NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A COMPARATIVE ANALYSIS OF NETWORK APPROACHES FOR TACTICAL WIRELESS COMMUNICATIONS, VALIDATED BY JOINT COMMUNICATION SIMULATION SYSTEM (JCSS) SIMULATIONS: A SWEDISH PERSPECTIVE

by

Fredrik Maxén

September 2011

Thesis Co-Advisors: Alex Bordetsky
Terry E. Smith

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE A Comparative Analysis of Network Approaches for Tactical Wireless Communications, Validated by Joint Communication Simulation System (JCSS) Simulations: A Swedish Perspective		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Fredrik Maxén			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number: N/A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis project explores two approaches for military tactical wireless communications solutions in the context of being useful for the Swedish Armed Forces. The study's tactical perspective focuses on a force of battalion size. The two network approaches, ad hoc networking and infrastructure based, were analyzed and compared via simulation. As a baseline for this thesis project, research was initiated based on appropriate communication requirements for the tactical force. This was followed by background research into current technologies for ad hoc networking and infrastructure-based systems. In order to analyze and compare the two technology approaches, a model was developed using the software Joint Communication Simulation System (JCSS) and a battalion-sized network simulation using ad hoc and infrastructure-based technology.

This thesis project addressed tactical force requirements from the perspective of the basic Swedish Armed Forces principle for command and control, which is Maneuver Warfare. Evaluation of the technologies is discussed through the important perspectives of capacity, mobility, flexibility, robustness, interoperability, and cost. By analyzing the technology approaches from these perspectives, this thesis project attempts to provide the Swedish Armed Forces with more information and understanding, which in-turn will allow better-suited future developments of all tactical wireless communication systems.

14. SUBJECT TERMS Ad Hoc Networking, Infrastructure Based Systems, Tactical Communications, Software Defined Radio, JCSS, Modeling, Simulation			**15. NUMBER OF PAGES** 110
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A COMPARATIVE ANALYSIS OF NETWORK APPROACHES FOR TACTICAL WIRELESS COMMUNICATIONS, VALIDATED BY JOINT COMMUNICATION SIMULATION SYSTEM (JCSS) SIMULATIONS: A SWEDISH PERSPECTIVE

Fredrik Maxén
Lieutenant Colonel, Swedish Army
B.S., Swedish National Defence College, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRONIC WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Author: Fredrik Maxén

Approved by: Alex Bordetsky
Thesis Co-Advisor

Terry E. Smith
Thesis Co-Advisor

Dan Boger
Chair, Department of Information Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis project explores two approaches for military tactical wireless communications solutions in the context of being useful for the Swedish Armed Forces. The study's tactical perspective focuses on a force of battalion size. The two network approaches, ad hoc networking and infrastructure based, were analyzed and compared via simulation. As a baseline for this thesis project, research was initiated based on appropriate communication requirements for the tactical force. This was followed by background research into current technologies for ad hoc networking and infrastructure-based systems. In order to analyze and compare the two technology approaches, a model was developed using the software Joint Communication Simulation System (JCSS) and a battalion-sized network simulation using ad hoc and infrastructure-based technology.

This thesis project addressed tactical force requirements from the perspective of the basic Swedish Armed Forces principle for command and control, which is Maneuver Warfare. Evaluation of the technologies is discussed through the important perspectives of capacity, mobility, flexibility, robustness, interoperability, and cost. By analyzing the technology approaches from these perspectives, this thesis project attempts to provide the Swedish Armed Forces with more information and understanding, which in-turn will allow better-suited future developments of all tactical wireless communication systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

2G	Second Generation (Mobile Communications System)
3G	Third Generation (Mobile Communications System)
4G	Fourth Generation (Mobile Communications System)
ADSL	Asymmetric Digital Subscriber Line
AMF	Airborne, Maritime Fixed-Station
AOR	Area of Responsibility
ANDVT	Advanced Narrow Band Digital Voice Terminal
AN/PRC	Army Navy / Portable Radio Communication
CBMANET	Control Based Mobile Ad hoc Network
CDMA	Code Division Multiple Access
CIMIC	Civilian and Military Cooperation
CIS	Communication and Information Systems
COFDM	Coded Orthogonal Frequency Division Multiplexing
CPFSK	Continuous Phase Frequency Shift Keying
DARPA	Defense Advanced Research Project Agency
DISA	Defense Information Systems Agency
DSSS	Direct Sequence Spread Spectrum
EA	Electronic Attack
EDGE	Enhanced Data Rates for GSM Evolution
EMP	Electronic Magnetic Pulse
EU	European Union
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FTP	File Transfer Protocol
GMR	Ground Mobile Radio
GOP	Guidance for Operational Planning
GSM	Global System for Mobile Communications
GTRS	Gemensamt Taktiskt Radio System (The Swedish Project for developing Software Defined Radios)
HAIPE	High Assurance Internet Protocol Encryption

HMMWV	High Mobility Multipurpose Wheeled Vehicle
HMS	Handheld, Manpack, Small Form Fit
HPM	High Power Microwave weapons
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISAF	International Security Assistance Force (NATO Force in Afghanistan)
J	Joint
JCSS	Joint Communications Simulation System
JEM	JTRS Enhanced MBITR
JFC	Joint Forces Command
JTRS	Joint Tactical Radio System
JTRS JPO	Joint Tactical Radio System Joint Program Executive Officer
KFOR	Kosovo Force (NATO Kosovo Force)
LAN	Local Area Network
LOG	Logistics
LTE	Long Term Evolution
MANET	Mobile Ad hoc Network
MBITR	Multiband Inter/Intra Team Radio
Mech	Mechanized
MIDS	Multifunctional Information Distribution System
NATO	North Atlantic Treaty Organization
NBG	Nordic Battle Group
NCW	Network Centric Warfare
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing
OODA	Observe, Orient, Decide, Act (from John Boyd's OODA-loop)
OPP	Operational Planning Procedure
OSI	Open Systems Interconnection
PCMS	Programmable, Modular Communications System
PN	Pseudo Noise
PRNet	Packet Radio Network

PRT	Provincial Reconstruction Team
PSO	Peace Support Operation
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
SCA	Software Communications Architecture
SCPT	Single Channel Plain Text
SDR	Software Defined Radio
SINCGARS	Single Channel Ground and Airborne Radio System
SRW	Soldier Radio Waveform
SwAF	Swedish Armed Forces
STANAG	Standard NATO Agreement
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TDRS	Tactical Data Radio System
TETRA	Terrestrial Trunked Radio
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UGS	Unattended Ground Sensor
UGV	Unattended Ground Vehicle
UMTS	Universal Mobile Telecommunications System
UN	United Nations
UNPROFOR	United Nations Protection Force
US	United States
WCDMA	Wideband Code Division Multiple Access
WNW	Wideband Networking Waveform
WP	Warsaw Pact
WWII	World War II

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to thank my thesis advisors, Dr. Alex Bordetsky and Lieutenant Colonel Terry Smith, for providing me with professional guidance and support throughout this thesis research.

I would also like to thank Johan Sigholm and Dr. Martin Norsell at the Swedish National Defence College (SNDC) for assisting me in developing the idea for this thesis project.

I would like to express a sincere thanks to Dennis Andersson and Mattias Sköld at the Swedish Defence Research Agency (FOI) for providing knowledge and accurate, timely responses to information requests for my thesis research.

I would like to thank Chris Miller, Steven Crum and Imran Umar at the Defense Information Systems Agency (DISA) for training and assisting me when developing the simulations in JCSS.

I would also like to thank Varun Lalchandani, Prasanna Sukumar, and Alejandro Talavera at OPNET in Bethesda, Maryland. They provided exceptional support, debugging the network models and providing a special support when developing the UMTS network model.

A special thanks to Captain Terry Traylor USMC who initially helped me getting started using JCSS.

I would also like to thank Robert Broadston and Albert Barreto at the Naval Postgraduate School, for assisting me with laboratory facilities and computer configuration.

