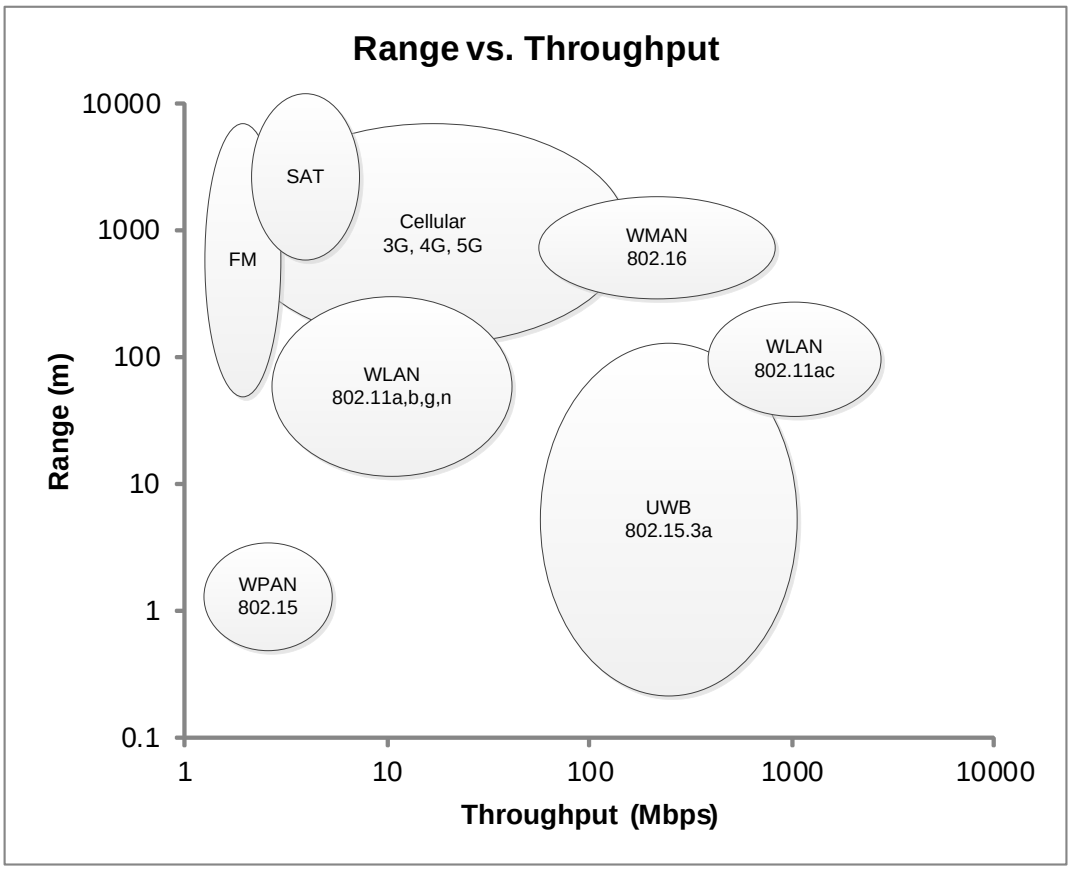

Figure 2-1 A Comparison of Wireless Access Technologies

Although RATs vary widely in their performance characteristics, they share many properties such as data rate, range, reliability, latency, object penetration, cost of transmission, channel capacity, service quality and military safety level. Figure 2-1

provides an approximate overview of different RAT performance in terms of the key properties: range and throughput.

2.4.3.1 Currently Prevailing: Point to Point Radio

FM Radio is the most widely used RAT in traditional armed forces around the world. In the UK military, the primary technology to communicate over HF, VHF and UHF radio is the Bowman [9] communications system.

Performance

Bowman provides the capability to transmit secure voice and data at a maximum data rate of 750 kbps. The system's transmission range is in the order of several kilometres, but is highly dependent on the exact configuration, antenna type and location of the radio. Different configurations of the Bowman communications system can be carried as a man pack, as well as mounted on a wide range of land vehicles, ships and aircraft. Bowman provides frequency hopping capabilities enabling it to avoid interference and interception.

Drawbacks

Although the simplicity and ubiquity of systems such as Bowman in the modern military and the existing knowledge and training in how to operate them are clear advantages for FM Radio Communications systems, due to increasing bandwidth demands, modern network enabled vehicle fleets require a next generation fleet communications system. Bowman will not be able to fulfil the needs of modern vehicle fleets alone.

Applicability to Battlefield Communications

While FM Radio will likely play a role in future military operations, it will be used as one of many radio access technologies in a data centric communications architecture where it can be deployed in situations that play to its strengths rather than its weaknesses.

2.4.3.2 Satellite Communications

Satellite communications is enabled by constellations of satellites orbiting the earth which relay information around the globe. Communications satellites are typically deployed in a variety of orbits that provide near-world-wide and world-wide coverage as well as geo-stationary satellite positions depending on the application.

Performance

Some examples of word-wide communications satellite constellations include the US Air Force Milstar [49], the UK Skynet [50] and the Iridium Satellite Constellation [51]. Due to the high cost of satellite communications, they are mainly used for low bandwidth applications where low latency communications is not a significant requirement. The Iridium constellation, for example, is capable of a typical data rate of 2.4 kbps [52] and a latency of approximately 1.8 s [53]. However, Military Satellite systems may be cable of much higher data rates, such as the Skynet constellation with a data rate of 155 Mbps [54].

Drawbacks

Due to the high costs associated with launching satellites into orbit, the use of these systems also carries a higher cost. Satellite usage is highly prioritised for this reason so that it is reserved only for the most critical communications data. The high latency caused by the travel time of the signal to orbit and back also presents a QoS challenge prohibitively high for real time applications.

Applicability to Battlefield Communications

Satellite communications are of great utility for applications in remote areas. In addition to search and rescue tasks and emergency beacons, they are used for communications with remote sites and assets such as ships and aircraft deployed in remote areas where FM communication is infeasible. Satellite communications may also be used as an emergency fall-back when other radio equipment fails. This way they can also provide the ability to communicate with disjointed vehicle clusters over great distances when other means of communications are unavailable.

2.4.3.3 Cellular Networks

Cellular networks are organised on the principle that a geographic area is divided up into cells which are each served by at least one stationary backbone transceiver, or cell base station. Clients can move freely between cells because they are handed over from base station to base station seamlessly. The use of directional antennas and the reuse of frequencies in non-adjacent cells make cellular networks very efficient in their use of the wireless spectrum. There has been a steady evolution of wireless network standards 1G, 2G, 3G, 4G [55] and due to consumer demand of high availability mobile phone communications networks, cellular networks now cover large areas of the globe.

Performance

There has been a progression in cellular technology since the first generation of mobile phones from the early days of analogue 1G with a maximum bandwidth of 2.4 kbps until 4G which is in widespread use today in certain cases capable of delivering data rates of more than 100 Mbps.

The development of 5G by the Next Generation Mobile Networks Alliance as the fifth generation of mobile network standards is planned to be completed by 2020 and aims to support data rates of at least 50 Mbps for tens of thousands of simultaneous users up to 1 Gbps for tens of users in some specific environments. 5G is also planned to enable lower latency connections than previous generations as well as network based positioning with a typical accuracy of less than 10 m [56].

Drawbacks

In contrast to Ad-Hoc networks, cellular network require a significant amount of infrastructure to be built before it can operate. Cellular networks cannot typically be mobile, they need to be set up at specific geographic locations, and therefore their setup time is costly both in terms of time and resources, reserving them for semi-permanent and permanent forward operating bases.

Applicability to Battlefield Communications

Although cellular networks require an existing infrastructure they are of interest to modern vehicle fleets because they can be built semi-permanently or in some cases it may be possible for armed forces to take command of existing cellular networks to supplement their communications capability. Due to the consumer demand, these are some of the most advanced communications technologies available today. Cellular standards can provide very high data rates across vast areas.

2.4.3.4 Wireless Metropolitan Area Networks - IEEE 802.16

802.16 describes a set of Wireless Metropolitan Area Network (WMAN) standards intended to operate on the scale of the size of a city. It was developed by the IEEE and specifies the PHY and MAC layers of RATs.

Performance

Utilising Multi-Input-Multi-Output (MIMO) technology, emerging technologies, such as IEEE 802.16 WiMAX are capable of providing data rates of up to 1 Gbps. WiMAX operates from 2 - 66 GHz, allowing for both high speed line of sight backhaul type links as well as object penetration using lower frequency bands [57].

Drawbacks

WMAN are not widely deployed and availability of COTS equipment is limited. Due to its lack of popularity, compared to its commercial competitor - cellular networks, 802.16 standard development is evolving at a significantly slower rate.

Applicability to Battlefield Communications

Its wide frequency range and subsequent inherent resistance to interference and high speed make 802.16 a useful RAT for battlefield communications; However, similar to cellular networks, 802.16 requires an existing infrastructure to be utilised effectively, therefore their use is reserved for semi-permanent to permanent bases.

2.4.3.5 Wireless Local Area Network - IEEE 802.11

Intended for the use within limited areas, such as within one or several buildings, similarly to 802.16, the 802.11 standard represents a set of interoperable implementations of wireless standards originally developed by the IEEE. The 802.11 standards specify the PHY and MAC layers and include several different types of Wireless Local Area Network (WLAN) with varying frequencies and data rates.

Performance

Like in other wireless networks, effective transmission range varies significantly depending on the environment, transmission speed [58] and antenna used [59], but a typical effective range of an 802.11 RAT can be characterised approximately with 250 m in a line of sight scenario and less than 50 m indoors.

802.11b transceivers operate on the 2.4 GHz Industrial, Scientific and Medial (ISM) band and provide a maximum data rate of 11 Mbps, however, depending on congestion of the channel they can adapt to a lower throughput of 5.5 Mbps, 2 Mbps, or 1 Mbps. 802.11g transceivers are capable of a maximum throughput of 54 Mbps, however, effective throughput can be estimated to approximately 22 Mbps [60]. 802.11a transceivers operate on the 5.8 GHz ISM band to avoid interference commonly encountered in the 2.4 GHz band and similarly to 802.11g, are capable of a maximum data rate of 54 Mbps with an effective throughput of approximately 22 Mbps [60]. 802.11n is a MIMO technology capable of transmitting and receiving using up to four spatial channels on both, the 2.4 GHz and 5.8 GHz band to achieve increased data rates. With a channel width of 40 MHz, 802.11n is also capable of utilising twice the channel width of 802.11b, g and a. 802.11n is capable of a maximum data rate of 54 Mbps to 600 Mbps depending on the number of MIMO antennas used and the amount of interference encountered.

802.11ac is an emerging technology operating on the 5.8 GHz band. 802.11ac significantly improves upon the performance of previous 802.11 standards. Using a channel width of up to 160 MHz and up to eight spatial channels 802.11ac is capable of a maximum data rate of 3.47 Gbps [61].

Another 802.11 standard is the MANET standard 802.11s [62], unlike other 802.11 standards, specifies a MAC layer intended for multi-hop mesh networking, it requires the use of one of the 802.11a/b/g/n family of technologies at the physical layer.

Drawbacks

Operating on the 2.4 GHz ISM band, 802.11b and g transceivers are subject to much unintentional external interference. One of the reasons why the 2.4 GHz band is unlicensed in the majority of the world is the fact that the resonant frequency of water resides at 2.45 GHz, which microwave ovens take advantage of and hence operate at this frequency [63]. Interaction with water in the 2.4 GHz Band also means that weather and foliage can have a significant effect on the characteristics of this type of transceiver, resulting in a highly variable performance, depending on the application. Typical COTS implementations of 802.11 also lack security and error correction, therefore battlefield implementations of 802.11 have to ensure that these QoS requirements are fulfilled by the implementation of the technology.

Applicability to Battlefield Communications

Under the brand name WiFi, 802.11 standards have become some of the most widely used wireless communication standards world-wide. The majority of mobile COTS technology in the consumer market today is equipped with an 802.11 RAT. Although 802.11 standards come in many varieties, the most common 802.11 standards today are 802.11a, 802.11b, 802.11g and 802.11n. The worldwide ubiquity of 802.11, its ever improving performance characteristics, scalability and backward compatibility make it a prime candidate for all scales of battlefield vehicle platform including manned and unmanned vehicles of all types and sizes.

2.4.3.6 Wireless Personal Area Network - IEEE 802.15

A Wireless Personal Area Network (WPAN) is a short range wireless network with a range on the order of centimetres to metres. Traditionally used for low power and low data rate applications, many mobile COTS devices were equipped with a WPAN

capability. The most widely used implementations of 802.15 in mobile devices today are Bluetooth IEEE 802.15.1 and ZigBee IEEE 802.15.4.

Performance

802.15.1 is commonly used to provide wireless connectivity between Human Interface Devices (HID) and Personal Computers (PC) as well as mobile phones and wireless speakers. 802.15.4 implementations typically have significantly lower power requirements than 802.15.1 and are therefore commonly used for low power mesh network applications. An 802.15.4 link provides data rates of 250 kbps at a distance of 10-100 m.

Ultra Wide Band (UWB) IEEE 802.15.3a is an emerging technology with significantly higher data rates than traditional WPAN. UWB floods the spectrum with wide band pulses rather than occupying a single band continuously. Like other WPANs, it operates at short range; however, it has been shown to deliver data rates up to 675 Mbit/s. UWB can also be used to provide accurate distance measurements between nodes by measuring the time the signal takes to travel between nodes. UWB occupies large bandwidth, making it more resistant to multipath interference as well as harder to locate than other RAT.

Drawbacks

802.15 shares the same 2.4 GHz band as many of the 802.11 standards and will therefore not only suffer from the same interference problems as 802.11, but also directly interfere with other 802.11 RAT. Its viable areas of use are therefore reduced to niche applications.

Applicability to Battlefield Communications

Like 802.11, 802.15 is used in a wide variety of COTS equipment worldwide, however, the WPAN's low power, short range and susceptibility to interference makes 802.15 suitable only for applications without safety requirements and a very short range, such as body sensors and personal device communications [16].

2.4.3.7 Software Defined Radio

Software Defined Radio (SDR) is a wireless RAT where the physical radio frequency front-end hardware of the radio transceiver has been reduced to a bare minimum and its functions are instead implemented in software.

Performance

In a modern network enabled vehicle fleet context, the SDR approach has several advantages. SDR is significantly more flexible in terms of frequency bands, because a single RF frontend is physically capable of transmitting a wide range of frequencies. This way the modulation frequency can be changed rapidly in order to adapt to changing environments and interference or to fill a gap in a vehicle's communication capability. Software Defined Radio is extremely reconfigurable; because most of the functionality is programmed in software, one set of hardware can be compatible with a wide range of legacy communications hardware by switching between frequencies and frequency bands [64].

Drawbacks

Software defined radios also have disadvantages. Because the amount of passive analogue hardware is reduced and the amount of processing is increased, SDR power consumption tends to be higher than that of conventional radios. SDRs also tend to have lower dynamic range, i.e. conventional radios are better able at receiving both very weak and very powerful signals than SDRs. The inability to handle large signal powers introduces the problem of "blockers" which saturate a band to the extent that it is no more receivable for SDRs [64].

Applicability to Battlefield Communications

Integrating most radio functionality into software instead of hardware can reduce the cost of radio transceivers drastically, enabling the deployment of large numbers of inexpensive radio nodes to build more redundant and therefore reliable wireless networks. Additionally, SDR systems can be updated and upgraded with very little cost and novel communication techniques enabling increased resistance to interference and reduced detectability can be prototyped and deployed quickly [1].

SDR technology is now mature enough to be implemented by the French military in form of the CONTACT program [65].

The backwards compatibility of SDR with legacy communications systems on the market and with an ever increasing number of RAT types being used for wireless communication, software defined radios are currently an intensely researched topic. The NATO IST conference recommends increased effort in the fields of SDR in order to mitigate a saturated EM spectrum [1].

2.4.4 Preliminary Conclusion

The rapid pace of development of the range of platform equipment is fundamentally driven by civilian demand; however, the advances in communications technology cannot be ignored for battlefield applications. Technology transfer from the civilian sector to the battlefield has the potential to yield significant benefits in battlefield communications effectiveness.

Although diverse, these communications technologies are fundamentally similar and share many of their basic performance characteristics, such as throughput, latency, etc. By characterising these technologies using key performance characteristics and link types it should be possible to abstract them by considering them as ‘black boxes’ with specific stated interfaces and behaviour.

The diversity resulting from the use of these advanced technologies may provide significant improvements in the future; however, to use them effectively in a battlefield context where the correct delivery of a message may require specific and stringent QoS requirements to be satisfied, it is crucial to recognise the strengths and weaknesses of each of these technologies. A management system is one viable approach which allows the use these technologies in appropriate situations and configurations recognising which RAT are best used in which combination to fulfil prevailing network QoS requirements

2.4.5 Mobile Ad-Hoc Networks

Mobile Ad-Hoc Networks (MANETs) are an emerging technology. They are a type of Wireless Mesh Network (WMN) that is dynamically self-organising and self-configuring ad-hoc communications network, arranged in a mesh topology with no existing infrastructure or centralised control [26, 66, 67].

MANETs differ from other WMNs in a number of ways. WMNs are typically comprised of static nodes, seldom stand alone and integrate with other networks. Their purpose is to enhance ad-hoc capabilities or act as a last mile solution to those networks [66, 68].

MANET nodes are designed to be completely self-sufficient, have no centralised control and function without external intervention. They are optimised for vehicular networks, comprised of highly mobile nodes and feature stand-alone capabilities in the event that a group of vehicles becomes separated. In the battlefield MANET technologies are superior to traditional static radio technologies because of their inherent support for a highly dynamic topology [67]. Manufacturers of commercial MANET implementations include Mesh Networks [69], Mesh dynamics [70], Radiant Network Services [71] and Persistent Systems [72].

2.4.5.1 Routing

Wireless routing in ad-hoc networks as opposed to wired routing is characterised by a lack of prior knowledge about the network topology which has to be discovered through probing [27]. In contrast to point-to-point networks, MANETs are not limited by a single transceiver's range [73]. To transmit information over large distances a technology called multi-hopping [62] is used in which messages can be forwarded from node to node. Multi-hopping routing protocols include IEEE 802.11s [62], TORA [74], AODV [75], DSDV [76], DSR [77], BABEL [78], etc. Routing tables are used to store established routing paths; however, since in a highly dynamic environment, successful routing paths cannot be trusted to work more than once, routing tables quickly become obsolete. The result is large packet loss, frequent message retransmits and a large overhead consumed by route discovery packets which make the transmission of time critical data extremely difficult.

2.4.5.2 Scalability

Multi-hopping allows MANET to become very large in size, however, since every additional hop a packet has to take increases latency, the network experiences a rapid drop in throughput as the number of hops increases, subsequently inhibiting the networks scalability [66]. To solve these emerging scalability problems, some MANETs employ clustering protocols which enable nodes of a MANET to form groups in order to split the network into multiple smaller parts. These clusters are easier to manage and reduce latency by locally sharing information which does not need to be transmitted throughout the whole network frequently, increasing bandwidth efficiency as well as scalability [79]. In cases when a MANET becomes fragmented, clustering enables fragments to reconfigure into an independent subnet and coordinate locally until the fragment is able to reintegrate with the main network.

2.4.5.3 Applicability to Battlefield Communications

Despite all of these challenges, MANETs have many advantages. Their rapid deployability makes them ideal for modern vehicle fleet operations in military as well as disaster relief applications. Even when existing infrastructure is damaged or unusable, MANETs can be constructed rapidly with few resources. Their dynamic self-configuration means that nodes automatically form a network and no set up or external management is necessary, even when individual nodes fail or the environment changes [1].

2.4.6 Quality of Service

Quality of Service (QoS) is the measure of the performance of a communications network as observed between two network endpoints i.e. the useful communications capability of a network between two nodes [80]. QoS can be assessed on multiple layers of the Open Systems Interconnection (OSI) model [81], e.g. throughput on the Physical Layer or Video Quality on the Application Layer.

Although there exists no universally accepted list of common QoS parameters for either a network QoS provision or traffic QoS requirements myriad lists of QoS

parameters have been proposed to describe a wide variety of diverse networks [82]. The burden of a QoS parameter classification of a network is to adequately represent the performance of the network using a limited set of QoS metrics. To this end the Data Link Provider Interface (DLPI) Standard is one approach that measures common basic network performance by a list of six performance parameters: Throughput, Delay, Priority, Protection, Error Rate and Resilience [83].

2.4.6.1 Throughput

Throughput measures the amount of useful information in bits which can be transmitted over the network end-to-end in a given time. Battlefield networks are required to transport data with diverse throughput requirements. Throughput requirements can range from a node transmitting a heartbeat at a predefined frequency to a group of vehicles platforms transmitting multiple high definition video streams.

2.4.6.2 Transit Delay (Latency)

The latency of a network is the measure of the end-to-end delay of a message; it is the time it takes for the information to be transmitted from one point of the network to another [84]. In a battlefield network, there are several traffic types with diverse latency requirements. For example, daily map updates are not time critical, whereas UGV control data has a stringent latency requirement to guarantee that the UGV responds to a control input within a given time.

2.4.6.3 Priority

Because a limited QoS can be delivered based on prevailing constraints, traffic is prioritised according to its importance. High priority traffic is generally prioritised ahead of best-effort data in order to avoid lower priority traffic hindering high priority traffic. Battlefield networks transport traffic with diverse priorities from weather information to armament discharge commands.

2.4.6.4 Protection

Protection indicates the extent to which the traffic is guarded against unauthorised monitoring or manipulation [80]. This QoS parameter is especially relevant within battlefield networks to protect against unauthorised interception or tampering with traffic. Protection requirements in battlefield networks are enforced by strong encryption, authentication and authorisation.

2.4.6.5 Residual Error Rate

Residual Error Rate is the ratio of lost, incorrect and duplicated packets to the total amount of packets transmitted end-to-end over a network [85]. It is the proportion of useful data received. As discussed previously, battlefield networks, especially MANETs are subject to harsh and dynamic environment and thus typically experience a high error rate.

2.4.6.6 Resilience

Resilience measures the network's ability to provide a certain QoS level despite unwanted outside influences, i.e. the network's resistance to jamming and other Electronic Counter Measures (ECM). Battlefield networks are required to possess a particularly high level of resilience which is provided by a variety of Electronic Protection Measures (EPM) including multi-hopping and other anti-jamming measures.

For the purposes of assessing a network according to these parameters, in a stable network, QoS can be modelled as a function of a limited number of factors, such as the number of transceivers available, their transmission rate and power, the distance between nodes and interference between nodes [25], however, a stable topology is seldom achieved in battlefield networks. The QoS which can be provided in a diverse and dynamic battlefield network is also a function of several external factors including node mobility, hostile forces, vehicle stealth, etc.,

Communications traffic transmitted over a battlefield network has diverse and dynamic QoS requirement which have to be fulfilled by the network. This traffic needs to be transmitted using existing resources therefore modern vehicle platforms

commonly transmit mixed QoS data on the same link [86]. To enable the use of the same link for multiple concurrent types of traffic, care must be taken to deliver appropriate QoS for each type of traffic.

2.5 Technology Integration Approaches

Traditionally, civilian and battlefield vehicle platform technology consisted of independent analogue systems, which were hard wired to perform a single function. Actuators and effectors were typically controlled by a single dedicated control interface, i.e. a switch; operator feedback functioned similarly.

The increasing complexity of battlefield vehicle platforms described in the previous chapters presents a new management challenge for military vehicle designers and operators. Changing mission goals, increasing performance requirements and data demands mean that network efficiency and capacity must be improved by increasing the amount of interoperability and cooperation between nodes on the fleet level [1]. To cope with the added complexity of multiple RATs and other battlefield vehicle equipment and the resulting added cost, it is necessary to use existing resources more efficiently.

One approach that aims to address these needs is a drive towards modularity and standardisation from a fleet level management perspective. Seamless use of heterogeneous technologies can yield higher efficiencies; more standardisation and integration of components can significantly reduce costs by enabling the use of mass produces COTS hardware and prolong the service time of vehicles by extending their future utility. Common standards result in more flexible battlefield equipment which can be upgraded to perform its function more effectively, or be repurposed when necessary.

2.5.1 Generic Vehicle Architecture

The Generic Vehicle Architecture (GVA), UK MOD Defence Standard 23-09 [87] is an MOD owned and maintained, mandatory vehicle architecture for all new MOD vehicle projects. It is aimed at standardising military vehicles in order to benefit from

a common approach to vehicle design. The nine basic principles of the GVA are as follows:

- “Be MOD owned and maintained.
- Take account of previous MOD investment.
- Specify the minimum necessary to achieve MOD's desired benefits and avoid unnecessary constraint in implementation.
- Be applicable to current and future systems.
- Be open, modular and scalable.
- Facilitate technology insertion (upgrade, update, replace, repair, remove and add).
- Not to implement in hardware any functionality that can be implemented in software.
- Take a ‘whole platform’ systems view.
- Be done in conjunction with industry.”

The GVA provides guidelines on vehicle design in areas such as electronic architecture and technologies, physical architecture, power supplies, human factors, integration and others. It is an ongoing effort to standardise military vehicle design. It provides a platform level data model that offers abstraction from individual pieces of equipment and standardises the set of interfaces for connecting equipment to the modular architecture.

The GVA aims to facilitate a reduction in cost of components through the economies of scale and a reduction in cost of vehicle design and ownership. It eases the process of replacing faulty or out-of-date vehicle components, as well as increasing the compatibility of systems across a fleet of vehicles. Due to its open and modular nature it enables vehicle design to incorporate tried and tested legacy systems, as well as possible future systems. Vehicle functionality can be updated more frequently by the use of software defined systems and a modular design of vehicle components.

2.5.2 Future Integrated Soldier Technology

Future Integrated Soldier Technology (FIST) is a UK MOD program designed to enhance the British Military's effectiveness by providing improved situational awareness, lethality and survivability through the use of highly modular and interoperable infantry soldier equipment. FIST uses COTS equipment, such as radios, GPS receivers, computers, optics and cameras and aims to integrate all technology worn by dismounted soldiers in order to enhance their overall combat effectiveness.

FIST takes advantage of a number of capabilities generated by interoperability between standardised systems. FIST allows soldiers to communicate within their group as well as with a forward operating base. Using a multihop protocol, the FIST system can integrate with unmanned platforms to transmit information over larger distances.

By integrating these technologies, FIST enables group capabilities beyond those of any individual unit, such as the ability to share location data and video from helmet and weapon mounted cameras, as well as route planning and tactical planning capabilities. Bowman is used as the main underlying communications technology; for PAN applications FIST uses Bluetooth, i.e. to interconnect different FIST components.

2.5.3 The Vehicle Integration for C4ISR/EW Interoperability

The Vehicle Integration for C4ISR/EW Interoperability (VICTORY) is a program developed by the US Army in order to solve the problems caused by the current additive approach to vehicle design in which new vehicle systems are simply added to military vehicles, causing space, power and efficiency issues [88].

VICTORY aims to solve these problems by reducing the number of discrete systems which are unable to communicate with each other by combining systems and instead using standard interfaces between modular components. This increases systems integration and efficiency while reducing cost and redundancy [89]. In order to improve combat effectiveness, VICTORY uses an architecture of open standards of

physical and logical components which are shareable and interchangeable between vehicle systems and communicate in a data bus centric fashion, enabling automation and reducing lag introduced by the need for crew to manually perform operations, such as target acquisition [89].

2.5.4 Vehicle Systems Integration

Vehicle Systems Integration (VSI) is a research programme by the UK MOD [90]. It aims to identify and develop open standards for vehicle architectures and form and maintain close links to domestic and international vehicle research communities to enable effective and state-of-the-art vehicle research.

2.5.4.1 VSI Metrics for Electronic Architecture Assessment

To ensure future battlefield vehicle design integration and interoperability, the VSI program has developed the VSI Standards and Guidelines Metrics for Electronic Architecture Assessment [91]; a list of standards and metrics which can be used to test the level of integration and VSI compliance of a system. The metrics are derived by and are used to design vehicle systems by prominent Vetronics systems manufacturers, such as QinetiQ, BAE Systems, General Dynamics, Selex SAS, Ultra Electronics, Thales Air Defence and Thales Land & Joint; they define common standard by which any future vehicle system can be assessed in an objective manner [90]. Many of these metrics have also been incorporated into the current GVA 23-09 Standard.

The standards and metrics compliance study uses qualitative analysis of vehicle system's characteristics with the assessments being used to synthesise a quantitative assessment result. It focuses on the six key metrics: Reconfigurability, Enhanceability, Integration, Logistics Support, Scalability and Openness that are assessed on a scale of 0 to 5 in order to assess a system's compliance to VSI standards. The six metrics required for the compliance rating are calculated by assessing 15 distinct characteristics. The score for each characteristic is obtained by matching the performance of the system with a specific set of statements associated with each characteristic detailed in the VSI Standards and Guidelines document. Each of these statements has a score associated with it and the system scores

according to the statement that most closely resembles the actual performance of the system.

The **Reconfigurability** metric assesses the extent to which the system allows modifications on the fly. It is broken down into two characteristics, **Adaptability,** which is the ability to change like for like components in the field to meet short term needs and **Interchangeability,** which is the ability to interchange components from different platforms to meet short term needs.

The **Enhanceability** subsection assesses the extent to which major modifications to the system are enabled, such as the addition of new hardware and software, in this case RATs and RCMA. The subsection is broken down into three characteristics: **Capacity**, which measures the spare capacity available for additions to the system; **Modularity** is the measure of the extent to which the system can be upgraded and **Enablers,** which assesses the ease and availability of skills with which the system can be modified and upgraded.

Integration is the measure of how well the system is integrated with the rest of the vehicle platform and how well it communicates with other parts of the platform and the fleet. It is divided into three characteristics: **Internal Platform Data Provision** is the ability to transmit to and receive data from other architectures on the platform via the vehicle platform backbone. **External Platform Data Provision** is a measure of the system's ability to communicate with other platforms in the fleet. **System Control** is the level to which human or automated uses can access and controlled relevant resources of the system.

Integrated Logistics Support (ILS) is the measure of the extent to which the system supports vehicle platform logistics such as Health and Usage Monitoring, self-testing, etc. It is broken down into two characteristics, **Built-In-Test,** which measures how comprehensive the system can assess its own health and performance and **ILS data transfer,** which measures if the system is able to transport ILS data off the vehicle platform, i.e. via USB stick. Etc.

Scalability measures how the scalable the system is in response to increased performance demands. The metric is divided into two characteristics: **Vertical**

Scalability measures the extent to which additional resources can be added to the system; **Horizontal Scalability** measures the extent to which elements can be added or removed in response to changing requirements.

Openness is a measure of the interfaces of the system in a systems integration context. It is divided into three characteristics: **Standards & Technology Selection** measures how closely the systems design follows the VSI metrics and guidelines, **Documentation** measures the quality of end user documentation of the system and Interface Control Documents (**ICDs)** measures the quality of the interface control document for the system.

2.5.5 Shared Data Models

Shared Data Models (SDM) are an emerging technology developed in an effort to integrate vehicle subsystems by creating a distributed shared contract which indicates to subsystems on a vehicle platform where all available information about these subsystems is stored. "A data model is a wayfinding tool […], which uses a set of symbols and text to precisely explain a subset of real information to improve communication and thereby lead to a more flexible and stable allocation environment" [92]. The purpose of this common agreement is to share information between subsystems and thus improve interoperability on the platform level as well as the fleet level. SDMs are an efficient way to share information between vehicle subsystems as well as vehicles in the network and thus significantly reduce the amount of redundancy in the vehicle system. Being able to access an SDM also reduces the amount of traffic overhead, since information can be accessed from the SDM directly. By increasing the use of modular systems, modules can be easily replaced and upgraded without a negative impact to the rest of the system.

2.5.5.1 GVA Data Model

The Generic Vehicle Architecture (GVA) [87] data model approach is a platform level data model implementation currently under development by the UK MOD. It provides intra-vehicle communication between the increasing number of discrete and modular systems in modern vehicles. Modular systems provide the ability to easily upgrade or replace components in the case of damage, but also introduce increasing

complexity in military vehicles. Specifically the Object Management Group (OMG) Data Distribution Service (DDS) [93] middleware is an implementation that enables sharing of information between subsystems with the use of publish and subscribe relationships. For example a communications controller on a vehicle equipped with a number of wireless transceivers and access to the rest of its vehicle platform will subscribe to topics, such as *radio.throughput*, *radio.range*, as well as *nav.location* or *nav.velocity*. Upon reception of the subscribe request, each radio is required to publish up-to-date information about itself depending on the mode of subscription agreed upon.

The UK MOD specifies that in modern vehicle architectures that the GVA Data Model "shall be used to define all functionality and messaging across the infrastructure" [87]. Therefore the GVA data model is to be used as the primary communications infrastructure on all near future battlefield vehicle platforms. The Foxhound [10] is the first GVA Data Model compliant protected patrol vehicle and has been tried and tested in recent UK operations in Afghanistan [94].

2.5.5.2 Land Open Systems Architectures

Through Land Open Systems Architectures (LOSA) [95, 96], the data model concept is being expanded to the fleet (system of systems) level (see Figure 2-2), enabling platforms to publish and subscribe to topics published by other vehicles and even their subsystems. Thus if one vehicle's communications controller needs to know its neighbour vehicle's location, it simply subscribes to a topic like *vehicle(i).nav.location*. This way a whole fleet can be more interconnected, information sharing vital for situational awareness is facilitated and interoperability is enhanced.

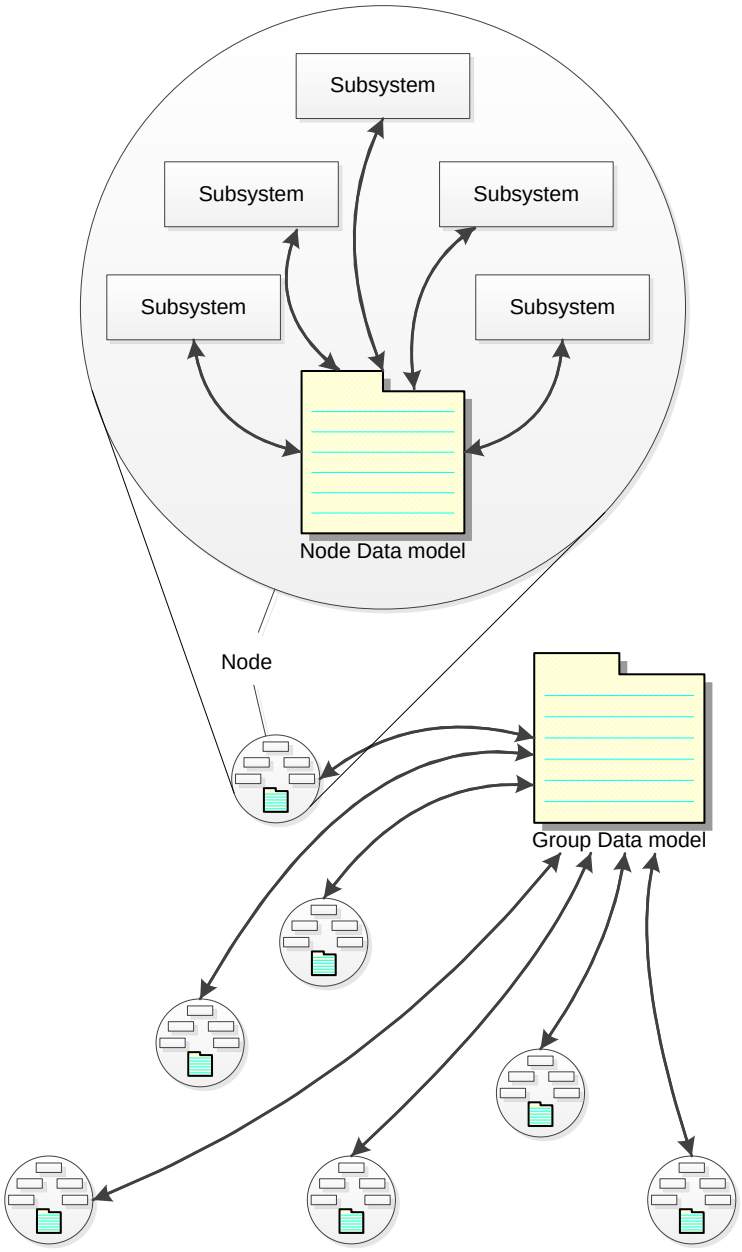

Figure 2-2 Data Model, Node Level vs. Fleet Level

2.6 Conclusions

The ability to relay information is now considered one of the most mission critical capabilities of battlefield assets. An increasing focus on data gathering and information sharing results in modern military forces which are increasingly reliant on wireless communications. This communication is fundamentally enabled by a variety of wireless technologies and the topologies they build. Preserving the integrity of these networks is therefore crucial, however, the wireless spectrum is

inherently dynamic and unpredictable, unintentional and intentional interference as well as the risk of equipment failure and damage makes wireless networks inherently unreliable.

Battlefield networks are required to operate in a wide variety of environments with a wide range of dynamically changing requirements. Mountainous terrain, dense foliage, adverse weather conditions and other factors significantly influence the performance of wireless networks. The Urban battlespace presents the most challenges to wireless communications, since in a 3-dimensional battlefield the wireless system has to penetrate walls of buildings and tunnels. Battlefield networks have to be resilient against intentional interference from jamming devices. Their implementation must be lightweight enough to enable personal area network applications as well as scalable enough to stretch over many kilometres. Battlefield networks must simultaneously provide high throughput for video applications, low latency for real time tele-operation and a high safety and security level for mission critical data. Battlefield networks have to operate on different types of nodes and remain highly scalable. They can be comprised of as little as two stationary sensor nodes or vast swarms of autonomous platforms. To enable the inevitable growth of unmanned nodes in the battlefield, wireless networks need to accommodate a growing number of increasingly complex nodes while remaining reliable and dependable.

The armed forces are increasingly adopting a Commercial off-the-Shelf (COTS) philosophy. Faster innovation cycles driven by highly innovative industries provide hardware closer to the state-of-the-art. The commercial sector is not only supplying a large amount of the electronic devices on the battlefield, but is also ever accelerating the development of military grade equipment. Mass production of equipment fit for both civilian and military applications and the resulting economies of scale result in significant cost savings. Competing COTS standards promote diversity and as a result, a large number of different Radio Access Technologies (RATs) are available today, each with different strengths and weaknesses.

Future technologies such as 5G, 802.11ac and Software Defined Radio (SDR) show great promise to match future capacity needs. Although still in its infancy, SDR is an

emerging technology which has great advantages. It is very flexible, it can be reconfigured or upgraded instantly by reprogramming and it is not physically limited to a specific operating frequency. This makes SDR a powerful enabler for multiband communication systems.

Although diverse in their properties, fundamentally all RATs share common key performance characteristics. They are a means to exchange data with certain other nodes in the network with a certain performance characteristic, they can thus be characterised accurately through a set of performance metrics such as Type, Throughput, Latency, Protection, Error Rate, Resilience, Range and Power Consumption, etc. This way a wide range of RAT can be represented by black boxes with predefined interfaces, which can be used to increase compatibility and enable the effective management of current and future RATs.

Novel fleet level distributed systems such as Mobile Ad-Hoc Networks (MANETs) have many advantages, such as increased range through multi-hopping and self-configuration in an infrastructure-less environment. MANETs have been specifically designed for highly dynamic topologies and their distributed and redundant nature improves reliability and provides increased resilience to attacks.

Emerging technology management approaches dictate a strong drive toward standardisation, modularity and interoperability of battlefield platform systems. Modular and interoperable systems reduce costs, enable rapid upgradability and repair capability using standard components and assure a degree of future proof vehicle design. Data centric approaches such as Shared Data Models (SDM) are now mandated across all near future battlefield vehicle platforms to provide fleet-wide information sharing and increased interoperability through data centric communications, opening up a wealth of application layer contextual information to be exploited to improve wireless reliability. Integration assessments such as the VSI Standards and Guidelines can be used to ensure that novel vehicle systems are able to integrate with other systems and reap the benefits from this integration. It is therefore advisable to subject any new vehicle system to the VSI metrics and guidelines assessment.

In order to satisfy diverse and conflicting performance requirements it is necessary to exploit the strengths of a wide range of RATs. Traditional communications technologies, such as Bowman are unable to fulfil the increasing QoS demands alone. A platform level management system is required which can use many concurrent heterogeneous RATs more effectively by utilising different technologies in different situations depending on their properties.

Recognising that modern vehicle fleets are systems of systems, in addition to achieving better QoS on the platform level, increasing complexity must also be addressed on the fleet level. A two layer management approach is therefore necessary; managing the nodes in the network, in this case equipment on the battlefield and managing the communications equipment inside these nodes. These two layers are interrelated and any solution to providing appropriate QoS to communications traffic across the network must be harmonious across the layers.

Chapter 3 Resource & Capability Management

3.1 Introduction

As discussed in the previous chapter, battlefield networks are comprised of an increasing variety of vehicle platforms with diverse mission goals. These platforms are required to operate in a number of different environments and are equipped with a diverse set of Radio Access Technologies (RATs) with limited capacity to transport an increasing amount of more diverse data throughout the network.

In this context it is necessary to manage limited platform resources through understanding the equipment available and how this equipment is currently performing in order to operate it at its maximum effectiveness within the context of current platform and fleet mission goals.

Increasingly stringent requirements imposed by complex environments and mission goals require an application aware Resource and Capability Management (RCM) approach. In a modern battlefield context, mission success often critically depends on the right information being available in the right location and at the right time. Additionally, resources are not homogeneously dispersed amongst vehicles and capabilities are not required to be available equally throughout the fleet, therefore it is not enough for each vehicle to attempt to be individually best connected. As nodes in a network, heterogeneous vehicle platforms in a fleet must ensure that the right QoS is delivered to the right nodes in order to enable mission relevant capabilities of the appropriate platforms in the correct locations.

Modern vehicle fleets are systems of systems, consisting of numerous individual platforms, each equipped with its own communications equipment. A reliable battlefield communications infrastructure depends both on individual vehicle platforms receiving, transmitting and retransmitting wireless data as well as an intact network topology at the fleet level to carry the data to its destination reliably. It is therefore necessary that resources are managed both on the platform level as well as the fleet level. At the platform level it is necessary to manage resources in the form of interoperating subsystems; at the fleet level it is necessary to manage resources in

the form of co-operating platforms (see Figure 3-1). This chapter presents RCM approaches which aim to use these existing resources to create platform and fleet capabilities.

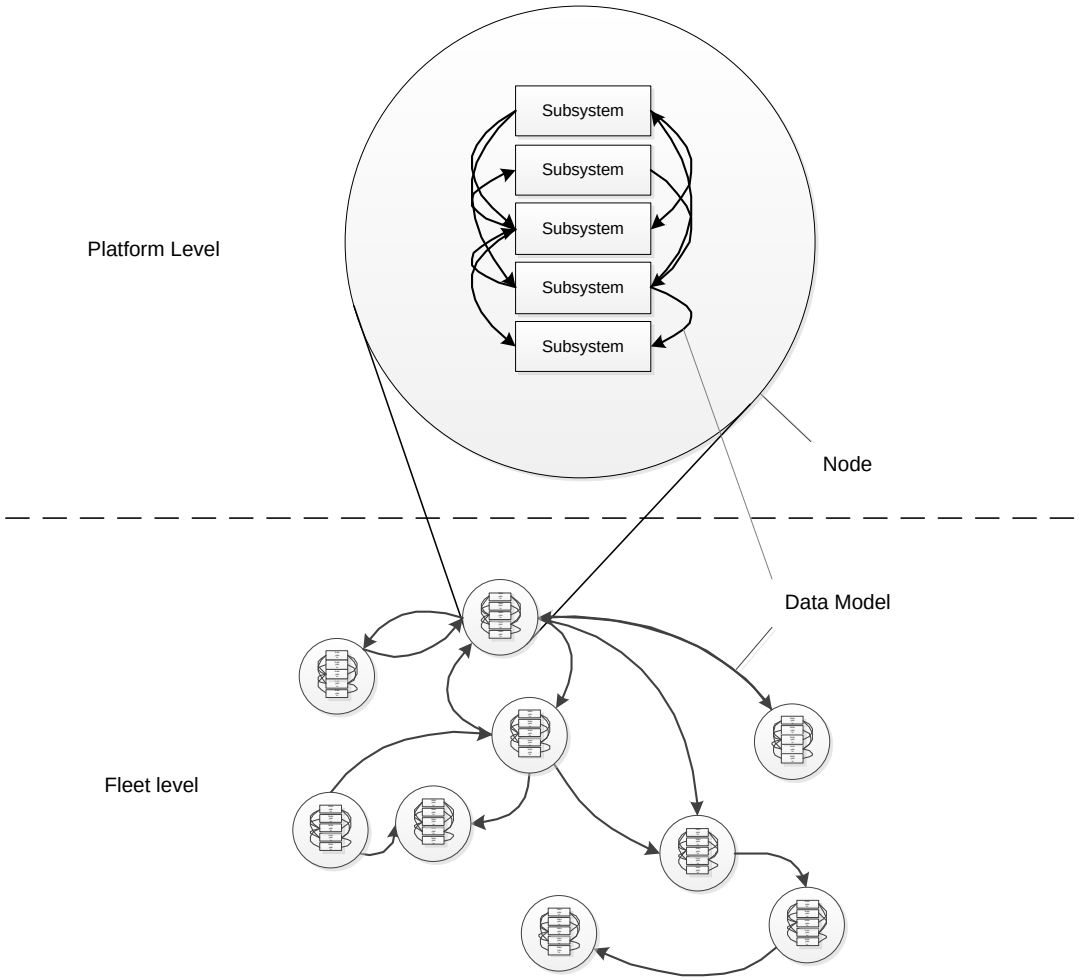

Figure 3-1 Platform Level vs. Fleet Level RCM

3.2 Platform Level Resource and Capability Management

Platform level RCM in a wireless communications context involves managing resources within a single node and its interconnected subsystems (see Figure 3-1) such as wireless communications resources, i.e. the array of RATs available within a vehicle platform, in order to satisfy prevailing traffic Quality of Service (QoS) requirements. This includes both the detection and performance monitoring of the communications equipment as well as the effective leveraging of this equipment by RCM Algorithms to achieve QoS goals.

3.2.1 Equipment Management

Platform level equipment management involves assessing, monitoring and managing resources in the form of equipment attached to the vehicle platform.

3.2.1.1 Equipment Management Events

Equipment management is vital for maintaining communications capability because the performance of any Resource and Capability Management Algorithms (RCMA) is dependent on the relevance and accuracy of the performance metrics it uses to base RCM decisions on, especially in heterogeneous networks [97]. Therefore in order for communications equipment to be managed effectively as a resource on a vehicle platform, the vehicle system must be aware of the type of equipment it has available and the equipment's performance.

As discussed previously, varying mission goals may demand that platform equipment be reconfigured. RAT equipment may be added to or removed from the vehicle. To support reconfigurability, a modern RCM system should allow RATs to be attached and detached seamlessly. Several events can occur which prompt the need for equipment management.

Equipment Installation and Upgrade Events

When new equipment is attached to the platform, other subsystems should be made aware of its presence. In vehicle platforms which are not highly integrated adding new technology may require designing custom hardware to ensure compatibility with the existing systems and specialised training of the crew.