Lastly, and most importantly, I would like to thank my fantastic wife, Maria, and our two awesome children, Johan and Saga, for their unconditional love and endless support throughout my studies for my master's degree at the Naval Postgraduate School and completing this thesis project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND TO WIRELESS COMMUNICATION

Mobile systems for radio communication were first used in the early years of the twentieth century. When radio systems were installed in tanks during WWII, the ability for these forces to maneuver increased vastly. The armored units could now act fast and with precision, and the commander could lead his force by using real-time communication systems. In the early days, the available technology provided only analogue communication with a very limited level of service. Digitization matured the development for radio communications one step further. Digital communications technology made it possible to not only increase the amount of information that could be transferred, but also expand the kinds of information transmitted between two points. Initially, only voice and text could be transferred; with digital communication, however, it became possible to transfer pictures and video. Today's battlefield environment requires extensive and flexible capabilities for our fighting forces. Our battle space also requires sharing information between units and soldiers in very short time durations. The need to share information also goes beyond various services. In order to conduct joint operations, it is important for our communications infrastructure to have high interoperability so that units from one service can readily communicate with units from other services. The ongoing development for radio communications capabilities has evolved to create ad hoc networks where every radio acts as a node of a larger system. These nodes autonomously communicate and keep track of each other. If you want to communicate with a unit that is located far away from your current position, you must use many nodes between the two units in order to get the message through to the distant destination. An ad hoc system is a peer-to-peer configuration (no centralized server), which is extremely important because it allows military nodes and systems to be set up temporarily to meet an immediate need [1].

The extensive civilian development for wireless communication is another dimension that must be taken into consideration in the future development of military wireless communication. Substantial sums of money and resources are used in the

ongoing projects for systems ultimately intended to be used strictly for military tactical communications. At the same time, civilian communication technology can be expected to provide critical hardware and software that must be used for military purposes as well. On the commercial side, GSM was the first digital technology, and it was followed by UMTS/3G. In some countries, the next generation 4G/LTE have already been released. This infrastructure-based technology is an alternative, or at a minimum a backup, to military systems providing military mission capabilities and using software radios in an ad hoc network.

B. ONGOING DEVELOPMENT FOR MILITARY RADIO COMMUNICATION

1. Joint Tactical Radio System (JTRS)

The solution that the United States has chosen to meet future requirements for military radio communication is the Joint Tactical Radio System (JTRS) project, begun in 1997. The Department of Defense initiated the JTRS program in order to develop a family of software programmable tactical radios that would provide deployed military forces required voice, data and video communications support. This early JTRS design was titled Programmable, Modular Communications System (PMCS), and was intended to replace older hardware-intensive radios with software applications in order to support military operations over a wide range of systems, from Army units to airplanes and ships [2]. JTRS was restructured in 2005, falling under the leadership of a Joint Program Executive Officer with headquarter in San Diego, California. The identified goal for JTRS is to develop a family of interoperable, modular, software radios. The scope of the JTRS program is to be able to operate in ad hoc wireless networks and provide service for mobile and fixed forces that consist of U.S. joint forces, allies, coalition partners and disaster response personnel [3].

The family of software-defined JTRS radios was eventually divided into sub-programs. Initially, these sub-programs were named clusters, but were later renamed into function-oriented names. The sub-programs were defined as follows:

Figure 1. Example of hardware within JTRS (From [3])

JTRS Ground Mobile Radio (JTRS GMR), previously called Cluster 1

The sub-program JTRS Ground Mobile Radio is Army-led and focused to develop vehicle mounted radios for the Army and the Marine corps. The company Boeing helped develop the GMR program and they are now in the formal testing period. The JTRS GMR will be installed in U.S. Army vehicles such as Abrams, Bradley and High Mobility Multipurpose Wheeled Vehicles (HMMWV:s) [4]. The Wideband Networking Waveform (WNW) and the JTRS SINCGARS are waveforms that have been developed for JTRS GMR.

JTRS Multiband Inter/Intra Team Radio (JTRS MBITR), previously called Cluster 2

The sub-program JTRS MBITR is led by the U.S. Special Operations Command. The company Thales is the prime contractor for JTRS MBITR and the product name of their radio is AN/PRC-148 JEM (JTRS Enhanced MBITR) which is the first approved JTRS product. AN/PRC-148 is a handheld software-defined radio that is capable of operating with a various range of modulations and waveforms such as ANDVT, HAVEQUICK I/II, and SINCGARS [2].

JTRS Airborne, Maritime Fixed-Station (JTRS AMF), previously called Cluster 3 and 4

JTRS AMF initially consisted of two programs, the Navy-led Cluster 3 and the Air Force-led Cluster 4. The sub-program JTRS AMF is intended to modernize the communications system in the U. S. military fixed and rotary wing aircraft, ground installations and wide range of U.S. Navy ships [5].

Within the JTRS program, there is also a sub-program called Multifunctional Information Distribution System (MIDS). MIDS aims to develop a software-defined radio that will be the second generation of Link 16 (a high-capacity, jam-resistant, secure data link providing detailed interoperability and situational-awareness tactical information on air, land, surface and subsurface points of interest). The MIDS JTRS terminals will provide a solution for fighter aircraft, command and control centers, and ships [6].

JTRS Handheld, Manpack, Small Form Fit (JTRS HMS), previously called Cluster 5

The U.S. Army-led sub-program JTRS HMS focuses primarily on the small form factor (SFF) radio requirements of future land forces. This radio will not be used only for communications within combat forces; it will also be used for communication with and between sensors like Unattended Ground Sensors (UGS), Unmanned Aerial Vehicles (UAV), Unattended Ground Vehicles (UGV) and Intelligent Munitions.

The sub-programs JTRS GMR and JTRS HMS have entered the government testing phase. During 2010 and 2011, the system will go through a series of tests before being fully approved for use in the field [7].

2. The Swedish Project, GTRS

Sweden has started a JTRS-similar project for future tactical radio communication, named GTRS. From the Swedish perspective, the GTRS project is planned to be the base for the core system for all future radio communication in the Swedish Armed Forces (SwAF). Since the beginning of 2000, there has been a cooperative project between the SwAF and JTRS JPO in San Diego. An important part of this cooperative project is to share knowledge when developing new waveforms. On the hardware side, GTRS cooperates in many of the sub-programs within JTRS in order to follow the development in all the services, land, sea and air. An important intention of this cooperation with the JTRS program and the development of Software-Defined Radios is to ensure flexibility and modularity in the future.

Figure 2. GTRS (From [8])

C. THE PROBLEM

1. Area of Research

The ongoing development for future tactical wireless communications for the Swedish Armed Forces has focused on software-defined radio SDR and networking technologies. Parallel to the development of military systems, there has been a massive development of civilian wireless communications systems. The civilian systems are most often based on some existing infrastructure. These infrastructure-based systems could be an alternative to ad hoc networking systems based on software-defined radios.

This thesis focuses on comparing ad hoc networking systems with modern infrastructure-based systems in order to determine which will be the best technology for future tactical communications systems for the Swedish Armed Forces.

2. Research Questions

Primary question:

– From a Swedish perspective, what are the key success factors for a tactical communications solution that will be used for a land-based battalion?

Subsidiary questions:

– What are the key requirements for a tactical communications system?

– How does ad hoc networking compare to civilian infrastructure-based technologies?

– What recommendations from this study can be provided to the Swedish Armed Forces for developing wireless communications systems beyond the ongoing Software Defined Radio Program (GTRS)?

3. Methodology

The thesis project begins by examining what requirements the Swedish Armed Forces have for their tactical communications systems. In this initial part of the thesis, an analysis of the Swedish Armed Forces is conducted from an operational perspective. A further analysis of the structure for the command and control, together with past problem areas, leads to what the key operational factors/requirements are for future tactical communication systems.

In the next step of the thesis project, research is conducted in the today's technologies for wireless communications, including an investigation into the technology for an ad hoc network, which is the focus area for many of today's military tactical solutions. Parallel to the ad hoc networking technology, assessments are made of the technologies used for civilian wireless communications, such as 3G, 4G and LTE.

As a follow-up step in the thesis project, various technologies are analyzed. The ad hoc networking technologies and the civilian infrastructure-based technologies are compared against the key operational requirements that were found in the discovery portion of the earlier thesis project work. In order to analyze the different technologies, modern simulation software tools are used.

Finally, the results from the analysis of the different technologies are evaluated in order to determine which technology best meets the overall requirements. The results of the thesis project are discussed and summarized in order to make recommendations to the Swedish Armed Forces for future development of tactical communications systems.

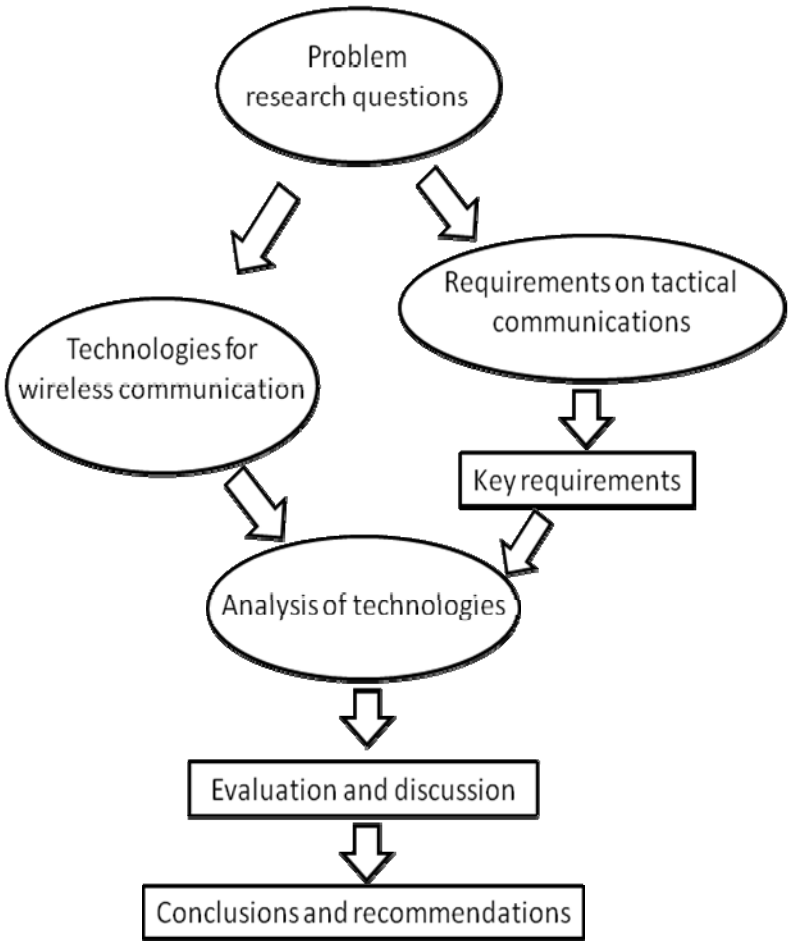

Figure 3. Method

4. Scope

This thesis focuses on studying today's existing and emerging technologies for tactical wireless communications in order to determine which technology will best satisfy requirements for the Swedish Armed Forces participating in future land-based operations.

Concerning the analysis of the Swedish Armed Forces requirements for tactical wireless communication, a study was conducted into relevant national doctrinal, strategic and operational, documents. The documents associated with the requirement for procuring radio equipment for GTRS were analyzed. This initial literature-based analysis provides a solid foundation for the stated purpose of the thesis project. The conclusions

part of the governing document review provides important key factors that are used as variables in the analysis of different technologies in the thesis project.

The thesis is limited to the study of tactical communications system for land-based operations, as this is the focus for ongoing and future international peace support operations where the Swedish Armed Forces participate.

For the analysis of different civilian technologies for wireless communication parallel to the military ad hoc networking, the focus will be on 3G and 4G. This perspective is chosen because these technologies are the most operationally relevant in relation to a time period from now to five to ten years from now. An effort is made to look into future technologies beyond 3G and 4G, but with an understanding that these technologies have not been in use long enough to ensure that the information on these systems is the most relevant. Future technologies like LTE, which is beyond today's operating technologies, are discussed in the evaluation part of the thesis.

In the analysis of technologies, a simulation software tool is used to measure efficiency in the different technologies. For these simulations, the software Joint Communications Simulation System (JCSS) is used. JCSS is based on OPNET, which is recognized as a well-known and accepted tool for planning communication networks. JCSS is an application that is used within the United States Armed Forces.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE SWEDISH ARMED FORCES IN OPERATIONS

A. BACKGROUND

Before 1989 and the fall of the Berlin Wall, Sweden was politically and militarily placed between the two major alliances in the world: the North Atlantic Treaty Organization (NATO) and the Warsaw Pact (WP). Sweden declared itself as a neutral country and chose not to be a member of either of these alliances. The focus in Sweden's military strategy was homeland defense. In order to maintain good communications with other countries, Sweden has always placed great value in the work of the United Nations. As a member of the United Nations, Sweden has tried to work for peace and democracy building. In the time period between World War II and up until 1989, Sweden, in the framework of the United Nations, participated in some international operations (i.e., in Africa and on Cyprus), but Sweden's main focus remained on homeland defense. This neutral status created an environment where Sweden became isolated from the rest of the world. Sweden could, of course, follow other countries' developments in tactics, doctrines and technology, but it was important for Sweden to have self-sustainability. All military equipment developed for the Swedish Armed Forces should also be used extensively domestically, and, therefore, little effort was put into interoperability requirements with other nations' armed forces. A positive spillover effect of dual-use technology, as described, was that it created a strong domestic defense industry with several companies, including BOFORS, SAAB, HÄGGLUNDS and ERICSSON, which have been, and still are, of great importance for the Swedish economy and employment.

After 1989 and with the fall of the Berlin Wall, along with the dissipation of the Warsaw Pact, a big change took place in the Swedish defense and security policy. A direct threat to Sweden is no longer imminent, and the focus is now on participating in international peace support operations (PSOs). Since 1994, Sweden has become a participating member of the European Union (EU). Within the EU, there is a range of common defense and security policies that Sweden, among the other member nations, is highly involved in. In the framework of the EU, the membership nations contribute military resources in order to form tools of strength supporting the common defense and

security policy of all member nations. One step in this direction is to form independent Battle Groups that can be deployed rapidly in different conflicts. In this modern era and in the view of the described Battle Groups, it has become important for the Swedish Armed Forces to have interoperability with the armed forces of other nations. This is not a unique concern for Sweden; many other countries have also followed the same path and developed their military concepts to be used mainly for homeland defense. In fact, the fall of the Berlin Wall and the dissipation of the Warsaw Pact not only made significant and observable geographical and political changes, it also constituted paradigm shift for how to use military forces in many European countries in support of national objectives.

B. MILITARY STRATEGIC OBJECTIVES

According to national defense doctrines, the most important goal for the Swedish Armed Forces is to maintain the ability to conduct armed combat. The overall goal for the Swedish Armed Forces is to see that Sweden, alone or in cooperation with others, can protect its basic foundation and its national interests. By preventing and managing conflicts and war, Sweden can ensure its sovereignty and protect its society and functionality.

The primary tasks for the Swedish Armed Forces are:

1. Protect Sweden and ensure our security, by conducting operations on Swedish territory and in the vicinity of Sweden, but also outside Sweden through Peace Support Operations.
2. Detect and reject violations of the Swedish territory in accordance with International Law.
3. Support the Swedish society with military resources, when needed.

Even if the change in the Swedish defense and security policy has made the Swedish Armed Forces more involved in international operations, the ability for building and sustaining homeland defense will always be an essential objective. The decreased direct threat against Sweden—the outcome after 1989—could rapidly change. All sovereign countries need the ability to defend itself at all times. Certain areas around Sweden will always be of special interest. The Baltic Sea is surrounded by many

countries and Sweden is one of them. Resources for energy and transportation are some of the important social and economic activities that have to be coordinated between all involved countries. There is always a risk of tensions between countries in the Baltic Sea area, and Swedish Armed Forces may be involved [9].

In order to defend Swedish territory, the Swedish Armed Forces needs to freely conduct land-based operations. On the tactical level for land-based operations, forces conduct all required operations within the framework of unit size—typically a brigade. The core units in this tactical land-based force will consist of high mobility armored units. Additional units for combat support and combat service support will migrate this brigade unit to a land-based tactical battle group. The tactical land-based force must be able to conduct operations in all parts of Sweden, which varies from flat agricultural terrain to hilly forests and urban terrain. In this diverse scenario, the tactical commander needs a reliable and sufficient communications system. The basic requirements for such tactical communications system are to provide transmission of voice, data and video.

The third primary task for the Swedish Armed Forces is to support society when needed. Under normal circumstances, the Swedish society is self-sustainable. Authorities such as the police, customs and coast guard have responsibilities to ensure that people follow the law, and that the borders are secured under normal, everyday conditions. The fire department is responsible for helping people in case of fire, flooding, accidents or other emergencies. Several additional authorities cooperate in order to maintain the functionality of the society, ensuring health and protection for all.

In some cases, the Swedish Armed Forces may be needed to support society. There can be particular accidents in which the regular authorities do not have the right assets to handle the situation. There can also be situations when the regular authorities simply do not have enough resources. In these cases, the Swedish Armed Forces can be called upon to support society. Also in these cases when supporting society, there are needs for tactical communications in order to command, control and coordinate the military units that participate. There is also a need for military units to communicate on the tactical level with units from the police, customs, coast guard and the fire department.