Similarly when equipment is upgraded, for example by installing a more efficient antenna, or when a RAT's routing algorithm is changed for a more efficient algorithm, other subsystems must be made aware of this performance change.

Equipment Removal and Degradation Events

In the battlefield it is critical that RCM on the platform level reacts to equipment performance change by adapting its communications resource management

automatically in order to preserve communications capability. Therefore when equipment is removed by the crew, is damaged, or is degraded by environmental factors, other vehicle subsystems which depend on these resources must be made aware of the change.

3.2.1.2 Assessing Equipment

Automatic equipment management can be performed in several ways. The available equipment types and their performance data can be manually coded into the RCM system. Subsystems can be manually reconfigured to reflect added, upgraded, removed and degraded equipment; however, this approach is infeasible in a battlefield context. Not only does this consume valuable time and crew resources, manual coding of performance parameters is static and inflexible as it does not address changing RAT performance caused by environmental and mobility factors and therefore cannot provide current performance data to the RCM system.

Ideally equipment status change should be recognised automatically so that equipment can be added in a modular and plug and play fashion requiring little training of the crew. This enables seamless altering of a vehicle to provide mission critical capabilities when they are needed. In addition to the fact that algorithms are better suited to this task due to the wealth of performance data they can access, particularly in unmanned platforms, autonomous communications resource management is the only option.

Performance Assessment

On a practical level attaining current and relevant performance data requires measurement of the communications link's performance and automatic dissemination of the performance results.

The dissemination of this performance data can be performed over the data model, or by using dedicated hardware at each node. For example Ratliff et al. propose the Dynamic Link Exchange Protocol (DLEP) [98] which operates between router and modem and gathers link performance data by interrogating the modem and thereby monitoring the communication channel over time. DLEP units in each node of the

network then use a heartbeat to discover each other and communicate performance metrics of their respective communication links.

To facilitate compatibility with a wide range of current and future RAT, a performance data interface must be generic enough to allow for differences between technologies and be well defined in order to capture essential performance characteristics of these technologies.

3.2.2 Quality of Service Management

Given any range of available communications equipment, Quality of Service (QoS) management in a platform level RCM context involves leveraging this equipment to deliver appropriate quality of service to fulfil current traffic requirements at all times.

QoS management is vital for maintaining communications capability because in a dynamic network environment the communications resources, i.e. RAT performance changes constantly. Diverse and dynamic traffic requirements can only be sufficiently fulfilled by dynamically assigning resources. Therefore in order to use diverse communications technologies most effectively, a management system is needed which aggregates available resources based on their diverse properties and assigns them to fulfil current communications requirements appropriately. For example, on smaller, battery powered platforms the use of power efficient QoS management techniques becomes mission critical, whereas for a base station acting as a communications hub, overall throughput and resilience might be crucial QoS.

3.2.2.1 Multi RAT Management

Multi RAT management is performed by assigning diverse communications resources to transmit and receive diverse traffic types. When performing RCM on a multi RAT platform, two distinctions must be made:

Switched vs. *Simultaneous* use of radio resource describes the difference between selecting one transceiver at a time to transmit data and transmitting data on multiple transceivers at the same time.

Homogeneous diversity vs. *Heterogeneous diversity* describes the difference between using identical RAT types on diverse channels and using different RAT types on diverse frequency bands.

Switching Between Transceivers – Handover

To use multiple RATs effectively, traffic can be switched from one RAT to another based on prevailing conditions. This is called traffic handover and can occur from one channel to another on the same transceiver, between homogeneous transceivers on different channels or between heterogeneous transceivers on entirely separate bands. The goal of handover is to seamlessly roam between different networks [55, 99] while staying always best connected [100-103].

Handover can be performed both traffic independent and traffic aware [104], however, in order to achieve appropriate QoS for dynamic traffic it is necessary to take into account the properties of the traffic when making a handover decision. Handover can be an effective tool in managing communications resources, especially between heterogeneous RAT; however, handover is a major challenge for mobile and heterogeneous networks due to many diverse requirements and a very dynamic wireless environment [102].

A handover can be initiated for several reasons, such as changes in the environment or when the current access technology is no longer sufficient to fulfil all the necessary QoS requirements. Frequent neighbour changes may also result in a traffic handover; when one node replaces another in a given route, it may not be capable of using the same RAT and thus to continue using the same route, a different transceiver must be used to transmit the same traffic.

Managing conflicting traffic QoS is a major challenge for handover decision making. For example if certain time critical traffic needs to be transmitted with a high safety level, but no RAT with an appropriate safety level is available, the RCMA must make the decision whether to transmit the data with a lower safety level, satisfying the priority requirement, or whether to wait for resources to become available. For this reason the type of algorithm used to interpret and weigh these metrics has a significant effect on the handover decision. Different algorithms will produce

different results given the same problem, hence appropriate algorithms must be chosen depending on the desired behaviour of the communications system [105].

Simultaneous Use of Transceivers

The use of multiple concurrent transceivers can have significant performance improvements over switched RAT use, such as the ability counteract multipath fading and interference [28]. Diverse channels may be subject to different amounts of interference, improving the probability of correct data delivery on at least one of the channels. Simultaneous transmission can be used to improve throughput by adding the bandwidth of multiple transceivers together, an example includes 802.11ac [61]. In order to improve energy efficiency, fewer transceivers can be used during standard operation, only waking up multiple transceivers when it becomes necessary. For these reasons, although redundant multiband transmission effectively multiplies the cost of transmitting data by the amount of redundancy, it is still a highly valuable multi RAT management method.

Multichannel Transmission Using Homogeneous RAT

Multichannel transmission refers to the use of multiple homogeneous transceivers tuned to different channels in order to transmit data across the network (see Figure 3-2). Multichannel transmission is seldom switched, to exploit the benefits of multiple identical RAT, they are typically used simultaneously and thus are subject to all the performance improvements detailed above.

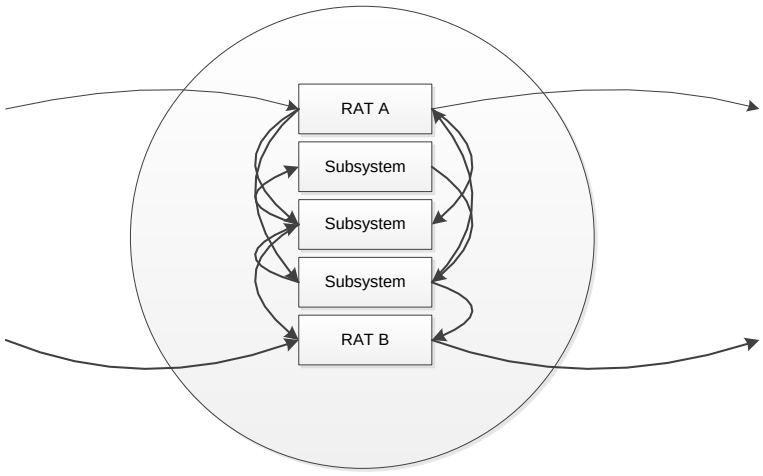

Figure 3-2 Simultaneous Use of Homogeneous RAT

As discussed, simultaneous multichannel transmission can improve reliability, however, since intentional external interference such as jamming and burst noise often occurs across a whole band and as opposed to a few select channels, multichannel transmissions still suffer from significant interference problems [26]. Internal interference is also a problem for multichannel communications, since even non-overlapping channels can interfere with each other [30], therefore care must be taken when managing homogeneous transceivers to avoid internal interference.

Multiband Transmission Using Heterogeneous RAT

Hardware redundancy is difficult to achieve in a radio system without the use of other physical transmission media which do not share a single wireless spectrum, however, a close approximation can be made with the use of multiple redundant heterogeneous RAT (see Figure 3-3). Similarly to homogeneous transceivers, heterogeneous transceivers can be used to improve resilience to interference and to transmit data redundantly. Additionally due to significant differences in RAT properties and performance, with appropriate RCM, other capabilities can be created; appropriate RCM of heterogeneous RAT can have significant performance benefits by choosing an appropriate RAT in the right situation.

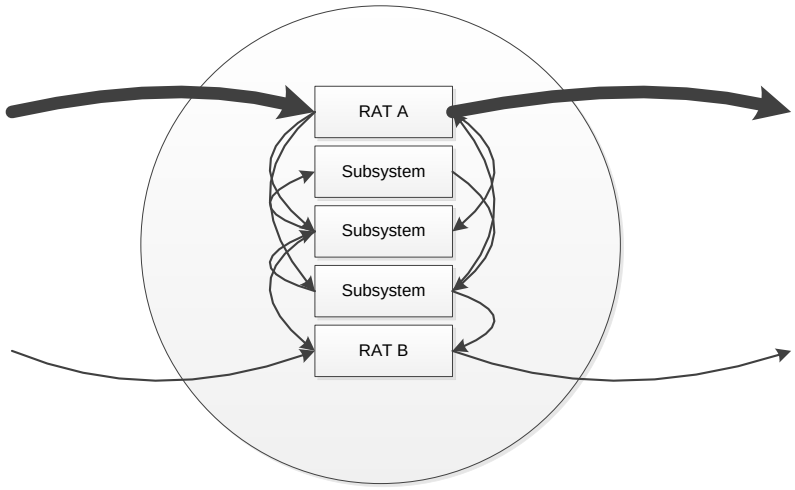

Figure 3-3 Simultaneous Use of Heterogeneous RAT

A vehicle platform equipped with multiple heterogeneous transceivers is able to provide appropriate QoS levels to various traffic types by transmitting each traffic type via a different RAT. E.g. traffic with high throughput requirements can be

transmitted with a high bandwidth RAT, traffic with a low delay requirement can be transmitted with a low latency RAT.

3.2.3 Related Platform Level RCMA - Existing Approaches

Resource management to achieve the behaviour described above, whether it is on the platform or the fleet level, is performed by algorithms functioning on the platform level. Fundamentally, all RCMAs use information they can gather in order to make decisions about how to best employ available resources in a given situation in order to create maximum capability.

Resource and capability management at the platform level is an intensely researched field. Many wireless transceiver management techniques, each with different advantages and disadvantages exist and the research is ongoing. Particularly the use of multiple heterogeneous wireless interfaces has been exploited to yield significant performance and reliability benefits. Due to the sheer wealth of different RCM approaches in existence, this related work section shall not serve as an exhaustive collection of the existing work, but rather a collection of management approaches relevant to this thesis.

3.2.3.1 Equipment Management

The Personal Computer (PC) system (including the operating system) is a common example of resource and capability management with future proofing through integration and modularity. Driven by consumer demand, PC hardware has a long history of standard interfaces, such as PCIe, SATA, USB, [106] etc. When new hardware is attached to a PC, a system of detection and negotiation determines the type of device attached, the speed it can operate at and the use of device drivers allow the interaction between the computer’s operating system and the attached hardware. Different interfaces have different performance characteristics, depending on the type of hardware attached, some interface, such as PCIe and USB are backwards compatible and are able to utilise older versions of the standards, albeit at a slower speed. Computer operating systems such as UNIX and Windows have access to driver repositories which provide device drivers when necessary. Using such an operating system, equipment can be added and subtracted, upgraded and

replaced seamlessly due to automatic equipment recognition and driver installation. This way the useful lifespan of a PC can be significantly extended.

While modem smartphones are typically an example of a hard-wired static implementation of a multi RAT platform, with Project ARA [107], google is developing a modular mobile phone prototype consisting of a Base Module which subcomponents attach to. Mimicking the app-store business model, project Ara allows third party manufacturers to produce subcomponents which integrate seamlessly into the base module. This approach allows the user to combine a variety of components with various performances in cost effective manner depending on the intended use of the device. Like any modern mobile phone, the device will be a multi RAT platform allowing access to heterogeneous communications technologies. Since the device is modular, the amount and type of RAT attached to the device is limited only by the operating system and the expansion capacity of the Base Module.

3.2.3.2 Decision Making

Policy Based Decision Making

Policy Based Decision Making (PBDM) is a decision making process to inform Multi RAT switching. The decision making is performed according to static policies informed by performance metrics, e.g. [at a specific time of day, use RAT A, otherwise use RAT B], or [if load exceeds 50 % use RAT A and B, otherwise use RAT B] etc. Any policy design relies on predictions and estimations of networking metrics. Generally it can be said that more accurate metrics will enable more accurate policy behaviour.

In networks with highly predictable loads, requirements and congestion patterns, this is an effective method, however, for diverse and dynamic battlefield environments, such static policies are insufficient, since they only function within predefined parameters and are unable to adapt to unpredicted circumstances.

Multiple Attribute Decision Making

Similarly to PBDM, Multiple Attribute Decision Making (MADM) is a decision making process to inform Multi RAT switching. In an effort to select the most

appropriate RAT for any given data transmission MADM algorithms adapt their behaviour dynamically by comparing several RATs and making a decision about which RAT best suits current needs. MADM algorithms are therefore well suited to environments with unpredictable and dynamic requirements where handover decisions need to be made automatically and on the fly without previous knowledge of interference patterns.

Many different kinds of MADM algorithms are available. These algorithms often involve simple mathematical operations on attributes in order to compute a numerical result. For example simple additive weighting (SAW) adds multiple networking metrics together in order to compute a score for each network [108, 109] and Multiplicative Exponent Weighting (MEW) [109] performs multiplication of weighted performance metrics.

In some cases, abstract problem solving techniques are being used to arrive at a solution. Examples of this include: Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [110], which selects a handover target by choosing a RAT which is both closest to the ideal solution as well as farthest from the least ideal solution, Analytic Hierarchy Process (AHP) [111] breaks down a task into objectives, decision factors and solutions, Grey Relational Analysis (GRA) [112] compares networks to a virtual ideal network by breaking them down into subsections and relating it to the corresponding subsection of the ideal network. Like PBNM, MADM algorithms rely on accurate and relevant performance metrics to base their decision making on.

3.2.3.3 Switched RAT Selection

Multi Radio Failover

In order to improve reliability, Yoon et al. [113] propose a scheme which uses multiple heterogeneous radios in a redundant failover fashion. They show a significant improvement in reliability and overall throughput when using a secondary higher range, lower throughput wireless interface to fall back on when the primary high throughput, low range interface fails.

Context Based RAT Selection

Porjazoski et al. [97] propose an algorithm which performs a RAT selection of either a WWAN or a WLAN interface based on QoS requirements and node mobility. If the node is mobile and communications traffic is not required to be transmitted in a time dependent manner, then the WLAN interface is chosen, otherwise the system choses the WWAN interface. The algorithm achieves better performance compared to single metric algorithms.

Ansari et al. [114] propose an algorithm which uses dual radios on different frequency bands to significantly improve the communications system's power efficiency by dividing idle listening and burst transmission tasks between the radios. This way the algorithm, determines the amount of interference in a frequency band in order to be able to decide which channel to use.

Yang et al. [115] propose a MAC agnostic MAC overlay protocol called "Jello" that senses and occupies an unused spectrum without central coordination. This way Jello maximises spectrum use and achieves reduced interference by using isolated channels for multiple simultaneous radio transmissions.

Internetworking Standards

Internetworking standards such as ambient networks [116], Generic Access Networks (GAN) [117] and 802.21 [118] are designed to enable wireless devices equipped with multiple RATs to seamlessly roam between heterogeneous networks. They are mainly focused on roaming between cellular and WiFi networks and thus much emphasis is placed on the ability to transfer user data and account information. This is achieved with an authorisation, authentication and accounting service within the cellular network infrastructure [119].

Ambient networks aim to facilitate interoperation between heterogeneous networks by using a common control plane across these networks. To support legacy networks, the control plane also functions as a wrapper to abstract legacy network control parameters into the common control plane language. Ambient networks use a generic link layer to hide the complexity of the heterogeneous RATs, only exposing

certain management capabilities and context data to applications. Ambient networks perform spectrum and load management based on triggers, such as mobility.

Generic access networks enable seamless handover between cellular and other heterogeneous networks, commonly 802.11. This is achieved by using a GAN Controller within the infrastructure of the cellular network which manages the heterogeneous network handover.

802.21 “Media-Independent Handover Services” is an emerging IEEE standard aimed at enabling handover between heterogeneous technologies while providing a continuous session to the user. Although designed to facilitate completely heterogeneous handover, 802.21 also mainly focuses on handover between cellular and 802.11 networks. 802.21 provides generic interfaces between the RATs and higher layers, namely the media independent information, command and event services which allows higher layers to access limited information about the RATs, such as neighbouring networks, or to initiate a handover [120].

3.2.3.4 Simultaneous Multichannel - Homogeneous Transmission

Yonghoon et al. [121] investigate multi-radio access networks where a node is permitted to transmit data over multiple wireless interfaces simultaneously and concludes that parallel multi-radio access is superior to switched multi-radio access.

As discussed previously, homogeneous multichannel transmission is widely studied and employed. An example of homogenous multichannel transmission includes 802.11ac which is capable of transmitting data on up to 8 channels to increase its maximum data rate.

3.2.3.5 Simultaneous Multiband - Heterogeneous Transmission

Dawson-Haggerty et al. [27] confirm that the simultaneous use of multiple heterogeneous RAT has significant performance and reliability benefits. It enables higher data rates, resistance to scattering environments, such as urban battlefields and improves temporal variation and reliability; however, they also find that the increase of reliability is not a linear function of the amount of redundancy. Kodialam et al. [18] also show that reliability and performance improvement is limited this

way, for example there is little difference in performance between a 3-radio and a 4-radio device.

As discussed previously, an example of commercial implementation of heterogeneous multiband transmission to serve multiple users includes 802.11n which uses both the 2.4GHz and 5GHz band.

Multi RAT Load Balancing

In order to provide higher throughput, De et al. propose the iCAR system [122], a load balancing scheme between heterogeneous RAT which uses two separate radio interfaces to ease congestion in cellular systems. By employing a secondary ad-hoc interface to offload traffic from the primary cellular interface onto another cell in the network, the iCAR system has been shown to significantly reduce cell congestion.

To a similar effect, Luo et al. propose UCAN [123], an architecture that uses an ad-hoc network in addition to a cellular network interface to reroute traffic and hence increase maximum throughput of a node.

QoS Based RAT Selection

Yiyue et al. [124] use multiple heterogeneous RATs simultaneously to optimise the capacity of a platform by taking into account traffic QoS requirements and link capacity. By allocating different types of traffic with diverse QoS Requirements, such as audio and video data to different RAT with appropriate performance, the approach achieved significantly higher performance than allocating traffic at random.

Shu-Ping et al. [125] use multiple heterogeneous RATs cooperatively in an effort to maximise throughput and fulfil prevailing QoS requirements. By scheduling traffic across RAT on the mac layer, allowing concurrent transmissions to share RAT, the approach achieved a significant performance increase compared to assigning a RAT for each traffic stream.

Simultaneous Multi RAT Synergy

Danzeisen et al. propose Cellular Assisted Heterogeneous Networking (CAHN) [126]. CAHN uses a low data rate cellular network such as UMTS to bootstrap a connection and exchange configuration and timing data between nodes before transmitting high bandwidth data. CAHN achieves this by separating the signalling plane and a data plane into two distinct radio access technologies and exchanging configuration data and security credentials before connecting with higher bandwidth radios, such as WLAN. This way a significant amount of energy can be conserved by switching off high energy usage radios while remaining reachable by other nodes via the low energy consumption cellular radio.

This is an excellent example of capability trade-off and the fact that in the right combination, multiple heterogeneous radio transceivers can be used in concert in order to create a system that makes use of the attached RAT strengths, in this case throughput, while mitigating the weaknesses, in this case power use. However, it is sacrificing reliability by making the high power transceiver's connection contingent upon the cellular system's successful configuration parameter negotiation. If the cellular system fails, the high bandwidth capabilities remain unused because they can't be configured and the node effectively loses all of its communication capability through the loss of a single radio unit. Additionally, the dependency on a specific technology and the lack of hardware independence prohibits CAHN from being applicable to a largely infrastructure-less battlefield scenario.

Generic Link Layers

A number of Generic Link Layer concepts have been proposed in order to manage several physical interfaces in a single node [103, 127-129]. These approaches combine several homogeneous and heterogeneous RATs at the link layer and present higher layers with a single unified communications resource. Using several multi radio techniques, such as simultaneous multiband transmissions based on their performance properties, generic link layer can harness the benefits of multiple heterogeneous radios effectively.

Although Generic data link layers are an effective and elegant solution to the multi RAT problem, they obscure and hide communications resources from the application layer, thus limiting application level decision making to influence the use of radio resources based on current mission parameters.

Draves et al. propose a new routing metric to take into account channel diversity in a multi radio environment and virtualise multiple radios per node into a single virtual radio concluding that diverse channel selection is beneficial [30].

3.2.4 Limitations of Existing Approaches

3.2.4.1 Implementation in the Battlefield

The research suggests that RCM can leverage existing resources to achieve significant performance benefits; however, much of this research is not currently being implemented in battlefield applications. While many of the prerequisites already exist in vehicle platforms, they are not being exploited to achieve increased performance as per the examples considered here. Multiple radio technologies are already in use in the battlefield, but are not managed to operate in a simultaneous or redundant fashion [130]. Significant unused potential exists with RCM to use these resources much more effectively.

The custom and propriety nature of battlefield equipment has the effect that implementation cannot keep up with the development in novel technologies. The dependency on a specific technology and the lack of hardware independence prohibits many of the existing approaches from being applicable in modern battlefield vehicle platforms.

In the context of consumer technology, RATs are optimised for performance; equipment failure is acceptable. In the battlefield context however, equipment must be managed to degrade gracefully, therefore it is seldom possible to use any COTS hardware or software by itself without major modifications.

3.2.4.2 RCMA Flexibility

Resource And Capability Management as it is implemented currently is inflexible. RCM approaches are often designed in an independent and hard wired fashion on a low level without regard for more than one use case or application. This has an efficiency advantage; however, since the algorithms are not modular, they are not transferrable easily into the modern battlefield context where the environments, threats and technology are diverse and dynamic.

Whenever a new RCM approach is implemented it is necessary to redesign the whole communications subsystem. There exists a lack of an easy and convenient way to integrate novel RCMA into existing military technology in order to take advantage of state-of-the-art research in battlefield technology.

In many cases RCM techniques have mutually exclusive goals and behaviours which each apply to different situations. Applying them dogmatically, statically and individually is not appropriate for vehicle platforms which are expected to be useful over a long lifecycle where the facilitation of upgradability is mission critical.

3.2.4.3 Equipment Management

From an equipment management perspective existing approaches are widely managed manually and statically. Few systems are integrated; equipment and RCM are hard wired so that they can perform only a singular task.

Existing approaches are very brittle, as little regard is taken for hardware damage and systems often have a single point of failure. Many of the existing systems rely on specific hardware to function and few intrinsically support a variety of different RAT. When hardware failure occurs, the failed communications equipment cannot be swapped for a different type, since there is no hardware discovery and management system in place. If the system can be replaced at all, unless performing major reconfiguration of most systems, it is necessary to replace like for like.

As highlighted briefly before, an example of this is CAHN, which assumes the presence of a specific, omnipresent, low data rate cellular network such as Universal Mobile Telecommunications System (UMTS) to bootstrap the connection and

exchange configuration and timing data between nodes before transmitting high bandwidth data. While achieving gains in throughput-energy efficiency and availability the system is sacrificing reliability by making the high power transceiver's connection contingent upon the cellular system's successful configuration parameter negotiation. If the cellular system fails, the high bandwidth capabilities remain unused because they can't be configured and the node effectively loses all of its communication capability through the loss of a single radio unit.

Existing approaches do not account for hardware upgrades, vehicles are assumed to be steady state. When a vehicle platform cannot perform its tasks sufficiently, due to hardware limitations, few facilities exist to upgrade the vehicle's equipment. In most cases additional RAT cannot be added to improve performance. If an additional communications resource is added to a vehicle platform it must be equally standalone or if it is integrated with other systems this prompts a major redesign of the vehicle architecture.

Currently no approach exists which is capable of managing the necessary range of present and future vehicle platform equipment dynamically and in a modular fashion while considering the stringent requirements of the battlefield environment.

3.2.4.4 Application Awareness

Although some algorithms such as [97] takes into account application data such as node mobility, few existing platform level RCM approaches are sufficiently application and context aware for a battlefield context.

Internetworking approaches such as 802.21 [118] are promising candidates to enable roaming among heterogeneous networks, but their lack of sufficient context awareness and their reliance on an infrastructure makes them unsuitable for battlefield operations.

The use of application level context and performance data is useful to modern battlefield vehicle platforms since many RCM are influenced by application layer factors, such as mission awareness, vehicle awareness, situational awareness as well as specific characteristics of the RAT, e.g. detectability, object penetration, etc.

Vehicle platforms equipped with RCMA that have mission awareness and situational awareness, could be capable of planning resources based on mission duration, adjusting transmission power based on the geographic location of neighbours, etc. Future battlefield vehicle platforms will need to use context and application data in order to fulfil their mission goals.

Existing approaches largely ignore the fact that vehicle platforms have other tasks besides communicating with other platforms and assume total control over all vehicle resources without considering mission goals, power states or other resource constraints. Many existing approaches only utilise a very limited and specific set of low level metrics, such as latency, power consumption and link quality because they do not reside on the application layer.

3.3 Fleet Level Resource and Capability Management

In addition to platform level equipment management, resource management on the fleet level is a powerful tool to improve the effectiveness of battlefield networks. Fleet level awareness can enable RCMA to redistribute resources to where they are needed, not only within a single vehicle, but for a whole group of heterogeneous vehicle platforms in a battlefield to create the maximum amount of capability from the resources that are available at any given time.

To enable resource management on the fleet level, services must be provided on the node level. For example if the goal of a fleet level resource management algorithm was to redistribute resources geographically in some fashion, cooperating platforms in the fleet need to provide services to detect these resources, assess their performance, provide information to the algorithm about the current distribution of resources and provide an interface for the algorithm to affect the cooperating platform's behaviours, i.e. to move platforms to new, more optimal locations.

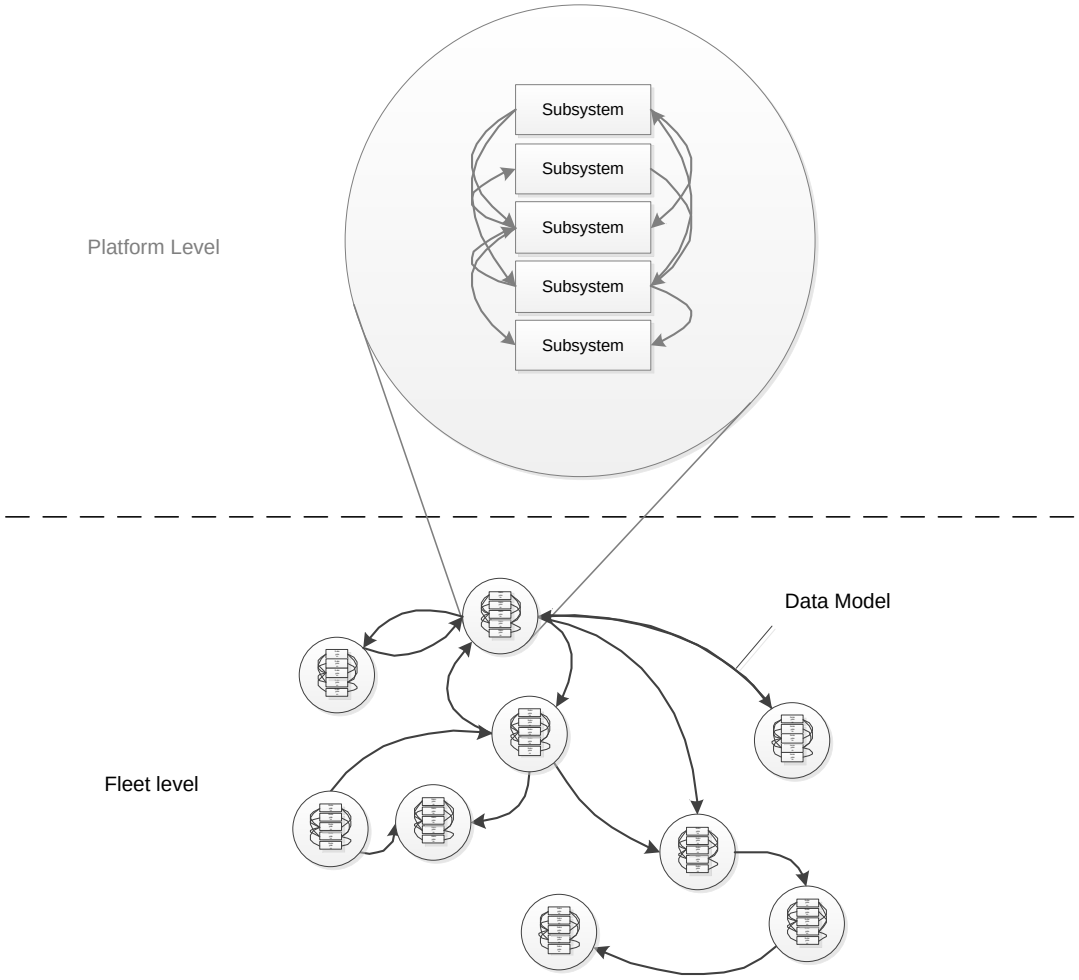

Figure 3-4 Fleet Level Resource and Capability Management

Any resource and capability management system contained within mobile platforms in a battlefield would ideally have an application level of awareness with access to application level data to achieve this goal. Data models are an example of a technology capable of dispersing such data seamlessly throughout multiple vehicle platform types that enables application level awareness (see Figure 3-4).

3.3.1 Topology Management

Topology management involves actively modifying a network's topology to achieve certain mission goals.

The ability to communicate is one of the most crucial capabilities within modern vehicle fleets, as it subsequently enables myriad other capabilities. Therefore maintaining reliable communications in a battlefield context is a mission goal in

itself. It is therefore logical that the full range of capabilities, such as mobility, weapons, etc. are deployed in order to achieve this goal. As such, any platform that is performing a task towards a goal that is of lower priority than the maintenance of the network should be re-tasked to topology maintenance duty if required. Using state-of-the-art Topology Management Algorithms (TMA) it is possible to modify the network topology to achieve these goals in a logical manner.

In a fleet comprised of mobile nodes, providing appropriate QoS to the appropriate parts of the network is a challenging task. Mobile nodes frequently move in and out of range of each other and depending on relative velocity between nodes, links can rapidly degrade from full signal strength to disconnection. Without actively influencing the topology with the use of TMAs, routing tables quickly become outdated and previously viable routes become broken. Awareness of node location and velocity is central to RCM in this context.

Furthermore, to manage QoS in modern vehicle fleets comprised of heterogeneous nodes, it is necessary to take into account application layer information such as whether a node is manned or unmanned, current power constraints and installed and available RAT diversity. In a fleet comprised of vehicles with diverse mission goals and capabilities it is not always beneficial to optimise overall QoS in the fleet. Depending on the importance of individual vehicles in the fleet to complete these mission goals, it is critically important to create a topology which provides a higher QoS to these nodes, even at the cost of providing lower QoS to other nodes.

3.3.2 Topology Optimisation

Topology optimisation consists of using TMA to provide improved QoS by adjusting the network's topology. By analysing performance data of the network and identifying bottlenecks, such as areas of low connectivity, a TMA can compute an improved network topology and relocate certain nodes to achieve significant performance improvements where they are necessary. TMAs can be used take advantage of node mobility to create self-healing and self-configuring networks by instructing certain nodes in the network to relocate to more advantageous location in an effort to improve network QoS or replace failed nodes in key positions.

3.3.2.1 Reliable Nodes

In order to mitigate unintentional and intentional node failure, some networks use a number of “reliable nodes” as a dependable network backbone. This involves the introduction of a number of nodes held by persons or mounted on vehicles which are subject to stringent requirements and therefore assumed to be reliable. Thus when the network consists of a certain density of these reliable nodes, it can be assumed to be reliable [6]. Although diverse vehicle platforms in the battlefield can be treated as more or less reliable, absolute reliability cannot be guaranteed for any node in a battlefield context.

3.3.3 Topology Repair

Topology Repair consists of the restoration of a network topology in case of a node failure event. Battlefield networks operate in very challenging environments; therefore, damage to nodes is common. Dust, moisture, weather events etc. are all sources of random and unpredictable node failure. Such random failure has a limited effect on the network; it typically does not raise the probability of subsequent node failures.

However, in some circumstances, damage to a node may be the result of an attack. Detecting these cases is crucial in order to avoid subsequent damage to more nodes and prevent further weakening of the network infrastructure.

To the rest of the network, a failed node typically only appears as a node which no longer responds to communication attempts, there is often very little data to decide whether a node has failed or is only temporarily unavailable, or whether the failure is random or due to an attack. However, if multiple nodes in an area experience low QoS or fail in close succession, it can be assumed, that there is agency behind the failure, especially if other nodes which are sent to replace the node also fail.

3.3.3.1 Types of Failure

Failure of vehicle platforms in a battlefield network can significantly reduce a network’s node density, making fewer paths available and thus weaken the overall topology and communications capability. Mesh networks with a low density can

only suffer a limited number of node failures before the network becomes segmented, therefore the reliability of a mesh network is proportional to its node density and the number of available network paths. For these reasons, equipment failure must be detected as part of RCM on the platform level, so repairs to the relevant components of the platform can be performed quickly and the platform's communications capabilities can be restored.

In some cases when a node failure occurs, the topology need not be modified due to other available redundant routes in the network. Similarly to using local redundancy on a platform level, fleet level redundancy can also be exploited for the purposes of increasing the probability of successful packet delivery. Particularly in mesh networks such as MANETs, it is possible to increase reliability in wireless ad hoc networking using techniques, such as multipath routing [6, 131] where a message is transmitted and forwarded on multiple redundant routing paths throughout the network (See Figure 3-5).

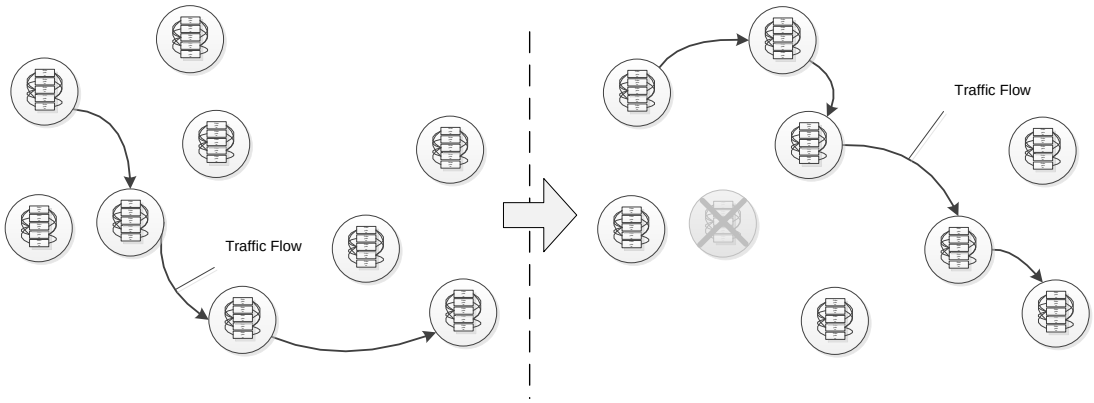

Figure 3-5 Redundant Routing

In extreme cases the destruction of several key nodes in the network leads to a complete division of the network into multiple disjointed subnets. This is one of the least favourable outcomes, since it means not only a reduction in QoS which could be mitigated on the platform level using prioritisation of critical messages, etc., but a complete lack of communication between subnets (See: Figure 3-6). As described previously, clustering algorithms are able to network these subnets locally so communication is still possible within the partitions, but communication between the subnets is disabled.

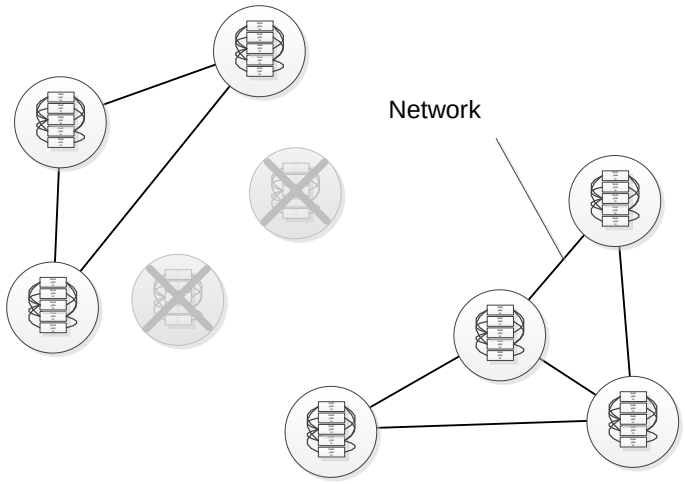

Figure 3-6 Network Segmented by Node Damage

In the event of a network being separated into multiple subnets, using TMA, the disjointed parts can be reconnected in two ways, either by using a dedicated relay or by swarm healing, thus changing the entire topology. In order to reconnect the two subnets efficiently, knowledge of the last known locations of the nodes in the other subnet and their status is required.

3.3.3.2 Swarm Topology Healing

A Swarm Topology Healing TMA analyses the network and computes a more optimal network topology of all nodes in the network (see Figure 3-7). It then relocates nodes to different coordinates in order to reconnect the disjointed network and improve overall connectivity. Depending on mobility and resource constraints a swarm TMA may relocate all nodes, or only some of them to preserve resources.

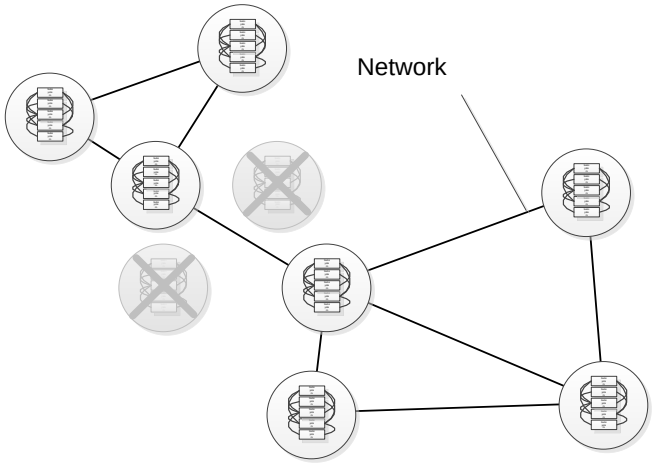

Figure 3-7 Swarm Topology Healing

3.3.3.3 Dedicated Relay Placement

In some cases networks are designed to employ surplus nodes solely for the purposes of network repair. In a situation where wireless nodes are unable to move or when a change in position would be disadvantageous, under certain circumstances, a TMA can assign a dedicated relay to reconnect the network. In this case, additional nodes not previously present in the network are dispatched in order to supplement the topology in an event of node failure. Relay node placement TMA may either dispatch nodes to simply replace the failed node, or compute a new, optimal location for the new node (see Figure 3-8). Relay node placement may be the only option in networks with a low node density, i.e. when there are not enough functioning nodes to take over the tasks of failed nodes, or when the nodes in a network are not mobile.

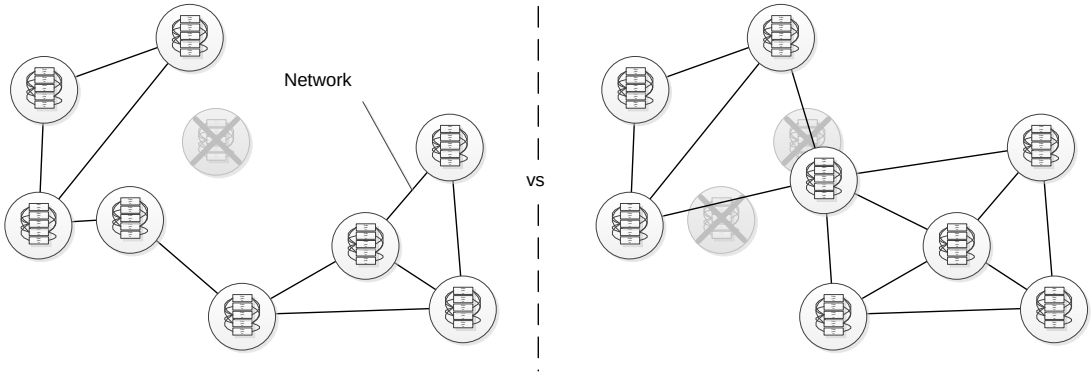

Figure 3-8 Node Replacement vs. Optimised Node Replacement

3.3.3.4 Proactive vs. Reactive Topology Repair

Topology repair can be performed in either a reactive or proactive fashion. Reactive TMAs only attempt to change the network topology in the event that QoS delivery becomes insufficient. Proactive protocols will adapt the network topology and provision additional nodes in the network in anticipation of insufficient QoS or a fault. Although proactive TMAs have great potential to pre-emptively redistribute resources to where they are needed, they have several drawbacks. Since battlefield network QoS is typically unpredictable, proactive TMA can be very wasteful. If node damage is non-random and affects an area equally, proactive TMAs cannot prevent damage to the network, because the nodes which have been proactively placed in strategic locations to serve as redundant nodes will likely also have been

destroyed due to being in the same area. Reactive topology management will still be necessary to adapt the network to reconnect nodes in damaged areas.

3.3.4 Capability Management

In addition to managing resources, it is also necessary to manage capabilities on the fleet level. Similarly to the emerging of platform capabilities from the cooperative use of platform resources, NECs can be the result of cooperation between vehicles in the fleet.

The close integration of information gathering capabilities through sensors with decision makes and weapon systems are crucial in creating support capabilities necessary for modern battlefield fleet operations [132]. Examples of this include:

- Increased survivability in urban reconnaissance by dismounted soldiers through the use of lightweight UGV providing Local Situational Awareness (LSA).
- Highly targeted long range strikes through accurate UAV targeting data.
- Long range dismounted soldier travelling enabled by an autonomous pack mule.
- Increased safety in convoy operations through early danger discovery by a scout UAV ahead of the convoy.
- Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) requires a communications relay to transmit any gathered intelligence to where it is required.

Many of these beneficial group relationships emerge when pairing manned and unmanned nodes, since they have fundamentally different properties, strengths and weaknesses [36].

In order for NECs to be created, participating platforms need to be present at their required location in order to collaborate with other nodes in the location. When an NEC is created by grouping several nodes together, each node in the group contributes towards a shared group capability and the loss of certain platforms in the

group impairs this (see Figure 3-9). RCM on the fleet level must be aware of these synergetic relationships between platforms in a group.

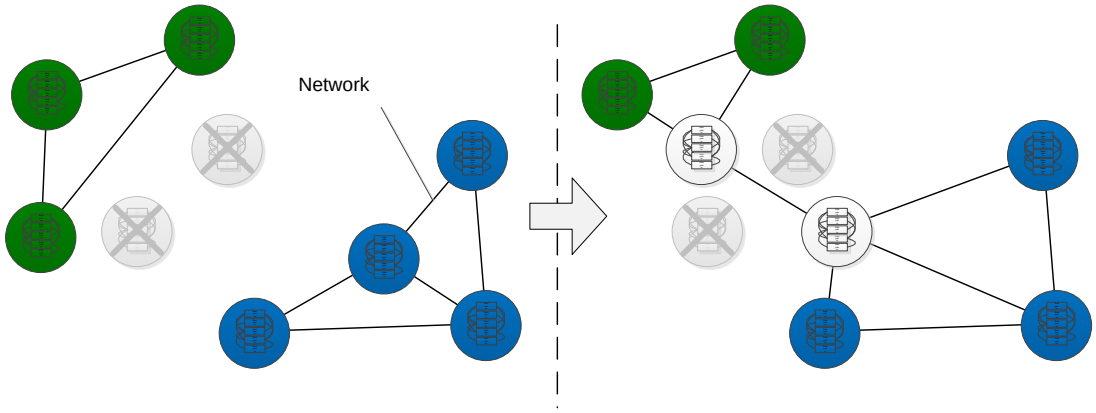

Figure 3-9 Topology Repair Affects Group Capability

3.3.5 Related Fleet Level RCMA - Existing Approaches

The fleet level RCM related work can be divided into two broad topology management techniques: topology optimisation and dedicated relay. While topology optimisation seeks to improve overall network integrity by utilising existing nodes in the network, dedicated relay algorithms generally assume that nodes in the network are stationary and new relay nodes are introduced into the network with the sole purpose of restoring a partitioned topology [133, 134].

The introduction of new relay nodes into the network is not always feasible from a resource perspective, however, in some cases when the network's node density is low or when it is comprised of mostly non-mobile or non-available nodes it may be the only option. Relay node placement is either performed based purely on the geographical locations of nodes, or by also taking route QoS into account. Topology management, which aims to repair segmented networks and improve overall performance is subject to ongoing research [133-140].

3.3.5.1 Topology Prediction

When attempting to predict geographic node movement, any map of a network has to be constantly revised and rebuilt through node discovery, which makes node mobility prediction very challenging. Baburam [141] addresses this problem by predicting the future geographic location of any given node in the network based on

its velocity vector, so that messages can be routed to a predicted node location, instead of the last know node location. Although geographic routing can in this case increase a MANET's packet reception ratio significantly the network still exhibits a large packet loss.

3.3.5.2 Overall Topology Optimisation

When a network becomes partitioned, a common approach for topology optimisation, as seen in RIM [142] and DARA [143], is the use of cascaded relocation where a node travels towards the position of a lost node or a gap in the network in order to replace the failed node and re-establish communications between network partitions. Gaps created by the repair nodes are subsequently filled by other repair nodes and so the network ripples, or cascades to an equilibrium.

3.3.5.3 Targeted Topology Optimisation

In order to deliver improved QoS to high priority nodes, Senel et al. [144] classify nodes depending on the function they serve. Nodes which serve a routing function are classified as dominators and nodes which are not relied upon by other nodes are designated as dominatees. In the event that the network becomes partitioned, the sub-network's dominators share an equal load of populating the gap between the partitions.

Grandi et al. [145] use consensus between multiple nodes equipped with laser range finders to manoeuver a group of mobile nodes through terrain obstacles while optimising the topology in order to maintain a compact group. The algorithm maintains a line of sight between nodes and ensures an optimal topology for wireless communication within the group.

3.3.5.4 Topology Repair

Lee et al. [146] and Akkaya et al. [147] recognise that node failure in inhospitable environments is not always random and localised to a single node, but may cause node failure in an area.

Lee et al. [146] propose an algorithm which introduces relay nodes in order to recover from such a large scale node failure, which partitions a network topology. Additionally, their algorithm creates a fault tolerant topology by producing a ring network which ensures that connection is redundant in an effort to make the network resilient against future failures.

3.3.5.5 Repair Node Selection

In a scenario where a node in the network needs to be replaced due to failure, instead of repairing the network by changing the topology in a cascading fashion, a single node may be chosen to replace the failed node. In this scenario it becomes necessary for a node selection algorithm to decide which node in a pool is chosen as the replacement node. This node selection can be based on a variety of metrics; repair nodes can be chosen at random, based on their proximity to the failed node or other factors.

While most TMA assume absolute control of all nodes in the network with little regard for the role the node is playing in the network beyond its communication function, algorithms such as C2AM [135], PCR [136], PADRA [137] and NORAS [138] take into account application layer data and seek to only exert control appropriate to the situation.