C. SWEDEN AND THE EUROPEAN UNION

Sweden became a member of the European Union in 1994, after which the European Security and Defense Policy became an important part of Sweden's own security policy and the development of the Swedish Armed Forces. In the European Security Strategy, the importance of cooperation is emphasized. A threat in the form of a large-scale aggression towards any of the members is not very likely, but there are other persuasive threats that the Union members are facing.

The emerging terrorism, which utilizes the openness in Swedish society, has become a threat. States within the European Union have become terrorism targets as well as a base for conducting terrorist acts that may have consequence elsewhere. Organized crime is a problem that the states in Europe have to deal with on an everyday basis. Drugs, trafficking, weapons and illegal immigrants are examples of security problems that are of great concern within the EU. Organized crime affects Europe internally because Europe has proven to be an easy target. Organized crime is also an external issue, and it is most often connected to states far from Europe. There could also be links between organized crime and terrorism. Another major threat is the proliferation of weapons of mass destruction. Biological science, together with the knowledge of how to use missiles, are potential tools against a perceived adversary in Europe. Regional conflicts and state failure are problems that can impact the European Union, directly or indirectly. State failure is often caused by internal problems such as bad governance and corruption. Problems described earlier as terrorism and organized crime can also be related to state failure, since these states can act as bases for organized crime as well as for terrorism. Countries such as Somalia, Liberia and Afghanistan are examples of states that have failed [9].

The strategy that the European Union has chosen to deal with these new threats is to be able to act before a crisis has started. The key elements in this approach are:

- More active
- More capable
- More coherent
- Working with partners

In order to achieve these key element objectives, certain strategies were agreed upon. The European Union should be active in working for peace and security globally, and should support the United Nations when it responds to threats to international peace. A joint effort to an upcoming crisis must be initiated before the problem becomes too severe. The military capabilities within the union have to be more flexible, mobile and able to be rapidly deployed. Efficiency can be accomplished if assets are pooled and shared, and the duplication of capabilities is avoided. A coherency in the response to a problem is best achieved by coordinating all the efforts, not only the military. In a comprehensive approach for building security, the European Union should coordinate diplomatic efforts, development, trade and environmental policies with military efforts. The last, but not least, key element is to work together with all other participating partners. A crisis or a problem can seldom be solved by one country alone. Cooperation with other states and organizations is essential. As previously mentioned, the connection between the European Union and the United Nations will most likely continue to be the baseline in future EU actions. Other relations, however, are also important. One relationship is emphasized and especially mentioned in the European Security Strategy.

> The transatlantic relationship is irreplaceable. Acting together, the European Union and the United States can be formidable force for the good world. Our aim should be an effective and balanced partnership with the USA. [10]

D. PEACE SUPPORT OPERATIONS

In accordance with the primary tasks for the Swedish Armed Forces, one of the most important is to ensure Sweden's security by conducting relevant military operations. The Swedish Armed Forces is required to have the ability to conduct operations not only on Swedish territory and in the vicinity of Sweden, but also internationally by Peace Support Operations.

Sweden's participation in international peace support operations (PSOs) increased during the 1990s. The major reason for this turn in Sweden's defense and security policy was a combination of the changes in Europe after the fall of the Berlin Wall and with Sweden's membership in the European Union. During the conflict in Bosnia from 1993

to 1995, Sweden participated with one armored battalion in UNPROFOR, led by the United Nations. The operation in Bosnia was followed by another PSO action on the Balkans, the KFOR operation in Kosovo. Both of those operations required high standards of tactical communications support. UNPROFOR and KFOR operations needed to be conducted over extensive geographic areas. The hilly terrain on the Balkans decreases the coverage for radio communication.

Since the beginning of 2001, Sweden has participated in the International Security and Assistance Force (ISAF) in Afghanistan. In early 2001, ISAF was led by a coalition of a number of European countries, and the force was mandated to conduct operations only in and near Kabul. Today, ISAF is led by NATO and operates in all of Afghanistan. Since 2006, Sweden has been responsible for a Provincial Reconstruction Team (PRT) in Mazar-e-Sharif in the northern part of Afghanistan. The present Swedish force in Afghanistan is of battalion size, with three infantry companies together with combat support and units for logistics and communications. The tactical requirements in Afghanistan are similar to those experienced previously on the Balkans. The Swedish force has to cover large areas, and the ranges for radio communication decrease because of the hilly terrain.

Sweden has also participated in peace support operations mandated and directed by the European Union. The operations on the Balkans, in Bosnia and in Kosovo, transformed from NATO-operations to EU-operations. The European Union has also conducted peace support operations in Africa. The most recent EU-operation Sweden participated in was EUFOR in Chad and in the Central African Republic.

According to established planning directions for the Swedish Armed Forces, Sweden must have the ability to deploy 2,000 troops simultaneously, distributed over four operational areas. At least one of these four operations must be of battalion size [9]. In the Headline Goal 2010 for the European Union, the ability to react fast to dynamic security challenges is emphasized. Using troop contributions from all member states, the EU must be able to deploy up to 60,000 troops within 60 days for engagement in major operation. Two major, simultaneous peace-building operations should possible, supported

by 10,000 troops. An additional capability is required for use in evacuation operations and rapid response situations where a battle group of about 3,000 troops is required [11].

Periodically, the Swedish Armed Forces is required to organize a Battle Group in the framework of the European Union. The first battle group that Sweden was responsible for was organized in 2008. It became a combined and joint force consisting of units from several neighboring countries and was named the Nordic Battle Group 2008 (NBG 08). In 2011, Sweden was once again responsible for organizing a similar battle group (NBG 11).

The tactical communication system used for forces deployed in international peace support operations must have high mobility and must be able to operate globally wherever needed. Communications are also required to operate in a wide range of climates. In some cases, when operating in Africa for example, the climate can be hot and with high humidity. When operating in the framework of NATO or EU, there is also a requirement for interoperability of communications among the many diverse players.

E. COMMAND AND CONTROL

1. General Principles for Command and Control

The system for command and control within the Swedish Armed Forces is based on basic principles. One of the most vital principles is that the overall strategic goal shall influence all levels of operations. Operational art is defined as the link between the military strategic goals and the tactical actions taken on the battlefield [12]. This fundamental principle comes basically from the military theorist Carl von Clausewitz and from his well-known book, “On War.” Clausewitz emphasizes that the use of military force should not be an isolated action. Using military force should be considered an extension of a nation’s political will and should be related to political goals [13]. This important factor leads to transparency in the military system and between levels within the operational hierarchy.

On the operational level, the dominant principle is *maneuver warfare*. In maneuver warfare, the goal is to affect your adversary’s mental desire to continue the fight. In other terms, the goal is to make your opponents surrender their will to fight.

When conducting this type of warfare, your own force tries to move so that it can get a favorable position towards your opponent [14]. Offensive actions against your opponent are aimed at his vulnerabilities. The term *maneuver warfare* should not be seen in only the direct operational context. It is more of a mindset that should influence all planning and actions taken within your tactical force. Key elements in maneuver warfare are:

- Initiative
- Tempo
- Mission type tactics or directive control

To take and maintain the initiative in operations, is important to be one step ahead of your adversary. Having the initiative, you can control what is going to happen on the battlefield. Your opponent will be forced to act defensively and follow your actions in order to protect himself.

Operations tempo is another important factor in maneuver warfare. In order to be one step ahead of your opponent, you need to have a high operational tempo. Working together, both initiative and tempo are related to the OODA-loop, which was founded by the United States Air Force Colonel John Boyd [15]. The essence in the OODA-loop is to maintain initiative and tempo so that your decision cycle (Kill-Chain) is faster than that of your opponent.