In order to decide which node is selected for network repair, PCR and PADRA base their node relocation on the importance of the node in the network. NORAS considers node criticality to connectivity as well as the importance of the geographic coverage it provides to its current location. C2AM considers the importance of the node's current task and favours nodes with less important tasks for relocation. To perform this node selection the least important node is chosen within a certain radius. NORAS and C2AM consider node criticality in a 2-hop distance, PADRA in a 1-hop distance around the failed node.

3.3.5.6 Resource Preservation

In fleets comprised of nodes with stringent resource limits, any topology management benefit must be weighed against the resources expended in the process.

Several algorithms attempt to improve resource efficiency by minimising the distance travelled or resources used [133, 134, 139, 140, 147].

For a comprehensive review and a discussion of current Fleet level RCMA, see Younis et al.'s survey paper [148].

3.3.6 Limitations of Existing Approaches

RCM on the fleet level, such as repair node selection, resource preservation and topology optimisation is well researched but many limitations still exist.

3.3.6.1 Hostile Environments

Battlefield networks must be equipped to function within hostile environments, however, existing fleet level TMA typically disregard the danger posed by hostile agents. Much research exists to combat intentional interference and a crowded spectrum; however, hostile environments also pose other threats to network topologies, such as damage or capture. As found by Younis et al. in a recent survey paper [148], existing TMA assume any node failure to be random and without agency. No existing TMA take into account localised threat or damage to nodes in the network, or agency behind this threat.

While individual platform survivability is improved through situational awareness improved by a functioning communications network, the network topologies' integrity is preserved by having a sufficient number of mobile nodes in locations appropriate to the terrain. One critical method to prevent bottlenecks and network separation is to protect the network's nodes from damage and destruction. To achieve this goal, shared intelligence between mobile nodes on a systems-of-systems level, such as mission information, must be harnessed and any node mobility must be informed based on this information.

In a battlefield context involving autonomous platforms, hostile forces creating localised danger to network assets pose a significant threat to mission success. While techniques and approaches in existing algorithms vary greatly, the majority share one behaviour in common; in a repair situation where a TMA attempts to recover a fragmented network due to a node failure, existing approaches cause nodes to

converge on the failed node either in an effort to replace it, or bridge the gap with an overall topology adjustment. In a Battlefield situation, however, converging on the failed node is a potentially fatal behaviour. Node damage cannot always be assumed to be random; hence, there is a clear need for a TMA that accounts for areas of threat.

3.3.6.2 Assumption of Homogeneity

Similarly to the platform level, fleet level RCM also requires management of heterogeneity. Diverse platform types in the battlefield generate various traffic types, have a wide range of capabilities and subsequently require different QoS. However, while resource heterogeneity is a well-researched topic on the platform level, [18, 27, 97, 114, 115, 121-126], existing fleet level RCMA typically assume that nodes in the network are physically identical and interchangeable [142, 143, 145-147], at most differentiated by their current task or importance to the network topology [135-138]. As discussed in Chapter 2, real world collections of vehicle platforms and therefore the nodes they represent in a battlefield network are highly heterogeneous [36] and thus require widely different RCM approaches.

3.3.6.3 Mission Goals

Fleet level RCMA often lack graduation in the amount of control they have over the network resources, a recent survey on the matter by Younis et al. [148] finds that existing TMA do not consider the implications of relocating a node beyond the immediate importance of its current task. TMAs typically assume complete control of either a set of relay nodes [133, 134, 139, 140] or the network as a whole.

It is true that communications management and the preservation of effective networks is a high priority, which deserves to have significant resources devoted to it, however, each vehicle platform deployed in a battlefield has a purpose beyond the repair and management of communications networks. Each platform in a fleet may have different mission goals and priorities and it cannot be assumed that network topology management supersedes these mission goals in the sense that any node in the network is immediately, or at all available for relocation in the aid of network topology management.

Few algorithms recognise the need for application awareness in the sense that nodes usually have a task besides network topology management, one of the best examples of such application aware fleet level topology management algorithm is C2AM [135], which repairs fragmented network topologies while attempting to cause the least impact on the node's application level tasks, but C2AM only considers mobility readiness.

3.3.6.4 Context Awareness

RCMA must also be capable of using context application layer information to influence topology management decisions. Since any fleet level RCM is fundamentally provided by the platforms that make up the fleet, a level of cooperation is required between these platforms, however, a distinct gradient exists not only in the importance of nodes but also in the type of QoS they require depending on current platform tasks and their context.

In many circumstances overall network QoS can be improved by greedy communications management algorithms where each node attempts to maximise their communications capability and expects others to do the same. A more complex, but often beneficial approach in terms of QoS delivery to the appropriate nodes, is to focus on the goals of the whole network. However, in a modern vehicle fleet context, it is not sufficient for platform communications management systems to optimise overall connectivity in the network. In certain circumstances preserving the communications link from one platform to a single neighbour may be significantly more valuable that preserving communications to the rest of the fleet; for example, the connection of a UGV to the single dismounted soldier tele-operating the UGV may be more valuable than the UGVs connection to the rest of the fleet. Similar scenarios can occur when it is important to optimise QoS within specific regions of the network or within a certain group of platforms to enable mission critical synergetic relationships such as shared group capabilities within the group.

3.3.6.5 Platforms with Diverse Capabilities

Fleets comprised of diverse battlefield vehicle platforms have specific capabilities deployed in specific areas for a reason, i.e. a pack mule in close proximity to a group of dismounted soldiers. Any topology management must be aware of these capabilities and the role they play in the vehicle fleet. TMAs which reassign nodes based on limited data, such as movement cost and the node's current routing function are insufficient for modern battlefield topology management. Disregarding mission and capability data when tasking a node for relocation may have highly undesirable effects, such as removing critical capabilities from an area or unit, resulting in a capability defeating topology, potentially jeopardising mission survivability.

Mission critical capability may not be solely provided by a single node, but groups of nodes. Group Capabilities emerging out of the cooperation of a group of nodes must not be broken in an effort to "optimise" the network topology.

In a real world scenario, relocation of battlefield resources without awareness of their capability may break mission critical capabilities. For example, an autonomous pack mule only provides a shared group capability of carrying heavy loads over long distances to a group for Dismounted Soldiers (DS) as long as it remains within close proximity to its group (see Figure 3-10). In this case depending on mission data, although the pack mule may be the closest node to the disconnected network segment of Armoured Fighting Vehicles (AFV) and may have the highest mobility readiness based on movement cost and its unmanned status, if it is autonomously re-tasked to repair the network topology, it may have an unacceptable impact on its group's mission.

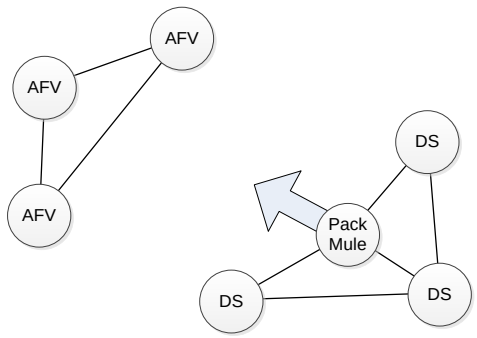

Figure 3-10 Topology Repair May Break Mission Critical Group Capabilities

Existing algorithms do not take into account application layer information, such as group capability and synergy between nodes. In an effort to improve overall QoS, these traditional TMA may inadvertently re-task nodes which are engaged in a cooperation that provides a critical capability to its local group.

3.4 Conclusions

Resource and Capability Management (RCM) is the management of available resources in an effort to create capabilities to fulfil the network's Quality of Service (QoS) requirements. For battlefield networks that are subjected to increasingly stringent requirements in a highly dynamic environment, autonomous RCM is suggested as a solution to aggregate available communications equipment and suitable RCM algorithms have to be chosen to manage this equipment to deliver appropriate QoS to communications traffic in the network.

From an equipment management perspective, RCM on the platform level must be capable of managing a wide range of present and future vehicle platform equipment dynamically and in a modular fashion. Highly flexible RCM capable of automatically recognising upgraded and replaced equipment can make use of currently available resources to best fulfil its requirements. Enabling seamless upgrade and reroll of battlefield platforms can also prolong the life cycle of a battlefield vehicle platform significantly, improving efficiency and saving costs. By providing standard interfaces where functionality can be added on demand, the use of fewer resources in strategic applications can yield a more effective fleet overall.

Automated QoS management is required for modern and future vehicle RCM. Using sophisticated RCM approaches it is possible to leverage existing resources to enhance communications effectiveness and create additional capabilities enabling reliable battlefield networks. Since different Radio Access Technologies (RATs) have different strengths and weaknesses, they can be used to best suit the current situation in order to mitigate different types of interference, improve QoS for high priority traffic, or preserve resources.

This way Existing approaches have used multiple homogeneous and heterogeneous radios to improve all aspects of network QoS. Algorithms like Cellular Assisted Heterogeneous Networking (CAHN) achieve the creation of synergy of heterogeneous RATs by acknowledging their strengths and weaknesses and using them to the platform's advantage to create a communications capability which is more powerful than the simple load balancing of the two RATs. RCM can benefit greatly by enabling algorithms which exploit such synergetic relationships.

Resource And Capability Management as it is implemented currently is inflexible. Resource And Capability Management Algorithms (RCMAs) are hard wired and any change to the RCMA often prompts a redesign of the whole communications subsystem. To take advantages of state-of-the-art RCMAs, technology transfer from the commercial and research sector should be facilitated by providing a framework which can easily integrate novel RCMAs into battlefield vehicle platforms. Within this framework, RCMAs should be interchangeable by providing predefined interfaces to performance data through black boxing any attached RAT as a standard communications interface.

As found by Younis et al. in a recent survey paper [148], existing Topology Management Algorithms (TMAs) assume any node failure to be random and without agency. No existing TMA takes into account localised threat or damage to nodes in the network, or agency behind this threat. In a battlefield context it is detrimental to assume that node failures, damage and degradation are always due to non-malicious causes. Disregarding the possibility of agency behind node failure events has the potential to cause significantly more node loss through subsequent node failures caused by the same agency. The fact that equipment is damaged or degraded should be used as information to inform the behaviour of the rest of the fleet and preserve other equipment. In this area of RCM there exists a significant amount of unused potential.

The assumption made by many of the existing approaches that all nodes in the network are homogeneous may be detrimental in a battlefield context. For RCM to be effective in delivering enhanced QoS where it is needed, it is crucial for modern RCM to account for heterogeneous battlefield resources which are not evenly

distributed throughout the network. Instead of optimising overall network performance homogeneously, modern battlefield networks require an RCM approach which is capable of delivering the right service to the right location and the right vehicle platform.

RCMAs may not in all circumstances assume complete control over all resources in the network for the purposes of network repair. In this sense RCMA performance is severely limited by the quality and relevance of the data it can access. The use of application level information, such as capability information, situational context and mission goals in RCM decision making is crucial. Performing topology optimisation without it may result in the creation of mission defeating network topologies.

Chapter 4 Battlefield Network Simulation Tool

4.1 Introduction

As discussed in the previous chapters, battlefield networks are required to operate in a wide variety of environments with a wide range of dynamically changing requirements. They are comprised of heterogeneous platforms equipped with heterogeneous Radio Access Technologies (RATs), which must be managed from the perspective of fleet level capabilities leveraged against mission level aims and goals.

Fulfilling the objective of this thesis to improve battlefield communications capability through improved management of existing platform and fleet level resources requires the development and testing of novel platform and fleet resource and capability management approaches.

The problem of designing and testing these novel approaches in a cost and time effective manner lends itself to a modelling and simulation toolset and methodology.

A recent think tank sponsored by the Defence Science and Technology Laboratory (DSTL) [3] and the Vetronics Research Centre (VRC) [4] has concluded that no adequate high level simulation tool is available which readily allows the modelling of the required functionalities within the problem space of a realistic battlefield environment.

Therefore this chapter presents the novel Battlefield Network Simulation Tool as the first contribution of this thesis. It forms the basis of the methodology used to develop and assess the proposed algorithms as well as future work in this problem space.

The simulation tool allows the user to develop algorithms under study both at the fleet and the node level, in this case allowing the novel Resource and Capability Management Algorithms (RCMA) presented in the following chapters to be developed and compared to existing approaches. The toolset provides a number of unique functionalities to simulate a realistic battlefield environment subject to

equipment damage, danger, hostile interference sources, etc. and allows the gathering of performance data of the algorithms under test.

4.2 Problem Definition

The problem to be solved by this contribution is the assessment of the performance of the proposed algorithms in a realistic battlefield environment. This involves the simulation of a fleet of vehicle platforms running the proposed algorithms and comparing them to existing solutions.

4.2.1 Advantages of Simulation

Assessing the performance of the proposed algorithms can be achieved with various methods on a spectrum of fidelity, complexity and cost. These methods can range from simple thought experiments and manual pen and paper calculations through software simulation to the actual prototyping and implementation of a fleet of vehicles in a real battlefield (see Figure 4-1). Since pen and paper calculations are insufficient to represent the level of detail and interaction required, and the building of a physical fleet of battlefield vehicle platforms far exceeds the scope and cost of this application, simulation was chosen as a trade-off between these two extremes. Simulation is the virtual representation of physical systems in software. Using simulation, a complex systems-of-systems scenario, such as a heterogeneous vehicle fleet can be modelled quickly while allowing performance measurement on a deep level, since it is possible to examine a simulated system at an arbitrary level of abstraction using a multitude of tools.

Although empirical results involving physical hardware are naturally higher fidelity simulation often provides sufficiently accurate results to negate the requirement for costly and time consuming prototypes.

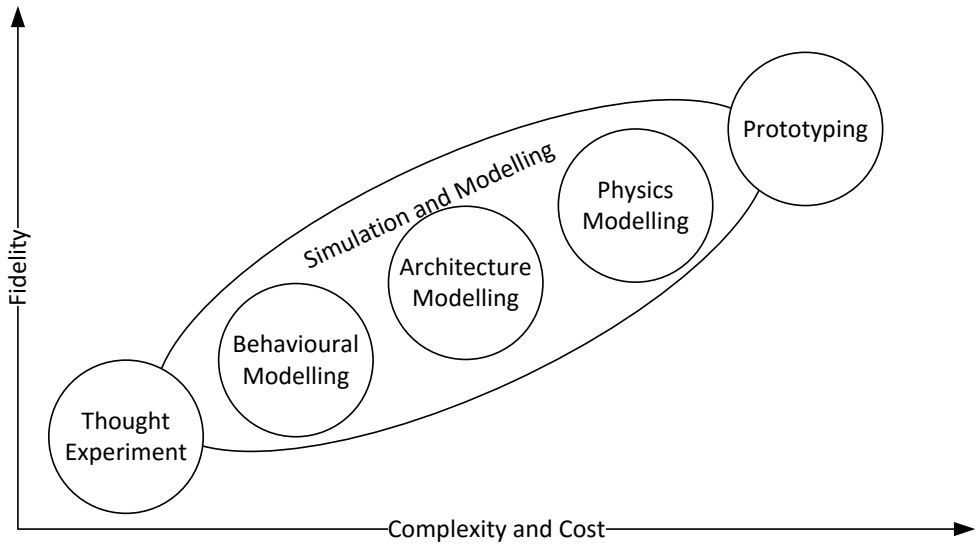

Figure 4-1 Spectrum of Complexity and Cost

In addition to drastically reduced cost and timeframes for analysis of battlefield vehicle fleets, a simulation is also much more flexible as it can be changed quickly and thus long lead times for physical implementation can be avoided. Using appropriate simulation techniques, the effectiveness of a novel system, as well as multiple alternative permutations can be assessed rapidly by changing parameters in the simulation environment. In this way a simulation also provides valuable early de-risking of vehicle platform systems.

As well as changes to the vehicle platform behaviour itself, a simulated environment can be changed in order to reflect challenges to the simulated environment. Examples include changes in prevailing weather conditions, the presence of obstacles and radio spectrum interference.

4.2.2 Aim

The aim of this contribution is to provide a method and develop tools for development, testing and performance metrics gathering of communications Resource and Capability Management algorithms in a realistic battlefield context.

4.2.3 Goals

The goal of this contribution is to create a toolset that allows the user to achieve the above aim by creating a simulation environment which enables the development, modification and iterative improvements of RCMAs in a battlefield context in order to achieve performance improvements over existing solutions. This toolset should fulfil a number of requirements:

- The tool should be able to model mobile vehicle platforms traversing a simulated battlefield and to simulate communication networks between these platforms using a variety of RATs.
- In order to capture the behaviour of the developed approaches within the realistic context of a dynamic environment with interference and unreliable hardware, the tool should account for these features and allow the user to model a hostile battlefield environment that causes a danger to vehicle platforms and damage to equipment.
- The tool should provide the user with the ability to model realistic and scalable battlefield vehicle fleets quickly and easily with provided functionalities to change the behaviour of these vehicle fleets in a straightforward manner.
- The tool should provide a high degree of flexibility during early assessment of the developed approaches so that changes and adjustments can be made during the development phase to better ensure that the proposed solutions are suitable in the context of the requirements of a complex battlefield environment.
- The tool should also allow the user to collect the measured results and provide storage and export facilities for further analysis of these results.

As a further goal, the tool should be validated using a known stimulus with a known set of results to ensure the correct operation and the reliability of the simulation tool.

4.2.4 Scope

The focus of the simulation is the modelling of vehicle platforms in a fleet from an application level perspective in order to enable the modelling and assessment of platform level and fleet level RCMA. Accurate modelling of layers below the application layer which are not necessary to produce a representative performance result in this context will not be considered. For this reason, routing algorithms are also outside the scope of this thesis. However, since the tool is designed to assess RCMAs in a Mobile Ad-Hoc Network (MANET) context, the functionality of the tool allows the simulation of MANET multihop communications using an implementation of the BABEL routing algorithm [78].

4.3 Modelling and Simulation Platform

4.3.1.1 Agent Based Simulation

Using an agent based simulation, each vehicle platform in the battlefield can be represented as an agent within an environment; the algorithms governing the behaviour of the agents can be contained within each agent allowing for realistic behaviour of individual vehicle platforms.

Agent based simulation is well suited to this application in particular, because once an agent has been created and given the appropriate behaviour, it can be replicated a desired number of times and positioned throughout the environment according to the chosen mobility model to simulate an realistic scenario with multiple vehicles traversing a battlefield communicating with each other based on the algorithms to be simulated.

4.3.1.2 Choice of Simulation Platform: AnyLogic

Many types of simulation platforms exist which can be used to build the tools required to achieve the above aims such as: OPNET [149], OMNeT++ [150], Ns2 [151], QualNet [152], NetSim [153], etc. From these simulation platforms it is

possible to create tools which are proficient at simulating mobile ad hoc networks and are therefore widely utilised for this task. However, the focus of this work is not the evaluation of low level networking metrics which these tools are specialised for.

The need to model heterogeneous mobile vehicle platforms equipped with heterogeneous resources and capabilities, both at the platform level and the fleet level in an expandable and flexible manner requires a broad approach using an Integrated Development Environment (IDE) with a high degree of flexibility.

Given the high level problem space and the anticipated need for high degree of flexibility, the simulation tools were developed using XJ technologies' AnyLogic [117], a Java based IDE, which allows for System Dynamics, Process-Centric and Agent Based simulation to be used in the same simulation. Java is an object oriented programming language which is powerful enough to describe a wide variety of systems. Java is ubiquitous; plentiful learning resources and examples are readily available which provide help in learning the language, ensuring that the developed simulation tool can be used effectively by future users.

With such a flexible tool, however, the dangers of Garbage-In-Garbage-Out are inherent. Care must be taken to model the system in question at an appropriate level of detail and to validate the performance of the tool to ensure the avoidance of errors.

4.4 Simulation tools

This section presents the range of functionalities which the tool provides to the user; these include a number of unique functionalities necessary to achieve the above aims which are not available in other simulation platforms, such as the ability to simulate damage, danger zones, enemy nodes and jammers.

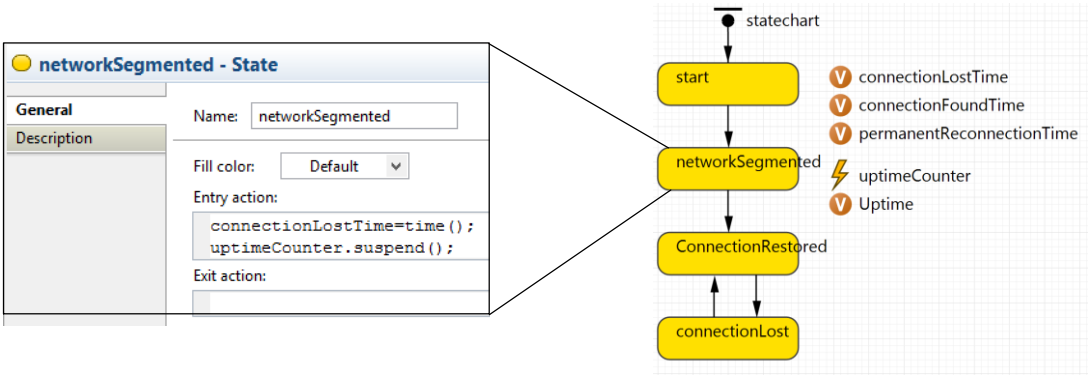

Figure 4-2 Statecharts Powered by Java Code

The behaviour of the simulation tool is defined by using statecharts containing java code within each element of the simulation (see Figure 4-2). The tool has been developed in a modular fashion to support the design paradigms of emerging technology management approaches and to enable more effective development by facilitating modifications later in the design process. The functionality of the tools has been realised from an application level perspective to achieve the modelling and simulation of the complex battlefield context and to gather results which are representative of real world systems.

4.4.1 Graphical User Interface

The main Graphical User Interface (GUI) of the simulation tool gives the user access to all of the functionality discussed in this chapter. It presents the user with a bird's eye view of the scenario and it is comprised of variables, functions and control devices (see Figure 4-3) which allow the user to modify the simulation at design time and at runtime.

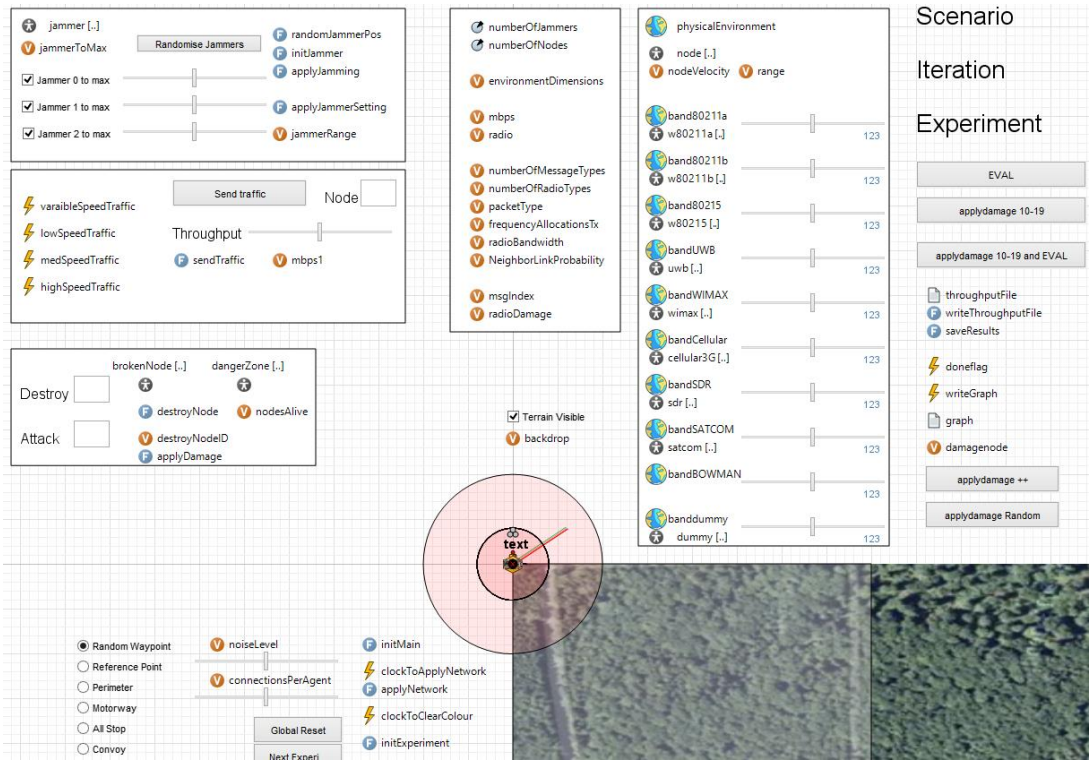

Figure 4-3 Design Time View: Fleet Level Interface

Connections between nodes and their RAT ranges are visualised using lines connecting agents with different colours representing heterogeneous RATs and vehicles are represented using a variety of graphical representations (see Figure 4-4).

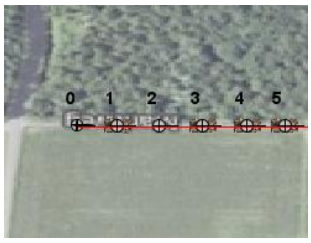

Figure 4-4 Runtime View: Vehicle Platforms

The use of GUI controls enables the user to influence many of the simulation parameters (see Figure 4-5), enabling rapid development of novel algorithms. This way the user can simulate an algorithm under test and introduce various stimuli at runtime without the need to redesign the simulation scenario, allowing quick and intuitive assessment of the behaviour of the algorithms. The control inputs available from the runtime GUI include mobility model selection, node velocity, RAT and jammer range, traffic throughput, danger zones and the ability to damage and destroy

select nodes. Detailed information about these functionalities is presented in the remainder of this chapter.

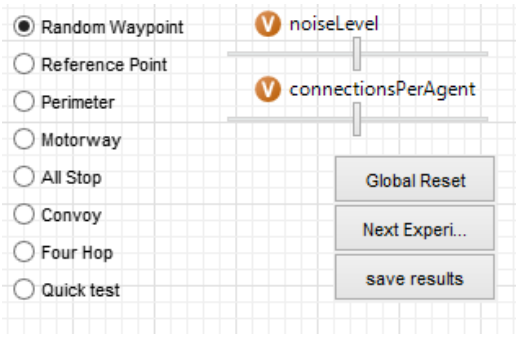

Figure 4-5 Runtime View: Mobility Model Controls

To further accelerate the assessment of RCMA under test, using different graphs and time plots, the user can monitor the real time performance directly within the simulation without the need to output the experiment data into another type of software (see Figure 4-6).

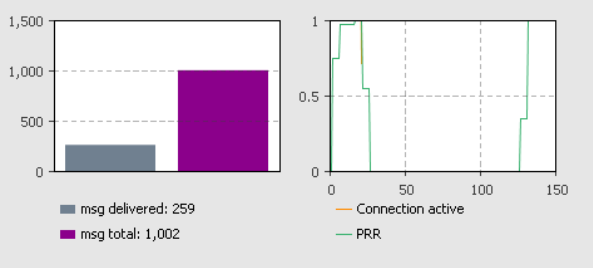

Figure 4-6 Runtime View: Graphs

4.4.2 Mobility

In order to fulfil the stated goal of simulating mobile nodes, the tool allows the user to implement node mobility by specifying a variety of mobility models. Many types of mobility models exist to simulate a fleet of vehicles on a virtual battlefield [155]. These mobility models vary in their degree of randomness from the most random examples where nodes freely roam the simulation area (see: Figure 4-7) to mobility models where node mobility depends on specific scheduled behaviour to emulate real scenarios.

Much research has been done on mobility models and since the mobility model can influence the results of a simulation involving mobile nodes, it is important to

choose and appropriate model for the type of scenario simulated [155]. The developed simulation tool is not limited by the mobility models listed here; it also allows the user to script new mobility models quickly by using the provided functions to assign nodes their mobility behaviour. For all mobility models the user can vary the velocity of individual nodes by simply modifying a velocity value in m/s within each node.

4.4.2.1 Random Waypoint

The Random Waypoint Mobility Model was realised by placing each node in a random location within the environment. The nodes then travel towards a random location determined by a uniform distribution with limits within the environment dimensions (see: Figure 4-7). When a node reaches its target location, it pauses for a selectable amount of time and is then set in motion towards another destination which is calculated in the same fashion. This cycle continues indefinitely (see Figure 4-8 for an example topology, using this mobility model).

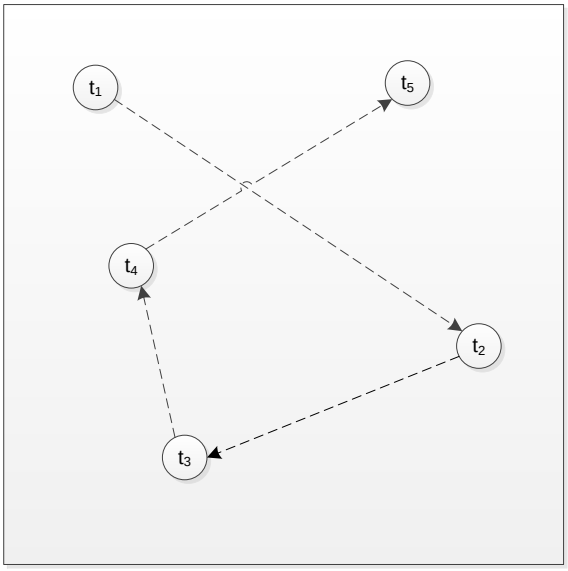

Figure 4-7 Random Waypoint Mobility Model

While the Random Waypoint Mobility Model is arguably one of the most straightforward, there are several known problems associated with it, making it an unsuitable model for some simulation scenarios. These shortcomings include the sudden changes in direction and velocity, unnatural to most mobile agents as well as an unwanted apparent decay in average velocity as the simulation progresses [156].

Therefore the user must take care to account for the limitations of this mobility model when using it in an experiment.

Figure 4-8 Runtime View: Random Waypoint Mobility Model

4.4.2.2 Reference Point Group Mobility Model

The Reference Point Mobility Model is similar to the random waypoint mobility model, however, instead of individual nodes picking a random location and travelling towards it, when using the reference point mobility model, nodes will chose a destination as a group, simulating a more realistic vehicle fleet behaviour (see Figure 4-9).

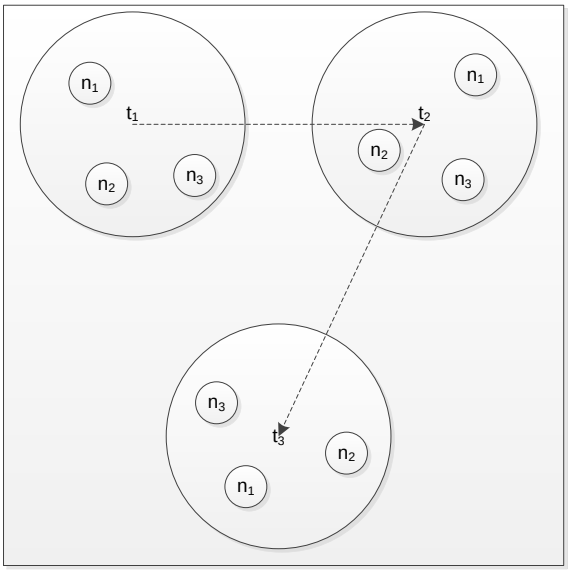

Figure 4-9 Reference Point Group Mobility Model

The reference point mobility model was implemented by positioning a selectable number of nodes in random locations and declaring them reference points. A selectable number of nodes are then assigned to each reference point. The reference point nodes behave according to the random waypoint mobility model within the environment dimensions and other nodes behave according to the random waypoint mobility model within selectable dimensions centred on each of the reference point nodes. See Figure 4-10 for a simulation runtime example.

Figure 4-10 Runtime View: Reference Point Mobility Model

4.4.2.3 Perimeter

When using the Perimeter Scenario, all nodes in the network will form a chain and patrol the perimeter of the environment with a selectable velocity (see Figure 4-11).

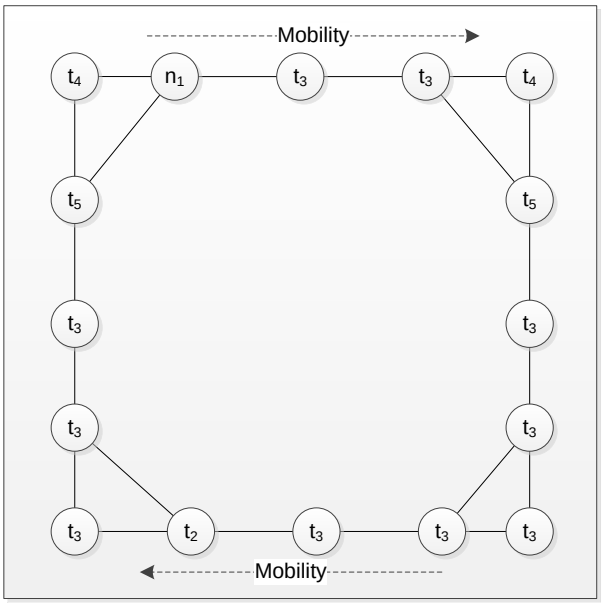

Figure 4-11 Perimeter Scenario

The perimeter mobility model was implemented by placing nodes a selectable distance away from the edge of the environment. The nodes are then set in a clockwise motion and as soon as an individual node is within the set distance to the edge of the environment, it turns 90 degrees Clockwise. This way the nodes travel around the perimeter of the environment indefinitely. See Figure 4-12 for a simulation runtime example.

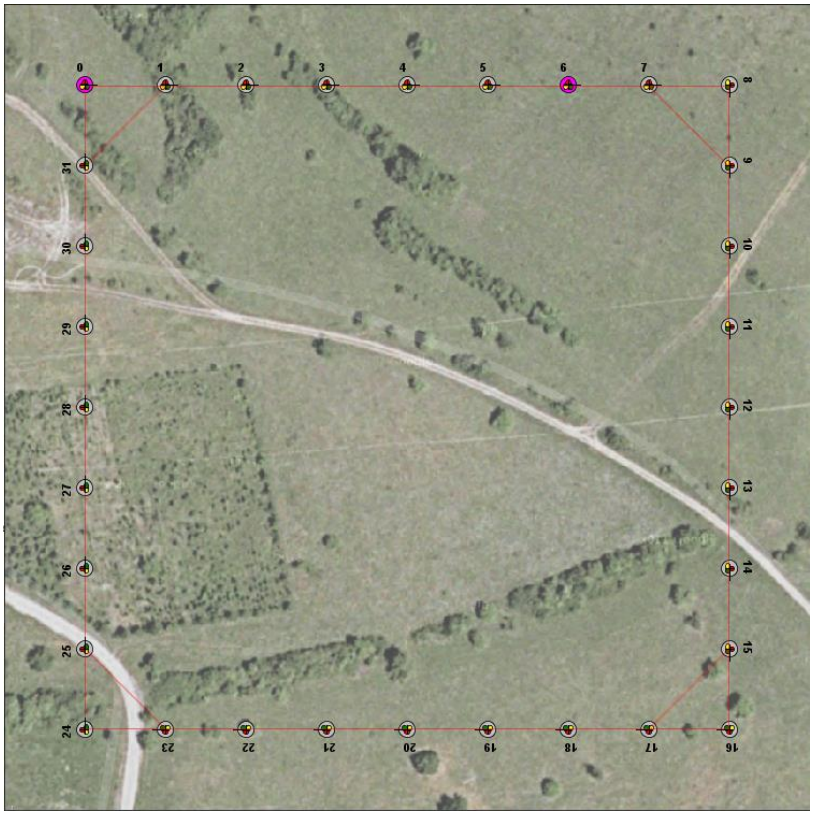

Figure 4-12 Runtime View: Perimeter Mobility Model

4.4.2.4 Convoy

To simulate a convoy of vehicles, the user can select the convoy scenario. The user has the ability to select the number of nodes which participate in the convoy as well as the distance between vehicles and the amount of random variation in distance modelled by a uniform distribution (see Figure 4-13).

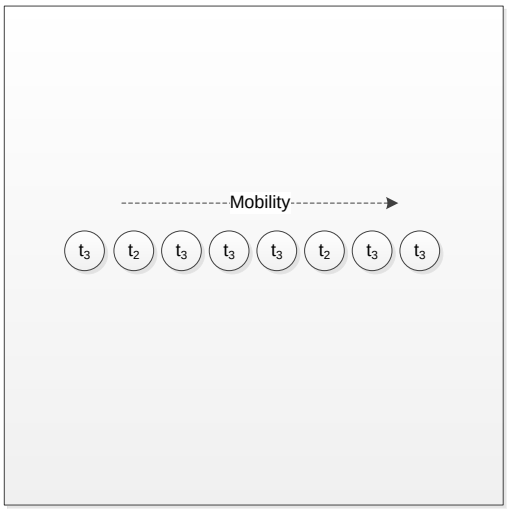

Figure 4-13 Convoy Scenario

The Convoy mobility model was implemented by placing nodes on a straight line in the centre of the environment along the W-S axis. This is to model realistic convoys with semi-random variation in distance between vehicles. See Figure 4-14 for a simulation runtime example.

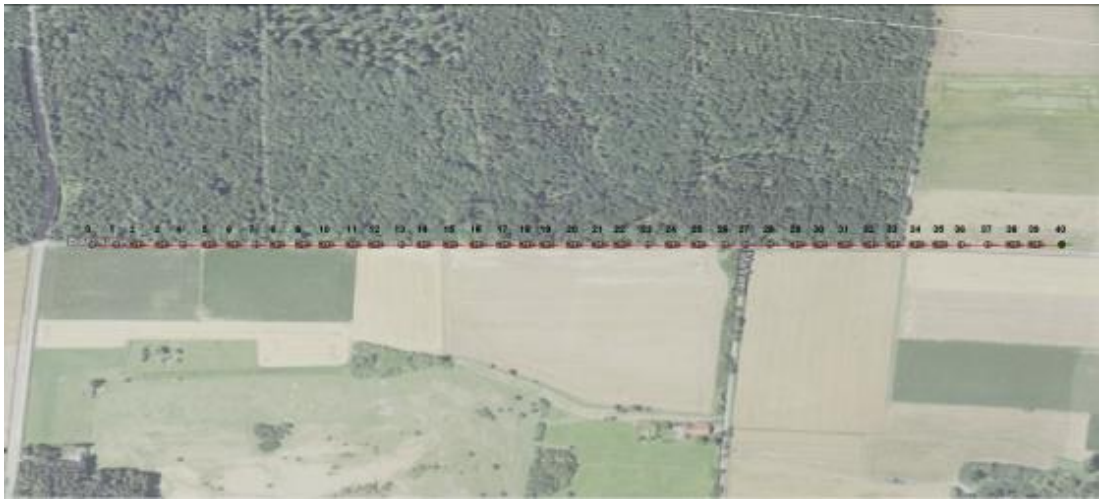

Figure 4-14 Runtime View: Convoy Mobility Model

4.4.2.5 Custom Mobility Model

Although the previously discussed mobility models provide the user with the ability to simulate a variety of realistic scenarios, in many cases it is necessary to design custom mobility models suitable for assessing specific characteristics of the algorithm under test. Therefore tools are provided to allow the user to program specific mobility models by providing times and coordinates for individual nodes in order to represent actual battlefield scenarios, such as the convoy-scout scenario described in 6.2.3.1. Custom mobility models can easily be created by entering a list of node coordinates and mobility vectors into a mobility file; e.g. by entering:

SetNodeLocation(0, 100, 200);

SetNodeTarget(0 , 100, 300);

Node 0 will move from (x=100, y=200) to (x=100, y=300). These commands can be listed and a script can be created in conjunction with timed events to simulate any type of mobility scenario.

4.4.3 Vehicle Platforms

As noted previously, individual vehicle platforms are implemented as agents in an environment. For the purposes of simulating a battlefield fleet, these agents can represent any manned and unmanned platform type and they are capable of carrying a variety of communications equipment (RATs). Beyond their mobility model, their behaviour is flexible and expandable and can be modified depending on the RCMA under test. The user can specify environment dimensions and modify them to simulate different scales of physical environment and the agents in the simulation will remain within the environment.

Although the agents can theoretically represent any type of platform, for the purposes of this thesis, two main vehicle platform types have been implemented; a generic manned platform and a generic unmanned platform. Both types of vehicle platform are represented by a small circle and indicate their direction of travel, but manned nodes have an additional graphic of an Armoured Fighting Vehicle (AFV) to differentiate them more easily from unmanned nodes (see Figure 4-15).

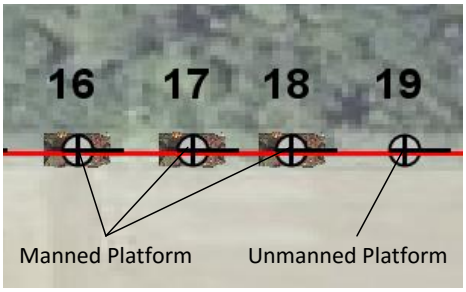

Figure 4-15 Runtime View: Unmanned and Manned Nodes

4.4.4 Communications

All nodes are equipped with the capability of transmitting and receiving data using multiple wireless communication links simultaneously. To simulate several independent nodes communicating on heterogeneous bands, each RAT type uses a unique agent environment to communicate. Thus each radio only has access to its corresponding band and is therefore only capable of transmitting and receiving traffic on that band.

By enabling or disabling an array of pre-made RAT for each individual node the user can easily chose which types of RAT are available to the vehicle platforms in the fleet. Fundamentally all RATs are treated as generic RATs, able to transmit and receive data with a set of selectable characteristics, such as Type, Throughput, Latency, Protection, Error Rate, Resilience, Range and Power Consumption (see Figure 4-16). As noted previously, RAT types are colour coded for easy assessment of the network topology from the main GUI.

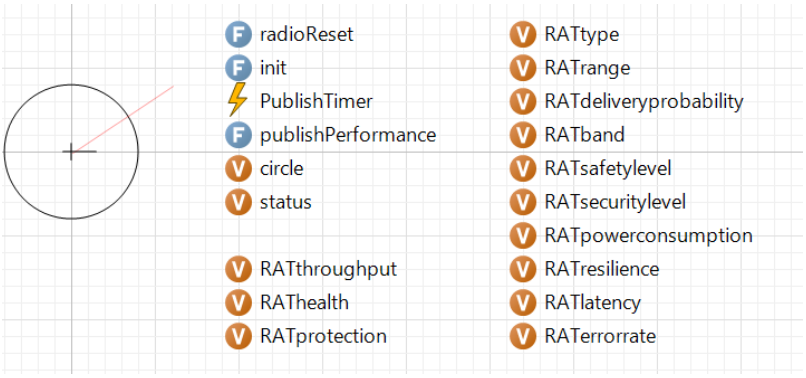

Figure 4-16 Design Time View: Generic RAT Characteristics

4.4.4.1 RAT Range

The range of each RAT is modelled by a circular area centred on the vehicle with a radius proportional to the range of the specific communication technology, i.e. a smaller radius for short range communications and a large radius for long range communications.

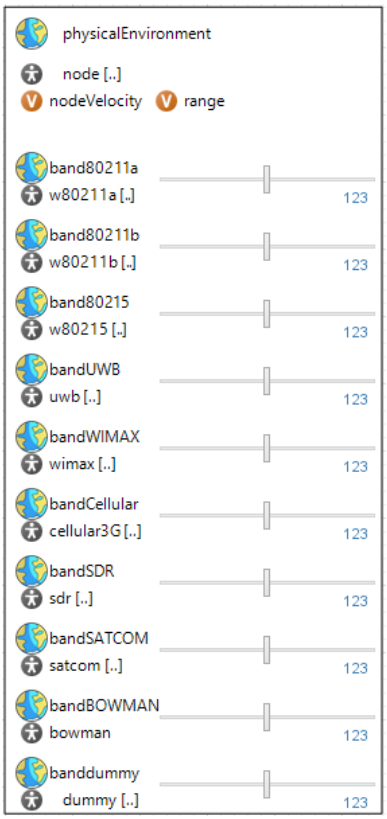

Figure 4-17 Runtime View: Adjusting RAT Range

When two agents have the same type of RAT available to them and they move within the range of each other, it is assumed that the two agents are connected and that they can communicate. The RAT range sliders, which can be found in the Main GUI, adjust the range of each RAT type for all nodes in the network (see Figure 4-17). This way the user can adjust the range of different RAT types at runtime and quickly simulate heterogeneous MANETs (see Figure 4-18).

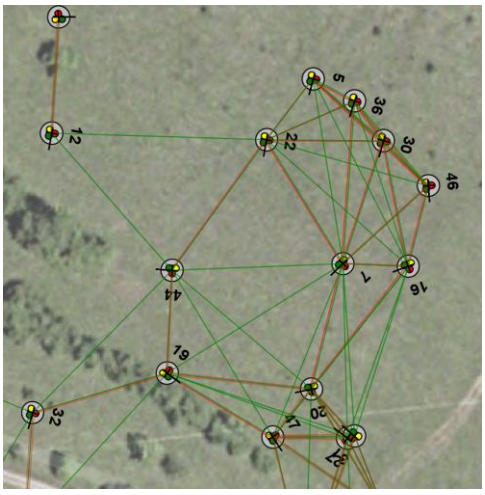

Figure 4-18 Runtime View: Heterogeneous MANET

4.4.4.2 Traffic

Data transmitted over the network is end-to-end, simplified packet based. Each packet of data represents 1Mbit and is comprised of a java object containing a string of text representing the packet header and payload. For the purposes of the simulation, any traffic transmitted through the system takes a specific format and includes all relevant traffic requirement information in the header, such as traffic type, required throughput, latency, priority, security level and safety level as well as the source and destination of the packet and it's time to live. By changing the contents of the java object the user can modify all of these parameters. Multiple different traffic types with selectable characteristics can be created easily by replicating the Java object.

4.4.4.3 Routing

Since routing behaviour of a RAT is integral to its performance, it is assumed that any RAT installed on a vehicle platform contains its own routing behaviour as part of the equipment. This simulation treats any attached radio equipment as a black box with interfaces to transmit and receive data therefore RAT routing algorithms are outside the scope of this thesis.

Nonetheless the implementation of a routing algorithm is still necessary to simulate packet based communications in a fleet of vehicles using message forwarding and multi hopping. For this reason the routing algorithm implemented for the purposes of the simulations is the loop free distance vector BABEL routing algorithm [78]. Node discovery is implemented using "Hello" packets transmitted at 4s intervals which are responded to with "I Heard You" packets as per BABEL specifications.

4.4.4.4 Sending Data

To send data at runtime the user can simply select a desired throughput and push a "send Traffic" Button (see Figure 4-19). The traffic data rate can be changed with the use of sliders in the main GUI and is modelled with an event that prompts a selected node to transmit traffic at the set rate.

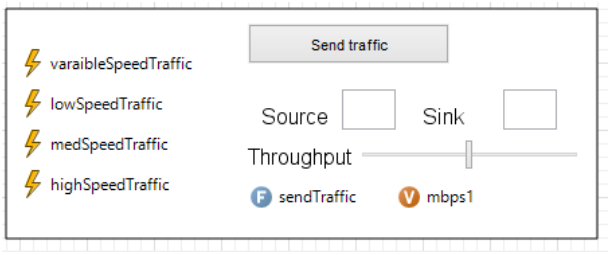

Figure 4-19 Runtime View: Sending Traffic

When the user generates traffic this way it is placed directly in the source RAT's transmit functions queue. To transmit data, the RAT's transmit function first pulls the oldest entry from its queue and then saves the contents of the packet in its history together with the current time for later performance analysis.