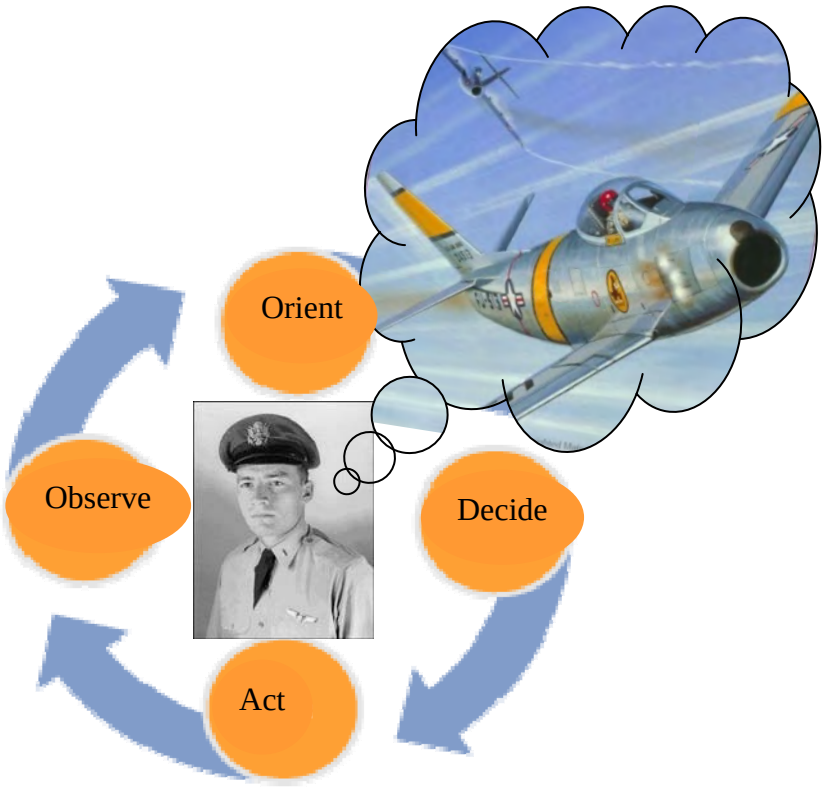

Figure 4. OODA-loop (From [16])

When acting against an adversary, the commander will try to disrupt and create confusion in the opponent's decision cycle in order to make the adversary lose initiative and slow down his tempo. In other words, disrupt your adversary's OODA-loop [17].

The third key element for maneuver warfare is mission-type tactics or directive control. This element considers the technique of how to command the sub-units within the force. The bottom line in mission-type tactics or directive control is to give your subordinated commanders the ability to make decisions on their level. When the commander is tasking his units, he will present and distribute the overall goal and the purpose for the operation, the so-called Commanders Intent. The orders to his subordinated commanders will be expressed as of what should be achieved and not how it should be done. Ideally, these expectations are formulated as minimum objectives (i.e., threshold requirements), as opposed to ideal or optimal goals. The opposite of this "directed order" principle is command guidance. Using command guidance, the commander gives orders with a high degree of detail, specifics and limitations. The

subordinated commanders will have very little room for creativity when conducting such an operation. There is a risk that command guidance in general will significantly slow the decision cycle. Giving your subordinated commanders too many restrictions and limitations will make them unable to take the initiative, and the whole operation will be slow and predictable. There are situations where command guidance is preferable, but the general principle used within the Swedish Armed Forces is still mission-type tactics or directive control.

2. Command and Control Structures and Processes

Since the 1990s, the Swedish Armed Forces has transformed, step by step, the structure for the operational command. Today's structure for the Swedish Joint Forces Command follows the same principles as an operational command in NATO or in EU. It was a natural step after the fall of the Berlin Wall in 1989, and further on when Sweden became a member of the European Union. The operational command for the Swedish Armed Forces is organized in a regular NATO joint structure. The joint operational command consists of the various J's, together with the component commands for the services, land, maritime and air (see Figure 5).

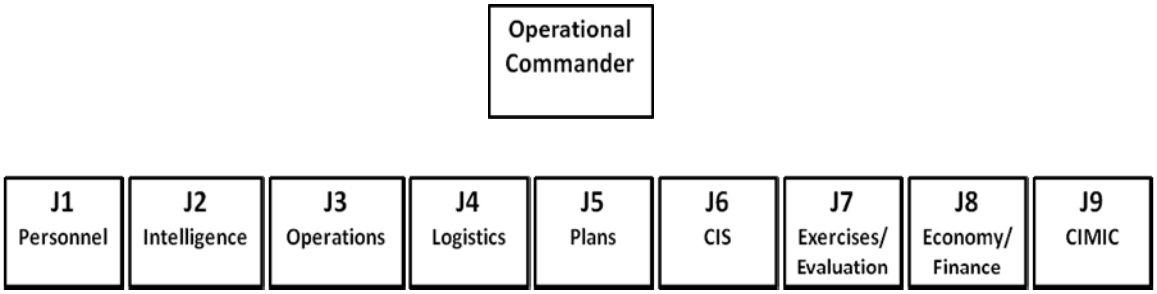

Figure 5. Joint Forces Command

The command structure on the tactical force level for land-based units is also organized in accordance to NATO. The functions are represented in an S-structure (see Figure 6).

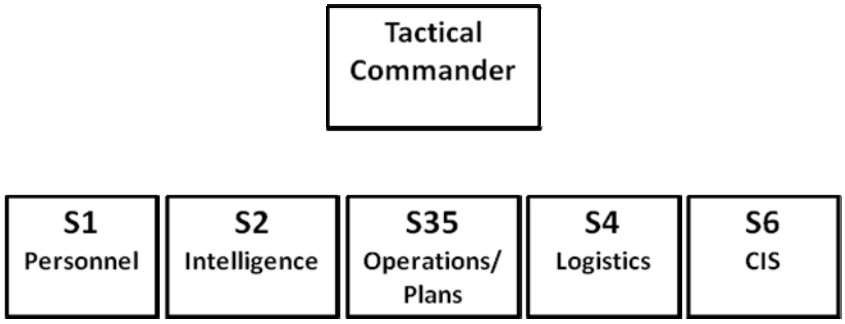

Figure 6. Tactical Force Headquarters

The term *interoperability* is not limited to the technical perspective. In order to cooperate with other nations, terminology and methods in planning are also important. For operational planning, the NATO Operational Planning Procedure (OPP) is used where the main joint publication is called Guidance for Operational Planning (GOP). The main idea of using the OPP and GOP is to have a comprehensive approach when planning the operation, which will ensure that the strategic goals are thoroughly considered throughout the plan. The actions on a tactical level are initiated from the strategic/operational level. When the operational plan is started, an ongoing process coordinates all tactical operations so that they meet the overall strategic goals. Typical planning methods used on the tactical level follow the principles for OPP/GOP, but are more simplified in order to satisfy the need for tempo in operations.

F. REQUIREMENTS ON RADIO COMMUNICATION

To identify the key factors for a tactical wireless communication system for the Swedish Armed Forces, it is essential to analyze relevant updated documents used for present radio communication systems. For this analysis, a study was made of the tactical and technical specifications documents for the Swedish software-defined radio system GTRS [18], [19]. These documents are relevant to identify generic key needs for an optimal, tactical communications system.

1. Tactical Requirements

In the GTRS specification document, the ability for the tactical force to maintain flexibility and mobility is emphasized. The tactical communication system must adapt to the speed and maneuverability in operations that any tactical force requires. Operations can be carried out on Swedish territory, in the vicinity of Sweden or through an International Peace Support Operation (PSO) outside of Sweden. In terms of international PSOs, the tactical communications system must support the doctrine for the European Union (EU) guidelines for crisis management. A tactical land-based force has to be able to conduct operations wherever needed, and the tactical communications system that supports the force is required to operate in all climate zones, from tropical to sub-arctic. A wireless tactical system also has to provide a near real-time communication capability.

Sweden has a general Network Centric Warfare (NCW) approach when developing communication systems within the Swedish Armed Force. The GTRS-system will bring the NCW approach to the tactical level. The software defined radios within the GTRS project are evolutionary based and must be readily upgradable to new versions and technologies.

The tactical communications system shall cover an area of 1,500 km^2 with a range up to 10 km between the nodes. If needed, the tactical force shall be able to divide itself into sub-units; in this case, the entire tactical communications system must extend its coverage to an area of 3,000 km^2 with a maximum range up to 100 km between the subunits. For a tactical force of battalion size, the area that is required to be covered will be up to 500 km^2 [18], [19].

2. Communications Requirements

The GTRS system has to provide communications for voice, data, text, pictures, video, and video conference. The hardware in the tactical communications system should be flexible to the authorized and allocated frequency spectrum used in order to adapt to the frequencies that will be allowed in the actual operation. When communications are designed for self-configured networking, the network should be able to contain up to 280 nodes. For a battalion, the numbers of nodes required are 140.

The waveform development shall be based on the Software Communications Architecture (SCA). The data communications shall support TCP/IP/Ethernet standard and shall be able to use both IPv4 and IPv6 data formats. The data rate between nodes in a network shall be adaptable, but the minimum requirement for data rate between any two nodes is 1 Mbps.

3. Security

The tactical communications system has to be able to operate in environments where the adversary uses electronic attack (EA). The communications system, therefore, needs to be resistant to hostile jamming. The system also needs to be resistant and endure through hostile environments due to high-power microwave weapons (HPM) and to electromagnetic pulse (EMP).

In terms of information security, the tactical communications system shall allow secure communication up to the level of SECRET.

4. Interoperability

The main purpose for GTRS interoperability is the ability to communicate with participating forces from other nations in international peace support operations. The tactical communications system has to be adapted to international standards and be interoperable to NATO and EU. For interoperability to NATO, the tactical communications system should be adapted to NATO STANAG.

According to standards for data communication, the software development shall be based on Software Communications Architecture (SCA) and support the protocols Transmission Control Protocol (TCP) and Internet Protocol (IP).

For domestic interoperability, the tactical communications system shall be able to communicate with systems used by units from Swedish civilian authorities, police, customs, coast guard and the fire department.

G. PAST PROBLEM AREAS

The predecessors of radio communications systems that have been used before our software-defined radios has served the Swedish Armed Forces well, but previous systems have operational, design, and interfacing limitations that must be overcome when the Swedish Armed Forces face future operations.

The limited bandwidth that older systems have offered is one factor of concern for the commander's need in a modern operational environment. Both the tactical commander and his subordinated commanders need a great deal of information, which requires a high throughput in the communication systems. The lack of ability to upgrade and improve the system performance is another problem area connected with older systems. In older hardware intensive radios, the performance of the radio was hard-coded in the equipment. Older radios gave little room to modify modulation, spread spectrum techniques, encryption or other elements associated with the waveform. Another problem area associated with older radio systems is the lack of compatibility and interoperability. When developing the core radio system that we use today, there was little concern over the ability to communicate with others units outside the force. The radio system was specified to be used for the Swedish Armed Forces, applied mainly for homeland defense. The interoperability track record with other nations' systems has proven to be limited when Sweden has participated in international peace support operations. This has to change in future designs.

H. CONCLUSIONS

After the analysis of the military context for future tactical wireless communications, the following key needs are recognized:

A future tactical wireless communications system must support the commander's needs for commanding and controlling his/her force. According to the principles that Sweden applies for command and control requirements, a tactical communications system with sufficient capacity for voice, text, data, pictures and video is needed. This need of information is not only for the commander's concern, it is also a concern for the subordinated commanders when they all need to share the same information base in a

joint common operational picture. A future tactical communications system must also satisfy the need for flexibility. The operations tempo is essential in maneuver warfare, and tactical communications systems have to be adaptable enough to the required force movements expected in the battlefield. A key word for today's operations is *cooperation*. In order to cooperate with other services, or other nations, Sweden needs to have interoperability with working partners

The following statements summarize the basis for technical requirements for a Swedish Armed Forces tactical communication system:

- Sustained operational capability (even during jamming, HPM and EMP)
- Ability to connect up to 280 nodes (for a battalion 140 nodes)
- Provide a minimum data rate at 1 Mbps
- Upward compatible with new /emerging technology
- Adaptable/flexible
  – Applications
  – Environment
  – Existing/available resources

When analyzing the Swedish defense and security policy and the military context concerning when and how to use the Swedish Armed Forces, the conclusion is that the most likely operational scenario is for international peace support operations. Sweden's membership within the European Union, together with the low probability of direct threats against Sweden, makes the focus for the Swedish Armed Forces requirement to be at international peace support operations (PSO). The modeling further on in this thesis will therefore be based on a PSO operational scenario.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TECHNOLOGIES FOR WIRELESS COMMUNICATIONS SYSTEMS

A. WAVEFORMS FOR SOFTWARE DEFINED RADIOS

This chapter presents more detail into various technologies available for wireless communications. In a software-defined radio, it is the waveform design that ultimately controls the performance of the communication system. The following analysis will therefore focus on the waveforms developed within the JTRS and GTRS projects previously mentioned.

1. JTRS Waveforms

JTRS SINCGARS

JTRS SINCGARS is one of the first waveforms developed especially for JTRS. SINCGARS stands for Single Radio Channel Ground-Air System and this waveform is similar to the Wideband Networking Waveform based on the Software Communications Architecture (SCA) 2.2. The JTRS SINCGARS is a high-profile waveform that serves as the baseline in JTRS Ground Mobile Radio (GMR). The waveform is modular, where most of the processing is performed in general processors, and it provides a variety of modes of operation. JTRS SINCGARS is based on Internet Protocol (IP) technology communication infrastructure, which means that it uses common protocols for routing and interoperable to other IP networks using commercial routers. The JTRS SINCGARS waveform uses both frequency modulation (FM) and continuous phase frequency shift keying (CPFSK), whereas the operating mode Single Channel Plain Text (SCPT) uses FM and all the other modes uses CPFSK. The minimum data rate in JTRS SINCGARS is 16kbps. The spread spectrum technique used in the waveform is Frequency Hopping Spread Spectrum (FHSS), but it can also operate in fixed frequency mode. The frequency-hopping mode operates in the frequency range of 30–88MHz and uses 2,320 possible frequencies [20]. The predecessor to JTRS SINCGARS is the regular SINCGARS waveform, which has been widely used since the 1980s in the U.S. Armed Forces.

Wideband Networking Waveform (WNW)

One of the first and primary waveforms developed for the JTRS GMR sub-program is called Wideband Networking Waveform (WNW). This waveform is based on IP-technology and designed to be used in tactical ad hoc networking systems [21]. WNW is a digital waveform that uses high data rate Coded Orthogonal Frequency Division Multiplexing (COFDM). The range for the WNW data transmission rate is from 47 kbps to 12.1 Mbps. WNW is based on the Software Communications Architecture and a state-of the art digital communication technique. WNW uses Differential Phase Shift Keying (DPSK) and Quadrature Phase Shift Keying (QPSK) modulation and encoding designs. As forward error correction, WNW employs Reed-Solomon and Turbo-code. COFDM provides a waveform that is bandwidth efficient and helps to suppress distortion caused by multipath, and also provides resistance against narrowband interference and impulsive noise [20]. Initially in the development of WNW, the standard data format IPv4 was used. For adaptation to future standards and increased demands on IP addressing, WNW will also be capable for IPv6 data format. In order to ensure secure networking, WNW uses High Assurance Internet Protocol Encryption (HAIPE). In JTRS networking architecture, packets will be transmitted in encrypted format between different radio frequency subnets. HAIPE will provide the required routing to reliably and efficiently manage different levels of security when nodes communicate in the network [22].

Soldier Radio Waveform

JTRS Handheld, Manpack, Small Form Fit (HMS) uses a waveform called Soldier Radio Waveform (SRW), which will operate in the frequency bands from 450MHz to 1,000MHz or 350MHz to 2,700MHz. The objective for the Soldier Radio Waveform is to provide network communication between a large numbers of distributed nodes. The typical situation is communication between soldiers in a platoon. Recent tests have shown very promising results, where up to 36 radios have been able to communicate with each other during field conditions. The testing was in a mixed type of terrain with both forests and mountains in the communications environment, but some tests were also done in terrain with small city structures [23]. The Soldier Radio Waveform is described

as a self-healing network because, when nodes lose communication with each other caused by the terrain, they try to re-establish connectivity by leveraging all other available nodes. The SRW, similar to many cellular mobile phone systems, uses code division multiple access (CDMA) as the modulation scheme in order to get efficient communication between nodes. CDMA allows many soldiers to use the radios simultaneously, because each soldier is identified with a unique IP address. The data rate for the SRW is designed to be in the range between 450 kbps and 1.2 Mbps. There is also a "stealth" mode with a data rate between 2 kbps and 23.4 kbps, which is being developed to be difficult to reliably intercept.

A radio system with SRW can be used to establish small ad hoc mobile wireless networks. Using separate frequencies allows a tactical communications subscriber to use one frequency for communications within the network and another frequency for the command and control of the unit. Other applications for this small version of JTRS are for Blue Force Tracking and Combat ID [24].

2. GTRS Waveforms

TETRA

Terrestrial Trunked Radio (TETRA) is the first waveform developed for GTRS. The technology in TETRA was used for several years as the basic communication standard within civilian emergency units, fire department and the police. In the early start for waveform development in GTRS, a software version of TETRA was chosen as the initial demonstrator. The initial design scope was to develop and implement a TETRA Mobile Station Waveform that will comply with Software Communications Architecture (SCA). TETRA is a digital mobile radio standard developed by the European Telecommunications Standard Institute (ETSI) that uses Time Division Multiple Access (TDMA). In early versions of TETRA, the data rate followed the NATO STANAG and was fairly low at 2,400 bits-per-second (bps). TETRA has developed an adaptive function that provides a variation of data rate from 15.6 kbps to 538 kbps [25] (see Figure 7).