The transmit function then checks its neighbour table for an appropriate next hop and transmits the traffic to that neighbour. If no route can be found, it publishes the fault to the data model so that other platform systems, such as the platform's mission computer can trigger a Topology Management Algorithm (see Figure 4-20).

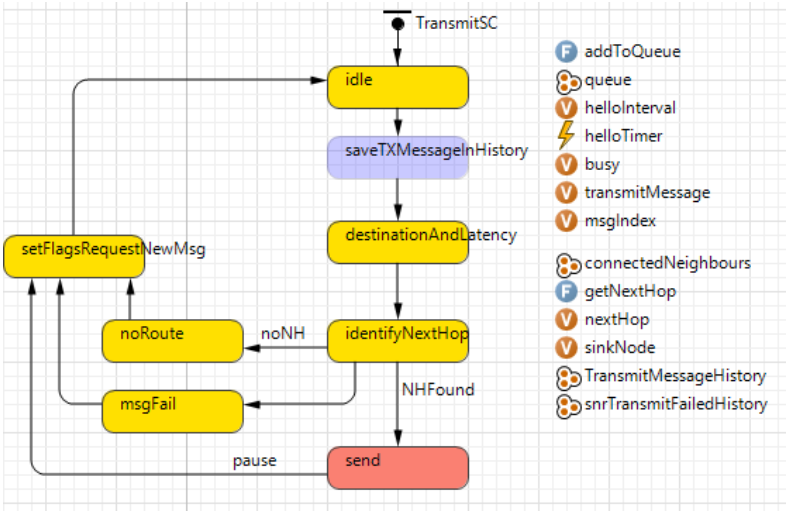

Figure 4-20 Design Time View: Transmit Traffic

4.4.4.5 Receiving Data

When a RAT receives a packet from another node's RAT, it first separates traffic used purely for routing functionality (in this case "Hello" and "I Heard You" packets used by the BABEL Routing Protocol). Relevant communications traffic is passed on and saved in the receiving functions history for later performance analysis (see Figure 4-21).

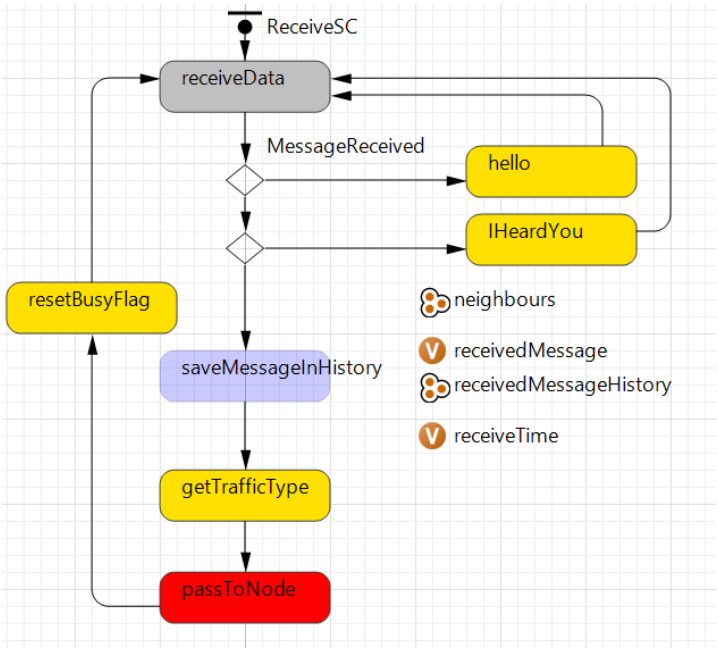

Figure 4-21 Design Time View: Receive Traffic

The packet is then passed on from the individual RAT to the node receive function which analyses all received packets from the attached RATs. If the received packet is unique, the function logs receive time, hop count and RAT type. The function then checks if its node is the intended destination of the packet and either logs it as successfully received, or proceeds to pass it on for retransmitting based on the RAT management of the RCMAs under test (see Figure 4-22).

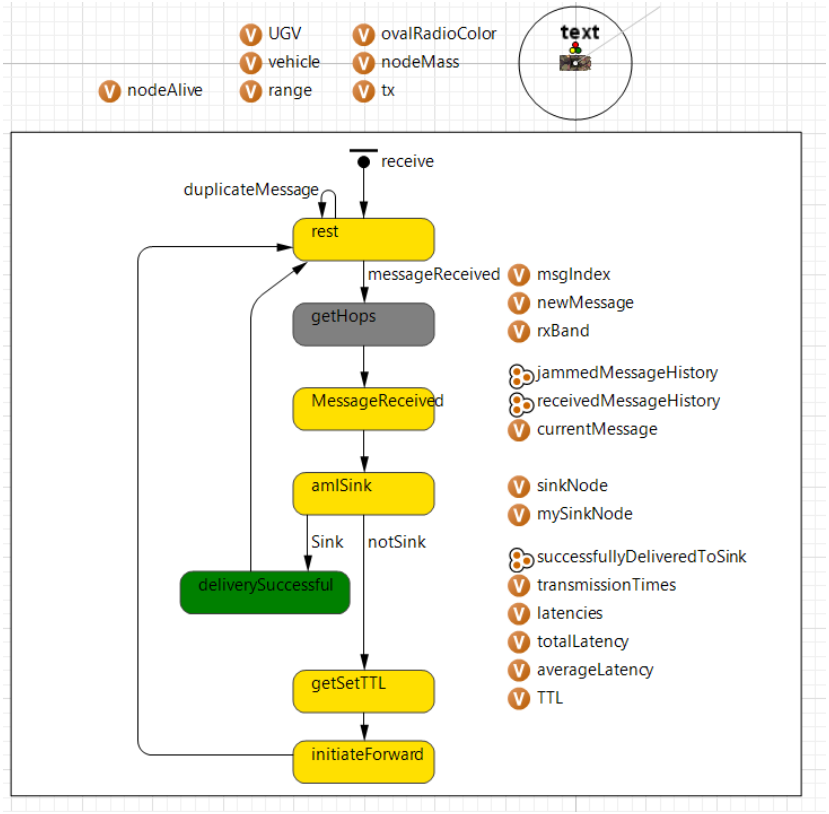

Figure 4-22 Design Time View: Node Traffic Analysis

4.4.4.6 RAT Health

The simulation tool gives the user the ability to model health of individual RATs on vehicle platforms to simulate damage and degradation of the radio hardware. RAT health affects both the transmit and receive function of the affected RAT, i.e. when a RAT's health is set to 0.1, only 10 % of packets are received by the receive function and only 10 % are sent by the transmit function.

4.4.4.7 RAT Latency

To model heterogeneous RAT with diverse latency characteristics, each node in the network is modelled to add a selectable amount of latency when it retransmits the packet; therefore, the end to end latency is determined by the number of nodes in the route of the packet.

When a packet is transmitted through the network, since each node automatically records its time of delivery and transmission in the node's log, by accessing these

logs the user can calculate the end to end latency times and display them in the main GUI, or record them for further analysis.

4.4.4.8 RAT Throughput

To model heterogeneous RATs with diverse throughput characteristics, each RAT on a vehicle platform is modelled with a selectable throughput. Throughput is modelled with a delay timer which blocks the receive function for a certain time before releasing it to receive another packet. Since each packet represents a data volume of 1mbit, for a throughput of (t) Mbps, the delay timer blocks the receive function for 1/t seconds.

Each node automatically calculates the throughput of the traffic it receives so the user can access the received throughput of any traffic simply by accessing the corresponding RAT throughput metric.

4.4.4.9 Packet Delivery Ratio (PDR)

The number of correctly received packets is counted by the receive function of each RAT and the delivery time of each received packet is stored. From this information it is possible to calculate PDR and the times of connection loss and reconnection. The tool provides easy access to these values by storing them in variables in the receive function of each RAT.

4.4.4.10 Power Consumption

The user can access the consumed power of each individual RAT on each node simply by accessing a variable within the RAT in question. Power Consumption is measured in Watt seconds (Ws) and is modelled by three counters which are triggered by the state of the RAT. When the RAT is not active, none of the counters are active, however, for every second the RAT is idle, receiving or transmitting, the respective power consumption counter adds a selectable amount of Ws to the RAT's cumulative power consumption.

4.4.4.11 Interference

To fulfil the goal to enable the modelling and simulation of RCMA in a battlefield context, the tool provides functionalities to model external interference. It is assumed that the effects of any internal interference are reflected in the performance characteristics of the attached RAT.

Unintentional external interference is modelled by a delivery probability value representing the amount of spectrum noise. The delivery probability value has a range of 0 to 1 where 0 represents a noisy environment with a 0 % chance of successful packet delivery and 1 represents a 100 % chance of successful delivery.

To model intentional external interference, the simulation tool provides the ability to generate localised jamming signals on specific bands. These jammers are themselves agents in the environment and modify the delivery probability value of the RAT within their range, which, like the range of other agents, is also modelled as a circle centred on the jammer. The effect of the jammers on the delivery probability of the nodes within their range and the jammer's range itself can be changed at runtime.

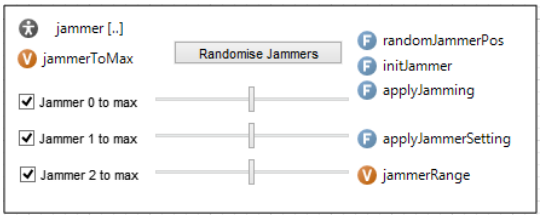

Figure 4-23 Runtime View: Jammer Controls

The jammers can be controlled in the GUI using various controls (see Figure 4-23). The location of the jammers can either be randomised or the jammers can be placed in specific location. In the GUI they are represented by a box with their range depicted by a circle with a semi-transparent colour representative of the RAT band they disable (see Figure 4-24). The controls for a total of three jammers are implemented in the GUI, but additional jammers can be added easily by replicating the jammer agent.

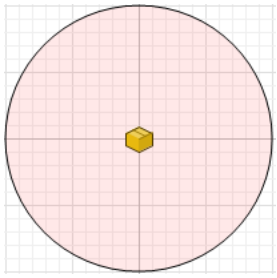

Figure 4-24 Runtime View: Jammer With Range

This way the user can easily introduce intentional external interference into a heterogeneous MANET. Figure 4-25 shows an example of a MANET equipped with three heterogeneous RAT denoted by the colours Red, Yellow and Green. Three Jammers, also Red, Yellow and Green are set to reduce the delivery probability of the RATs within their range to 0 and thus block their corresponding colour RAT. Within the range of each Jammer the corresponding RATs disconnect and in the region where the three jammers overlap, all three RATs are disabled.

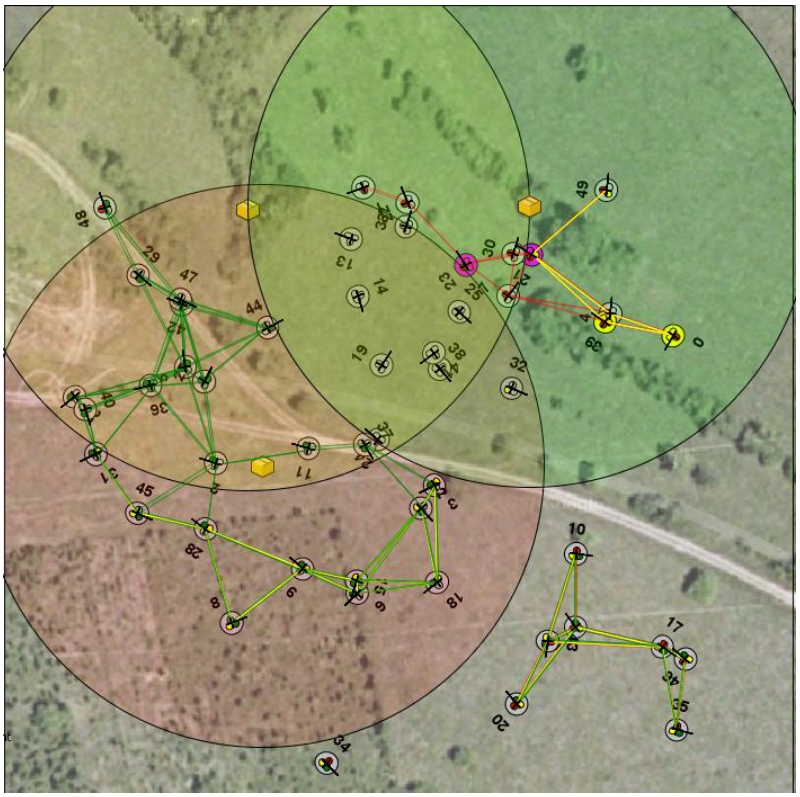

Figure 4-25 Runtime View: Jamming in a Heterogeneous MANET

4.4.5 Node Damage

To enable the user to model a hostile battlefield environment, the simulation tool simulates node damage and provides the user with tools to modify node behaviour when nodes become damaged. To model realistic behaviour when nodes are damaged, the user can choose to modify any of the above functionality, such as mobility, RAT Health, etc.

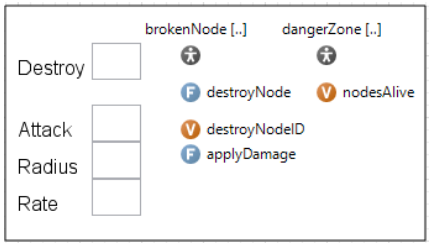

Figure 4-26 Runtime View: Node Damage Control

Nodes can also be disabled completely with a command found in the main GUI (see Figure 4-26). The user can enter any node ID and thus choose to attack or destroy any node at runtime. When entering a node ID to destroy, only a single node is destroyed, when a node ID is entered to attack, a danger zone is formed around the chosen node. Other nodes which are present within the chosen radius of the danger zone (in metres) become destroyed at a selectable rate (per second), i.e. when node 20 is attacked with a radius of 300 and a rate of 0.1, a danger zone with a 300 m radius is formed and agents within this zone become destroyed at a rate of one agent every ten seconds (see Figure 4-27 for an example of such a danger zone).

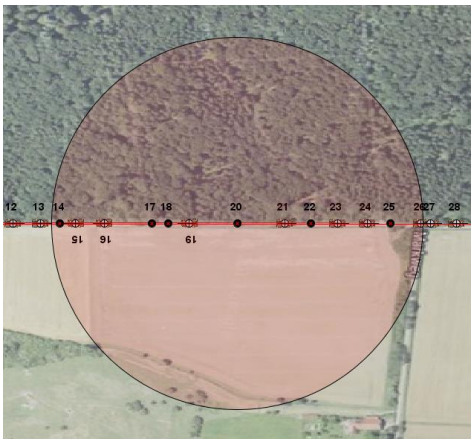

Figure 4-27 Runtime View: Danger Zone

Using timed events the user can also simulate realistic scheduled scenarios involving node damage and localised danger zones. When a node is destroyed, it cannot interact with other nodes in the network and is replaced “brokenNode” agent (see Figure 4-28).

Figure 4-28 Runtime View: Broken Node

4.4.6 Platform and Group Capabilities

To simulate heterogeneous vehicle fleets with diverse individual and shared group capabilities, the tool gives the user the ability to specify capability values of each node. These simplified capabilities are represented by an array of integers, each variable in the array representing the strength of the capability. To simulate shared group capabilities in a fleet, nodes can be grouped together with other nodes and sum of each type of capability is calculated as a group capability. In a topology repair scenario, when a node is tasked to repair the network, to model the fact that it no longer makes its capabilities available to the group and hence, its contribution is subtracted from the shared group capabilities.

4.4.7 Shared Data Model

To model Shared Data Models of modern battlefield vehicle fleets, each node in the network contains a data model object (see Figure 4-29) which contains list of arrays to represent and abstract the physical hardware contained on each vehicle platform as well as the vehicle state and situational context of the fleet (see Figure 4-30).

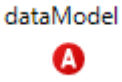

Figure 4-29 Design Time View: Data Model Object

The data model represents both a vehicle and fleet data model and thus gives a node the ability to easily access performance data from all other nodes in the network as well as bridging the gap between the attached RATs and the RCMAs. As long as

nodes are connected in a network, they have full access to the data model data of other nodes and therefore any implemented RCMA can utilise all data model information available throughout the fleet to perform Resource and Capability Management. The network overhead created by the data model is assumed to be negligible compared to other traffic and is therefore ignored.

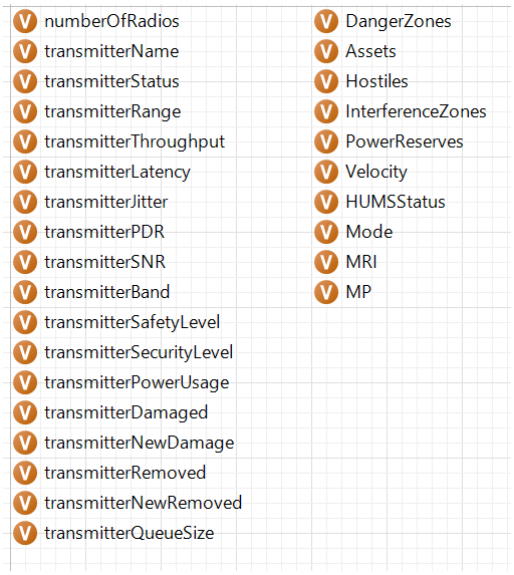

Figure 4-30 Design Time View: Data Model Parameters

4.4.8 Generating Output Data

The simulation tool provides straightforward facilities to record results of the simulation, and to gather statistical data on the algorithms under test. The user can export any performance metric or variable produced by the simulation by using timed events to record metrics to a log file. The log files are saved in the .csv format which can be read by readily available spread sheet software.

4.5 Simulation Tool Validation

In order to validate the simulation tool and to prove that with the same stimulus, the tool produces the same results as existing work, an existing RCMA: C2AM, was implemented in the tool and tested against the scenarios and the experimental setup described in [135].

C2AM is an application aware topology repair algorithm which accounts for current node tasks by using a Mobility Readiness Index (MRI) representing the importance of the node's current task, a Mobility Potential (MP) which indicates the potential of neighbouring nodes to move and node degree which indicates the node's connection number. C2AM aims to cause the least possible amount of application level impact on the fleet due to network repair efforts by seeking to reduce combined amount of MRI of the network repair nodes. When a network becomes segmented due to a node failure, C2AM replaces the failed node with the node which has the lowest MRI of the nodes within range of the failed nodes. The repair node is subsequently replaced by the node with the lowest MRI in *its* range. This cycle continues until the network is no longer segmented.

C2AM selects repair nodes according to the following criteria in descending order of importance:

1. Lowest MRI Value
2. Highest MP Value
3. Lowest Node degree
4. Smallest distance to the failed node.
5. Highest node ID (In case of a tie between two nodes)

[135] describes two experiments: The first experiment involves a specific topology and a specific set of initial conditions and is used to explain the operation of C2AM. The second experiment involves multiple averaged runs of the algorithm using randomised topologies and initial conditions.

4.5.1 Experiment 1: Specific Topology:

4.5.1.1 Experiment Design

The specific topology of the first experiment presented in the paper was recreated and as the authors provide detailed descriptions, diagrams and a table with their initial MRI, MP and Node Degree values, the experiment could be recreated and the behaviour of C2AM reproduced.

Figure 4-31 shows the initial network topology. On the left is the original topology taken from the [135], on the right the reproduction in the developed simulation tool (for clarity, the satellite map backdrop has been replaced by a grey background for these experiments). The node IDs are shifted by 1, since the original example counts the agents starting from ID = A1 and the developed tool counts nodes starting from ID = 0:

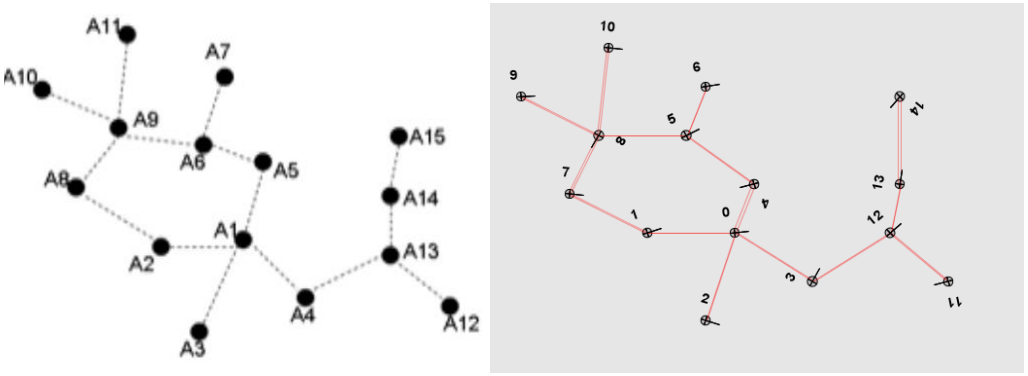

Figure 4-31 Simulation Validation, Experiment 1: Initial Topology

Table 4-1 lists the initial conditions of the experiment:

Table 4-1 C2AM Experiment 1 Specific Topology Values

Node ID	MRI	MP	Node Degree
0	Failed	Failed	Failed
1	5	1	2
2	5	0	1
3	3	1	2
4	1	0	2
5	5	3	2
6	3	0	1
7	4	1	2
8	3	3	3
9	3	1	1
10	2	1	3
11	5	0	1
12	5	1	3
13	5	0	2
14	5	0	1

Using these initial conditions, the original experiment destroys node 0 and examines the subsequent node movements in the network.

4.5.1.2 Results and Discussion

When node 0 fails, node 4 is selected as the repair node (see Figure 4-32) due to it's low MRI (see Table 4-1).

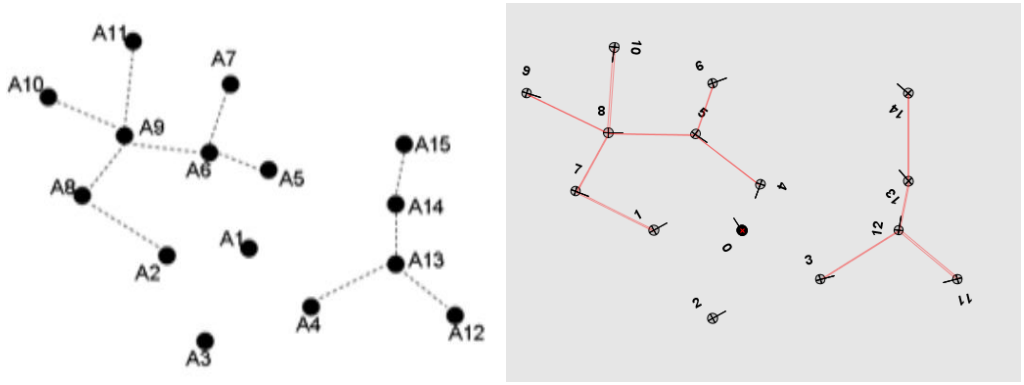

Figure 4-32 Simulation Validation, Experiment 1: Node Failure

Because Node 4 would partition the network if it leaves it's position, the only node in it's range, node 5, is selected to replace node 4. The cycle continues for nodes 8 and 10 at which point the algorithm stops and the network is reconnected (see Figure 4-33).

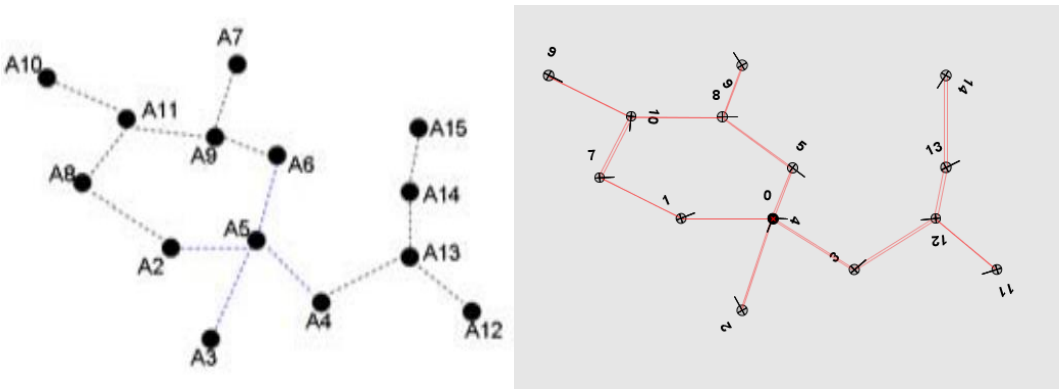

Figure 4-33 Simulation Validation, Experiment 1: Reconnected Network

Using the Battlefield Network Simulation Tools, the algorithm behaves in an identical manner to the original experiment.

4.5.2 Experiment 2: Generated Topology

4.5.2.1 Experiment Design

The second experiment presented in the paper uses randomised connected networks with the number of agents varying from 20 to 100 in a 1000 m x 600 m environment (see Figure 4-34 for an example topology with 60 agents). MRI is assigned using a uniform distribution with a range of 0 to 5. To achieve a connected network, the the random waypoint mobility model is used, which places nodes in the environment using a uniform distribution limited by the environment dimensions. In the event that a non-connected network is formed, the process is repeated until all nodes in the network are connected.

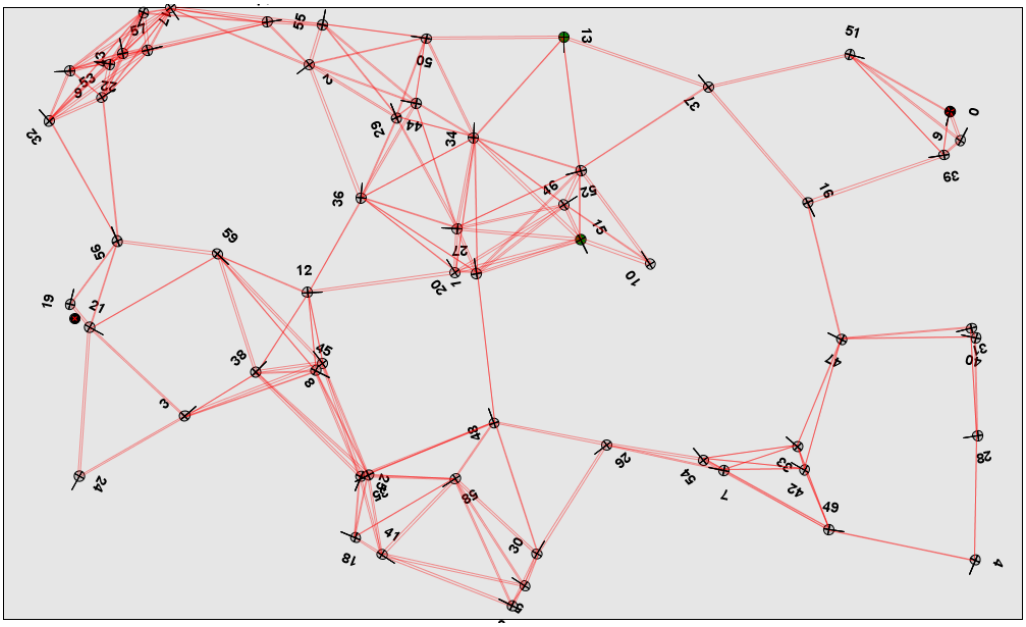

Figure 4-34 Experiment 2: Randomised Connected Network

The experiment is performed in two steps, First, the communication range is set to 100 m and the number of agents is varied in five scenarios with 20, 40, 60, 80 and 100 agents. The MRI value incurred due to node movements as well as the total distance moved by the agents is recorded for each of the scenarios and the results are compared to the original experiment.

Second, the number of agents is fixed to 60 and the agent communcation range is varied in four scenarios with a 50 m, 100 m, 150 m and 200 m range and the total MRI value and total distance are again recorded for each of the scenarios.

The scenarios are repeated a sufficent number of times to reach a 95 % confidence interval.

4.5.2.2 Discussion

The following graphs show the comparison of the experiments performed in [135] to the same experiment performed in the developed simulation tool:

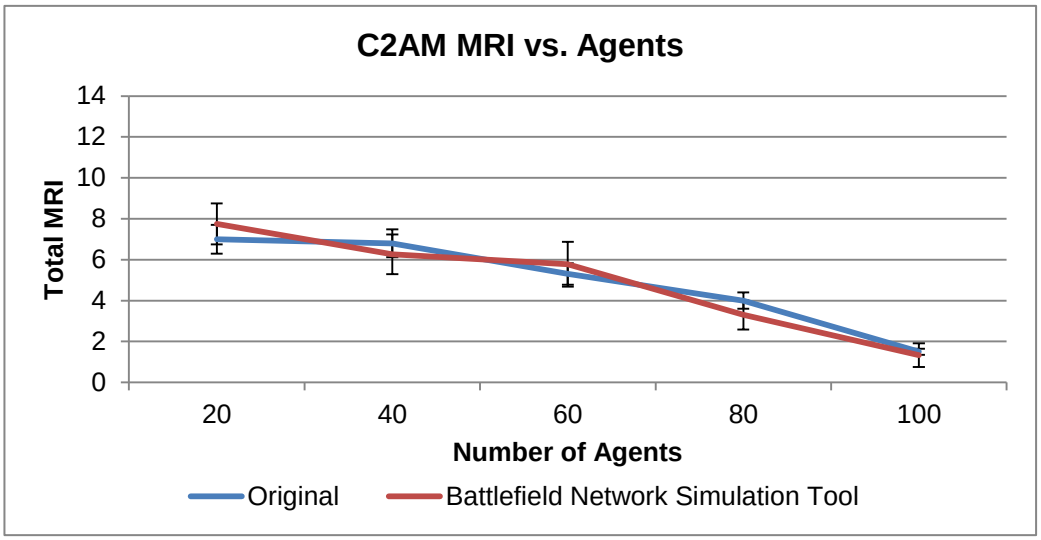

Figure 4-35 Number of Agents vs. Total MRI (Range = 100 m)

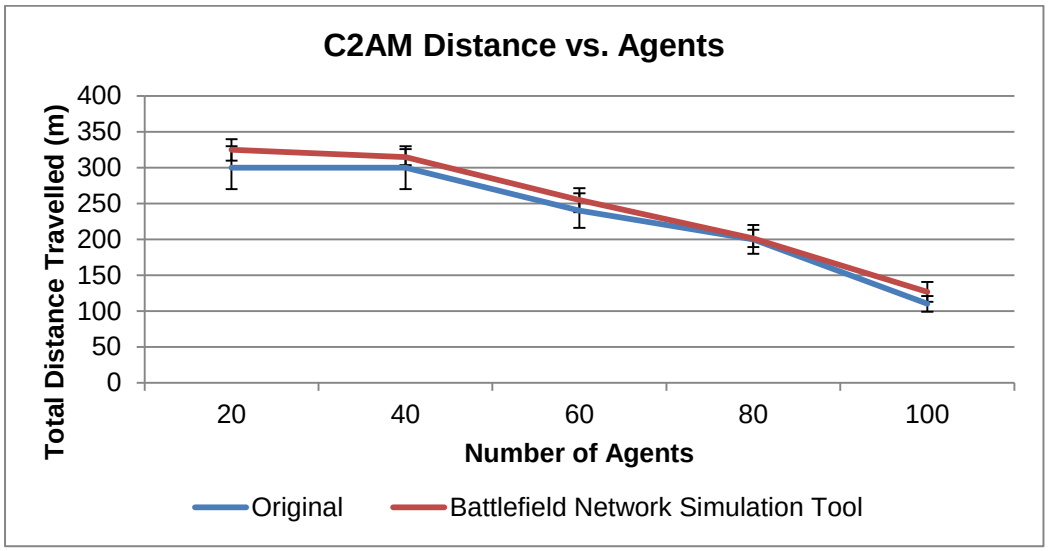

Figure 4-36 Number of Agents vs. Total Distance Travelled (Range = 100 m)

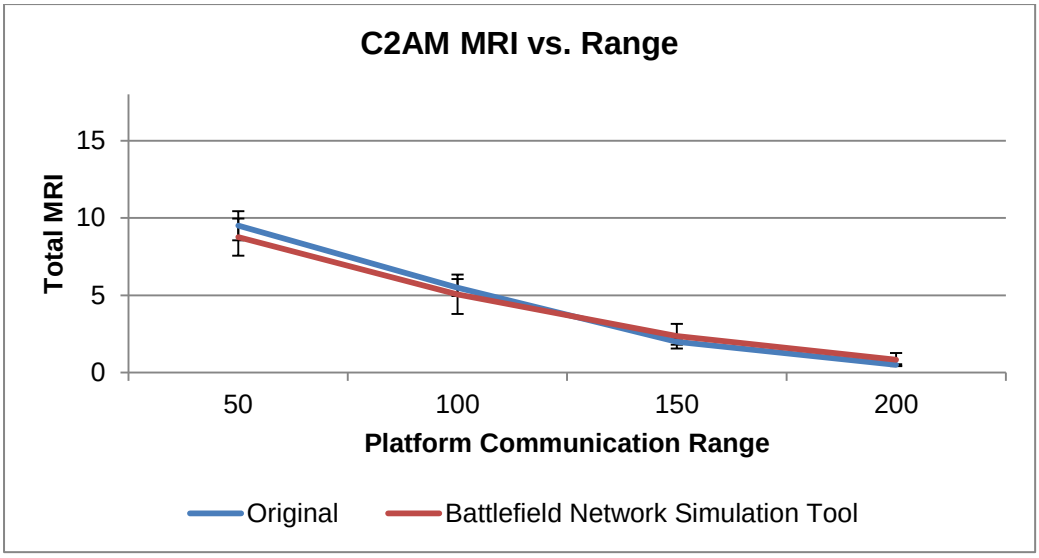

Figure 4-37 Communications Range vs. Total MRI (60 Agents)

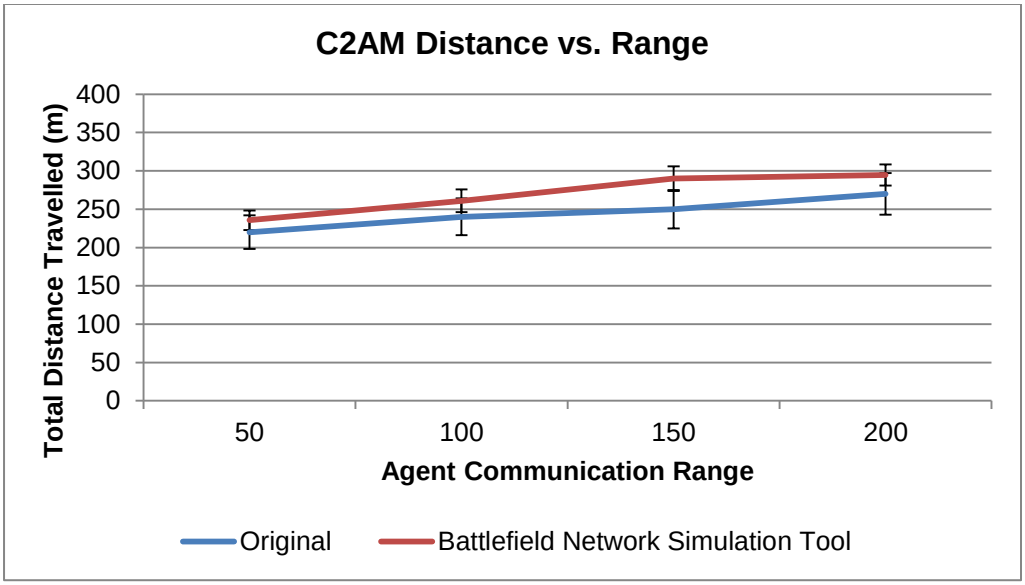

Figure 4-38 Communications Range vs. Total Distance Travelled (60 Agents)

Figure 4-35, Figure 4-36, Figure 4-37 and Figure 4-38 show that the experimental results produced by the Battlefield Network Simulation Tools closely resemble the original experiment. The average error in MRI between the original experiment and the developed simulation tool is 0.47 for the scenarios with the fixed range of 100 m (shown in Figure 4-35) and 0.46 for the scenario with the fixed number of agents (shown in Figure 4-37).

The total distance travelled by the repair nodes using the developed tool is an average of 8 % higher than the original experiment. Although the error is small, it is

consistent throughout the sample; since the authors of the original experiment only specify that nodes are placed randomly. A possible reason for this variation in total distance travelled may be minute differences in how the connected agent network is constructed.

4.6 Conclusions

The aim of this methodology and toolset is to enable development, testing and performance metrics gathering of communications Resource and Capability Management Algorithms (RCMA) in a realistic battlefield context. To achieve this aim, the Battlefield Network Simulation Tool is presented which provides a method to create a simulation of mobile, networked agents representing vehicle platforms equipped with a variety of heterogeneous Radio Access technologies (RATs) and RCMAs in a realistic battlefield environment.

Due to the complex problem space discussed in the previous chapters involving a wide variety of dynamic environments and the need for RCMA to manage diverse and dynamic resources and capabilities with management decisions based on application level fleet wide context information, the Battlefield Network Simulation Tool is capable of simulating a variety of vehicle types equipped with heterogeneous RAT equipment based on a generic templates with selectable performances and characteristics to model systems in a manner representative of the real world. The tool has been developed in a highly modular and flexible manner, allowing for future expandability.

Through the provided functionalities, the toolset enables the design and development process and thus fulfils its goal to facilitate rapid modification and iterative improvements of novel RCMAs in order to achieve performance increases over existing solutions.

Through the Graphical User Interface (GUI), the tool enables the user to make changes to the simulation, measure network communications performance data, such as latency and throughput, and provide different environmental and agent stimuli, such as enemy nodes, danger, node failure and external interference. The tool enables the user to gather performance data to either assess the performance directly

in the tool or to export the gathered data to other types of software for further analysis of the results.

The tool is validated by simulating an existing Resource and Capability Management Algorithm with a known input stimulus and comparing the output of the tool to known results. A specific topology and a randomised experiment presented in [135] were recreated; using the same input stimulus, the developed tool produces results which closely resemble the known results of the original experiment. A small consistent error can be attributed to the realisation of the node placement algorithm used.

Chapter 5 Context Aware Platform Level RCM

5.1 Introduction

From a vehicle platform perspective, diverse communications traffic has to be transmitted via state-of-the-art communications equipment, managed by state-of-the-art Resource and Capability Management Algorithms (RCMA), in order to achieve reliable battlefield communications.

This chapter presents the High Availability Wireless Communications (HAWC) system; a hardware independent communications middleware to manage any combination of existing and future communications resources in the form of Radio Access Technologies (RATs) and RCMAs to best fulfil prevailing traffic requirements.

A vehicle platform in a fleet will cooperate with several other platforms on the fleet level. Cooperating platforms share information via the Shared Data Model (SDM) and HAWC makes this information available to the RCMA used to manage the attached RAT (see Figure 5-1).

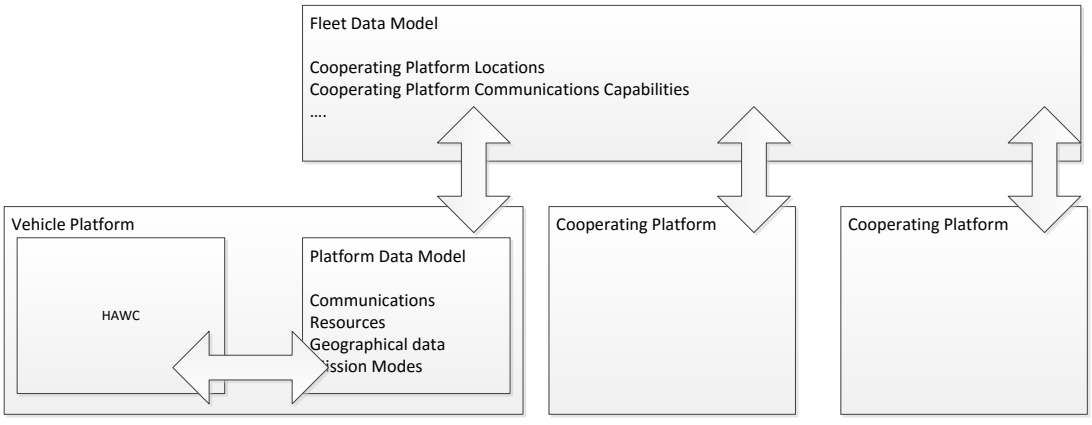

Figure 5-1 HAWC Communicates Through a Shared Data Model

The system is enabled by the recent paradigm of vehicle and fleet level SDM [87, 95, 96] that allows HAWC to gather information about available platform RAT resources, platform state data, mission status and situational awareness data at the fleet level in an integrated and secure manner.

5.2 Problem Definition

As identified in Chapter 2 and Chapter 3, existing approaches in battlefield networks have some significant shortcomings:

While existing systems, such as PC operating systems perform equipment management in a plug and play fashion, existing communications approaches lack sufficient equipment management to facilitate the use of heterogeneous communications resources with minimum integration cost. To effectively use state-of-the-art RAT hardware in battlefield vehicle platforms, a highly flexible Resource and Capability Management (RCM) framework is necessary to facilitate automatic recognition of upgraded, downgraded, damaged and replaced equipment in an effort to use currently available resources to best fulfil current mission.

The inflexible and hard-wired nature of current communications systems impedes systems integration and adaptability and is thus incompatible with the VSI Standards and Guidelines paradigm required for near future battlefield systems. Any modification to existing communications system's resource allocation behaviour requires a partial or complete redesign of the communications system. In order to facilitate technology transfer from state-of-the-art research into battlefield technology, a framework is necessary which facilitates the use of multiple concurrent, modular RCMA which can be selected according to current context information in order to be able to switch the communication's system's resource allocation behaviour on the fly to always leverage existing resources effectively and to meet current mission goals.

To manage platform level and fleet level resources in modern battlefield vehicle fleets, the use of application level information, such as capability information, situational context and mission goals in RCM decision making is crucial. Topology optimisation without application awareness may result in the creation of mission defeating network topologies. Although RCMA approaches exist which perform RCM informed by application level data, in a battlefield context, no mechanism exists to provide these RCMA access to relevant application level data. Existing information sharing systems, such as Dynamic link Exchange Protocol (DLEP) [98]

provide algorithms access to only a limited set of performance data which cannot be extended by algorithms without a redesign of the DLEP system. Existing approaches, such as generic link layers and state-of-the-art internetworking approaches such as 802.21 also only use limited performance data without considering context information and mission goals, which makes them unsuitable for modern battlefield operations. A framework is necessary which allows RCMA to access any available platform level and fleet level information from the platform and fleet SDM to provide maximum awareness to facilitate RCM decision making while being always best informed.

5.2.1 Aims

The aims of this contribution are:

- To improve fleet communications performance and fleet level capability using new advances in platform and fleet level data sharing
- To develop a highly flexible framework which facilitates plug and play behaviour that, given a set of requirements and predefined interfaces, “just works” given a viable hardware and software configuration.

5.2.2 Goals

The goals of this contribution are:

- To design a framework which performs equipment management to detect new or modified equipment and hardware degradation
- To design a framework which enable RCMA by providing access to all available platform level and fleet level application data through an SDM
- To design a framework which facilitates the use of multiple modular RCMA with minimum integration cost and to enable seamless switching between these RCMA
- To design this framework in a modular and flexible manner in compliance with the VSI Standards and Guidelines

5.2.3 Scope

Through the nature of Commercial off-the-Shelf (COTS) and the activist customer role that the United Kingdom (UK) Ministry of Defence (MOD) adopts, e.g. by developing standards, such as the Generic Vehicle Architecture (GVA) Def Stan 23-09 [87], it is assumed, that communications equipment designed to interface with any future vehicular system will adhere to MOD mandated specifications, such as the ability to provide interfaces to the vehicle and fleet SDM. It is therefore assumed that the SDM contains accurate and current information about communications hardware; however, the assurance of data model information is outside the scope of this contribution.

HAWC is designed to be an application level framework. Lower level functions which are integral to the operation of RATs are assumed to be contained within the attached RAT Line Replaceable Units (LRUs). It is therefore assumed that lower level functions such as routing, clustering, network discovery, network QoS management, etc. are performed independently of the proposed framework. Similarly it is assumed that a mutual authentication protocol is in place which allows RAT to automatically authenticate once they are powered up in order to participate in a network with similar RAT. Similarly it is assumed that the platform level and fleet level SDM facilitates reliable and secure communication. HAWC treats attached RAT LRUs and their lower layer function as a black box with performance control and performance reporting interfaces via the SDM.

5.3 Approach

5.3.1 Modularity vs. Efficiency to Achieve Effectiveness

A hardware and software management middleware can be designed in a number of ways depending on the goals to be achieved by the design. While the majority of communications management techniques are designed to achieve maximum efficiency by tailoring functions to one another as closely as possible, HAWC is designed to achieve maximum flexibility by emphasising modularity.

Challenges emerging from the battlefield, as well as the fast pace of COTS hardware development dictate a highly flexible system design where future military modules or resources can be treated as LRUs which can be hot-swapped, added, upgraded and re-distributed on the fly, facilitating mission adaption at near zero integration cost.

This doctrine, where military vehicles must be versatile and facilitate rapid re-rollment prompts a need to design for the unknown. An effort must be made to anticipate future technological improvement by restricting the possible path of a system as little as possible. HAWC is designed with this need in mind: In addition to the fact, that traffic, radio hardware and allocation algorithms are treated as distinct modules which can be interchanged, HAWC itself has been designed as a modular system. Each part of HAWC is a self-contained unit which cooperates with other parts of the system through defined interfaces. This ensures, that even HAWC itself can be improved in stages and adapted based on future technology improvements, rather than prompting the need to build a new system from the ground up.

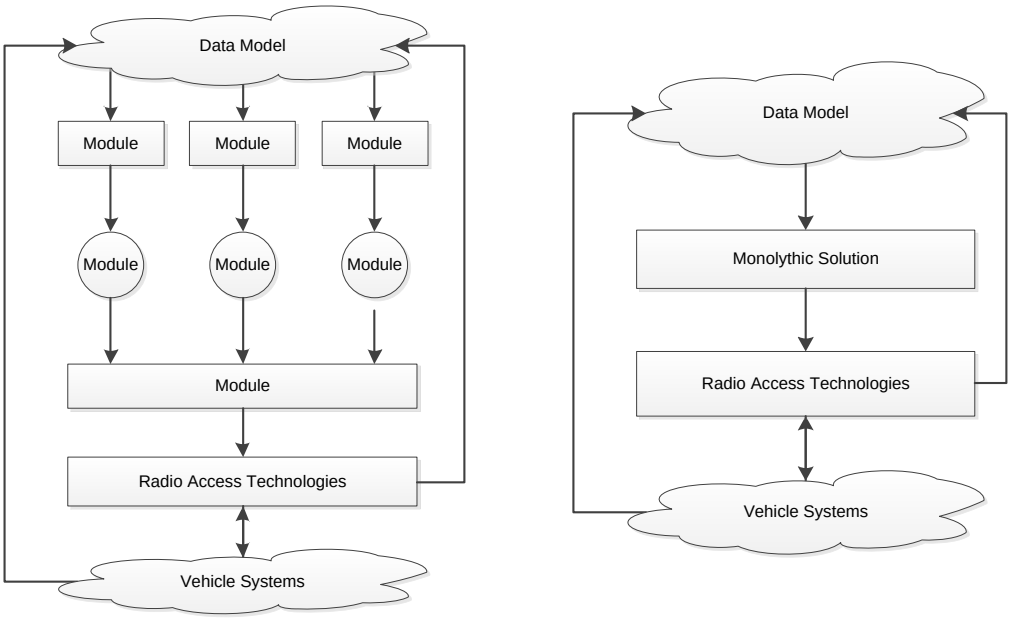

Figure 5-2 Modularity vs. Efficiency

HAWC passes data between several modules (see Figure 5-2). Although a monolithic design using a single module may be more optimised due to the lack of interfaces and latency arising from data being passed between modules, as previously discussed, in a practical battlefield scenario, modularity has many real world benefits which outweigh the benefits of optimisation in this case.