Packet Data Throughput (Downlink kbits/s)

Modulation \ Channel Type	25 kHz	50 kHz	100 kHz	150 kHz
π/4 DQPSK	15.6			
π/8 D8PSK	24.3			
4-QAM	11	27	58	90
16-QAM	22	54	116	179
64-QAM	33	80	175	269
64-QAM	44	107	233	359
64-QAM	66	160	349	538

Note: All channels are 4 slots

Figure 7. Packet data throughput in TETRA (From [25])

TDRS

A waveform called Tactical Data Radio System (TDRS) was developed as a key wideband networking waveform for the GTRS project. TDRS is specified to satisfy the requirements for battalion-sized tactical force. The waveform is based on SCA and will have ad hoc networking capabilities [19]. TDRS waveform is similar to another waveform called FlexNet developed by Rockwell Collins. FlexNet is an IP/Ethernet based waveform and has a standard OSI layered protocol architecture [26]. The frequency range is 2 to 2,000 MHz, and the possible throughput according to the manufacturer is up to 5 Mbps. During field conditions and when several nodes have to share bandwidth, a more realistic level for the throughput will decrease to approximately 1 Mbps. The FlexNet waveform will be flexible and highly configurable, and specified to connect up to 150 nodes.

B. MOBILE AD HOC NETWORKS

1. MANET and CBMANET

The main idea in a Mobile Ad hoc Network (MANET) is that all subscribers act as equal nodes within the system and are able to move freely and independently from each other. The nodes should be able to connect and disconnect with each other while the network adapts to the nodes' need for mobility. The origin for Mobile Ad hoc Networks was a DARPA project called Packet Radio Network (PRNet), which started in the beginning of the 1970s. PRNet was driven by what was, at that time, the newly invented packet switching technology. Since the start of PRNet, considerable development in technologies for coding, modulation and routing have been accomplished for wireless ad hoc networking. In 1997, a collaborative and coordinating group called MANET was formed within IETF to develop specifications and standards for ad hoc wireless networking [27].

Management in an ad hoc wireless network is decentralized, and the communication between nodes is peer-to-peer. The nodes have to autonomously configure and reconfigure the network topology by communicating with each other. Since the nodes will change in numbers, locations and capability, the network topology, which is continuously routing packets, will become complex. In a pure MANET there is not any exterior infrastructure in the form of base stations and towers with antennas. Instead of fixed infrastructure, a MANET relies on sophisticated hardware and software that will be required in every node [28].

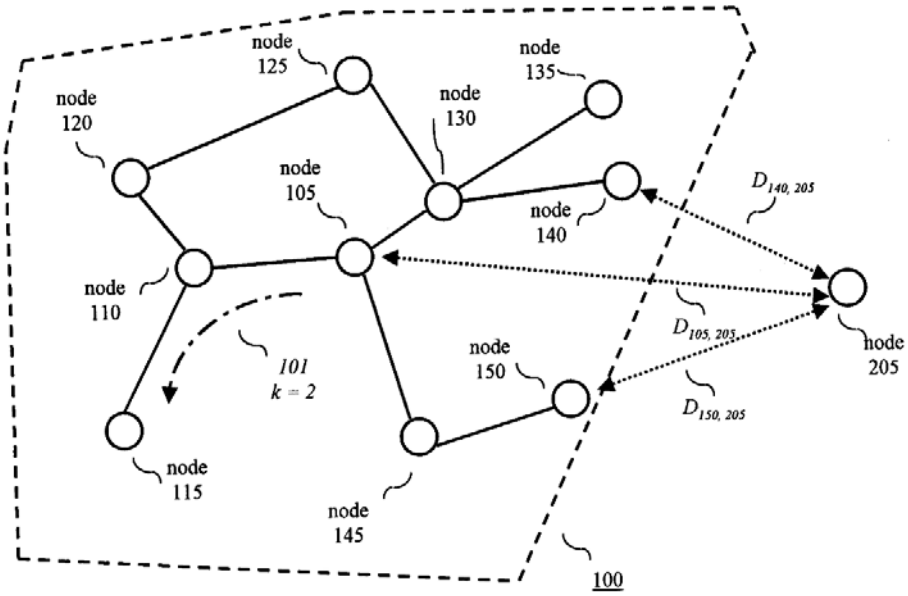

Figure 8. Mobile ad hoc network (From [29])

The basic idea that ad hoc networking provides adaptability and flexibility seems to be a perfect fit for a tactical communications solution, although some issues are inherent to this type of networking. Some of the problem areas addressed for MANETs are connectivity, bandwidth, resources, scalability and security [28]. The connectivity using wireless communication will always be affected by noise and the environment through which the signal has to propagate. In the case for MANETs in a land-based scenario, the links between nodes will be even more vulnerable because of limited antenna heights. Limitations in bandwidth will always be a reality for any wireless system in comparison to wired systems. For MANETs in general, factors such as multipath and fading decrease the available bandwidth. An increased need of an information flow in forms of routing between all nodes will also affect the available bandwidth. Limitations in resources are another problem area in a MANET. All nodes in a MANET require high storage capacity because there is no base station in the system to act as a centralized server and backup. In order to cover a large area in a battlefield, a MANET is also required to be highly scalable with the potential to respond to increased demand. When connecting the large amount of nodes required, it will again cause an additional need for routing information. The last problem area that should be emphasized

for MANETs is security. In general, there is an increased security concern for MANETs. Since nodes are continuously going in and out in the system, there is a risk for unauthorized access into the network. In a MANET where the networking is decentralized, this problem is even larger compared to a common wireless system where access control is centralized.

As addressed earlier, many variables in ad hoc networking have to be communicated between the nodes in order to control and manage a MANET. This need of information flow will require, at a minimum, some bandwidth that will interfere with useful tactical information. In a more severe sense, there is a risk that nodes cannot be reached because important routing information has not been established. In order to make improvements in MANETs, a new DARPA project was formed, called Control Based Mobile Ad hoc Network (CBMANET). Research in the CBMANET project aims to develop a new protocol stack that will be more efficient in ad hoc networking. A more sufficient protocol stack will make MANET more reliable and bandwidth efficient [30].

Various transmission technologies with different coding, modulation and spread spectrum techniques can and have been used for ad hoc networking. The well-known IEEE-standard 802.11 in different forms can be used, as well as WiMAX (802.16). For military use within the JTRS project, the Wideband Networking Waveform (WNW) is developed to be used for ad hoc networking [22]. OFDM modulation was chosen for WNW in order to satisfy the requirement for large throughput in a tactical communication system. The Soldier Radio Waveform (SRW) is also developed to be used for ad hoc networking. WNW is adapted to be used for larger Software Defined Radio (SDR) applications in vehicles, compared to the SRW that is adapted for use in smaller SDR applications on a lower tactical level—for example, within a platoon or as communications between networking sensors.

C. INFRASTRUCTURE-BASED SYSTEMS

1. 3G

The technology for digital cellular mobile phone systems used in Sweden started with Global System for Global Communications (GSM) in 1990s, and was defined as the

second generation (2G) of mobile phone systems. During this initial phase for digital mobile communication, the major focus was on voice communication. The GSM-technology was based on time division multiple access (TDMA) where the subscribers, when communicating in the system, had access to a dedicated timeslot in the TDMA frame. The data rate that could be provided for each channel with TDMA was between 9.6 kb/s to 14.4 kb/s [1]. The highly increasing need of dataflow for users demanding data and video capabilities made the GSM technology insufficient. Improvements to more efficiently manage the bandwidth between channels were accomplished through Enhanced Data Rates for GSM Evolution (EDGE). In some literature and articles, these improvements were called the “2.5G” of cellular mobile communications systems [31]. Still, the GSM-technology approach has its limitations when it comes to data communication.

For the third generation (3G) of mobile communications systems, Sweden chose the technology called Universal Mobile Telecommunications Systems (UMTS), beginning in 2003. Instead of the modulation technique TDMA used in GSM, the modulation technology in UMTS is based on Code Division Multiple Access (CDMA). An overall benefit with CDMA is that you can have several subscribers using the same channel; in a bandwidth perspective, this will be more efficient. In CDMA, the data input signal is modulated with a coded signal called a Pseudo Noise (PN) sequence that has a high data rate.