5.3.2 Heterogeneity

5.3.2.1 Heterogeneous Radio Transceivers

Although heterogeneity fundamentally introduces complexity and is therefore commonly seen as a difficulty that needs to be overcome, as discussed in Chapter 3, if managed appropriately, it can be a great asset. In contrast to the existing approaches such as generic link layers which seek to obscure and hide the individual RATs from the application layer, the proposed system exposes RCMA to the attached RAT performance data, through the use of a SDM, to make RCM decisions with more complete information. Given prevailing conditions, an RCMA is able to match communications traffic with given requirements to a suitable wireless interface in order to take advantage of each radio's specific qualities. The interface design and RAT parameters, along with the allocation algorithms are discussed later in this chapter.

5.3.2.2 Black Boxing RAT Resources

To address the challenges that arise from managing diverse communications equipment, the attached equipment is treated as a set of black boxes all of which provide a common generic interface. This allows the controller to utilise potentially any underlying means of communications technology, i.e. Satellite, radio, optical, sonar, x-ray etc. to the rest of the vehicle, each communications technology appears as a generic communications interface with the ability to communicate with a certain nodes in the network (see Figure 5-3). Since HAWC enables RCMA behaviour at the application level, all lower layers of the 7 layer Open Systems Interconnection (OSI) model are abstracted and performed independently of HAWC and the rest of the vehicle platform.

HAWC does not perform network discovery, clustering, routing, QoS management, authentication, etc. Instead HAWC surrenders these tasks to the attached RAT which ensures that upgraded radio transceivers can fully utilise their own upgraded routing, clustering, etc. taking full advantage of the performance of tailored routing algorithms designed for the technology in question. HAWC evaluates the effectiveness of the RATs and their built in network discovery, routing and

clustering algorithms via their reflected performance metrics that are published to the SDM (as a requirement of being SDM compliant) and manages them via the defined generic interface according to this information.

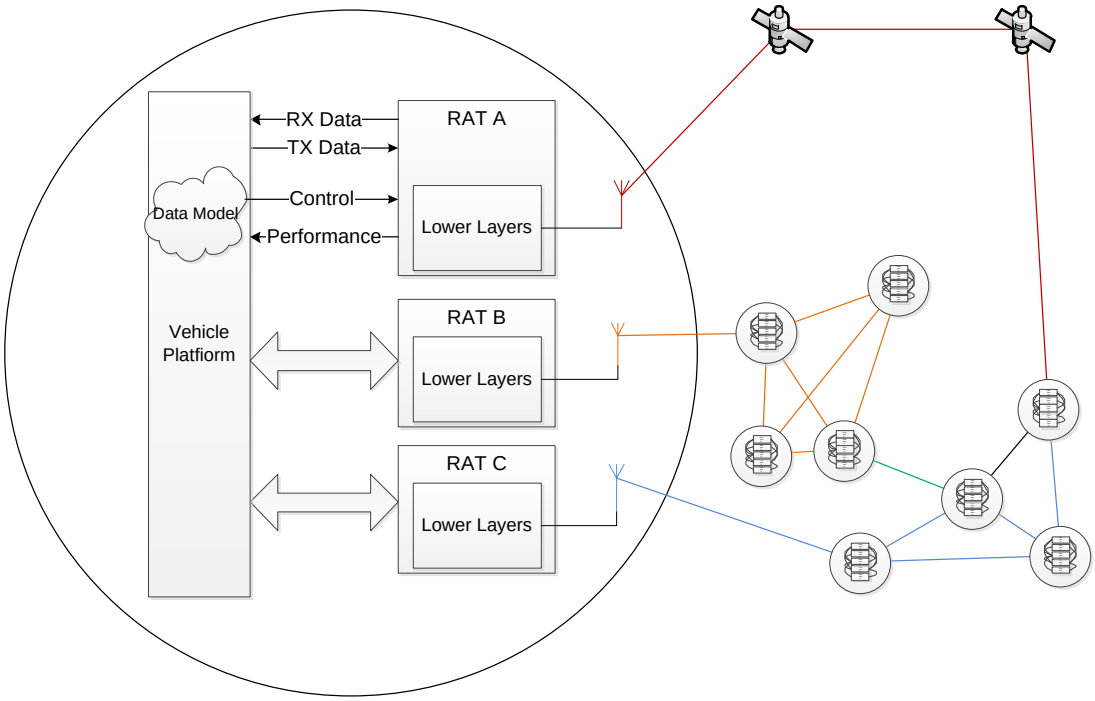

Figure 5-3 RATs as Black Boxes

5.3.2.3 Heterogeneous Traffic

As discussed previously, inter platform communication in a battlefield context consists of diverse traffic types, requiring diverse QoS. It is therefore important to transmit this data according to its requirements, for example it is of paramount importance that mission critical data is transmitted via a high safety level connection and is prioritised before low criticality or best effort data. This functionality is provided by the attached RCMAs.

5.3.2.4 Black Boxing RCMAs

HAWC is designed to contain a library of multiple modular RCMAs. Similar to RATs, RCMAs have strengths and weaknesses and thus achieve different RAT management goals with varying performance depending on the application. As discussed in Chapter 3, many different types of RCMAs exist which can be used in

specific situations in order to allocate RAT resources with maximum effectiveness at all times.

The RCMAs identified in Chapter 3 have two fundamental shared properties, they use certain input data, such as RAT performance data, traffic requirements or context data in order to arrive at a decision on which RATs to use given the current input data. Therefore RCMA can be treated as a black box given these interfaces (See Figure 5-4).

This way HAWC enables the use of state-of-the-art RCMA with minimum integration cost by enforcing modularity through defined interfaces via the SDM. When a more effective algorithm is available for a specific application, it can be added to the system to replace a deprecated RCMA or to be available in addition to the existing RCMA to provide its functionality when needed in order to take maximum advantage of what technology is available depending on the current operational condition.

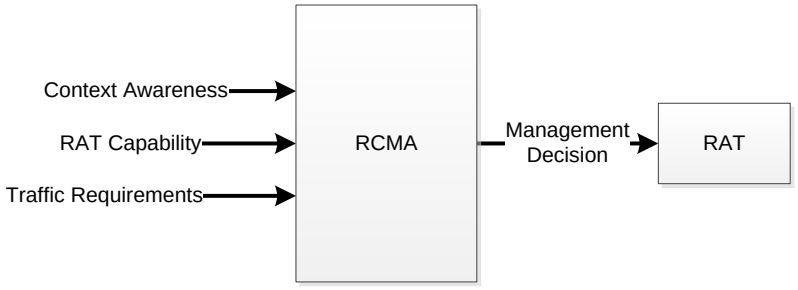

Figure 5-4 RCMA as a Black Box

5.3.3 Performance Profiles

In order to address the goal to enable RCMA by providing access to all available platform level and fleet level application data through a SDM, HAWC is designed to function on the application layer and harnesses application level awareness. Because this data is harnessed across a fleet of vehicles it must be cached locally to guarantee RCMA access to it when it is needed. For this reason HAWC is designed to provide this data via three locally cached profiles, the RAT profile, Context Profile and Traffic Profile. The profiles contain a limited number of parameters by default, but

can be extended by a subscribe request from the RCMA to the SDM. These parameters are discussed in detail in subsection 5.4.2.

5.4 Architecture Development

5.4.1 Overview

5.4.1.1 Communications Resource Allocation

In an effort to use available communications resources to best suit the current situation HAWC uses RCMA to act as a broker between communications traffic and RAT. HAWC uses available RCMA informed by the three profiles to match traffic QoS requirements with the attached RATs (see Figure 5-5).

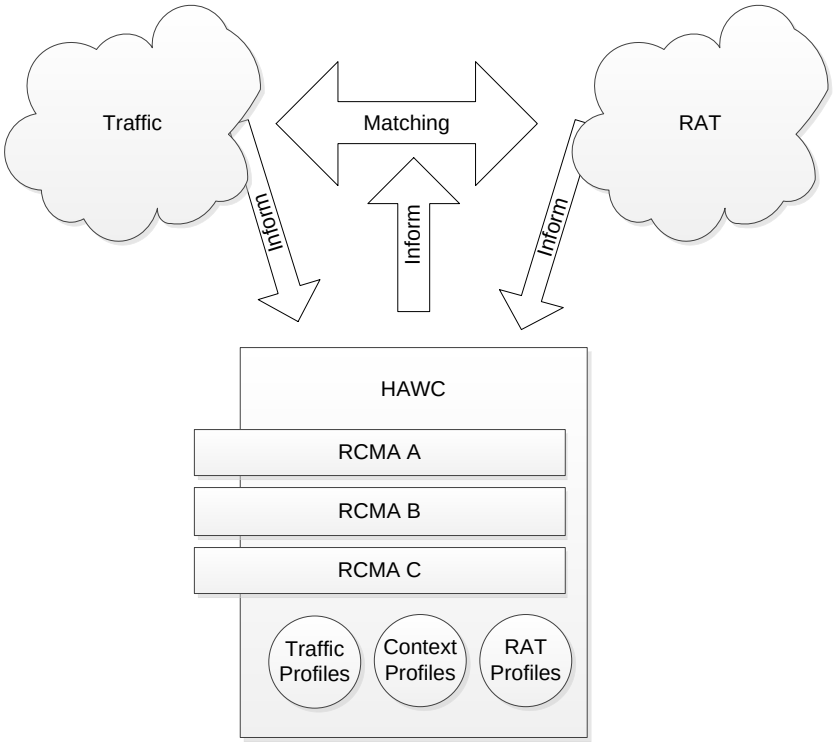

Figure 5-5 HAWC as a Broker

5.4.1.2 Physical

Each cooperating platform's HAWC system is implemented as a separate entity sharing a virtual backbone with other vehicle systems with full access to the SDM (see Figure 5-6). As a broker, HAWC matches communications data to be transmitted with the available RAT.

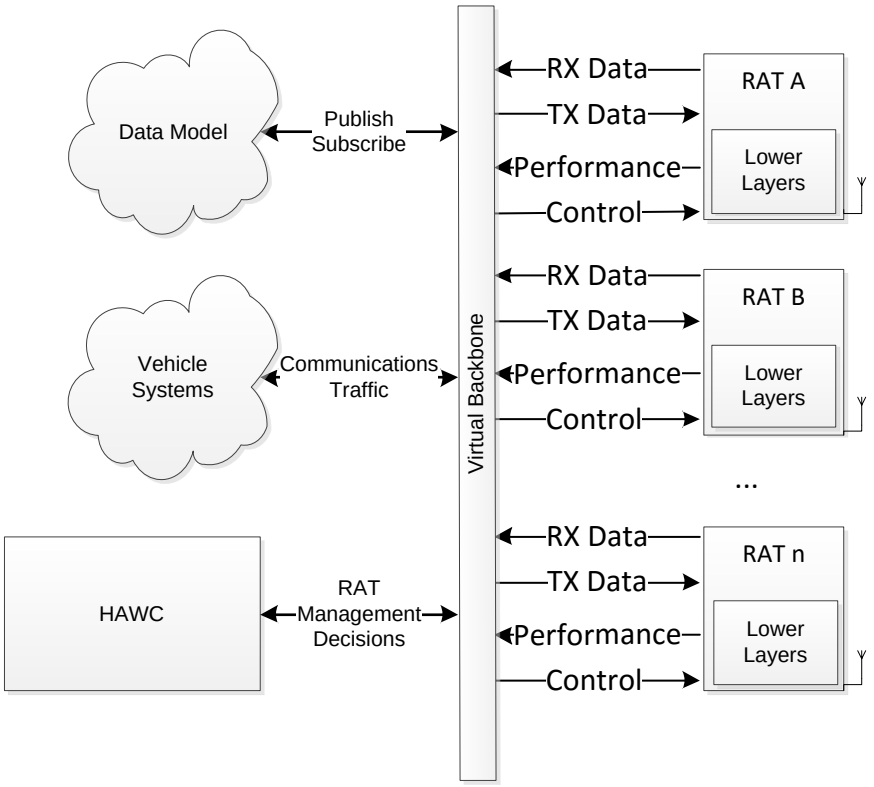

Figure 5-6 HAWC System Diagram

HAWC is comprised of several key components (see Figure 5-7):

- The **RAT Profile Handler (RPH)** generates a set of profiles which reflect the capabilities, performance and status of each attached RAT. It provides the ability to hot-plug RATs by constantly updating the associated link profiles.
- The **Traffic Profile Handler (TPH)** generates a set of profiles for each type of communications traffic that is transmitted over the network and its respective requirements.
- The **Context Profile Handler (CPH)** handles mission, situational and platform state data and generates a profile reflecting this data.
- The **RCMA Handler** uses available RCMAs depending on the context profile to match the profiles in an effort to be always best connected.

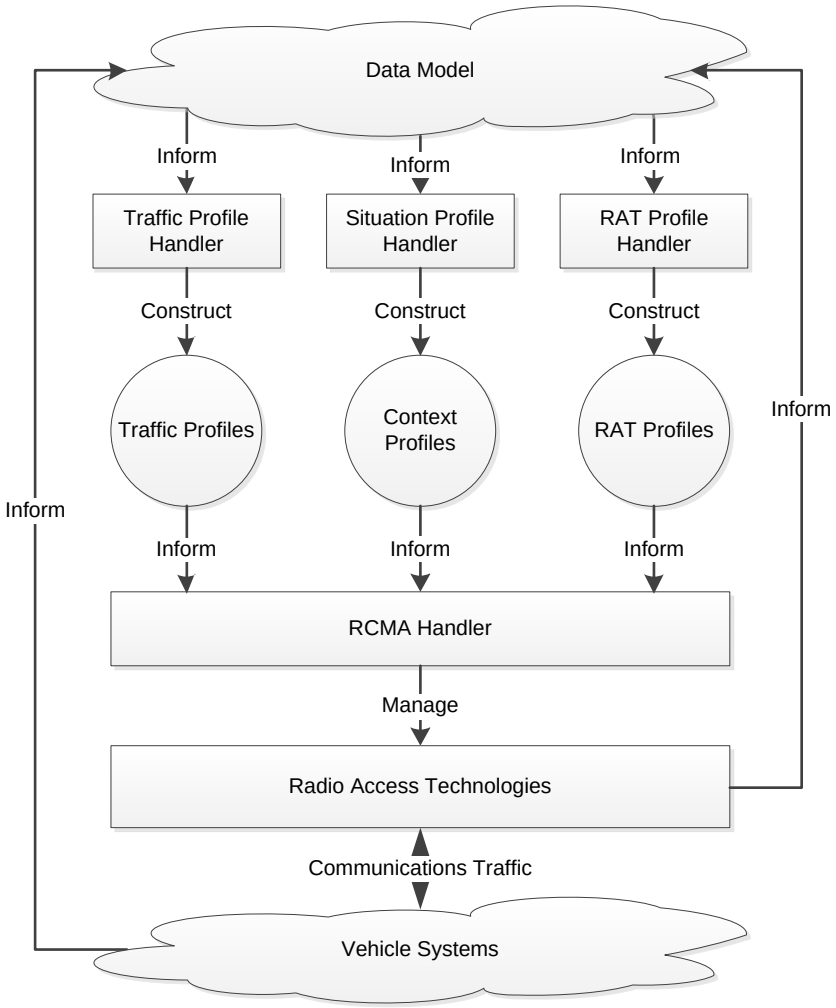

Figure 5-7 HAWC Functional Diagram

The following sections provide a detailed description of the design of each HAWC component

5.4.2 HAWC Profile Handlers

5.4.2.1 HAWC RAT Profile Handler (RPH)

RAT Performance Reporting

As battlefield vehicle subsystems are subject to interoperability and integration requirements, such as those specified by the VSI Standards and Guidelines [90], HAWC assumes all attached RATs to provide a minimum level of performance reporting via the SDM which includes mandatory continuous evaluation of basic performance metrics necessary to describe the RATs to RCMA; these parameters

have been identified in Chapter 3 and are described below. Any additional performance data provided by the attached RATs is assumed to be also available via the SDM ready for RCMA to subscribe to, on an individually negotiated basis.

Equipment Management

The HAWC RPH is responsible for the equipment management of the available radio hardware, thus it provides hardware independent plug-and-play functionality to the attached RATs in order to facilitate user friendly addition of new or improved communications hardware as well as handle the removal of damaged or deprecated communications hardware on the fly without reconfiguration of the system. This involves regularly polling attached RAT via the data model and allows HAWC to detect and register hardware which is added to the platform as well as interrogate this hardware through the SDM so that a profile can be built that describes the performance of the communications hardware unit to the rest of the HAWC system. If a radio is removed or damaged, the SDM will reflect this change by reporting the RAT unreachable or reporting a high error rate. When a RAT is missing or the error rate is over a set value, e.g. 90 %, the profile is adjusted to reflect the change in order to discourage RCMAs from attempting to select that radio link for any subsequent transmissions, at least until the radio is replaced or repaired. This constant monitoring enables HAWC to mitigate damage, interference, jamming faults and failures and offload traffic to other hardware capabilities until any deprecated capability is restored by the user or interference subsides. Similarly when a transceiver is replaced with a newer model with improved performance, the TPH recognises the new resource and re-evaluates the communication performance profile accordingly, in order to make the most use of its enhanced capability. The RPH information flow is described by Figure 5-8.

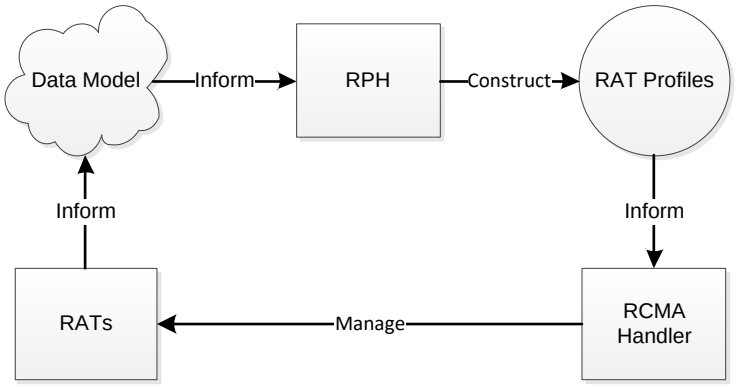

Figure 5-8 RPH Information Flow

The RPH creates a performance profile reflecting the performance of each RAT available to the platform. This reflects the most up do date information generated by the RATs and available via the data model. In a real word application the QoS data may have a certainty factor attached to it, which reflects the accuracy of the link QoS data based on context information and other factors, such as time of last update of the profile. Assessing QoS data certainty is beyond the scope of this thesis, HAWC is a modular framework for this reason; each component can be changed and upgraded as technology advances.

RAT Profile Parameters:

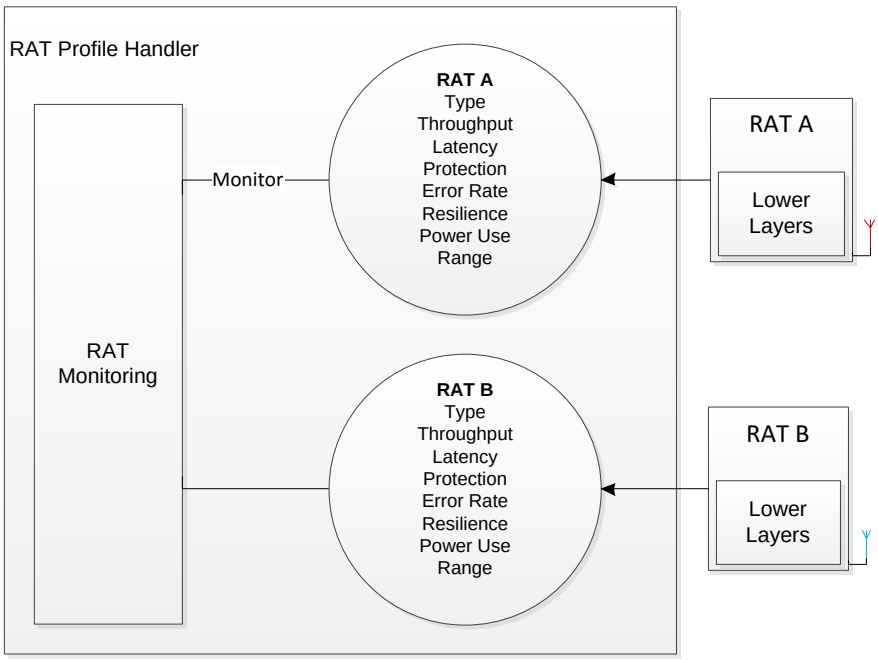

Figure 5-9 Heterogeneous RATs Identified by RAT Profiles

Applicable RAT Profile Parameters necessary for RCMA to make management decision have been identified in Chapter 2 and 3. The following parameters are contained in the RAT profile (see Figure 5-9 for examples):

- Knowledge of the **RAT Type** is a vital metric for many platform level RCMA exploiting RAT diversity [18, 27, 30, 97, 114, 115, 121-123, 126]. The RAT profile expresses RAT Type as a string containing the RAT standard, e.g. 802.11ac.
- The **Throughput** of a link including its minimum, maximum and average value is a vital and basic metric to determine if a link is able to transmit data at the required speed. Several RCMA identified use different RAT depending on the remaining link capacity [124] or perform throughput sharing among different types of traffic [125]. Throughput is also a commonly used metric for Multiple Attribute Decision Making algorithms. Throughput is expressed as an array with maximum, minimum and average throughput in Mbps.
- The link **Latency** including its minimum, maximum, average and jitter value is a vital metric when transmitting time critical data. Although Latency is typically a characteristic of a network as opposed to a RAT, in some cases the type of technology may be the limiting factor, for example satellite communications commonly have a high latency value [53] whereas 3G typically has a low latency. Latency is expressed as an array with maximum, minimum, average and jitter in ms.
- The **Protection** capability of a link is a measure of its encryption, authentication and authorisation capabilities. Data with a high security level must be transmitted using a RAT with a sufficient Protection Capability. In a battlefield context, resource assignment based on protection is vital since it may be necessary to transmit restricted information over the air, such as mission data. Protection is expressed as a range from 0-9 with 0 as the highest protection level and functions as a requirement for security level, i.e. data with a security level of 5 must be transmitted with a RAT capable of protection level 5 or better.

- **Error Rate** of a link may be used by RCMA or by other system to determine the historical availability of a RAT to infer future availability. Error rate is expressed as a percentage.
- The **Resilience** of a link is a measure of the reliability of a communications link. This is a particularly important metric when transmitting safety critical data such as an armament discharge command. The RCM suite must ensure that safety critical data is transmitted over a link with an appropriate safety level in a timely manner. Resilience is expressed as a range from 0-9 with 0 as the highest resilience level and is matched with Traffic Safety Level requirements.
- The **Range** of the RAT including minimum, maximum and typical range may be used by RCMA as indication for determining link reliability to neighbours. RAT range is expressed in metres (m).
- As previously discussed, the **Power Consumption** of an attached RAT including idle, transmitting and receiving power requirements are important metrics for RCM particularly on small vehicles with stringent resource constraints. Power consumption of different RAT may be used to significantly alter RAT assignment [126]. Power consumption is expressed as an array of idle, rx and tx power consumption and measured in Watts (W).

In order to accurately describe the performance and characteristics of different RATs, it would be necessary to include a multitude of additional information. The above list of parameters has been identified from related work, however, it is clear that future RCMA may use additional performance metrics, thus HAWC has been designed in an extendable fashion. RCMA are permitted to subscribe to any information available from the SDM and thus the RPH can be amended at any time during the operation of the systems by an attached RAT publishing or an RCMA subscribing to additional information.

5.4.2.2 HAWC Traffic Profile Handler (TPH)

In order to enable RCMA to match traffic types with appropriate RATs, the traffic is represented by requirement parameters. When traffic is to be transmitted from one of the vehicle systems using an available RAT, the traffic profile handler accesses the requirement parameters of the traffic via the SDM and an RCMA selects an appropriate set of RATs to transmit the traffic. The communications traffic does not pass through HAWC itself, it travels from its origin via the vehicle backbone to the selected RAT and is transmitted off platform. See Figure 5-10 for the TPH information flow diagram.

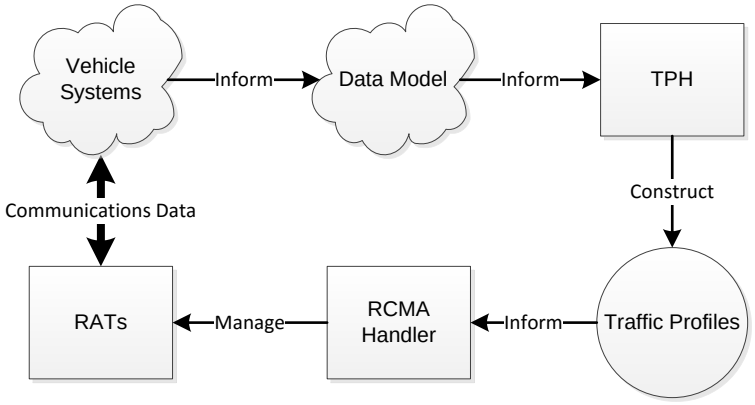

Figure 5-10 TPH Information Flow

HAWC Traffic Profile Parameters:

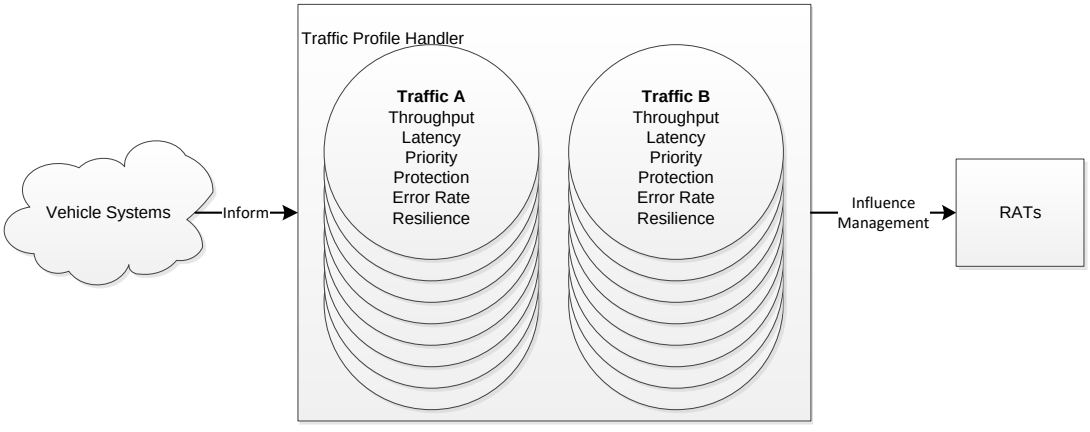

Figure 5-11 Heterogeneous Traffic Identified by Traffic Profiles

As discussed previously, dynamic and diverse traffic is transmitted over battlefield networks, the properties of which have a direct impact on the type of RAT to be

selected for transmission of this data. The following traffic requirement parameters are contained in the Traffic Profile (see Figure 5-11 for examples):

- The **Throughput** requirement of certain types of data, such as large file transfers or continuous video or audio streams enables resource assignment and may reduce unexpected strain on the network. In some cases the throughput required by certain traffic may be too large for a given RAT, thus a different RAT must be chosen. Throughput is expressed as a minimum throughput requirement in Mbps.
- Especially for time critical data, the **Latency** requirement by a data transmission may influence the type of RAT chosen for transmission, e.g.[97] sends data either on a WWAN or WLAN interface depending on the time criticality of the data. Latency is expressed as a maximum latency requirement in ms.
- **Priority**. Although methods exist to infer the priority of a type of traffic [157], in a battlefield scenario where mixed priority data is commonly transmitted on wireless links, the data priority hierarchy is known in advance and traffic is marked according to its priority level. It is therefore assumed that the priority of any traffic transmitted or received by HAWC is known. Priority is expressed as a range of 0-9, 0 being the highest priority.
- **The Security Level** of communications traffic must be recognised by the RCMA in order to ensure that traffic with a high security level is only transmitted via RAT which is capable of providing the required protection capability. Security level is expressed as a range from 0-9 with 0 as the highest security level to be matched with RAT protection level.
- **Safety Level** requirement is a measure of the importance successful delivery of the data. It may range from “best-effort” for non-critical data to “safety critical” for the most important types of data. As discussed previously, in a battlefield context traffic may have highly diverse resilience requirements which may impact RAT selection. Safety Level is expressed as a range from 0-9 with 0 as the highest Safety Level and is matched with RAT resilience level.

5.4.2.3 Context Profile Handler (CPH)

The Context profile handler provides application aware RCMAs access to mission, situation and platform state data via the SDM. In contrast to the other two profiles, the Context Profile contains context information from the platform and fleet SDM. See Figure 5-12 for the SPH information flow.

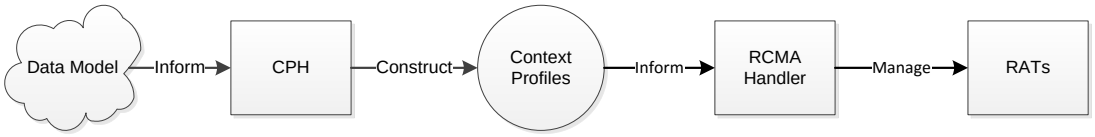

Figure 5-12 SPH Information Flow

HAWC Context Profile Parameters:

In order to fulfil the goal to make all relevant application level information available to the RCMA, HAWC provides RCMA access to context data necessary to fulfil modern vehicle platform communications requirements. Context information can enable RCMA to make RAT management decisions based on additional relevant information such as mission goals, situational awareness data and vehicle status. Therefore the CPH Context Profile is split into three categories: mission data, situational data and platform state data. Additional application dependent information required by any RCMA must be requested from the SDM by the RCMA and is subsequently also contained in one of the context profiles (see Figure 5-13).

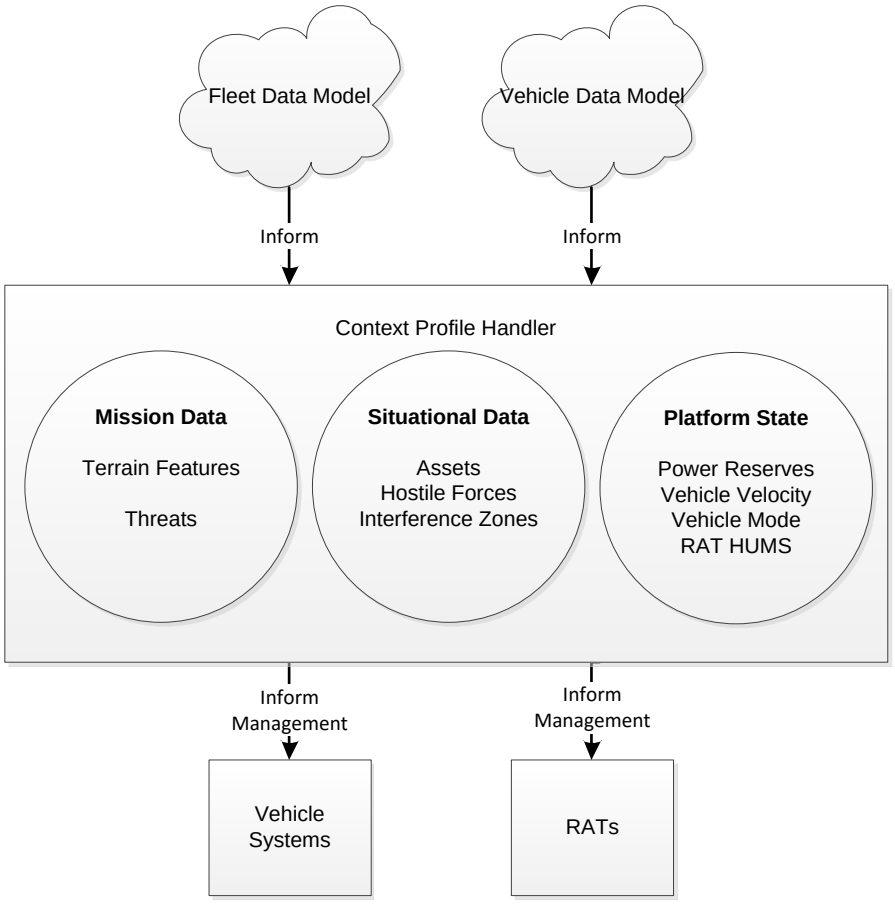

Figure 5-13 CPH Context profiles

Based on the RCMA analysis in Chapter 3, to provide a basic level of service, several parameters for each of the categories are provided by HAWC by default:

Mission data includes Battle Management System Data [158]. Detailed BMS information is restricted; therefore the exact parameters used depend on the implementation of the BMS Data in on the SDM. Mission awareness such as the terrain and scope of a mission, as well as the anticipated threat level within a certain area may be critical information towards the success of the mission and may thus be essential to making an appropriate communications policy decision autonomously.

- **Mission Terrain Features** encountered throughout a mission may be of critical importance in achieving reliable communications in avoiding jamming and signal attenuation due to physical obstructions in a diverse battlefield [27]. As discussed previously, particularly urban scenarios are challenging for wireless communications [24]; RCMA utilising suitable RAT may significantly improve communications effectiveness in these scenarios.

Mission Terrain Features are expressed as a list of arrays which lists the location, range and type of feature.

- **Mission Threats** may influence the appropriate choice of RAT, since some RATs such as UWB are fundamentally harder to locate than others, depending on the threat they may be favoured. Conversely since certain threats may be aggravated by certain types of RAT, e.g. an IED detonated by a certain frequency range, in other cases narrowband communications should be favoured. Mission Threats are expressed as a list of arrays which lists the location, range and type of threat.

Situational data includes C4I data from the platform BMS. As discussed previously, weather conditions and hostile terrain can each have a significant impact on the communications effectiveness of vehicle platforms. The avoidance of danger by taking into account the location of hostile forces can prevent node loss and avoid network fragmentation. Therefore the use of situational awareness data to influence communications RCM decision making can improve a fleet's communications effectiveness.

- **Geographic location of assets** in conjunction with the radio capabilities of those assets allows the node to infer several kinds of information, such as network topology density and distance to next hop neighbours. Knowledge of the location of other vehicle platforms in the fleet may cause RCMA to favour RAT capable of multipath routing [6, 131]. Asset Locations are expressed as a list of arrays which lists the location and type of asset.
- **Geographic location of enemies** can significantly improve survivability by enabling RCMA to favour less detectable RAT when in the vicinity of hostile platforms. Hostile node locations are expressed as a list of arrays which lists the location and type of hostile node.
- **Geographic location of Interference Zones**, such as dense foliage, frequency spectrum jamming or areas with adverse weather conditions allow resource management algorithms to make decisions which aid the availability of the network [8]. If a node is present within a certain kind of interference zone, a capable RCMA can select a RAT with a higher resilience, e.g.

capable of Electronic Protection Measures (EPMs) to penetrate the interference. Interference Zones are expressed as a list of arrays which lists the location, range and type of interference zone.

Platform State data indicates the overall status of the vehicle:

Maintaining communications capability is an important mission goal for vehicle platforms in a battlefield context, however, in certain situations the behaviour of the communications suite should be adjusted based on other higher priority mission goals, such as remaining platform power, platform damage etc. Therefore vehicle awareness data may have significant impact on the goals of the communications suite and thus also alter the requirements for wireless communication.

- **Power Reserves** may inform the capability management suite to use more conservative communications policies, especially in battery powered UGV where the communications suite consumes a significant amount of power compared to the rest of the vehicle. Algorithms such as CAHN [126] use radio power consumption as a metric for RAT selection. Because depleted platform power reserves can be a mission ending condition [6], power reserves can influence RCMA decision making in significant ways. Power reserves are expressed as a percentage.
- **Platform Velocity** may be an indicator for the confidence in short range multihop RAT performance. Since neighbour tables go out of date quickly in networks comprised of mobile nodes, a high velocity may indicate a more dynamic network topology. RCMA such as [97] therefore use node mobility to factor into their RAT selection. The CPH provides velocity in km/h.
- **Health and Usage Monitoring System (HUMS) Data** provides information about the health and damage of individual components on the vehicle which can be made available to the RCMAs. RAT Health can be used to request repairs or to figure into the RAT selection process. RAT Health is expressed as a percentage.
- **Vehicle Mode** may significantly change the way communications capabilities are assigned. For example if a vehicle is operating in stealth mode in order to avoid detection, wireless communications may be reduced

to a minimum, or avoided completely. During limp mode, critical damage to the vehicle may impose stringent limits on resource allocation. Mode is expressed as a string; RCMA need to have policies in place to activate given a specific vehicle mode.

5.4.2.4 RCMA Handler

Management of diverse traffic transmitted via heterogeneous mobile nodes in the battlefield is a nontrivial problem. As discussed, many Resource and Capability Management Algorithms exist which are able to leverage limited available RAT resources to create effective communications capabilities in a variety of scenarios and research into these algorithms is active and ongoing. From an RCM perspective there is no silver bullet; no single RCMA improves QoS in all cases. Variable mission, environmental and Context parameters have an impact on what the optimum resource management solution is at any moment [97, 114, 115].

The RCMA Handler is a central component of the HAWC architecture; it contains the algorithms responsible for the RCM decision making. It is designed to enable any applicable RCMA to perform resource assignment and make the best possible resource assignment decision at any given time by providing up-to-date, application level information gathered by the RPH, TPH and SPH (see Figure 5-14).

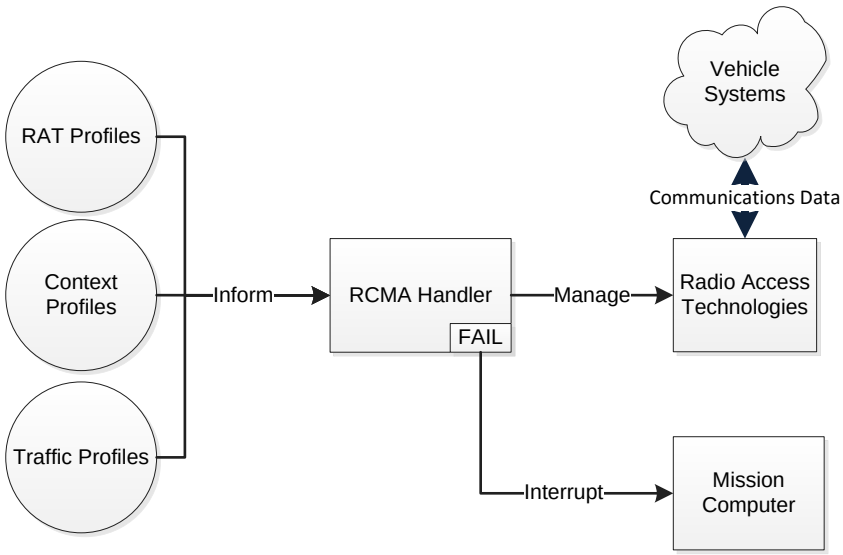

Figure 5-14 RCMA Handler Information Flow

RCMA Activation Policy

In order to fulfil the goal to enable seamless switching between RCMA with minimum integration cost, the RCMA Handler is designed to contain multiple concurrent RCMAs, each with different resource and capability management behaviour informed by the Link, Context and Traffic profiles and enabled depending on context data. Different algorithms will be used to perform the resource assignment in order to achieve behaviour which is appropriate to the situation. Figure 5-15 shows a schematic of the RCMA Handler.

In order to decide at which time and under which condition the different RCMA are enabled, each RCMA must also be accomplished by a policy entry. These policies may be phrased as simple if statements:

IF condition = x THEN enable RCMA(1) ELSE enable RCMA(2); etc.

For example, in order to invoke CAHN when the platform power reserves drop below a certain level, the corresponding RCMA activation policy will be:

IF platform.power.reserves =< 50 % THEN enable CAHN ELSE enable FAILOVER.

In line with the modularity of HAWC, algorithms can be swapped and reconfigured depending on prevailing operational requirements. The actual operation of these algorithms and how they are triggered is entirely application dependent and is therefore determined by the RCMA themselves.

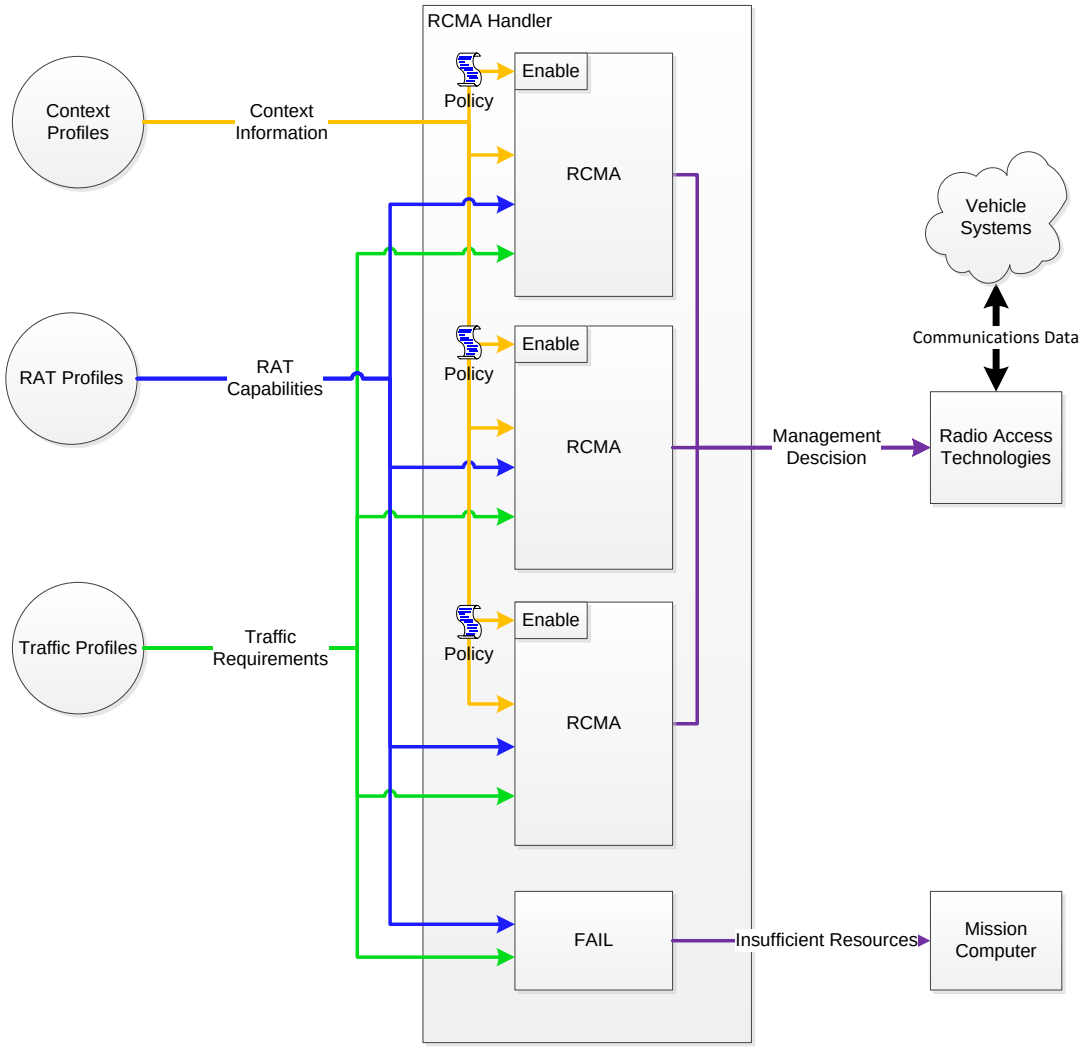

Figure 5-15 Context Based RCMA Switching

Communications Failure

When all RATs on the platform are damaged or the network becomes segmented and HAWC is unable to reconnect the network solely by using different RATs, such as a SATCOM link or a long distance link, etc. then maintaining network connection is beyond the capabilities of HAWC and additional platform level or fleet level resources have to be requested. In order to gain additional resources in the form of additional, or more powerful RATs or to prompt fleet level topology management to reconnect the vehicle platform with other platforms in the fleet it is necessary to report the failure of HAWC to the Mission Computer (see Figure 5-14 and Figure 5-15).

Since maintaining effective communications capability is one of several mission goals with a given priority, the mission computer must weigh the importance of this goal against its other goals. Depending on the criticality of other mission goals as well as the context and type of platform, the mission computer may proceed in a number of ways. In a manned vehicle the mission computer may alert the crew via an advisory or alert message and advise the crew on the calculated best course of action including various outcomes and the crew will decide how to react to the situation. In an unmanned vehicle if the mission computer deems communications as a high enough goal, the platform may be chosen as a network topology repair node and re-tasked to bridge the gap between two separated network segments. Fleet level topology and resource management of this type is discussed further in Chapter 6.

5.5 Evaluation

5.5.1 Experiment Design:

In order to evaluate HAWC against its stated goals a series of experiments have been derived and HAWC has been subjected to the VSI Standards and Guidelines Compliance Test.

5.5.1.1 Experiment 1: Equipment Management

A steady state, agent based simulation is developed using the Battlefield Network Simulation Tool. Each mobile node is modelled as an agent in a 2D environment. A complete description and discussion of the developed Battlefield Network Simulation Suite is included in Chapter 4.

The agents represent a fleet of HAWC enabled sentry nodes; each agent is equipped with two RATs, the primary RAT is a low power consumption, low bandwidth point to point FM radio with a range of 1000 m and a throughput of 0.5 Mbps; the secondary RAT a high power consumption, high bandwidth multi-hop 802.11a transceiver with a range of 250 m and a throughput of 22 Mbps. Ten stationary sentry nodes guard a 200 m x 200 m perimeter around their base station (see Figure 5-16) and transmit a periodic basic telemetry including a heartbeat signal to register that they are still alive and periodic video frames to their base station which is

capable of receiving any communications data using any RAT type. Sentry nodes remain within range of their base station at all times.

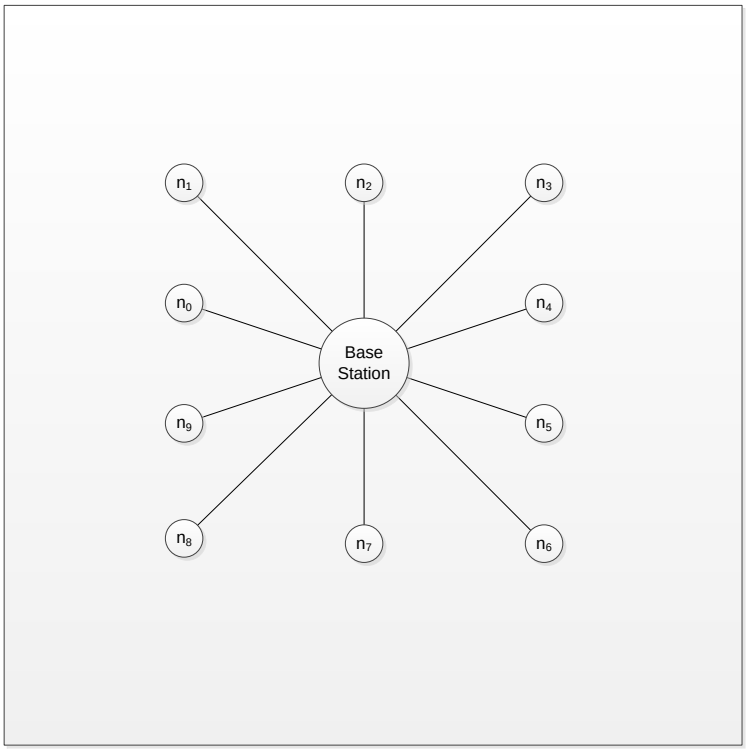

Figure 5-16 HAWC Evaluation, Experiment 1: Sentry Nodes

Table 5-1 HAWC Evaluation, Experiment 1: Simulation Parameters

FM Range	1000 m
802.11 Range	250 m
Mobility model	Perimeter
Total number of Nodes	11
Node Speed	0 km/h
Scenario duration	300 s

At t = 0 s node n1 operates within normal parameters and thus transmits a periodic heartbeat on its primary, low throughput FM transceiver and periodic video frames via its secondary, high throughput 802.11a transceiver.

Prolonged operation in a harsh environment has caused the degradation of the 802.11a transceiver of the sentry node, thus at t = 100 s, the 802.11a transceiver fails

permanently and the node is no longer able to transmit video data back to its base station.

At t = 200 s, a maintenance engineer replaces the 802.11a with a different RAT by removing the faulty LRU containing the 802.11a transceiver and substituting an available functional 802.11b unit with a range of 250 m and a throughput of 11 Mbps.

5.5.1.2 Experiment 2: Context Based RCMA Switching

In order to further evaluate HAWC against its goals, experiment 1 has been modified and the simulation is repeated. The purpose of experiment 2 is to evaluate HAWC against its stated goals to:

- Enable RCMA by providing access to all available platform level and fleet level application data through an SDM.
- Facilitate the use of multiple modular RCMA and to enable seamless switching between these RCMA.

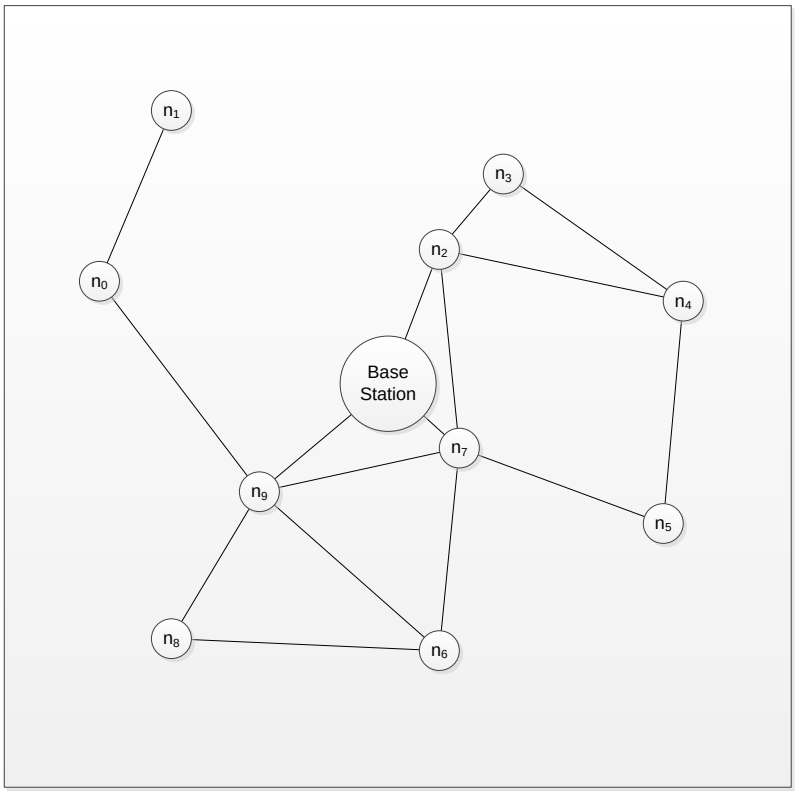

Figure 5-17 HAWC Evaluation, Experiment 2: Sentry Nodes

The sentry nodes are now moving according to a random waypoint mobility model within a 500 m^2 environment with the base station at its centre (see Figure 5-17).

The sentry nodes are equipped with the point-to-point FM transceiver connected directly to the base station and the 802.11a transceiver transmits data back to the base station via multi hopping. HAWC's RCMA handler is equipped with the failover algorithm [113] and the synergetic RCMA CAHN [126].

The failover algorithm always favours the higher throughput 802.11a transceiver and uses the FM Transceiver as a backup channel if the 802.11a channel fails due to node mobility. CAHN seeks to preserve power by using the low power FM transceiver for configuration data and only enabling the high power 802.11a transceiver when necessary. The RCMA Activation policy switches from the failover algorithm to CAHN when the vehicle drops below a power level of 50 % in the platform state profile. This is triggered by a timer at t = 150 s which sets the power reserves to 49 %.

5.5.1.3 VSI Standards and Guidelines Compliance

In an effort to assess the level of integration and interoperability of the proposed system as per an accepted methodology of assessment of battlefield vehicles, HAWC has been subjected to the VSI Standards and Guidelines compliance study. The VSI compliance rating has been performed using the VSI Standards and Guidelines Metrics for Electronic Architecture Assessment [91].

The purpose of this experiment is to evaluate HAWC against its stated goals to be modular and flexible in compliance with the VSI Standards and Guidelines

Methodology of This Test

The VSI Standards and guidelines use a qualitative assessment of a vehicle systems based on how the system under test compares with predefined statements in the VSI Vetronics Standards and Guidelines. Statements in the document are compared to the performance of the system and the category is scored according to which statement matches closest with the performance of the system. The statements are designed so that one of the statements matches each possible case.

As an example of the test's methodology, the first characteristic of the first metric, adaptability, is scored according to the following table:

Table 5-2 VSI Standards and Guidelines Adaptability Scoring Matrix

Score:	5	4	3	2	1
Matching Statements	All relevant changes can be made in the field (i.e. with available tools and skills and in an acceptable time) without making any modifications to parts of the system/platform.	All relevant changes can be made in the field with only minor modifications needed. OR The majority of relevant changes can be made in the field without making any modifications.	The majority of relevant changes can be made in the field with only minor modifications needed.	The minority of relevant changes can be made in the field with no, or only minor, modifications needed.	No relevant changes are possible in the field.

In this case, all components attached to HAWC, the RAT, the RCMA and the data accessible via the SDM can be changed in the field without modifications to the vehicle platform; therefore the performance of HAWC most closely matches the first statement and is therefore scored with 5: all relevant changes can be made in the field without making any modifications to parts of the platform.

5.5.2 Results and discussion

5.5.2.1 Experiment 1: Equipment Management

At t = 0 s the sentry nodes are operating within normal parameters. Figure 5-18 shows the outgoing traffic of a single sentry node transmitting a periodic heartbeat and video frames via FM radio and 802.11a respectively.

At t = 100 s the 802.11a transceiver fails and video frames seize to be transmitted. HAWC detects the degradation; the node continues to transmit its heartbeat via the FM radio.

At t = 200 s the new 802.11b transceiver is added to the system. The new transceiver registers itself in the SDM and the RPH detects the new resource. It builds a new Link Profile for the 802.11b RAT and enables the RCMA to use it seamlessly.

At t = 212 s the sentry node resumes periodic video frame transmission on the now secondary 802.11b link. Both transceivers continue to be monitored by the RPH.

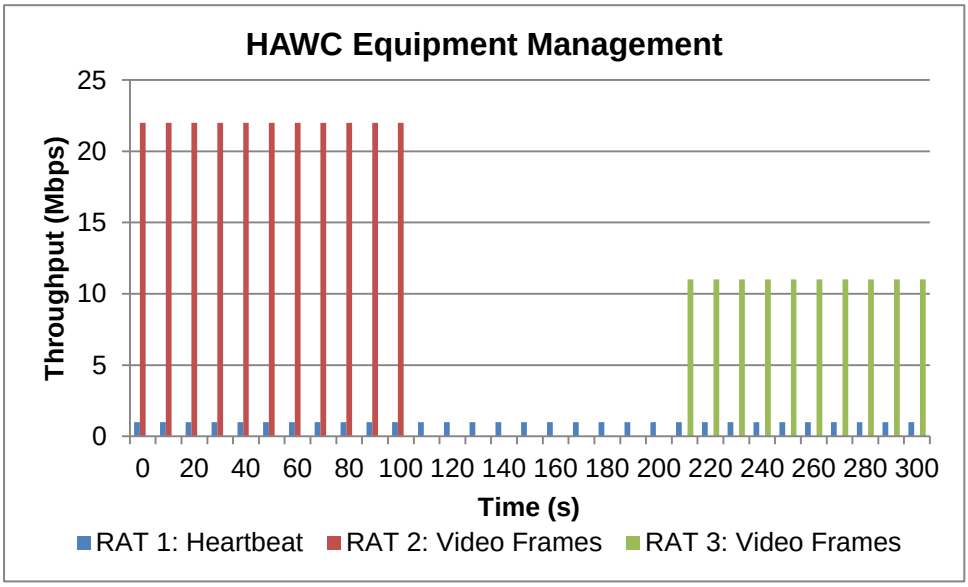

Figure 5-18 HAWC Evaluation, Experiment 1: Equipment Management

Despite this seemingly simple result, in the context of an NEC scenario this functionality represents a powerful capability to use any available communications LRU in any vehicle platform to enable effective communications. When a communications resource is degraded, it is no longer necessary to replace like for like, but any failed communications equipment can be replaced by any other available RAT seamlessly and with zero integration cost, which is a significant improvement over the current state-of-the-art discussed in Chapter 2 and Chapter 3.

5.5.2.2 Experiment 2: Context Based RCMA Switching

As the nodes randomly travel around the base station, while the FM transceiver remains permanently connected to the base station, due to its range of 250 m the connection of the 802.11a transceiver to the base station is intermittent.

At t = 0 s the sentry nodes are operating normally and are using the failover algorithm to transmit video frames via the 802.11a transceiver. At t = 70 s Figure 5-19 shows that when no route can be established back to base via multi hopping due to node mobility, the failover algorithm transmits the video frames over the FM radio instead.

At t = 150 s the vehicle power reserves drop below 50 %; application layer context information reflects this and the RCMA activation policy causes the RCMA Handler to switch to the CAHN RCMA. CAHN uses the FM Radio for configuration data and uses the 802.11a transceiver only when a viable route exists and a new frame is ready to be transmitted. When no route can be established, CAHN is unable to transmit video frames.

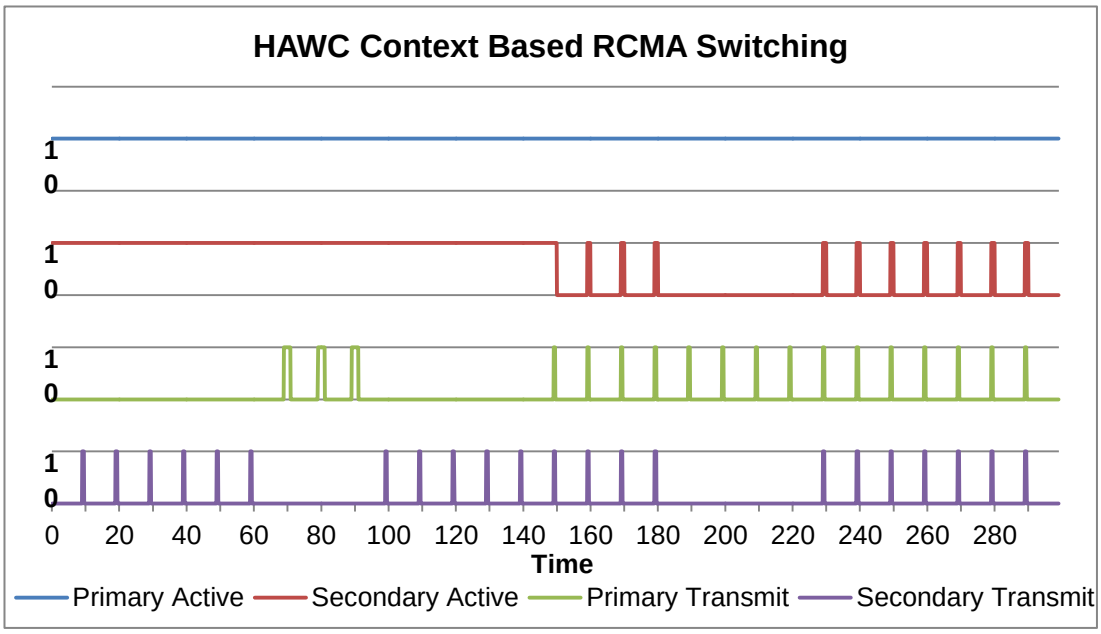

Figure 5-19 HAWC Evaluation, Experiment 2: Context Based RCMA Switching

This experiment has shown how HAWC facilitates the use of advanced RCMA by leveraging platform level and fleet level application layer data from the SDM and how this context data can be used to switch between different RCMA seamlessly without the need for major reconfiguration of the communications system.

5.5.2.3 VSI Standards and Guidelines Compliance

The results of the test are as follows:

Reconfigurability

Adaptability. As demonstrated in the above example, HAWC performs equipment management which constantly monitors the status of existing RAT resources and scans for newly available resources. HAWC offers the capability to change components such as radio units easily in the field, system algorithms etc. can be reconfigured on the fly with available tools and skills.

Matching VSI statement: All relevant changes can be made in the field (i.e. with available tools and skills and in an acceptable time) without making any modifications to parts of the system.

Score: 5.

Interchangeability. All elements of the system can be moved between platforms with minor modification at zero integration cost. HAWC and its attached systems are identical for all platforms and thus ensure complete interchangeability. More specifically, the attached RAT LRUs and the RCMA used within HAWC can be hot swapped with near zero cost.

Matching VSI statement: All relevant system elements can be moved between all relevant platform types in the field (i.e. with available tools and skills and in an acceptable time) without making any modifications to the system/ platform.

Score: 5.

Enhanceability

Capacity. The relevant capacity aspects of the system are limited by the hardware it is attached to and the information available through the SDM. HAWC itself does not impose a capacity limit on the RATs, RCMA or traffic. For all relevant aspects, the system has more capacity than is needed.

Matching VSI statement: For all relevant aspects (interface bandwidth, processing, protocol /message structure capacity, power supply, physical space, etc.) of the system, the architecture has more spare capacity than is needed, as suggested by experience and predictions of future need.

Score: 5.

Modularity. HAWC is highly modular in terms of hardware and software. Every relevant part of the system, such as the RCMA, the attached RAT and the communications controller itself are can be changed and substituted by alternatives.

Matching VSI statement: The architecture is highly modular.

Score: 5.

Enablers. Skills necessary to enhance the communications resources of the systems are available in depth. To upgrade RATs attached to the HAWC, the user can simply connect and disconnect RAT LRUs. While radios can be replaced in a relatively simple fashion, integration of new algorithms in the field requires some level of specialised knowledge.

Matching VSI statement: Some important relevant skills, etc. are available in depth.

Score: 3.

Integration

Internal Platform Data Provision. Internally, the system is designed to build upon the platform SDM which is assumed to provide intra vehicle communication in a timely and secure manner. The design of HAWC does not harm this functionality, therefore, all data is accessible from the rest of the platform in a timely and secure manner through the SDM.

Matching VSI statement: All relevant information is available in a timely and secure manner

Score: 5.

External Platform Data Provision. HAWC interfaces with the fleet level SDM which is assumed to provide inter vehicle communication in a timely and secure manner. However, due to damage or interference, an appropriate radio may not always be available, hence, it can be said that the majority of data can be transmitted and received in a timely and secure manner.

Matching VSI statement: The vast majority of the data is transmitted and received in a timely and secure manner.

Score: 4.

System Control. As provisioned by the platform SDM, information is accessible by simple publish and subscribe mechanisms. It is assumed that the SDM provides reliable access to intra vehicle resources, therefore within the platform all relevant resources can be controlled by users or subsystems in a secure manner.

Matching statement: All relevant resources can be controlled by users/subsystems in a secure and safe manner and with an acceptable quality of service under all relevant conditions.

Score: 5.

Integrated Logistics Support

Built In Test (BIT). The radios attached to HAWC are required to perform Built in Test and publish the results to the SDM. HAWC itself does not perform BIT, however, relevant RAT BIT data is published to the SDM and the architecture supports routing of BIT data.

Matching VSI statement: A minority of main LRUs generate BIT and the architecture supports the routing of the BIT data.

Score: 3.

ILS Data Transfer. Metric is not applicable, since the transfer of data is contingent on the RAT attached to HAWC.

Matching VSI statement: Note that if parts of an architecture, or logical architectures, are assessed individually then this metric will not always be applicable. When it is not applicable no mark (0) should be assigned.

Score: 0.

System Scalability

Vertical scalability. Significant gains in performance of existing hardware can be achieved with simple replacement of modular algorithms. HAWC can be upgraded to run on more powerful hardware if required.

Matching VSI statement: Significant increased performance is possible through exploiting existing spare capacity or through “form and fit” module replacement.

Score: 5.

Horizontal scalability. The system is able to scale significantly by adding or removing resources, such as RATs and RCMA. If more RATs are added to the system, significant gains in capacity can be achieved and synergy can be created by using appropriate RCMA; the utility of the available resources can be improved by adding upgraded RCMA to the HAWC. RAT can be removed to scale the system back, e.g. for unmanned vehicles to save mass and reduce power consumption.

Matching VSI statement: Significant increases in performance across a number of areas are possible by the addition of different system elements. Adding system elements requires minimal user intervention.

Score: 5.

Openness

Standards & Technology Selection. The majority of recommended VSI standards and guidelines are to be followed in the implementation of the system. Otherwise communication occurs via the SDM.

Matching VSI statement: The majority of standards and technologies used are combined from the VSI recommended lists or open standards AND any non-open standards used are fully justified

Score: 3.

Documentation. Detailed end user documentation does not exist for the system.

Matching VSI statement: High quality documentation does not exist for any of the relevant aspects of the architecture.

Score 1.

ICDs. An interface control document does not exist.

Matching VSI statement: There is no populated ICD

Score: 1.

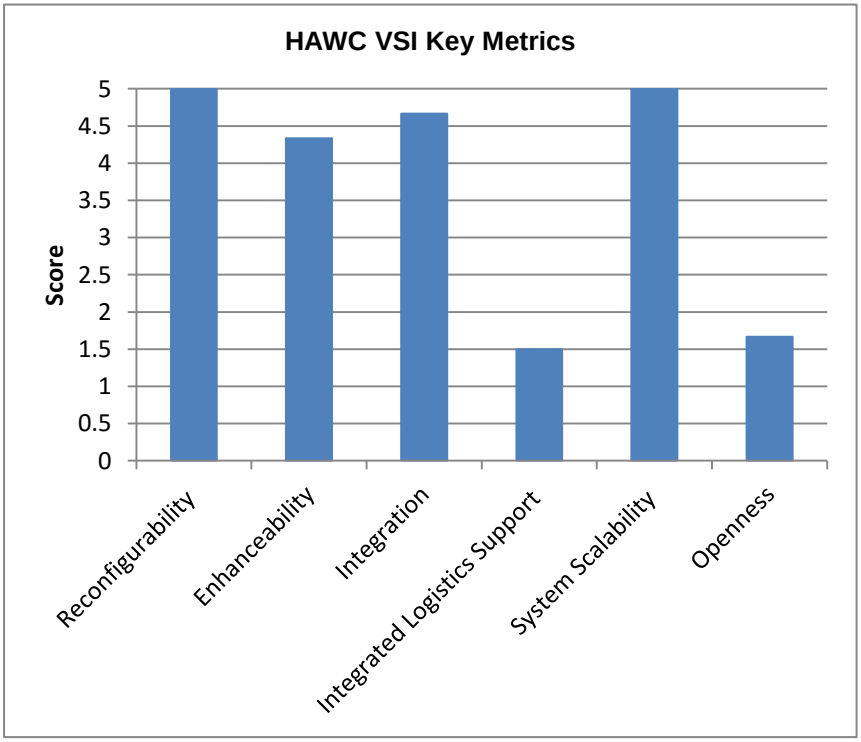

Figure 5-20 VSI Compliance Key Metrics

HAWC scores highly in the areas of Reconfigurability and System Scalability. Enhanceability and Integration score 4.3 and 4.7 respectively due to the skillset needed to alter system algorithms in the field the fact that the reliability of the attached radios cannot always be guaranteed by HAWC itself. Integrated logistics support and openness score at 1.5 and 1.7 respectively due to ILS being solely a factor of the attached radios and the lack of detailed user documentation required for deployment in the field (see Figure 5-20).

See Figure 5-21 for a breakdown of the individual characteristics that comprise the key metrics:

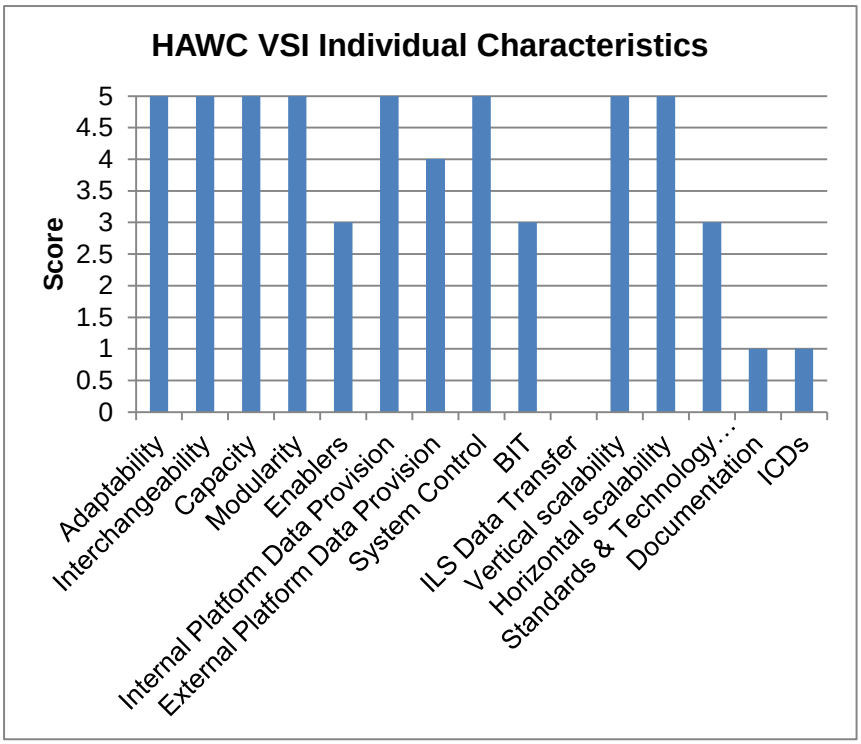

Figure 5-21 VSI Compliance Characteristics

5.6 Conclusions

Battlefield communications networks transport a variety of traffic types with diverse requirements using diverse equipment on heterogeneous vehicle platforms subject to a harsh and unpredictable environment. In this context it becomes necessary to employ a system which manages a vehicle's communications resources while considering current mission goals, situational awareness data and vehicle platform data.

This chapter presents the High Availability Wireless Communications (HAWC) system, a context aware, application layer communications framework designed to enhance communications effectiveness between battlefield vehicles on the platform level. HAWC uses relevant context information from a common Shared Data Model (SDM) to use available platform resources most effectively at all times. By gathering information from the platform level and fleet level SDM, HAWC is highly integrated with other systems within the vehicle platform and other vehicles in the fleet. This way HAWC is simultaneously enabled by shared information via the SDM while also facilitating information sharing of itself and other systems via the SDM.

In accordance with technology integration goals, HAWC is built as a modular architecture and is therefore comprised of several components: The Traffic Profile Handler generates profiles reflecting the requirements of communication traffic; the Radio Access Technology (RAT) Profile Handler generates profiles to reflect the communication resources and capabilities and performs RAT management including plug-and-play upgradability and replacement; the Context Profile Handler generates profiles which reflect context awareness data, such as mission data, context data and platform state data. These profiles are exposed to the Resource and Capability Management Algorithms (RCMAs) within the RCMA Handler. HAWC does not interfere with attached RAT's discovery, routing and clustering operations and assesses the effectiveness of these functionalities only by their reflected performance in the SDM.

Compared to existing approaches, HAWC possesses several key features and functionalities which improve upon the limitations of the state-of-the-art discussed in Chapter 2 and Chapter 3.

While existing approaches lack sufficient context awareness and thus limit the performance of novel RCMA to mitigate an increasingly heterogeneous, more demanding and complex environment, HAWC enables RCM on the application layer informed by mission awareness, situational awareness and platform state awareness. By subscribing to application layer performance metrics from the platform and fleet SDM, HAWC provides essential facilities to novel RCMAs which require high level data in order to manage resources effectively.

The inflexible and hard-wired nature of existing approaches results in excessive integration costs of novel RCMA in vehicle platforms and impedes systems integration and adaptability required for near future battlefield systems. In contrast, HAWC is designed to be a highly flexible architecture to allow the use of any underlying communications resources managed by state-of-the-art RCMAs to best fulfil current and future communications requirements in a "just works" fashion given any viable combination of the attached vehicle hardware and software. To this end HAWC is designed with modularity and flexibility as its core principles. While the monolithic design of existing approaches may be more efficient than HAWC's modular and flexible design, technology integration goals dictate, that flexibility is prioritised before efficiency in a battlefield context.

HAWC performs equipment management by monitoring the SDM for upgraded equipment and hardware degradation. In contrast to existing approaches, this enables transparent upgrading and hardware adaption, maximising effectiveness of limited resources by enabling the use of any available equipment in the field to provide communications capability to vehicle platforms. Failed communications Line Replaceable Units (LRUs) can be replaced rapidly without the requirement to replace like-for-like, since HAWC recognises newly attached hardware and classes it as a black box with generic interfaces. Likewise, as mission parameters change, vehicles can be rapidly upgraded with more powerful communications hardware with zero integration cost.

In contrast with existing approaches, HAWC facilitates the use of multiple RCMA in the same system with zero integration cost and enables seamless switching between these RCMA**.** Based on user input or context information, an appropriate RCMA can be selected from a library of available algorithm to refocus the communications performance of a vehicle to fulfil current mission goals.

These functionalities have been demonstrated using simulated scenarios of a group of unmanned sentry nodes guarding a base station. Experimental evaluation of HAWC has shown that HAWC fulfils its goals. HAWC has also been subjected to a VSI Standards and Guidelines assessment. In coherence with its goals, HAWC scores highly in the fields of Reconfigurability, Enhanceability, Integration and System Scalability. Integrated Logistics Support and Openness are lacking due to the system not being ready for deployment.

Chapter 6 Context Aware Fleet Level RCM

As discussed in 3.3.1, to facilitate new defence paradigms of interoperability, shared situational awareness and network enabled capabilities, maintaining fleet communication is a primary mission goal and as such a full complement of fleet capabilities should be applied to its preservation. To this end Chapter 3 has also discussed a variety of different Topology Management Algorithms which are used in the case of a communications failure such as the failures described in section 5.4.2.4.

If such a failure occurs to all Radio Access Technologies (RATs) on a node, or the node is destroyed entirely, it can no longer participate in the network topology unless its communication capabilities are restored. In a dense network with multiple routes available, traffic can be rerouted in an attempt to circumnavigate the deprecated node, however, this might not be always possible in a low node density situation, or in certain network topologies dictated by mission goals, e.g. a convoy of vehicles. This chapter explores the exploitation of node mobility as a method to heal a network topology and reintegrate disjointed node clusters.

6.1 Mission Aware Topology Healing

As discussed in Chapter 3, at the fleet level a common approach to handle the dynamic network topology of Mobile Ad-Hoc Networks (MANET) and the resulting unreliability is to exploit and directly influence node mobility and to change the topology of the network itself to better fulfil certain goals. In addition to improving overall network integrity and Quality of Service (QoS), this methodology can also be used to mitigate a communication failure event, typical of a military scenario.

This chapter presents the Mission Aware Topology Healing (MATH) approach and supporting algorithms which have been designed to address the shortcomings of existing Topology Management Algorithms (TMA) through the use of shared application level data. The algorithms act to actively protect mobile nodes in the event of an attack by enabling them to escape from and avoid Danger Zones (DZs).

6.1.1 Problem Definition

Battlefield networks face a harsh environment; environmentally induced faults, intentional interference and node destruction by hostile agents are only a few examples of non-random factors that threaten communication and node health as a result of an underlying cause.

Many algorithms exist that attempt to repair segmented network topologies by replacing failed nodes with dedicated relays or neighbouring nodes, or by changing the overall network topology to absorb the load of the failed node. However, in a battlefield context, TMA which are not sufficiently situationally aware may cause nodes to travel into hostile areas and thus put themselves in danger. Current TMA approaches do not recognise possible underlying causes for this danger and thus may cause further damage as a direct result of their topology management efforts [148].

Chapter 3 also discusses many existing TMA which assume that nodes are under complete control of the TMA and which assume that node movements can be manipulated without any constraints during network topology healing operations; however, in a battlefield setting, with limited number of unmanned nodes each vehicle usually has a task to perform besides healing the network topology. Some approaches, such as C2AM [135] are application aware and recognise that not all nodes are equally ready to be used for topology repair by employing a mobility readiness and mobility cost index in order to select the most ready node with the least important task. However, C2AM fails to recognise group relationships and is thus unaware of potentially mission critical capabilities which emerge out of group cooperation.

Therefore given that some nodes may be key to realising mission critical capabilities in a group, it is important that a TMA is aware of neighbour relationships which give rise to group capabilities and recognises the impact of the removal of a node from its group. Topology repair without recognising group capabilities may result in the creation of mission defeating network topologies.

In order to address these shortcomings, this chapter presents two additional algorithms working in conjunction with each other in order to achieve the

reconnection of a disjointed network while preserving group capabilities within the network. Group Capability Integrity Management (GCIM) is an application aware node selection algorithm which preserves mission critical group capabilities during network repair by selecting topology repair nodes which have the least impact on mission critical group capabilities. Coordinated Node Selection (CNS) is a data model aware algorithm which enables disjointed node segments to anticipate the node selection decisions made by other segments. This way CNS minimises the total number of nodes required for topology repair and thus also minimises the amount of group capability lost, during network repair efforts. The novel algorithms are verified by modelling and simulation and significant performance gain is demonstrated when compared to traditional TMA without application awareness.

6.1.1.1 Aim

- To preserve fleet communications capability by protecting fleet resources during catastrophic node failure events caused by hostile forces.
- To protect and maintain communications capability by using fleet resources.
- To preserve capabilities created from group interaction during topology repair.
- To avoid mission defeating capability loss.

6.1.1.2 Goals

- To maintain fleet level communications capability using node mobility.
- To use situational awareness data to evaluate danger zones and to avoid damage.
- To use situational awareness data to repair the network topology whilst avoiding danger.
- To minimise the number of nodes necessary for topology repair.
- To reduce the amount of group capability lost due to node re-tasking by performing group capability based repair node selection.

6.1.1.3 Scope

The following assumptions are made:

- Situational awareness data is available from the data model.
- Node failure is non-random and implies an area of threat surrounding the failed node.
- Danger zone location and size is known, its detection and discovery are outside the scope of this work.
- Battlefield MANETs are heterogeneous; some nodes have a higher mobility readiness or mobility cost. These variables are predetermined.
- Nodes are relocated in order to improve network topology in the event of a communication failure.
- Heterogeneous mission critical and non-mission critical capabilities exist within the fleet producing NEC when matched up appropriately.
- Capability information and group affiliation is known in advance and available from the fleet Shared Data Model (SDM).
- Removal of a node from a group results in a loss of group capability, no node benefits the group through absence.
- Last known node locations and capability values are available from cached data model data.
- Classifying the capabilities of nodes is beyond the scope of this work, it is assumed that each node is classed with a capability value based on its capabilities.

6.1.2 Approach

6.1.2.1 Fleet Level Communication Capability

While individual platform survivability is improved through situational awareness gained by a functioning communications network, the network topology's integrity is preserved by having a sufficient number of mobile nodes in locations appropriate to the terrain. An effective way to prevent bottlenecks and network separation is to protect the network's nodes from damage and destruction. To achieve this goal,

shared intelligence between mobile nodes on a systems-of-systems level, such as mission information, must be harnessed and any node mobility must be both informed and constrained based on this information.

In a battlefield context, when an asset which has been assigned a mission critical task is lost or incapacitated, SDM mission data should reflect this and thus the network's TMA should cause the replacement of the failed node with another in the network to ensure that the failed node's tasks are taken over by the replacement node. When the lost asset was not assigned a mission critical task, but is vital to the network topology, mission data should also account for the loss of the node and the TMA should attempt to redirect other nodes to heal the network in an effort to restore the topology in accordance with prevailing QoS requirements.

6.1.2.2 Damage Zone Detection and Avoidance

There are many reasons why a node is lost from a network, such as the node moving out of range of its neighbours, low QoS through unintentional interference by environmental factors, such as weather, intentional interference, such as jamming, as well as damage due to the terrain or hostile forces. The fact that an asset providing communications capability has been damaged can provide information about the location it was operating in i.e. further assets are likely to be damaged if deployed there.

Additionally, modern vehicle mounted Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) systems, such as the Raytheon Boomerang system [159] exists which is able to detect the location and area of an attack and make this information available to other members of the network via the common data model. For the purposes of automatic danger avoidance, this information can be captured and utilised in the form of a terrain danger zone which nodes are discouraged to trespass on in their efforts to recover a partitioned network topology.

6.1.3 Algorithm Development

6.1.3.1 MATH Algorithm Design

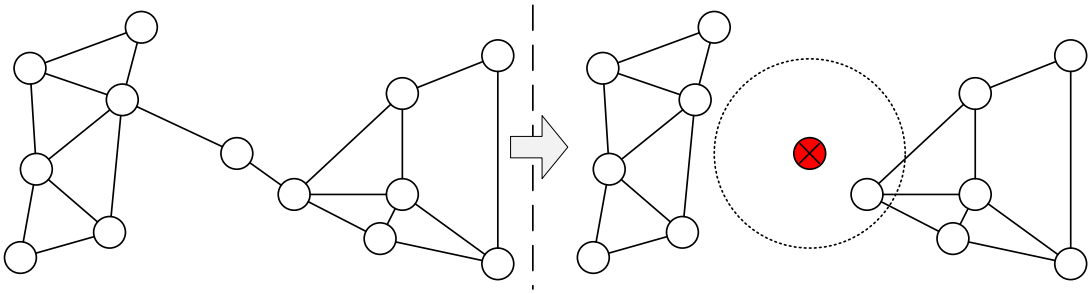

Figure 6-1 A Node Is Destroyed and a Danger Zone is Established

When a Danger Zone is detected based on updated situational awareness data from the data model (see Figure 6-1), each MATH enabled node in the fleet first checks its current location is within the detected DZ, whose location and dimensions are also available from the data model. If the node is located within the danger zone, it attempts to evacuate the DZ by travelling towards its closest edge. When the node is no longer within the DZ and the network topology remains segmented, it elects a Repair Node (RN) from its neighbours (see Figure 6-2). Many repair node selection algorithms exist to choose a suitable repair node [133-140]; in this context the choice of repair node has no impact on the performance of MATH in avoiding danger zones.

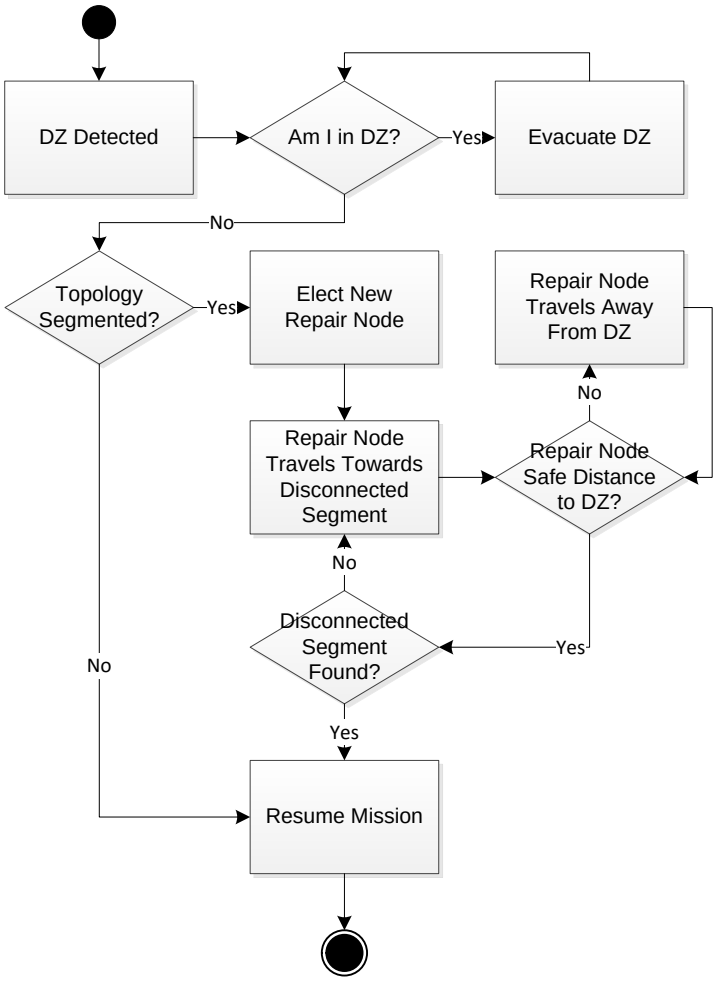

Figure 6-2 Danger Zone Avoidance Flowchart

The RN continues to travel towards the disconnected segment while the topology remains segmented. Figure 6-4 shows that if the RN travels within an unsafe distance from the DZ (determined by situation data), it adjusts course away from the DZ and then resumes travel towards the disconnected segment. See Figure 6-3 for a legend.

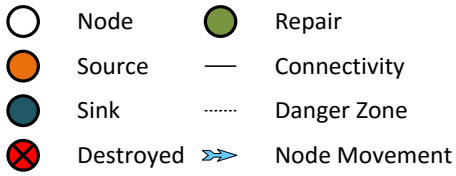

Figure 6-3 Legend

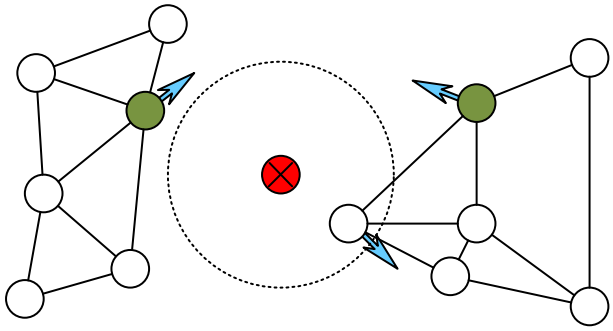

Figure 6-4 MATH Repair Node Selection and DZ Escape

Due to the fact that repair nodes now have to traverse the perimeter of the danger zone as opposed to simply replacing the failed node they have to travel much larger distances, therefore following this behaviour alone may lead to the RN themselves becoming disconnected from their network segment (see Figure 6-5)

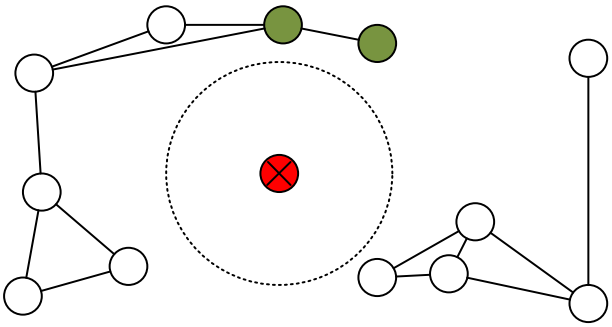

Figure 6-5 Repair Node Disconnection

6.1.3.2 Repair Node Chaining

To prevent RN disconnection during topology repair, a process of chaining RN together to retain network connection to its segment is employed.

Consider the flowchart Figure 6-6 from a vehicle platform perspective, if a node is chosen as a repair node (RN1) and is travelling towards the disconnected segment, if RN1 loses network connection at any time during the topology repair process, it stops and waits while it remains disconnected from its segment before resuming the repair process.

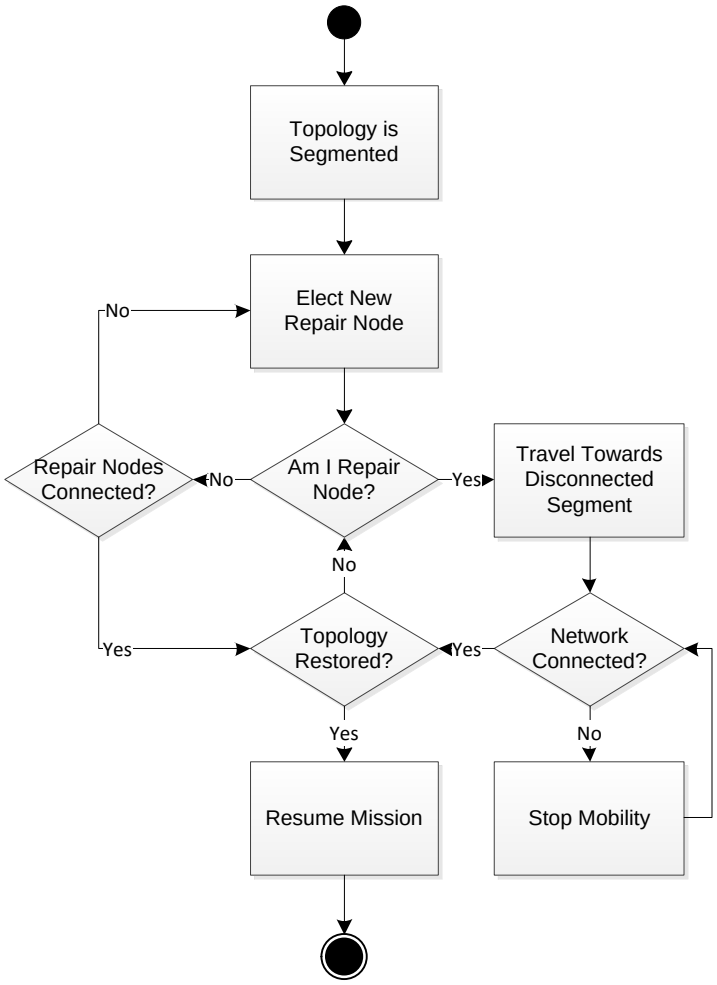

Figure 6-6 Repair Node Chaining Flowchart

If the node is not itself chosen as RN1, it continues to monitor the network connection to RN1. If RN1 loses connection to the network, another election process is started within the remainder of the segment to elect another Repair Node (RN2) which travels towards the last known location of RN1.

When RN2 reconnects to RN1, RN1 continues with its topology repair process until it disconnects from the network again, at which point the process is repeated, or until both network segments are reconnected at which point the fleet continues according to its mission goals (See Figure 6-7). The algorithm will continue to elect additional available nodes as RN chain links as long as the topology remains segmented and nodes eligible for topology repair remain in the segments.

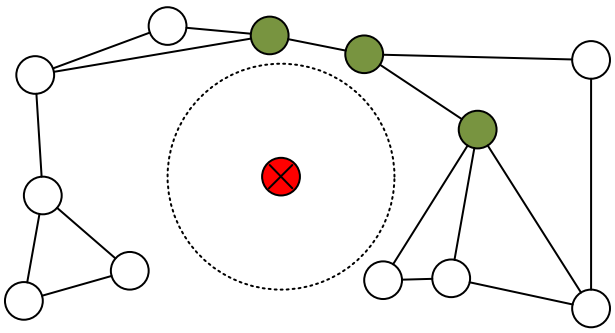

Figure 6-7 Topology Repair and Secondary Repair Node Selection

6.1.3.3 MATH Behaviour Flowchart

Thus MATH is comprised of the combined behaviour of Danger Zone Avoidance and Repair Node Chaining. See Figure 6-8 for a flowchart of the behaviour of MATH.

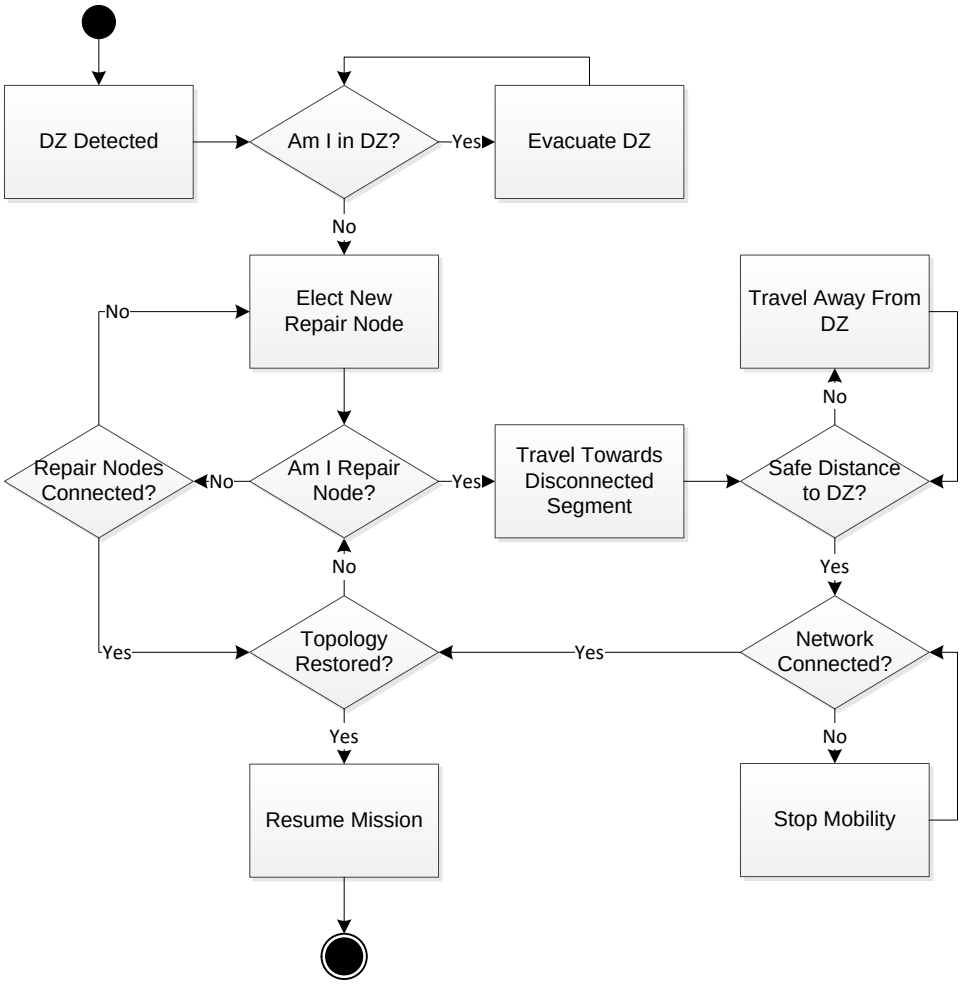

Figure 6-8 Combined MATH Flowchart

6.1.4 Experimental Modelling

6.1.4.1 Experiment Design

In order to evaluate the performance of MATH and to compare that performance with the existing approach: C2AM [135], an agent based simulation is developed using the Battlefield Network Simulation Tools. C2AM is chosen as a comparison to MATH due to its similar goals and application awareness.

The agents have mobility behaviour defined by a convoy model and the mission goal to proceed east at an average speed of 20 km/h (see Figure 6-9). The convoy is modelled to contain 30 manned vehicles, such as main battle tanks, light protected patrol vehicles and logistics vehicles, as well as 10 unmanned, autonomous, light UGV to perform network repair (see Figure 6-10).

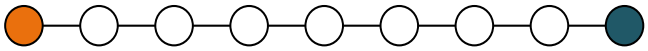

Figure 6-9 Convoy

The agents possess multihop communications capability and the ability to detect whether the network is intact or segmented. Each node is able to communicate with other nodes using a radio transceiver modelled on an 802.11 transceiver with a typical range of 250 m. This communication range was chosen both to represent MANET class communications as well as a fall-back case of a heavily saturated / jammed spectrum of longer range wireless battlefield technologies, such as Bowman. The data rate of any of wireless communication links is assumed to be of sufficient capacity to not present a bottleneck.

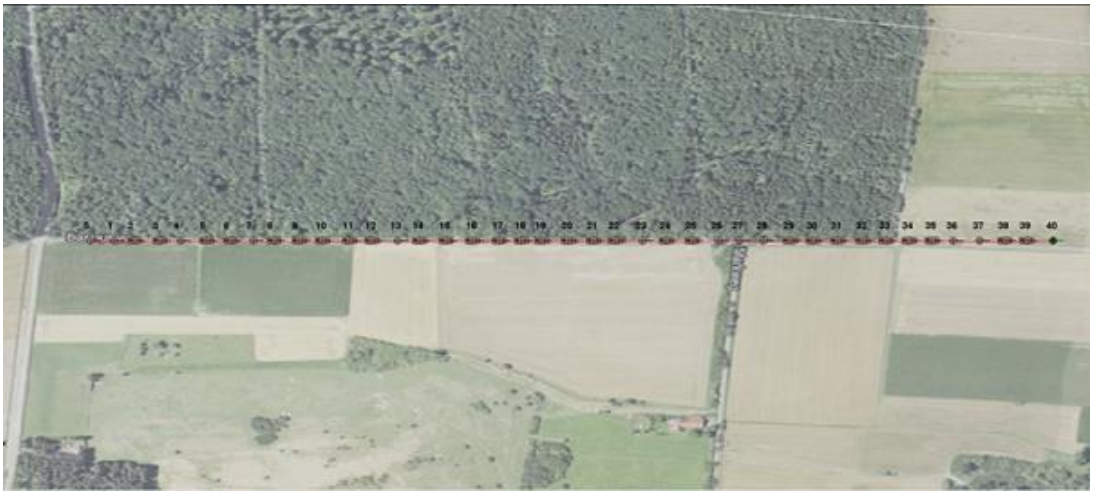

Figure 6-10 Simulation Tool, Runtime View: Vehicle Convoy

Node damage (see Figure 6-11) is modelled by disabling the damaged agent's mobility and communications capability. A complete description and discussion of the developed Battlefield Network Simulation Suite is included in Chapter 4.

The results of these experiments determines whether the MATH algorithms are superior to existing approaches in escaping from and avoiding terrain danger zones while performing network topology repair.

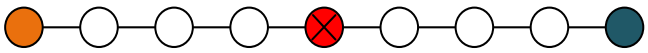

Figure 6-11 One Node Is Destroyed

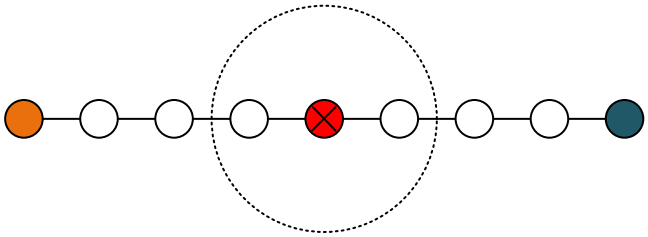

Figure 6-12 Destroyed Node and DZ

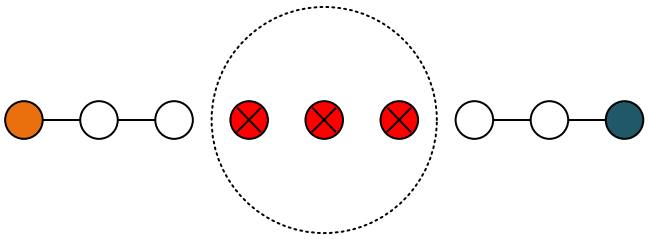

Figure 6-13 Nodes Within the DZ are Destroyed

The convoy is placed on a road moving east (see Figure 6-9). At t = 10 s, one of the nodes in the centre of the convoy is attacked (see Figure 6-11) and a DZ is established with its epicentre at the destroyed node's location (see Figure 6-12). To simulate hostile forces as the source of the localised danger, any nodes present within the danger zone are destroyed at a rate of 0.1 nodes per second (see Figure 6-13). The diameter of the danger zone is varied throughout multiple iterations of the simulation from 0 m (attack on a single node) to 600 m (see Table 6-1 for full simulation parameters).

Table 6-1 MATH Evaluation: Simulation Parameters

Transmission Range	250 m
Mobility model	Base – FB Convoy
Total number of Nodes	40
Number of Manned Nodes	30
Number of UGV	10
Node Speed	20 km/h
Length of convoy	1200 m
Distance between vehicles	30 m +- 10m
Danger Zone diameter	0-600 m
Danger Zone Lethality rate	0.1 nodes/s
Time to attack	10 s
Scenario duration	300 s

For the purposes of the simulation, both algorithms use the repair node selection process of C2AM which elects a suitable RN by rating nodes in the network according to a Mobility Readiness Index (MRI). The MRI is predetermined; in order to simulate the fact that UGV are more expendable for network repair purposes, UGVs are assigned an MRI value from 0-9; manned Vehicles are assigned an MRI

Value from 10 to 19 where 0 represents the node which is most ready to be relocated. When a node fails, the most suitable repair node is selected from the failed node's neighbours within a two-hop distance.

6.1.5 Results and Discussion

6.1.5.1 Results: Scenario 1, Convoy attack, Non-Mission-Aware

When C2AM detects the segmentation of the network, it attempts to replace the destroyed node by selecting an appropriate node in a two hop radius taking into account the node's mobility readiness and mobility cost (see Figure 6-14).

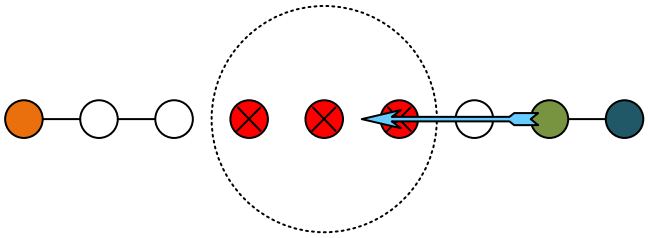

Figure 6-14 C2AM: Selected Node Travels Towards the Failed Node

Since C2AM does not assume agency behind the failed node's destruction, the RN is sent directly into the danger and destroyed, at which point C2AM will elect the next available RN until no more nodes are available (see: Figure 6-15 and Figure 6-16).

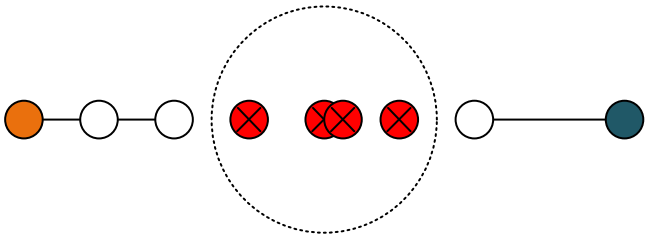

Figure 6-15 C2AM: Nodes are Drawn Into the DZ One by One and Destroyed.

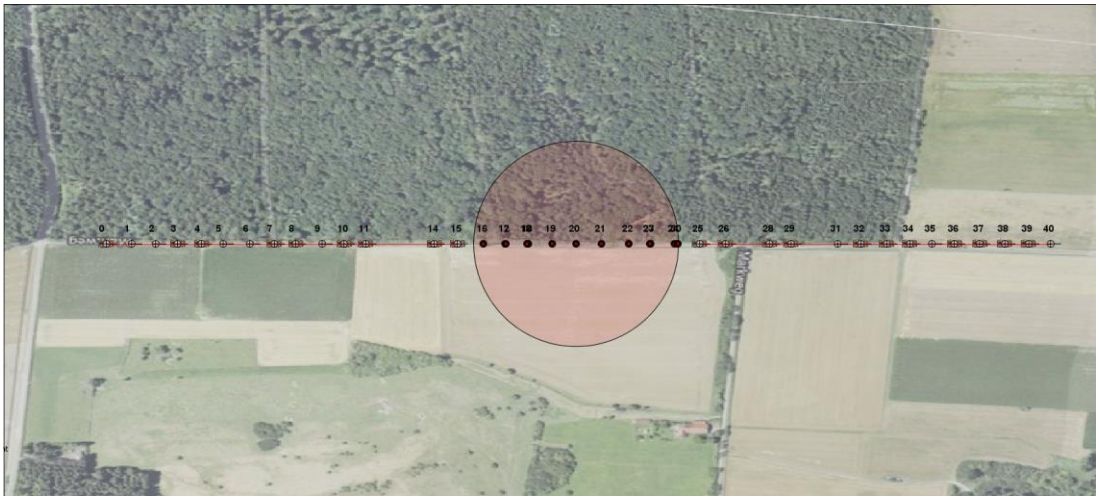

Figure 6-16 Runtime View: C2AM: Nodes Are Drawn Into the DZ

6.1.5.2 Results: Scenario 2, Convoy attack, Mission Aware Topology Healing

In contrast to the above example, MATH is aware of the location and diameter of the DZ and commands nodes within the zone to attempt to escape (see Figure 6-17 and Figure 6-18). While some nodes are destroyed, many manage to escape the danger zone; this divides the network into two segments.

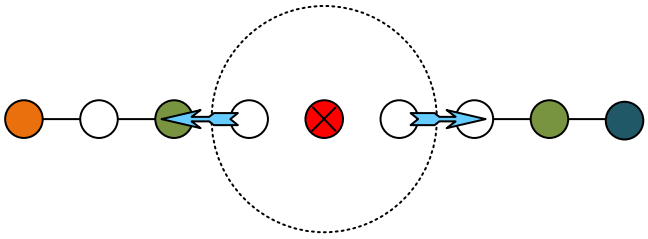

Figure 6-17 MATH: Nodes Within the DZ Attempt to Escape

Figure 6-18 Runtime View: MATH: Some Nodes Escape

Upon segmentation of the network, since the network is now divided into two partitions which can no longer communicate, each partition starts their own RN election process, hence an RN is selected from each partition independently (see: Figure 6-17).

To recover and repair the topology, each RN is instructed to travel the circumference of the danger zone (see Figure 6-19). Through situation data available from the data model, both partitions are aware of the DZ's location and size and can therefore dispatch the RNs to the location of the other partition while maintaining a safe perimeter around the DZ.

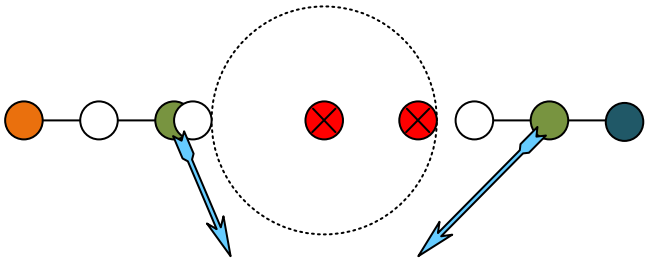

Figure 6-19 MATH: The Selected Discovery Nodes Search for Other Partition

In this theoretical example, the RN may travel either northwards or southwards around the DZ and may therefore miss each other entirely. In that case, the nodes will form a chain around the DZ and eventually reconnect, however, in a real world situation, the two disconnected segments will never be precisely equidistant, therefore it is assumed that the RN select the same direction each time.

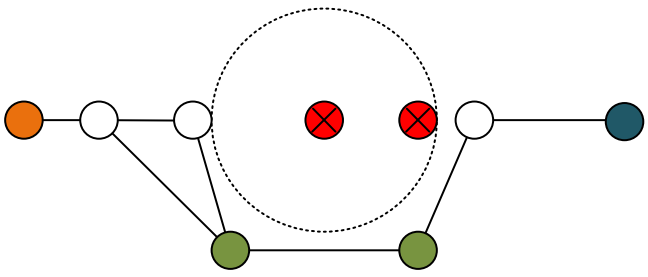

Figure 6-20 MATH: Connection Re-established

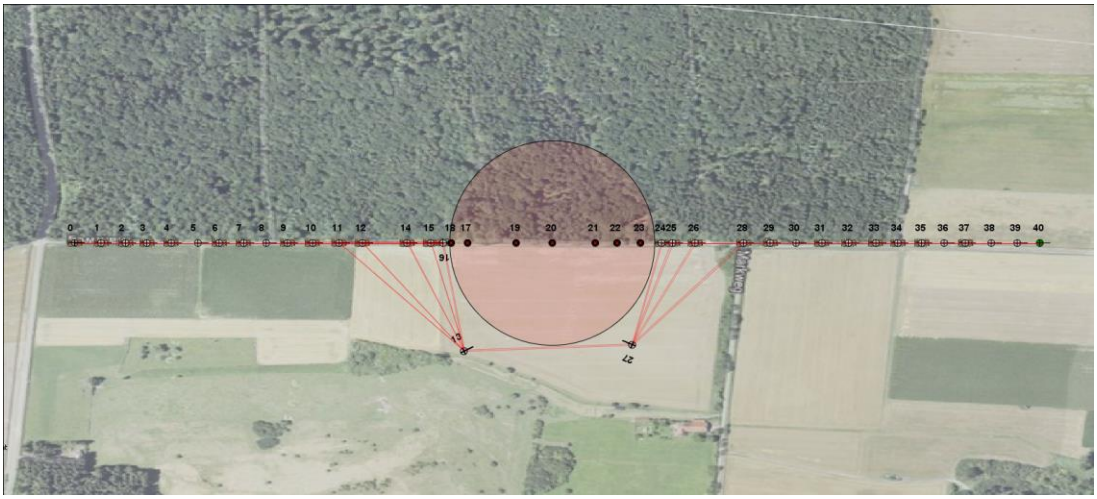

Figure 6-21 Runtime View: MATH: Nodes Re-establish connection

When the two RNs meet (see: Figure 6-20 and Figure 6-21), the connection between source and sink is re-established and the nodes halt position until mission data indicates new mobility instructions, or another danger zone is discovered. If the DZ is too large to circumnavigate with two nodes, each RN will lose connection to its network segment which will in turn start a new election process and effectively form a chain of nodes around the DZ (see Figure 6-22).

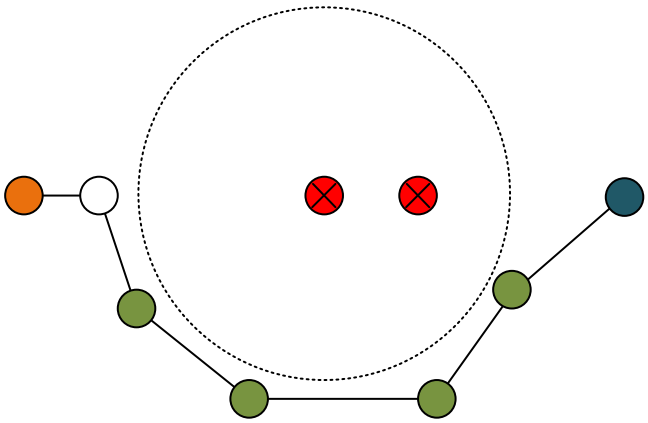

Figure 6-22 MATH: Repair Nodes Form a Chain Around a Large DZ

The two data models are merged, each node is updated with the revised waypoints to avoid the DZ the convoy's mission is resumed. Unless the threat is removed and the data model mission data updated once more, the convoy now uses the new mission waypoints to circumnavigate the DZ (see: Figure 6-23).

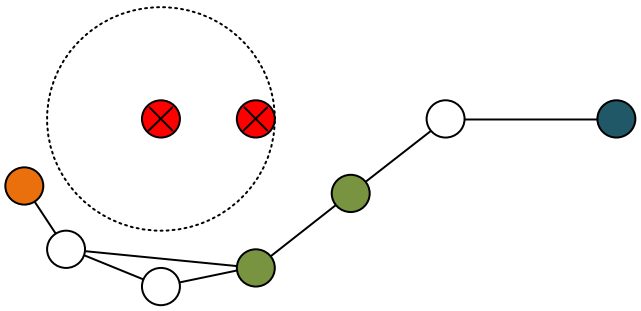

Figure 6-23 MATH: Waypoints are Updated and the Convoy Avoids the DZ

6.1.5.3 Results and Discussion

The simulation is carried out in 7 iterations varying the DZ diameter from 0 m to 600 m in 100 m increments. Each scenario is simulated a sufficient number of times to reduce the standard deviation of the samples sufficiently achieve a 95 % confidence interval.

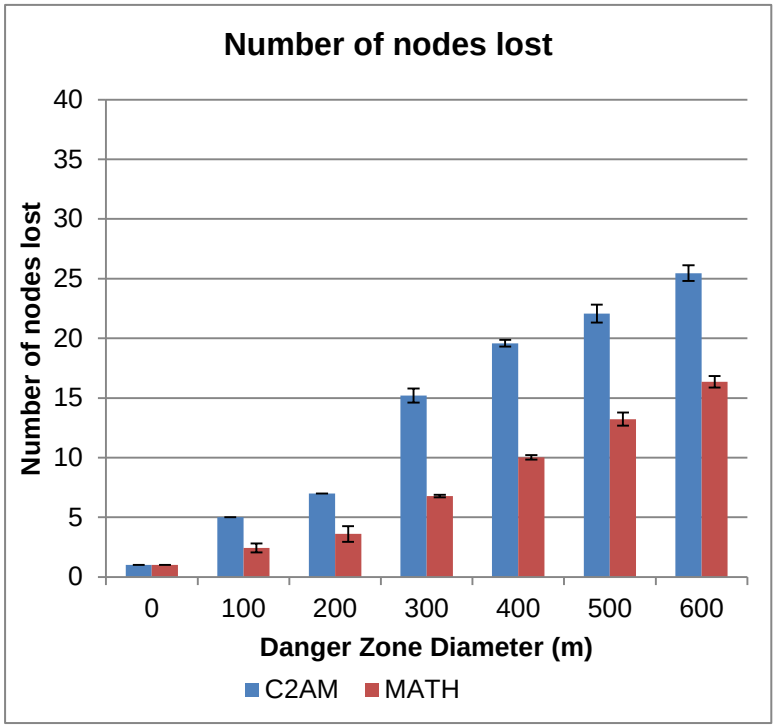

Figure 6-24 C2AM vs. MATH Results: Number of Nodes Lost vs. DZ Diameter

When a DZ is established and the network is segmented, while MATH seeks to escape from the danger zone (see: Figure 6-17), the C2AM has no knowledge of the location and size of the DZ and hence cannot escape, causing higher immediate node losses (see: Figure 6-15). During repair, while MATH avoids the DZ; C2AM, in an effort to replace the failed node consecutively sends all availble nodes within a two-

hop radius directly into the danger zone (see: Figure 6-15), causing much higher node loss overall. Both algorithms incur higher node losses which increase approximately linearly with the danger zone diameter from an average of 5 nodes at 100 m DZ diameter to 25 nodes at a 600 m diameter for C2AM and an average of 2.4 nodes at 100 m DZ diameter to 16 nodes at a 600 m diameter for MATH. C2AM loses on average 1.8 times as many nodes as MATH (see: Figure 6-24).

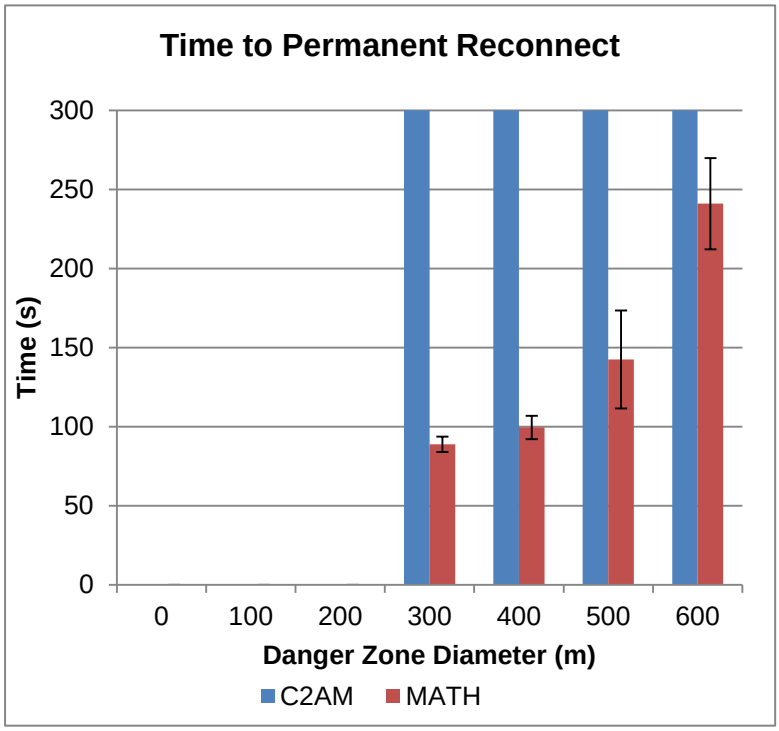

Figure 6-25 C2AM vs. MATH Results: Time to Reconnect vs. DZ Diameter

With a danger zone diameter of up to 200 m, both algorithms have a 0 s reconnection time, since neither of the algorithms lose connection due to each node's transmission radius of 250 m. When the DZ diameter is increased to 300 m and larger, an algorithm unaware of the danger zone, such as C2AM fails to reconnect the partitioned networks permanently, while MATH achieves reconnection in most cases. MATH's time to permanently reconnect increases exponentially with an increasing danger zone (see: Figure 6-25). This exponential increase can be explained by two factors. While a larger danger zone means that nodes have to travel longer distances, also more nodes are needed to form a chain and an increasing proportion of the simulation fails to reconnect due to a lack of nodes available for network repair. This is also the reason for the larger confidence interval at 500 m and

600 m. The increasing amount of simulation scenarios where MATH fails to reconnect both parts of the network increases the average time to reconnect from 89 s to 241 s and confidence interval of the sample from 5 s to 29 s.

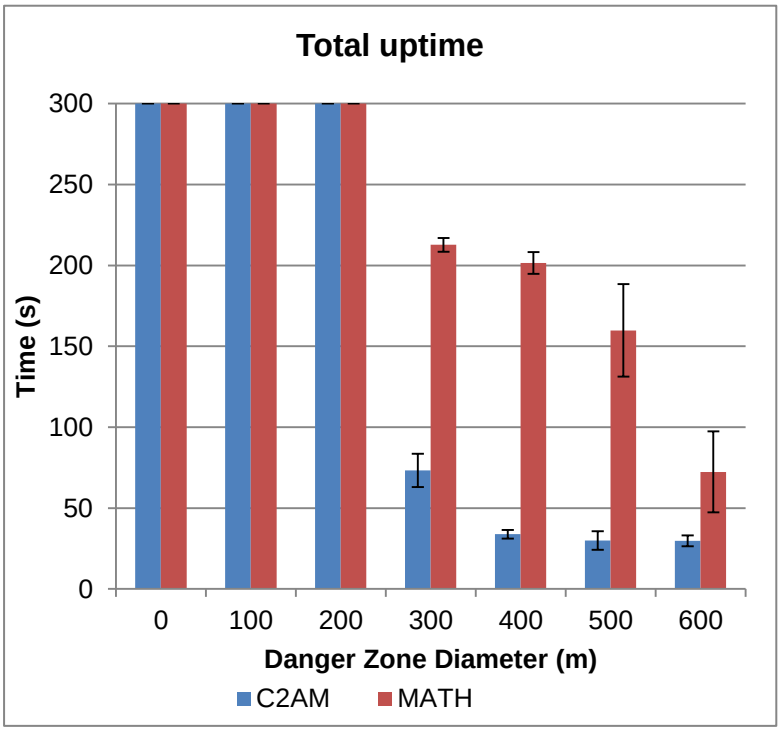

Figure 6-26 C2AM vs. MATH Results: Total Uptime vs. DZ Diameter

The total uptime represents the total amount of time that the network is connected, i.e. while the last vehicle in the convoy is able to transmit data to the first. Similarly to the Time to reconnect (see Figure 6-25) neither of the algorithm's uptime is affected by a danger zone of 200 m or less. At a DZ diameter of 300 m, even though C2AM never manages to permanently reconnect the partitioned networks, nodes sent into the danger zone briefly re-establish connection before they are eventually destroyed, increasing the overall uptime marginally (see: Figure 6-26). At a DZ diameter of 400 m and larger, C2AM's uptime is equal to the time when the networks first become partitioned at the start of the simulation at an average of 31 s. MATH's total uptime (see: Figure 6-26) is directly and inversely proportional to its time to permanently reconnect (see Figure 6-25) and decreases with an increasing DZ diameter from an average uptime of 213 s at 300 m DZ diameter to 72 s at a 600 m diameter.

MATH fulfils its goals:

- To maintain fleet level communications capability using node mobility
- To use situational awareness data to evaluate danger zones and to avoid damage
- To use situational awareness data to repair the network topology whilst avoiding danger

MATH is compared to C2AM [135] which has been chosen due to its enhanced application awareness making it a realistic RCMA candidate in a battlefield scenario. However, due to existing topology management approaches' shared behaviour, in this context C2AM is representative of the majority of current topology management approaches discussed in Chapter 3, such as Grandi et al. [145] which use swarm movement; PCR [136], PADRA [137] and NORAS [138] which use relay node placement; RIM [142] and DARA [143] which use cascaded movement to despatch repair nodes *towards* a failed node thus risking massive subsequent damage as a direct result of their repair effort. Even the algorithms [146] and [147] which are designed to recover large scale failure by non-random causes do not presume hostile agents posing future risk in the area beyond placing additional redundant relay nodes in the area. Therefore MATH would likely be similarly superior in the aspect of preventing subsequent node damage due to hostile forces compared to these algorithms.

6.2 Preserving Group Capability Integrity

As discussed in Chapter 2, the future battlefield contains a diverse range of nodes possessing diverse abilities. There are many factors and capabilities that differentiate types of vehicle platforms, such as manned vs. unmanned, size, armed and unarmed, etc. Not only are these types of platforms different from each other and need to be treated accordingly, they are also grouped depending on their interoperability in order to maximise their effectiveness. To perform a given mission it is often necessary for multiple nodes to cooperate, providing specific capabilities and services to each other.

The paradigm of Network Enabled Capability (NEC) encapsulates this notion. Through strong interaction between mobile nodes, new capabilities emerge that are beyond the capability of any individual node, e.g. a main battle tank can achieve high accuracy through detailed targeting data supplied by a UAV, dismounted soldiers have a higher survivability when assisted by a UGV for building search. In NEC warfare, the creation of synergetic capabilities within these groups of appropriately selected nodes is one of the ways in which new functionality can be created from existing hardware and can be a significant asset.

6.2.1 Approach

6.2.1.1 Group Capability Integrity Management (GCIM):

GCIM is an application aware node selection algorithm which performs topology management while recognising local vehicle platform group capability relationships.

Group Capabilities may have various requirements and constraints on node behaviour. In order for group capabilities to be leveraged, nodes are required to operate at specific locations or within certain distances to each other, i.e. a targeting UAV needs to be on location in order to record relevant targeting data, an autonomous pack mule carrying ammunition needs to stay close to a group of dismounted soldiers in the event of an attack. All this mission data, i.e. mission goals, waypoints, radius of permitted deviation from waypoint, Radius of permitted distance to a neighbour, etc. is available to each node via the shared fleet SDM.

Treating all connections between nodes equally and optimising overall network QoS will at best result in suboptimal organisation of important network segments and at worst result in weakened performance of important segments. Moreover, depending on the type of mission, some capabilities may be considered critical, while others are expendable. Maximising overall group capability as opposed to mission critical capabilities can therefore be just as detrimental to mission survivability as maximising overall network QoS. GCIM recognises these problems and hence optimises essential capabilities while sacrificing expendable ones.

6.2.1.2 Coordinated Node Selection (CNS):

When network partitioning results in two partitions of unequal size, it is possible for the larger partition to envelop the smaller one. In this situation, if each partition only sends a single node for network repair, in some cases the repairing nodes can miss each other, thus increasing the time to reconnect and wasting resources travelling in the wrong direction (see Figure 6-27).

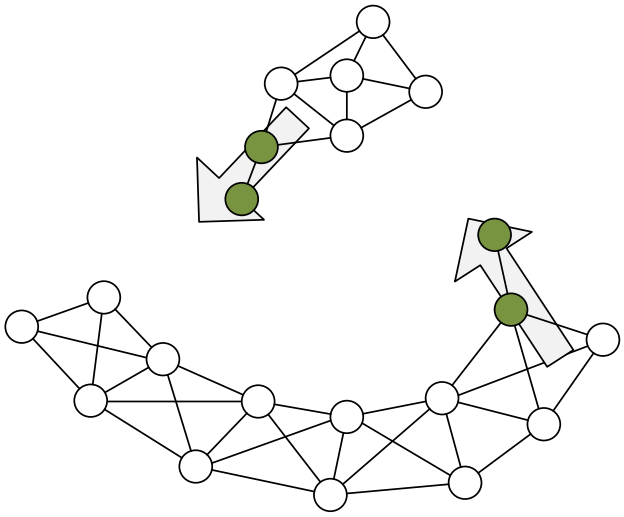

Figure 6-27 Partitions of Unequal Size Result in Wasted Resources

Disconnected network segments have no way to communicate and therefore no way to coordinate repair efforts directly, however, if each network segment retains a cache of the fleet data model, each disconnected segment is able to interpolate the node selection decision of the other segment and thus the location of a node sent from the other segment as a means of topology repair. CNS makes use of this cached data and is therefore able to indirectly coordinate network repair efforts between two disconnected network segments. This way, the two selected nodes can be instructed to travel directly towards each other to achieve a minimum reconnection time with least movement cost and the least number of nodes necessary to repair the network.

6.2.2 Algorithm Development

6.2.2.1 Group Capability Integrity Management (GCIM)

In order to enable GCIM to preserve mission critical group capabilities, each node in the network is affiliated with a group based on its types of NEC. The NECs it

contributes to its group are divided into two categories: Mission Critical Capabilities (MCC) and Secondary Capabilities (SC) depending on the NEC's relevance to the current mission goals. Nodes retain their group affiliations as long as they are not actively engaged in network topology repair.

Consider the flowchart in Figure 6-28 from a node perspective. When the network is separated and topology repair is started, each node in a group starts the group capability based repair node selection algorithm. Each node accesses the data model and reads its group members' MCC values. If a node discovers it contributes the lowest MCC value to the group, it assumes the RN function. Since the node cannot simultaneously provide its capabilities to its group and perform topology repair, it unregisters its group affiliation before it begins topology repair. All nodes which do not possess the lowest MCC value continue according to their mission parameters.

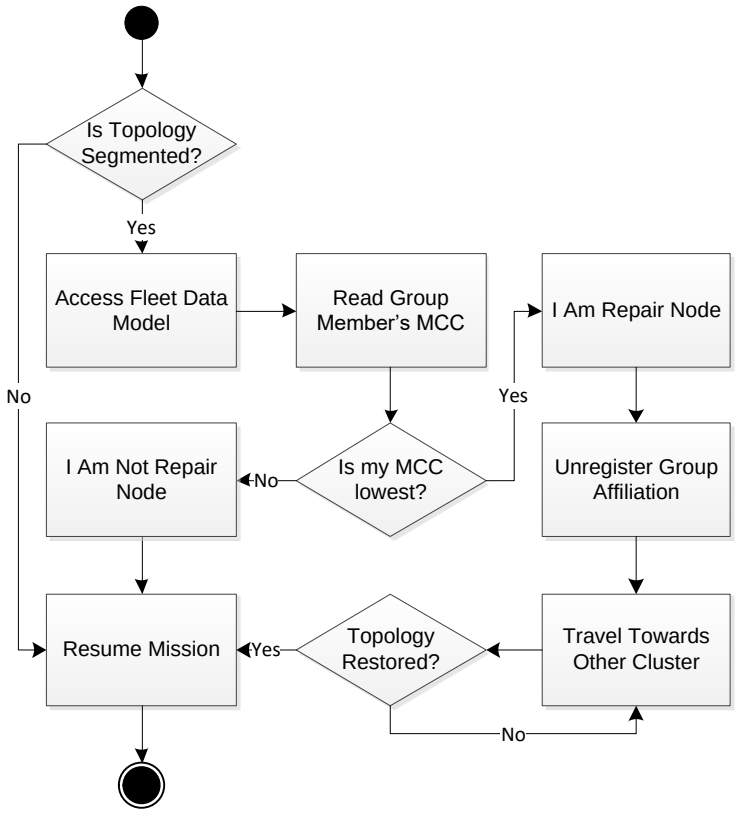

Figure 6-28 Group Capability Based Repair Node Selection Flowchart

This way the node which is most expendable in terms of its mission critical capabilities will be chosen to repair the network topology. Similarly to the MATH

algorithm, in practice this algorithm is combined with the repair node chaining algorithm to avoid the disconnection of chosen repair nodes from their group.

6.2.2.2 Coordinated Node Selection (CNS)

To perform coordinated node selection between two disjointed node clusters, each node possesses a cached snapshot of every node's MCC value and last known location in the network. When an RN is selected, the RN analyses its cached MCC values of the nodes in the disconnected group and registers the last known location of the node with the lowest MCC value in the other group. The RN then travels towards this location until it connects with the other group.

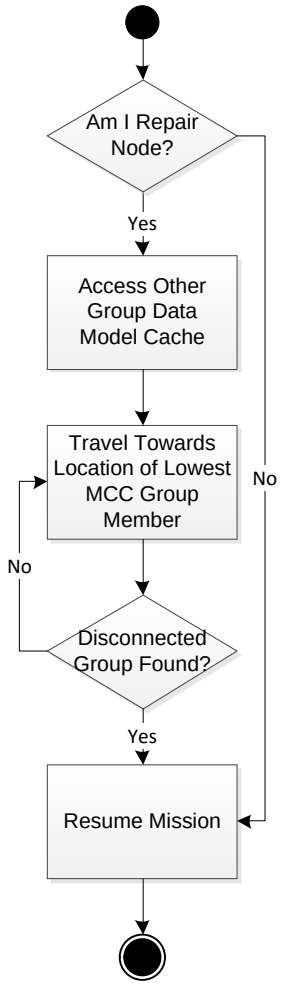

Figure 6-29 CNS Standalone Functionality Flowchart

This way each disconnected network segment will dispatch RN towards the other segment's RN and ensure that both segment's RN meet in between the two segments.

6.2.2.3 GCIM Behaviour Flowchart

Thus GCIM is comprised of the combined behaviour of Group Capability Based Node Selection, Repair Node Chaining and the Coordinated Node Selection algorithm. See Figure 6-30 for a detailed flowchart of GCIM.

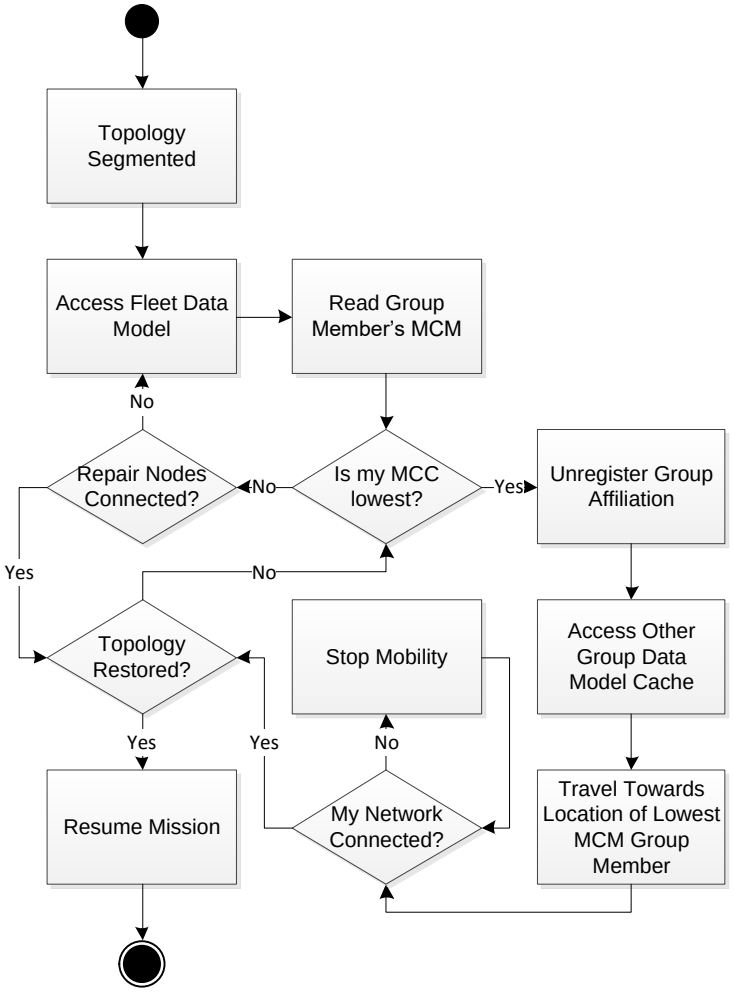

Figure 6-30 GCIM Combined Functionality Flowchart

6.2.3 Experimental Modelling

To measure the relative performance of GCIM and demonstrate its advantages over existing approaches, it is compared to the C2AM algorithm which recognises variable requirements among different nodes but does not take into account the NEC factors involved in battlefield networks.

6.2.3.1 Experiment Design

A steady state, agent based simulation is developed. Each mobile node is modelled as an agent in a 2D environment. For MANET communications, nodes use an 802.11 transceiver with a range of 250 m. For long range communications, selected nodes are equipped with a point to point transceiver with a range of 1000 m. The data rate of any of the wireless communication links is assumed to be of sufficient capacity to not present a bottleneck.

To model the capability value each node adds to the overall capabilities of a group in a scalable way, every node is assigned five capabilities, each of which is represented by a unique capability value between 1 and 10. When a communication failure occurs and a node is re-tasked to leave its group for topology repair, this capability value is used to represent group capability loss incurred due to the absence of the node from its group.

The scenario involves of two groups, a Convoy Mission comprised of 20 platforms and a Scout Mission comprised of 10 platforms, see Figure 6-32 and Figure 6-33. A single node within each of the two clusters is equipped with a long range P2P transceiver enabling communication between them. Nodes travel at an average speed of 20 km/h. See Table 6-2 for detailed simulation parameters. See Figure 6-31 for a legend.

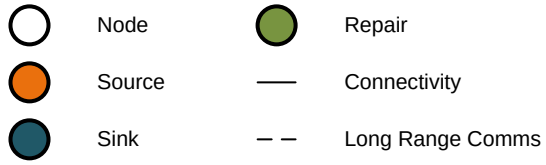

Figure 6-31 Legend

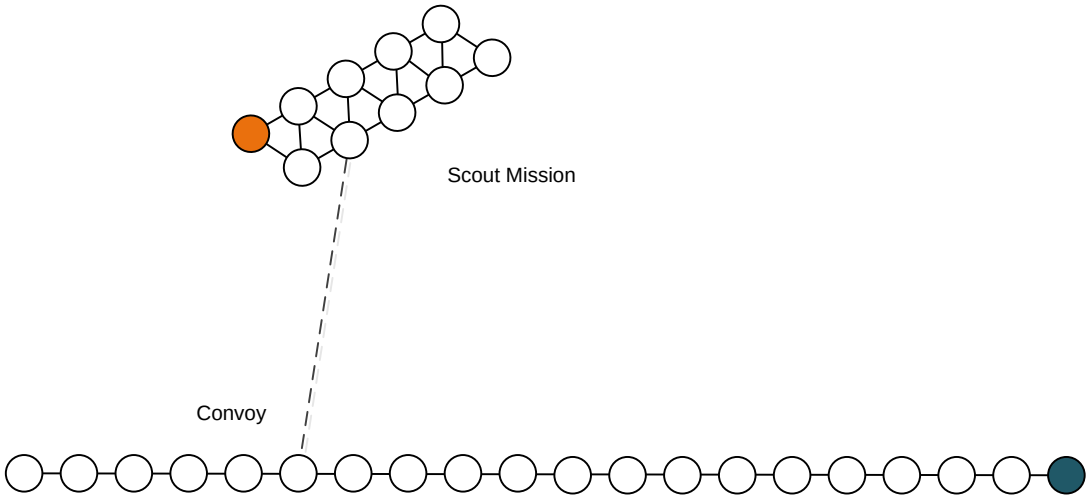

Figure 6-32 GCIM / CNS Simulation Scenario

Figure 6-33 Simulation Tool, Runtime View: Convoy and Scout Connected

Table 6-2 GCIM / CNS Simulation Parameters

MANET Range	250 m
P2P Range	1000 m
Mobility model	Convoy / Scout Mission
Total number of Nodes	30
Node Speed	20 km/h
Number of MCC	1
Number of SC	4
Time to failure	10 s
Scenario duration	300 s

At t=10s the long range communication link of the Scout Mission fails, prompting the network repair process. Repair nodes are being selected from each partition based on the algorithm used, if a single node per partition cannot achieve reconnection with the other partition, the platform chaining algorithm causes additional RN to form a chain to relay the information between the two partitions (see Figure 6-34).

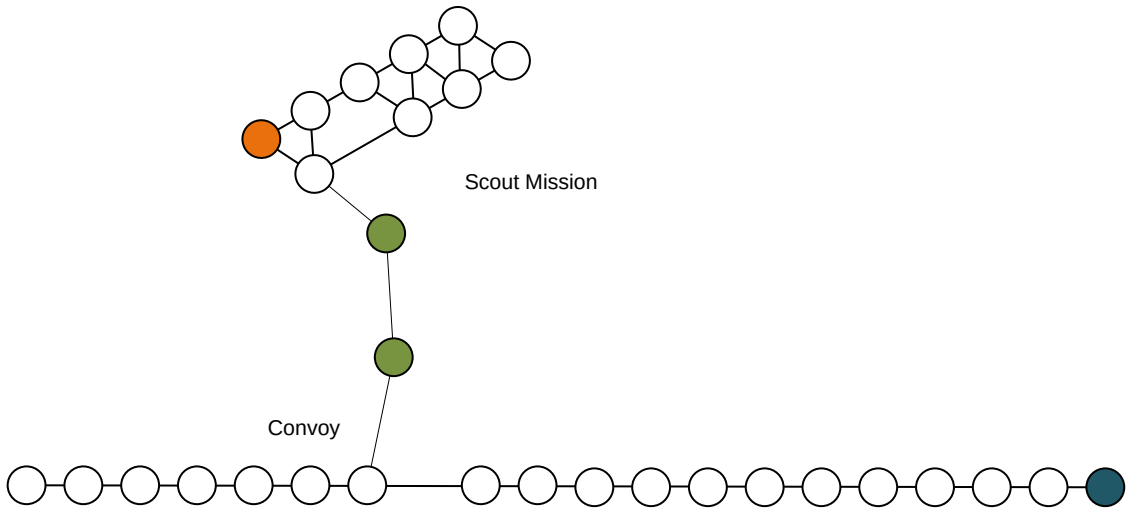

Figure 6-34 Network Repair

A total of four scenarios are simulated. The first scenario simulates the behaviour of the existing algorithm C2AM, which is unaware of group capability relationships and dispatches repair nodes in an effort to replace any failed nodes. During the second scenario, CNS is enabled which allows the two group to coordinate their

topology repair. During the third scenario CNS is disabled and GCIM is enabled, so that each group chooses the repair node with the lowest MCC. During the fourth scenario both GCIM and CNS are enabled.

For each of the scenarios the simulation measures total downtime incurred by the network during link failure, number of nodes used for network repair and total MCC loss due to node re-tasking. During all four scenarios, the first of five capabilities is chosen as the MCC, while the four other capabilities are declared SCs. Since dispatch of a node for network repair always results in a loss in capability, each time a node is chosen to repair the network, the loss in capability caused by this node is counted towards the total fleet capability loss. Experiments are repeated a sufficient number of times to reach a 95 % confidence interval.

6.2.4 Results and Discussion

Network Downtime

Between the failure of the long range communications link and reconnection of the two segments, the network experiences downtime. The three factors influencing the amount of downtime are node's MANET communication range, the distance of the separated clusters and whether nodes repair the topology using the shortest path during network repair. CNS has a significant impact on the latter variable, ensuring that nodes meet in the middle of the two partitions and therefore always travel the shortest path given the choice of repair node. When compared to an algorithm unaware of the other partition's location, CNS, on average, reduces the network's downtime by 17.2 % (see Figure 6-35). The choice of mission critical capability has no effect on downtime.

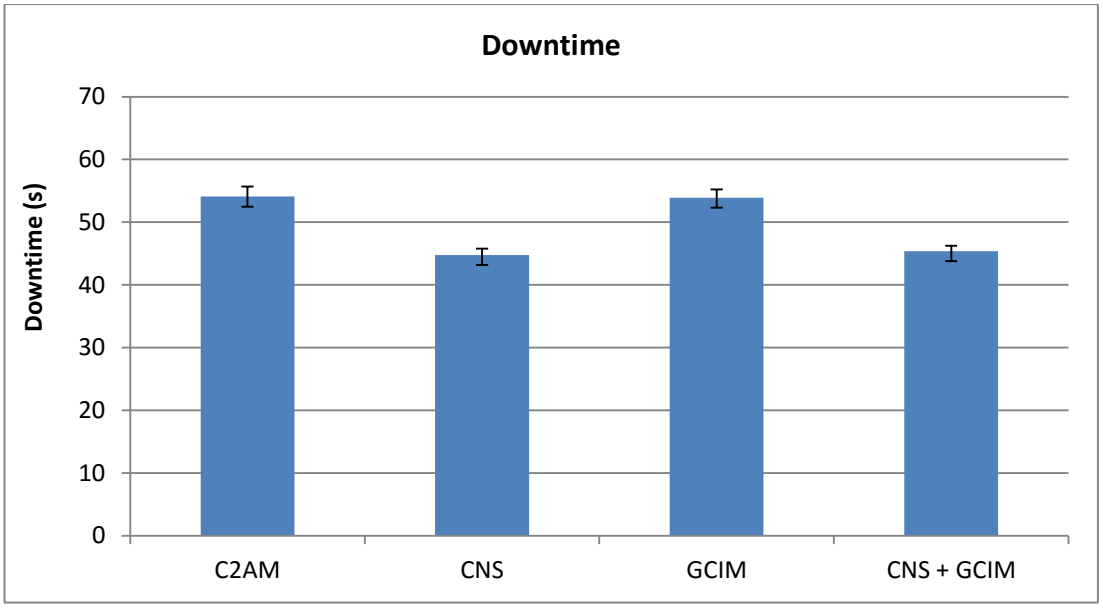

Figure 6-35 C2AM vs. CNS vs. GCIM Results: Downtime

Repair Nodes Used

During topology repair, since at least one chain of nodes must bridge the complete distance between the partitions, when C2AM selects repair nodes from the far side of the convoy, significantly more nodes are used as a result of the repair nodes not meeting in the centre of the two partitions (see Figure 6-36). CNS, due to being able to reconnect the segments using the shortest topology repair path also uses the least amount of RN (see Figure 6-34). This way CNS reduces the average number of nodes used for network repair by 23.5 %. GCIM has no effect on the amount of nodes used for topology repair, since it has no effect on node behaviour after they are chosen and only affects which nodes are chosen. GCIM assigns the same number of repair nodes regardless of their capability (see Figure 6-37).

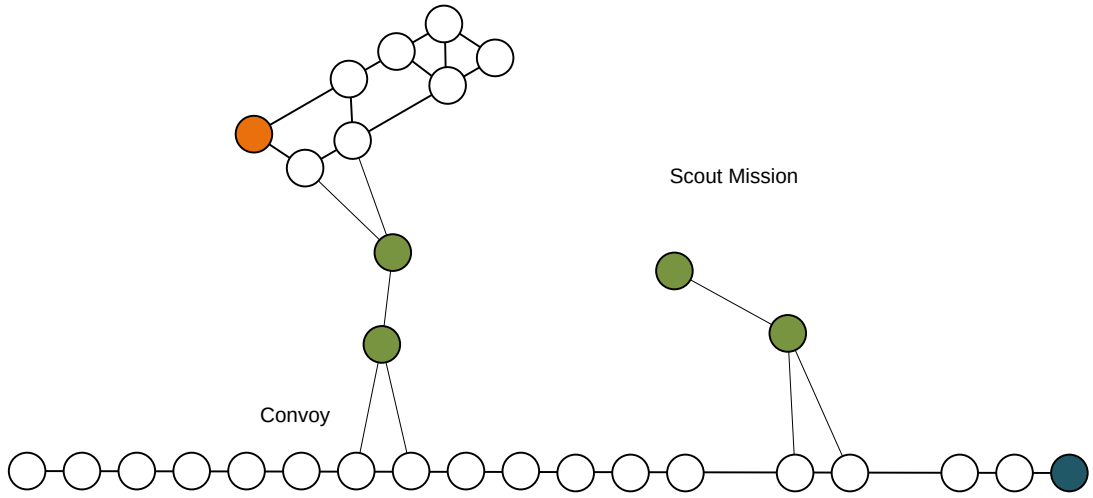

Figure 6-36 Resources wasted without CNS

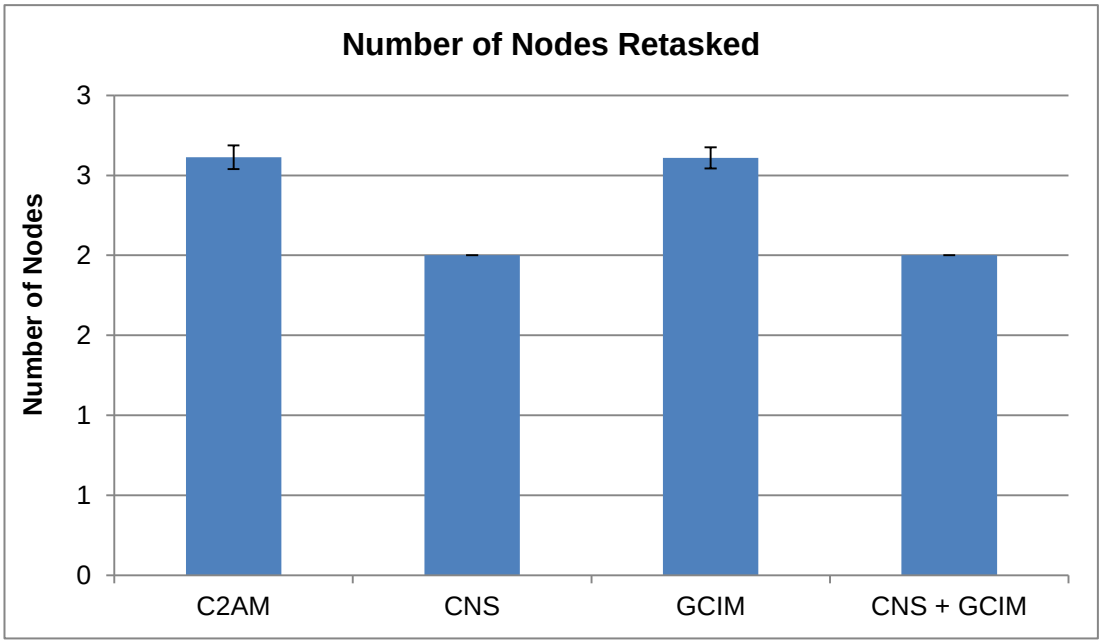

Figure 6-37 C2AM vs. CNS / GCIM Results: Number of Nodes Used

Capability Degradation

Capability degradation is the result of nodes being retasked for topology repair and leaving their respective groups as a result. Every time a node is sent to repair the network, its group loses a certain amount of capability value depending on the group capabilities of the node. By selecting the node which results in the least amount of loss of a certain capability, capability degradation can be minimised. Additionally,

the longer the distance that needs to be bridged, the more nodes are required for repair, resulting in higher capability degradation.

Because CNS reduces the number of nodes used for topology repair, it has a similar effect on capability loss due to node re-tasking. Thus CNS alone achieves an average capability loss reduction of 23.8 % of all capabilities. While C2AM determines node selection based on the importance of a node's mobility readiness and movement cost, GCIM evaluates the overall capability loss of each node in the group and selects a node for network repair which results in the least degradation of a selected mission critical capability. Compared to C2AM, GCIM alone results in an average 52.1 % reduction in capability degradation. When enabled together, CNS and GCIM reduce the Mission Critical Capability loss compared to the C2AM algorithm by 75.6 % and SC loss by 23.8 % (see Figure 6-38).

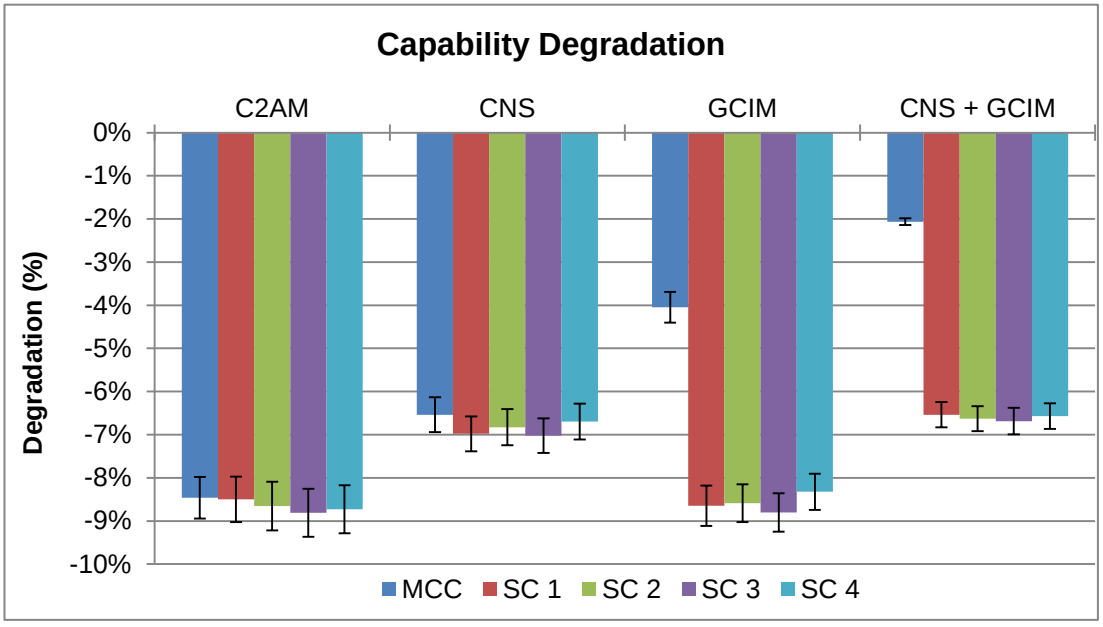

Figure 6-38 C2AM vs. CNS / GCIM Results: Capability Degradation

As is evident form the cumulative capability degradation (see Figure 6-39), CNS reduces the overall capability degradation by a larger amount then GCIM (CNS: 21 % reduction vs. GCIM: 11 % reduction, however, GCIM is able to reduce the capability degradation by a larger amount than CNS (CNS: 23.8 % vs. GCIM 52.1 %). Together GCIM and CNS achieve a cumulative capability degradation reduction of 34 %.

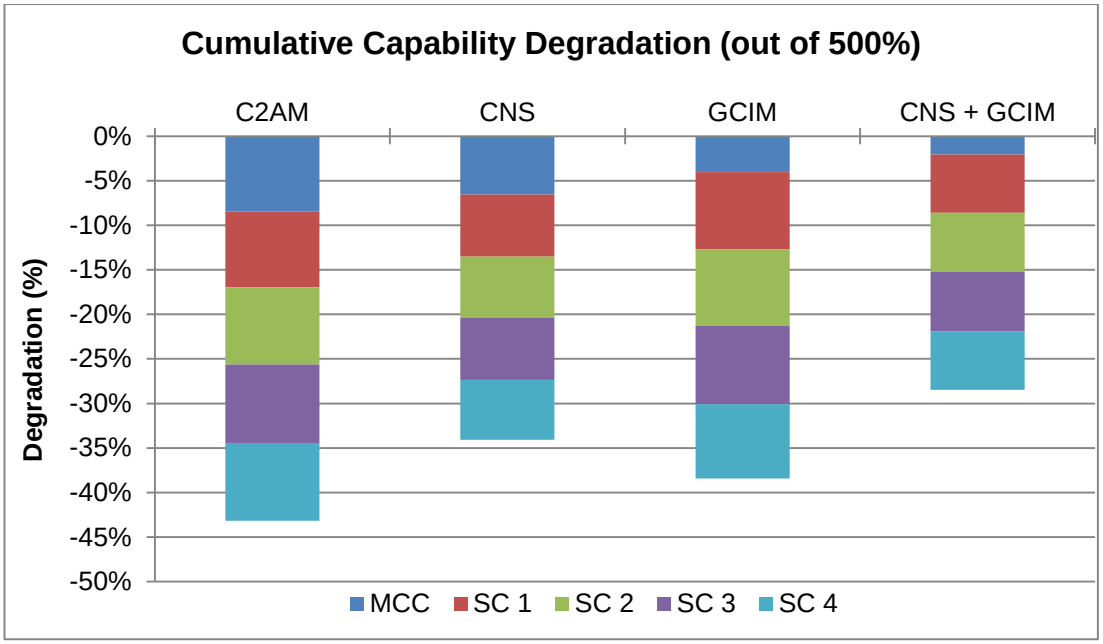

Figure 6-39 C2AM vs. CNS+GCIM Results: Cumulative Capability Degradation

Overall CNS and GCIM achieve significantly lower capability degradation than C2AM. CNS achieves its goal to minimise the number of nodes necessary for topology repair. And GCIM achieves its goal to reduce the amount of group capability lost due to node re-tasking by performing group capability based repair node selection. C2AM fails to achieve these goals.

6.3 Conclusions

6.3.1 Mission Aware Topology Healing

Mission Aware Topology Healing (MATH) fills one of the key gaps identified by [148], which notes that Relay placement in a certain region susceptible to threats or damage is an unsolved problem.

Exploiting node mobility by replacing failed nodes is an effective solution to reintegrate clusters of mobile nodes in a topology disjointed by random failure, however, in a battlefield environment, Mobile Ad-Hoc Networks (MANETs) face non-random threats, such as jamming and targeted destruction of nodes in the network. Unaware and unable to detect these non-random threats, existing approaches result in a massive subsequent loss of assets.

To address these shortcomings, MATH is proposed. It is a mission aware TMA which harnesses mission data available on a fleet data model. MATH recognises, escapes from and avoids the Danger Zone (DZ) and relocates available nodes in the network to repair a network partitioned by a localised attack by using a platform chaining algorithm to bridge long distances and effectively route around the perimeter of any DZ.

The proposed algorithm is verified using simulation and reduces the average reconnection time by more than half (52.3 %) on average compared to C2AM which relocates repair nodes without mission awareness and danger zone awareness. As is common with many conventional Topology management Algorithms (TMA), C2AM attempts to replace failed nodes with another node available for network repair, MATH reduces the amount of node loss by 40 % on average and almost triples (2.8 x) the total measured uptime compared to C2AM. When the diameter of the DZ is larger than the wireless range of the nodes, C2AM fails to reconnect the network permanently while MATH is able to reconnect the partitioned network if a sufficient number of nodes are available for network repair.

MATH's use of shared data model situational information to avoid danger zones is a significant improvement over the majority of existing algorithms such as C2AM which do not consider the possibility of danger zones and thus incapable of reacting to them, causing massive node loss as a direct result of their topology repair efforts.

As described in Chapter 3, the implications in the battlefield context are evident. MATH's significant reduction in node loss translates directly to improved communications capability and results in improved Network Enabled Capability (NEC) and Shared group capability through a higher node density.

6.3.2 Group Capability Integrity Management and Coordinated Node Selection

Coordinated Node Selection (CNS) has been designed to solve the problem of preserving the maximum amount of overall shared group capability in a group of battlefield vehicle platforms. It achieves this by coordinating repair efforts of two asymmetrically sized node segments by using cached data model data. As

demonstrated in the above experiments, by using the platform chaining algorithm, CNS is also able to mitigate the failure of a long distance Radio Access Technology (RAT) by bridging the gap between the two network segments with a chain of several nodes equipped with short range multihop RATs while using the smallest amount of repair nodes and thus preserving the largest amount of overall group capability.

Group Capability Integrity Management (GCIM) has been designed to combat the prevailing assumption of fleet homogeneity and the resulting greediness of existing topology management approaches without application awareness which may translate directly into mission defeating topologies. Specifically the fact that certain capabilities may be broken when removed from a group of other platforms is commonly ignored in the existing research.

Strong interaction among heterogeneous networked vehicle platforms gives rise to group capabilities, some of which may be mission critical. When battlefield networks become segmented, exploiting node mobility is an effective way to reconnect disjointed network segments, but a TMA must be aware of the effect that node relocation can have on the mission capabilities of a group.

When attempting to repair a network topology by relocating nodes, a TMA cannot assume that all mobile nodes are equally available to be relocated. Existing topology repair approaches such as C2AM recognise vehicle platform heterogeneity and differences in mobility readiness and mobility cost between nodes, but fail to recognise group capabilities which emerge as a result of cooperation between networked vehicle platforms and thus may create a mission defeating topology in an effort to repair a segmented topology

To address these shortcomings of existing approaches, CNS and GCIM are proposed. GCIM preserves mission critical group capabilities by performing application aware node selection which focuses on preserving mission critical capabilities within a group of nodes by using repair nodes which least impact mission critical group capabilities.

CNS preserves mission critical and secondary group capabilities by ensuring that the least amount of nodes necessary is used for network repair. It achieves this by using cached node location information from a common data model to predict the repair node selection made by disconnected segments and dispatching a repair node in the appropriate direction to ensure that repair nodes meet in the centre of the disconnected segments, thus reducing reconnection time, movement cost and number of nodes used for repair.

Experiments have been performed to measure the performance of the proposed algorithms compared to an existing application aware repair node selection algorithm, C2AM [135], which performs node selection on current node task and movement cost. Compared to C2AM which dispatches repair nodes to a random part of the disconnected network partition, CNS reduced communication downtime by an average 17.2 % and the number of nodes used for network repair by 23.5 %. Subsequently, by using fewer nodes, CNS reduced the fleet's capability degradation by 23.8 %. By selecting repair nodes which least impact the group capability, GCIM reduced Mission Critical Capability degradation by an average 52.1 %. Compared to the C2AM algorithm, the combination of GCIM and CNS reduce Mission Critical Capability degradation by 75.6 % and Secondary Capability Degradation by 23.8 %.

GCIM and CNS demonstrate a significant improvement over existing approaches by recognising that nodes in a network have mission goals and tasks beyond topology repair. Compared to existing approaches, GCIM and CNS significantly reduce the network's group capability degradation and thus avoid the creation of a mission defeating network topology.

Chapter 7 Conclusions

The main objective of this thesis has been to improve battlefield communications capability through improved management of existing platform and fleet level resources.

At the platform level, the main objective has been achieved through development of the novel High Availability Wireless Communications (HAWC) Framework which yields significantly improved functionality compared to existing approaches in several key areas:

HAWC takes advantage of available technology and enables seamless Line Replaceable Unit (LRU) plug-and-play by performing equipment management to detect new or modified equipment and hardware degradation and detecting performance changes via the Shared Data Model (SDM). In this manner HAWC enables the use of any SDM compliant Radio Access Technology (RAT) through a process of black boxing RATs and the use of defined interfaces.

HAWC also provides access to all available platform level and fleet level application data through the SDM by providing the attached Resource and Capability Management Algorithms (RCMA) with a set of performance profiles, namely the Traffic profile, RAT profile and Context Profile. This way HAWC enables the use of any current and future RCMA informed by relevant application level data from the SDM.

HAWC facilitates the use of multiple modular RCMA with minimum integration cost and enables seamless switching between these RCMA by black boxing the RCMA and using defined interfaces to pass contextual information to the RCMA. A policy document which defines the use cases of the different RCMA allows for seamless switching between RCMA based on context information.

HAWC is highly modular and flexible in compliance with the Vehicle Systems Integration (VSI) Standards and Guidelines and facilitates future modifications and upgrades through its modular design. In coherence with VSI requirements, HAWC has been assessed using the VSI Standards and Guidelines.

At the fleet level, the main objective of this thesis has been achieved by developing a set of novel topology management algorithms that are executed on the vehicle platform mission computer. The novel algorithms outperform existing approaches in the restoration of fleet communications capability in case of damage and degradation through the use of context awareness:

Mission Aware Topology Healing (MATH) is a novel distributed topology repair algorithm that uses node mobility informed by situational awareness data in order to repair a segmented network topology while evacuating and avoiding Danger Zones (DZ). MATH has been simulated in a convoy attack scenario and compared to the C2AM algorithm [135]. C2AM is chosen as a comparison to MATH due to its similar goals and application awareness to the proposed novel algorithms. In this scenario MATH reduces the average reconnection time of two separated network segments by 52.3 % and reduces the number of nodes lost by 40 %. This allows MATH to achieve a 180 % higher total uptime of the network. MATH achieves this improvement compared to C2AM by breaking a behavioural pattern common to the majority of state-of-the-art Topology Management Algorithms (TMA) and not converging on the failed node, but travelling the perimeter of any danger zones.

Coordinated Node Selection (CNS) is a novel distributed topology repair algorithm which uses cached data from the shared data model in order to minimise overall group capability loss by coordinating repair node mobility to achieve the shortest repair path and minimise nodes used for repair. CNS has been simulated in a communications failure scenario between two asymmetrically sized network partitions and compared to C2AM, CNS reduces network downtime by an average 17 % and the number of nodes used for network repair by 23.5 %. Subsequently by reducing the amount of nodes used, CNS reduces the fleet's overall capability degradation by 23.8 %.

Group Capability Integrity Management (GCIM) is a novel distributed topology repair algorithm designed to reduce fleet capability degradation of mission critical capabilities. GCIM achieves this by selecting topology repair nodes based on their contribution to shared mission critical capabilities. Using this process of selecting the node with the lowest contribution to a shared group capability allows GCIM to

reduce the degradation of a shared mission critical capability by a further 52.1 % compared to C2AM. Thus GCIM working in conjunction with CNS receives an average reduction of all capability loss by 34 %, a reduction of non- critical capability loss of 23.8 % and a reduction of Mission critical capabilities by 75.6 %.

To enable the design, implementation, performance analysis and comparative evaluation of the proposed algorithms, the novel Battlefield Network Simulation Tool has been developed which allows a user to implement algorithms both at the node level and at the fleet level and collect performance results.

Compared to existing tools, the Battlefield Network Simulation Tool enables the development and modelling of a fleet of heterogeneous battlefield vehicles equipped with heterogeneous communications resources in a realistic battlefield context subject to diverse, dynamic and hostile environments in a straightforward manner.

The tool has been validated by simulating multiple experiments using a known stimulus from [135] and comparing the output of the simulation tool the results of this work. Using the same input stimulus, the novel tool is found to produce results comparable to the existing tools used in [135] reliably.

The simulation tool has greatly benefited the design, implementation and testing of the proposed communications management framework and the proposed algorithms and has been of great utility during fault finding and iterative improvement of these algorithms.

Overall, the approaches presented in this thesis improve the current state-of-the-art in battlefield communications through improved management of communications capability of battlefield vehicle fleets.

Under the new paradigms of modern battlefield vehicle fleets, the focus of capability shifts from the individual platform to the capability of a cooperating fleet, the work presented here provides a necessary corresponding shift in focus for communications capability. The presented approaches enable this change by achieving significantly improved platform level capabilities which enable fleet level, context aware decision making to support the improved operation of battlefield communications resources

through intelligent and reactive systems that exist across multiple platforms in the fleet in a well-defined manner.

7.1 Further Work

Several avenues exist to extend this work:

Software Defined Radio (SDR) is a powerful new technology, which can be configured based on available High Availability Wireless Communications (HAWC) profile data to fill gaps in the vehicle's communications capability. Through its Shared Data Model (SDM) integration, HAWC has access to a wealth of information and with modular Resource and Capability Management (RCMA) integration; SDR can be specifically addressed in order for HAWC to become a decision maker for any attached SDR.

Using available information from the SDM, a runtime learning algorithm could be developed to select radio resources at runtime based on history. Context data could be used to build a history profile which correlates situational, vehicle and mission data with historically successful Resource and Capability Management (RCM) strategies to improve RCM robustness and eliminate historically unsuccessful techniques.

Battlefield platforms are equipped with heterogeneous Radio Access Technologies which create multiple superimposed network topologies. From these overlapping topology maps, it may be possible to interpolate certain context data, such as danger zones (DZ) and interference zones, etc. An algorithm could be developed which is able to map and analyse the overlapping topologies and thus error check, amend and enhance mission data based on interpolated information.

An algorithm could be developed to perform context based traffic scheduling. Using data available from the HAWC profiles, especially DZ and interference zone location, a platform on an unavoidable trajectory into such a zone may reschedule transmissions in order to ensure delivery of high profile traffic before reaching the zone.

In reality, a DZ is not uniformly risky for nodes. Treating DZs as a graduated risk zone emanating from the epicentre with risk decreasing with distance from the centre and an appropriate behavioural change by Mission Aware Topology Healing (MATH) should be investigated.

Missions are often carried out by a number of heterogeneous nodes which possess a specific set of capabilities necessary for specific missions, therefore it is more important that those nodes remain connected than the whole network remaining connected. An algorithm could be developed to recognise this and favour reconnection with important neighbours.

In addition to repairing the network in the event of a failure, Group Capability Integrity Management (GCIM) could be used to exchange nodes between clusters in an effort to maximise overall maximum capability. More research is needed on the feasibility and overhead of this approach.

Coordinated Node Selection (CNS) enables each separated partition to anticipate the decisions of the other cluster, thus it could also be applied to the repair node selection, prompting only a single repair node in the event of a communications failure, to preserve more group capabilities.

References

1. NATO, *IST-083 Technical Evaluation Report*, 2008.

2. Department-Of-Defense. *Dictionary of Military and Associated Terms*. 2010; Available from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

3. DSTL. *Defence Science and Technology Laboratory (DSTL)*. 2015; Available from: https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory.

4. Vetronics-Research-Centre. *Vetronics Research Centre (VRC)*. 2015; Available from: http://www.vetronics.org/.

5. Zhao, J. and R. Govindan, *Understanding packet delivery performance in dense wireless sensor networks* in *Proceedings of the 1st international conference on Embedded networked sensor systems* 2003, ACM: Los Angeles, California, USA. p. 1-13

6. Ye, Z., S.V. Krishnamurthy, and S.K. Tripathi, *A framework for reliable routing in mobile ad hoc networks*, in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*2003. p. 270-280.

7. Ngai, E., et al., *A delay-aware reliable event reporting framework for wireless sensor-actuator networks.* Ad Hoc Networks, 2010. 8(7): p. 694-707.

8. Shanshan, J. *Optimal Wireless Network Restoration under Jamming Attack*. 2009.

9. General-Dynamics. *Bowman - Command Battlespace Management (Land) (CBM(L))*. 2015; Available from: http://www.generaldynamics.uk.com/solutions-and-capabilities/bowman-command-battlespace-management.

10. Ministry-of-Defence. *Foxhound*. 2015; Available from: http://www.army.mod.uk/equipment/23437.aspx.

11. General-Dynamics. *Scout SV* 2015; Available from: http://www.generaldynamics.uk.com/scoutsv/.

12. Ministry-of-Defence. *Warrior infantry fighting vehicle*. 2015; Available from: http://www.army.mod.uk/equipment/23237.aspx.

13. Rayment, S., *'Broken' £2.4bn radio put troops' lives in danger*, in *The Telegraph* 2008.

14. defence-and-security.com, *Over, but not out*, in *Defense and Security Systems International*2015.

15. Rheinmetall-AG. *Bundeswehr fields new Gladius soldier system*. 2013 27/02/2013]; Available from: http://www.rheinmetall-defence.com.

16. army-technology.com. *FIST - Future Infantry Soldier Technology, United Kingdom*. 2012 Available from: http://www.army-technology.com/projects/fist/.

17. McKinney, D., *Impact of Commercial Off-The-Shelf (COTS) Software and Technology on Systems Engineering*, 2001.

18. Kodialam, M. and T. Nandagopal, *Characterizing the capacity region in multi-radio multi-channel wireless mesh networks*, in *Proceedings of the 11th annual international conference on Mobile computing and networking*2005, ACM: Cologne, Germany. p. 73-87.

19. Ossama Younis, L.K., Anthony McAuley, Kyriakos Manousakis, David Shallcross, Kaustubh Sinkar, Kirk Chang, Kenneth Young, Telcordia Industries Inc., Charles Graff, Mitesh Patel, U.S. Army CERDEC, *Cognitive Tactical Network Models.* IEEE Communications Magazine, 2010. 48(10).

20. Ketil Lund, A.E., Dinko Hadzic, Trude Hafsoe, Frank T. Jonsen, Norwegian Defense Research Department, *Using Web Services to Realize Service Oriended Architecture in Military Communication Networks* IEEE Communications Magazine, 2007. 45(10).

21. Michael Street, D.M., *Software Defined Radio to Enable NNEC: Technical Challenges and Opportunities for NATO*, in *RTO-MP-IST-083 Military Communications with a Special Focus on Tactical Communications for Network Centric Operations* 2008: RTO Information Systems Technology Panel (IST) Symposium held in Prague, Czech Republic.

22. NATO, *RTO-MP-IST-083 Military Communications with a Special Focus on Tactical Communications for Network Centric Operations*, 2008: RTO Information Systems Technology Panel (IST) Symposium held in Prague, Czech Republic.

23. Linear-Technology. *Wireless Sensor Networks - Dust Networks*. 2015; Available from: http://www.linear.com/products/wireless_sensor_networks_-_dust_networks.

24. NATO, *Technical Communications in Urban Operations* 2010.

25. Khandani, A.E., et al., *Reliability and Route Diversity in Wireless Networks.* Ieee Transactions on Wireless Communications, 2008. 7(12): p. 4772-4776.

26. Ortiz, J. and D. Culler, *Multichannel reliability assessment in real world WSNs*, in *Proceedings of the 9th ACM/IEEE International Conference on*

*Information Processing in Sensor Networks*2010, ACM: Stockholm, Sweden. p. 162-173.

27. Dawson-Haggerty, S., et al., *The Effect of Link Churn on Wireless Routing*, 2008.

28. Pister, P.K., *Wireless Sensor Networks: Technology and Applications*, 2007.

29. Kan, Z., et al., *Survey of Large-Scale MIMO Systems.* Communications Surveys & Tutorials, IEEE, 2015. 17(3): p. 1738-1760.

30. Draves, R., J. Padhye, and B. Zill, *Routing in multi-radio, multi-hop wireless mesh networks,* in *Proceedings of the 10th annual international conference on Mobile computing and networking*2004, ACM: Philadelphia, PA, USA. p. 114-128

31. Elsner, J., *Interference Mitigation in Frequency Hopping Ad Hoc Networks.* 2012.

32. Taewon, H., et al., *OFDM and Its Wireless Applications: A Survey.* Vehicular Technology, IEEE Transactions on, 2009. 58(4): p. 1673-1694.

33. Molisch, A.F., et al., *A survey on vehicle-to-vehicle propagation channels.* Wireless Communications, IEEE, 2009. 16(6): p. 12-22.

34. Di Renzo, M., H. Haas, and P.M. Grant, *Spatial modulation for multiple-antenna wireless systems: a survey.* Communications Magazine, IEEE, 2011. 49(12): p. 182-191.

35. Baccour, N., et al., *External radio interference*, in *Radio Link Quality Estimation in Low-Power Wireless Networks*2013, Springer. p. 21-63.

36. Steve Jameson, J.F., Robert Szczerba, Sandy Stockdale *Collaborative Autonomy for Manned/Unmanned Teams.* 2005.

37. Fuller, S.B., et al., *Controlling free flight of a robotic fly using an onboard vision sensor inspired by insect ocelli*. Vol. 11. 2014.

38. Darpa. *TIME MAGAZINE RECOGNIZES DARPA'S HUMMINGBIRD NANO AIR VEHICLE*. 2011; Available from: http://www.darpa.mil/newsevents/releases/2011/11/24.aspx.

39. Shen, S., *Autonomous navigation in complex indoor and outdoor environments with micro aerial vehicles*, 2014: University of Pennsylvania.

40. GRASP Lab, U.o.P. *Aggressive Maneuvers for Autonomous Quadrotor Flight*. 2010; Available from: https://www.youtube.com/watch?v=MvRTALJp8DM.

41. GRASP Lab, U.o.P., *Cooperative Grasping and Transport using Quadrotors.* 2010.

42. Bekmezci, İ., O.K. Sahingoz, and Ş. Temel, *Flying Ad-Hoc Networks (FANETs): A survey.* Ad Hoc Networks, 2013. 11(3): p. 1254-1270.

43. Robotics, R. *Throwbot*. 2015; Available from: http://www.reconrobotics.com/products/Throwbot_XT_audio.cfm.

44. Boston-Dynamics. *Atlas*. 2015; Available from: http://www.bostondynamics.com/robot_Atlas.html.

45. Boston-Dynamics. *BigDog*. 2015; Available from: http://www.bostondynamics.com/robot_bigdog.html.

46. Ministry-of-Defence, *Logistics For Joint Operations.* 2007.

47. Hodge, N., *Killer App: Army Tests Smartphones for Combat*, 2011: The Wall Street Journal.

48. Connor, R.M., *Vetronics Standards & Guidelines* 2009.

49. Los-Angeles-Air-Force-Base. *MILSTAR*. 2014; Available from: http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5328.

50. Ministry-of-Defence. *MOD launches new Skynet satellite*. 2012; Available from: https://www.gov.uk/government/news/mod-launches-new-skynet-satellite.

51. Iridium-Communications-Inc. *Iridium Everywhere*. 01/06/2015]; Available from: https://iridium.com/default.aspx.

52. Mailsail-Satellite-Communications. *Iridium Bandwidth and Internet Download Speeds*. 2015 10/05-2015]; Available from: http://www.mailasail.com/Support/Iridium-Bandwidth.

53. McMahon, M.M. and R. Rathburn, *Measuring latency in Iridium satellite constellation data services*, 2005, DTIC Document.

54. Airbus. *SKYNET 5 X-BAND*. 2015 18/05/2015]; Available from: http://www.satcom-airbusds.com/products-solutions/government-satcom/products-systems/bandwidth/skynet-5-x-band/.

55. Ridhawi, I.A., *Simulation-Assisted QoS-Aware VHO in Wireless Heterogeneous Networks*, 2014: Canada.

56. Next-Generation-Mobile-Networks-Alliance, *5G White Paper - Executive Version* 2014.

57. Richardson, M. and P.S. Ryan, *WiMAX: Opportunity or Hype?* 2006.

58. Anastasi, G., et al. *IEEE 802.11 ad hoc networks: performance measurements*. in *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on*. 2003. IEEE.

59. Stein, J.C., *Indoor radio WLAN performance part II: Range performance in a dense office environment.* Intersil Corporation, 1998.

60. Flickenger, R., et al., *Wireless networking in the developing world*2006: The Code.

61. Cisco, *802.11ac: The Fifth Generation of Wi-Fi Technical White Paper*, 2014.

62. Hiertz, G.R., et al., *IEEE 802.11s: The WLAN Mesh Standard.* Wireless Communications, IEEE, 2010. 17(1): p. 104-111.

63. Martin Cave, W.W., *Spectrum licensing and spectrum commons where to draw the line* 2004.

64. Svensson, C., *The blocker challenge when implementing software defined radio receiver RF frontends.* Analog Integrated Circuits and Signal Processing, 2010. 64(2): p. 81-89.

65. Thales. *CONTACT: the only SDR program of such magnitude in Europe*. 2014; Available from: https://www.thalesgroup.com/en/worldwide/defence/case-study/contact-only-sdr-program-such-magnitude-europe.

66. Akyildiz, I.F. and W. Xudong, *A survey on wireless mesh networks.* Communications Magazine, IEEE, 2005. 43(9): p. S23-S30.

67. Dr. S. Karthik, S.K., Dr. M.L. Valarmathi, Dr. V.P. Arunachalam, Dr. T. Ravichandran, *An Performance Analysis and Comparison of Multi-Hop Wireless Ad-Hoc Network Routing Protocols in MANET.* International Journal of Academic Research, 2010.

68. Kongara, H., Y.R. Kondareddy, and P. Agrawal. *Fairness and Gateway Classification Algorithm (GCA) in multihop Wireless Mesh Networks*. in *System Theory, 2009. SSST 2009. 41st Southeastern Symposium on*. 2009.

69. Mesh-Networks-Inc., *Mesh Networks.* 2012.

70. Mesh-Dynamics. *Mesh Dynamics*. 2015; Available from: http://www.meshdynamics.com/.

71. Radiant-Networks-Services-Inc. *Radiant Networks*. 2010; Available from: http://radiant-networks.com/.

72. Persistent-Systems, *Wave Relay 5.* 2015.

73. Mohseni, S., et al. *Comparative review study of reactive and proactive routing protocols in MANETs*. in *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*. 2010.

74. Park, V. and M.S. Corson, *Temporally-ordered routing algorithm (TORA) version 1 functional specification*, 1997, Internet-Draft, draft-ietf-manet-tora-spec-00. txt.

75. Perkins, C.E. and E.M. Royer. *Ad-hoc on-demand distance vector routing*. in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*. 1999. IEEE.

76. Perkins, C.E. and P. Bhagwat. *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers*. in *ACM SIGCOMM Computer Communication Review*. 1994. ACM.

77. Johnson, D.B., *The dynamic source routing protocol for mobile ad hoc networks.* draft-ietf-manet-dsr-09. txt, 2003.

78. Chroboczek, J., *RFC 6126 - The Babel Routing Protocol*, 2011: Internet Engineering Task Force (IETF).

79. Vetronics-Research-Centre, *Vehicle Technology Integration Demonstrator (VTID) RT/COM/4/048-VRC-Final-01082009.* 2009.

80. The-Open-Group, *Data Link Provider Interface (DLPI), Version 2* 2000.

81. ISO, *standard 7498-1*, 1994.

82. Prudencio, A.C., et al. *Quality of Service Specifications: A Semantic Approach*. in *Network Computing and Applications, 2009. NCA 2009. Eighth IEEE International Symposium on*. 2009.

83. The-Open-Group. *Quality of Data Link Service*. 2000; Available from: http://pubs.opengroup.org/onlinepubs/009618899/chap4.htm#tagcjh_05_05.

84. Bovy, C., et al. *Analysis of end-to-end delay measurements in Internet*. in *Proceedings of ACM Conference on Passive and Active Leasurements (PAM), Fort Collins, Colorado, USA*. 2002.

85. Smith, D.R., *Digital transmission systems*2012: Springer Science & Business Media.

86. Urzi, R., *A Research Agenda for Mixed-Criticality Systems.*

87. Ministry-of-Defence, *Defence Standard 23-09, Generic Vehicle Architecture (GVA)* 2010.

88. US-Army. *The Vehicle Integration for C4ISR/EW Interoperability (VICTORY)*. 2015; Available from: http://victory-standards.org/.

89. Jedynak, D., *VICTORY Standard Eliminates Costly Vehicle Redundancies.* COTS Journal, 2013.

90. VSI. *VSI - Vehicle Systems Integration*. 2015; Available from: http://www.vsi.org.uk/.

91. Press, S.J., *Annex to Vetronics Standards & Guidelines: VSI Metrics for Electronic Architecture Assessment*, 2009.

92. Hoberman, S., *Data Modeling Made Simple: A Practical Guide for Business and IT Professionals*2009: Technics Publications.

93. Object-Management-Group. *DDS The Proven Data Connectivity Standard for the IoT*. 2015; Available from: http://portals.omg.org/dds/.

94. Ministry-of-Defence. *Foxhound arrives in Afghanistan*. 2012; Available from: https://www.gov.uk/government/news/foxhound-arrives-in-afghanistan.

95. Ministry-of-Defence, *Defence Standard 23-12, Generic Soldier Architecture (GSA)* 2013.

96. Ministry-of-Defence, *Defence Standard 23-13, Generic Base Architecture (GBA)* 2012.

97. Porjazoski, M. and B. Popovski. *Radio access technology selection in heterogeneous wireless networks based on service type and user mobility*. in *Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on*. 2011.

98. Ratliff, S., et al., *Dynamic link exchange protocol (dlep).* 2014.

99. Mohanty, S., *A new architecture for 3G and WLAN integration and inter-system handover management.* Springer Science + Business Media, 2006.

100. Kang, J.-M., et al., *Autonomic personalized handover decisions for mobile services in heterogeneous wireless networks.* Computer Networks, 2011. 55(7): p. 1520-1532.

101. Fan, C., et al. *Managing Heterogeneous Access Networks Coordinated policy based decision engines for mobility management*. in *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*. 2007.

102. Stenio Fernandes, A.K., *Vertical Mobility Management Architectures in Wireless Networks: A Comprehensive Survey and Future Directions.* IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2012. 14(1).

103. Dimou, K., et al. *Generic link layer: a solution for multi-radio transmission diversity in communication networks beyond 3G*. in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*. 2005.

104. Marina, M.K., S.R. Das, and A.P. Subramanian, *A topology control approach for utilizing multiple channels in multi-radio wireless mesh networks.* Computer Networks, 2010. 54(2): p. 241-256.

105. Zanakis, S.H., et al., *Multi-attribute decision making: A simulation comparison of select methods.* European Journal of Operational Research, 1998. 107(3): p. 507-529.

106. Intel, *PHY Interface For the PCI Express, SATA, and USB 3.1 Architectures*, 2007.

107. Google. *Project Ara*. 2015 2015/06/23]; Available from: http://www.projectara.com/.

108. Liu, S.-m., et al. *A Simple Additive Weighting Vertical Handoff Algorithm Based on SINR and AHP for Heterogeneous Wireless Networks*. in *Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on*. 2010.

109. Stevens-Navarro, E. and V.W.S. Wong. *Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks*. in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*. 2006.

110. Hwang, C.L.Y., K., *Multiple Attribute Decision Making: Methods and Applications*1981: New York: Springer-Verlag.

111. Saaty, T.L., *Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World*1982.

112. Julong, D., *Introduction to Grey System Theory* The Journal of Grey System, 1989. 1.

113. Yoon, W. and N. Vaidya, *Routing exploiting multiple heterogeneous wireless interfaces: A TCP performance study.* Computer Communications, 2010. 33(1): p. 23-34.

114. Ansari, J., X. Zhang, and P. Mahonen, *Multi-radio medium access control protocol for wireless sensor networks.* Int. J. Sen. Netw., 2010. 8(1): p. 47-61.

115. Yang, L., et al., *Supporting demanding wireless applications with frequency-agile radios*, in *Proceedings of the 7th USENIX conference on Networked systems design and implementation*2010, USENIX Association: San Jose, California. p. 5-5.

116. Niebert, N., et al. *Ambient networks: a framework for future wireless internetworking*. in *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*. 2005.

117. 3GPP, *TS 43.318 V12.1.0* 2015.

118. IEEE, *IEEE Standard for Local and metropolitan area networks - Part 21: Media Independent Handover Services* 2008.

119. Ferrus, R., et al., *Interworking in heterogeneous wireless networks: Comprehensive framework and future trends.* Wireless Communications, IEEE, 2010. 17(2): p. 22-31.

120. Eastwood, L., et al., *Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based, IMT-advanced (4G) network.* Wireless Communications, IEEE, 2008. 15(2): p. 26-34.

121. Yonghoon, C., et al., *Joint Resource Allocation for Parallel Multi-Radio Access in Heterogeneous Wireless Networks.* Wireless Communications, IEEE Transactions on, 2010. 9(11): p. 3324-3329.

122. Swades, D., et al. *Integrated cellular and ad hoc relay (iCAR) systems: pushing the performance limits of conventional wireless networks*. in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*. 2002.

123. Luo, b.H., et al. *UCAN: A Unified Cellular and Ad-Hoc Network Architecture*. in *ACM MOBICOM*. 2003.

124. Yiyue, W., et al. *Capacity Optimization in Networks with Heterogeneous Radio Access Technologies*. in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. 2011.

125. Shu-Ping, Y., et al. *QoS Aware Scheduling and Cross-Radio Coordination in Multi-Radio Heterogeneous Networks*. in *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*. 2013.

126. Danzeisen, M., et al. *Simulations on Heterogeneous Networking with CAHN*. 2006.

127. Koudouridis, G.P., et al., *Generic Link Layer Functionality for Multi-Radio Access Networks*, in *IST Mobile and Wireless CommunicationsSummit*2005.

128. Sachs, J. *A generic link layer for future generation wireless networking*. in *Communications, 2003. ICC '03. IEEE International Conference on*. 2003.

129. Sachs, J., et al. *A generic link layer in a beyond 3G multi-radio access architecture*. in *Communications, Circuits and Systems, 2004. ICCCAS 2004. 2004 International Conference on*. 2004.

130. Ingvild Sorteberg, D.Ø.K., *Policy Based Dynamic Management for Tactical Military Networks*, 2008.

131. Koutsonikolas, D. and Y. Charlie Hu, *Exploring the design space of reliable multicast protocols for wireless mesh networks.* Ad Hoc Networks, 2009. 7(5): p. 932-954.

132. Ministry-of-Defence, *Joint Service Publication 777 Network Enabled Capability.* 2005.

133. Senturk, I.F., K. Akkaya, and S. Yilmaz, *Relay placement for restoring connectivity in partitioned wireless sensor networks under limited information.* Ad Hoc Networks, 2014. 13, Part B(0): p. 487-503.

134. Nigam, A. and Y.K. Agarwal, *Optimal relay node placement in delay constrained wireless sensor network design.* European Journal of Operational Research, 2014. 233(1): p. 220-233.

135. Abbasi, A., et al. *C 2 AM: an algorithm for application-aware movement-assisted recovery in wireless sensor and actor networks*. in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*. 2009. ACM.

136. Imran, M., et al. *Partitioning Detection and Connectivity Restoration Algorithm for Wireless Sensor and Actor Networks*. in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*. 2010.

137. Akkaya, K., et al. *Distributed Recovery of Actor Failures in Wireless Sensor and Actor Networks*. in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*. 2008.

138. Vaidya, K. and M. Younis. *Efficient failure recovery in Wireless Sensor Networks through active, spare designation*. in *Distributed Computing in Sensor Systems Workshops (DCOSSW), 2010 6th IEEE International Conference on*. 2010.

139. Tang, J., B. Hao, and A. Sen, *Relay node placement in large scale wireless sensor networks.* Computer Communications, 2006. 29(4): p. 490-501.

140. Bin, H., T. Jian, and X. Guoliang. *Fault-tolerant relay node placement in wireless sensor networks: formulation and approximation*. in *High Performance Switching and Routing, 2004. HPSR. 2004 Workshop on*. 2004.

141. ArunBaburam, *Adaptive Mobility Based Clustering and Hybrid Geographic Routing for Mobile Ad Hoc Networks*, 2006. p. 235.

142. Younis, M., L. Sookyoung, and A.A. Abbasi, *A Localized Algorithm for Restoring Internode Connectivity in Networks of Moveable Sensors.* Computers, IEEE Transactions on, 2010. 59(12): p. 1669-1682.

143. Abbasi, A.A., K. Akkaya, and M. Younis. *A Distributed Connectivity Restoration Algorithm in Wireless Sensor and Actor Networks*. in *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*. 2007.

144. Senel, F., K. Akkaya, and M. Younis. *An Efficient Mechanism for Establishing Connectivity in Wireless Sensor and Actor Networks*. in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*. 2007.

145. Grandi, R., R. Falconi, and C. Melchiorri. *Coordination and control of autonomous mobile robot groups using a hybrid technique based on Particle*

Swarm Optimization and Consensus. in *Robotics and Biomimetics (ROBIO), 2013 IEEE International Conference on*. 2013.

146. Lee, S., M. Younis, and M. Lee, *Connectivity restoration in a partitioned wireless sensor network with assured fault tolerance.* Ad Hoc Networks, 2014(0).

147. Akkaya, K., I.F. Senturk, and S. Vemulapalli, *Handling large-scale node failures in mobile sensor/robot networks.* Journal of Network and Computer Applications, 2013. 36(1): p. 195-210.

148. Younis, M., et al., *Topology management techniques for tolerating node failures in wireless sensor networks: A survey.* Computer Networks, 2014. 58(0): p. 254-283.

149. Riverbed. *OPNET*. 2015; Available from: http://www.riverbed.com/products/performance-management-control/opnet.html.

150. OpenSim-Ltd. *OMNeT++* 2015; Available from: https://omnetpp.org/.

151. ISI. *The Network Simulator ns2*. 2012 01/12/2012]; Available from: http://www.isi.edu/nsnam/ns/.

152. Scalable-Network-Technologies. *QualNet*. 2014; Available from: http://web.scalable-networks.com/content/qualnet.

153. Boson-Holdings. *NetSim*. 2015; Available from: http://www.boson.com/netsim-cisco-network-simulator.

154. XJ-Technologies. *Anylogic*. 12/12/2012]; Available from: http://www.anylogic.com/.

155. Bai, F. and A. Helmy, *A survey of mobility models.* Wireless Adhoc Networks. University of Southern California, USA, 2004. 206.

156. Jungkeun, Y., L. Mingyan, and B. Noble. *Random waypoint considered harmful*. in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. 2003.

157. Roughan, M., et al., *Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification*, in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*2004, ACM: Taormina, Sicily, Italy. p. 135-148.

158. Lickteig, C.W., *Design Guidelines and Functional Specifications for Simulation of the Battlefield Management System's (BMS) User Interface*1988.

159. Technologies, R.B. *Boomerang III*. 2014; Available from: http://bbn.com/products_and_services/boomerang/.