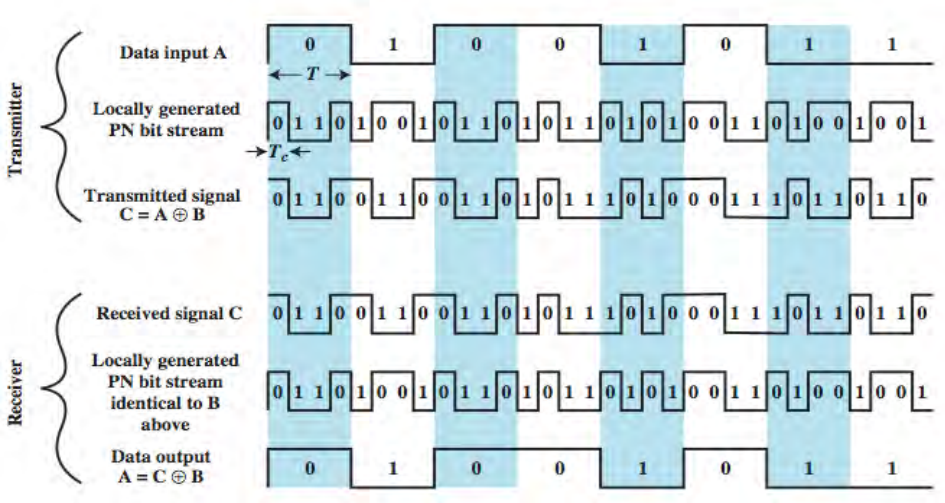

Figure 9. CDMA/PN-sequence (From [32])

The result will be an output signal with a unique code that is spread over a certain bandwidth. This spreading technique, combined with CDMA, is called Direct Sequence Spread Spectrum (DSSS) and offers some distinct advantages. The unique PN sequence provides privacy and prevents unauthorized actors from intercepting the information because only the authorized users who know the correct code will have access. Another advantage is frequency diversity. When the signal is spread over a larger bandwidth, it becomes less affected by noise and selective fading, which is typically narrowband. This characteristic also makes CDMA/DSSS more resistant against multipath, which is ever increasing in modern cell-phone environments. A CDMA/DSSS system is more adaptive in the relationship between the number of subscribers and the quality of service in the transmission. When the number of subscribers increases in a CDMA/DSSS system, the errors and the level of noise in the transmission will gradually increase. In a FDMA or a TDMA system, this relationship is fixed to the number of subscribers [1], [33].

There are also some disadvantages using CDMA/DSSS. If the subscribers are not synchronized precisely, the spreading sequence will not be perfectly orthogonal, which can create self-jamming in the system. The lack of orthogonality in the received spreading sequence can also create problems when receiving both weak signals from far away and, at the same time, strong signals from nearby [1], [33]. To overcome this

problem, it is important to use techniques to control the power in CDMA/DSSS systems. The base station continuously measures the signal strength of each subscriber and sends power change commands [33].

3G using UMTS has taken a big step to provide mobile use of IP. The previous 2G technology used circuit switching; however, when going into 3G-technology, this has transformed to packet switching, which is common standard on the Internet. A mobile UMTS subscriber can, with a modern Smartphone, have access to the same features, such as e-mail and Internet surfing, which are used when connected to a Local Area Network (LAN) with Internet access. UMTS can provide a data rate from 128 kb/s up to 2 Mb/s. The available data rate will be highly dependent on the quality of the connection. When users are moving, the quality of the connection will vary. Even if the 3G has provided a much higher data rate compared to 2G, there is still a big difference when comparing to the data rates that can be achieved in wired and wireless LANs [31].

A 3G cellular network will be based on an infrastructure where base stations will be deployed to cover a certain area. The structure of this network will be in the form of hexagons that can be clustered together to make it scalable and modular. The number of base stations that will be required for an area depends on environmental conditions and the number of subscribers to be served. Figure 10 shows the principles for how a cellular network can be built up.

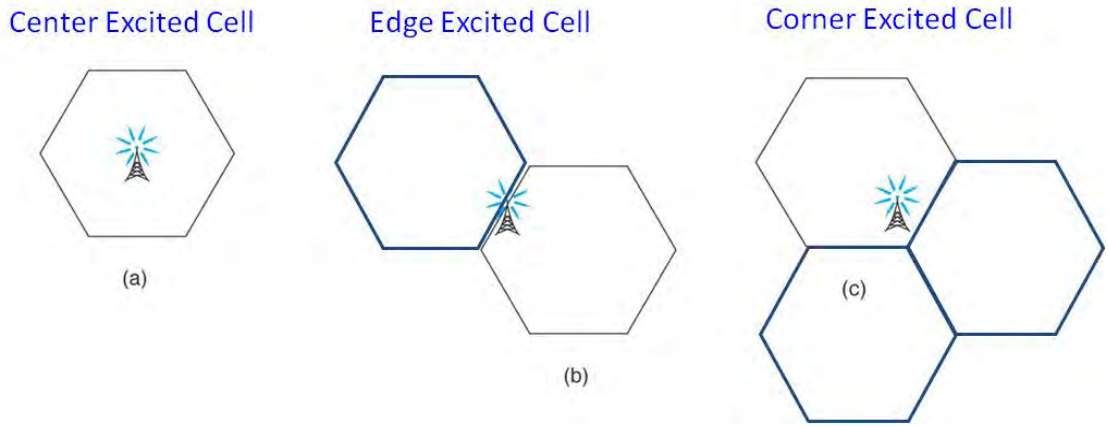

Figure 10. Structures for cellular networks (From [32])

The Ericsson telecommunications company has manufactured a 3G system named QuicLINK. This system is highly mobile and has been developed to be used in areas with limited infrastructure. QuicLINK is based on regular 3G technology and uses WCDMA modulation. The base stations in QuicLINK are small and modular in order to fit in various types of platforms.

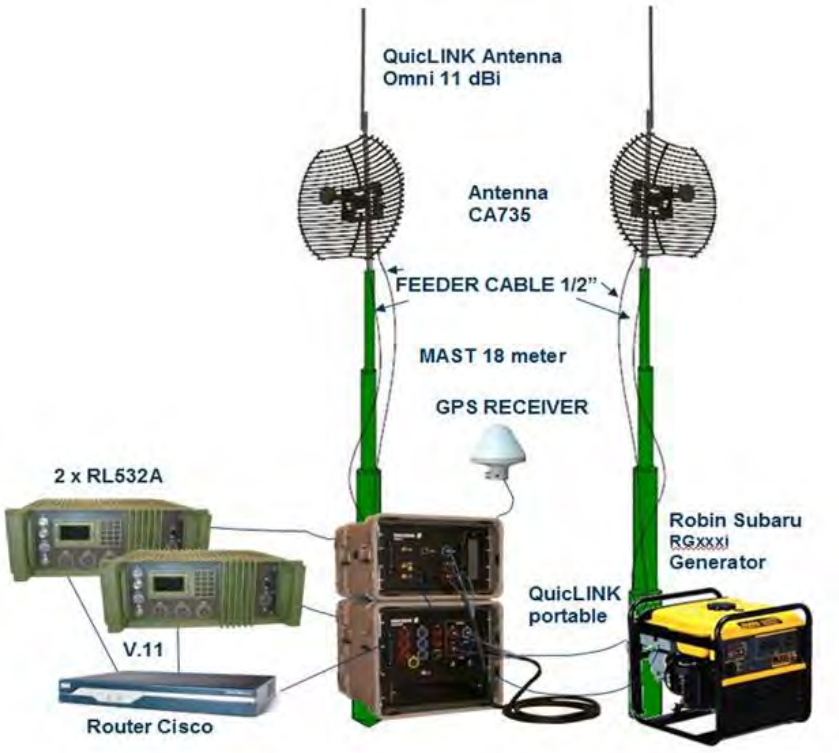

Figure 11. Ericsson QuicLINK (From [34])

In order to build networks, the base stations are connected to radio relay equipment [34]. The Ericsson QuicLINK should be seen as one example of how civilian infrastructure-based technology can be used as tactical communication in a military context.

D. EMERGING TECHNOLOGIES

1. LTE and 4G

The expression Long Term Evolution (LTE) is often associated with what will become the fourth generation of mobile communication, 4G. Originally, LTE was used since the development of 2G. A collaboration of groups within telecommunications formed a project called the 3rd Generation Partnership Project (3GPP), which has been involved in the development of the improving technologies after 2G, such as GSM/EDGE and UMTS.

The implementation of 4G cellular networks started in Sweden in 2010. During the first year, 4G networks were built in most of the major cities in Sweden. 4G will provide an IP-based mobile communication with a much higher data rate compared to 3G. The carrier frequency for 4G will be at 5GHz and the targeted data rate will be from 100 Mb/s up to 1,000 Mb/s [35]. To enhance the data rate from the previous system UMTS, 4G will use Orthogonal Frequency Division Multiplexing (OFDM). Digital video broadcasting and ADSL-modems for Internet-providers are examples of where OFDM already is used. The general idea in OFDM is to use a subset of sub-carriers that will be assigned to the different users. The frequencies for the sub-carriers are all multiples of the base frequency.

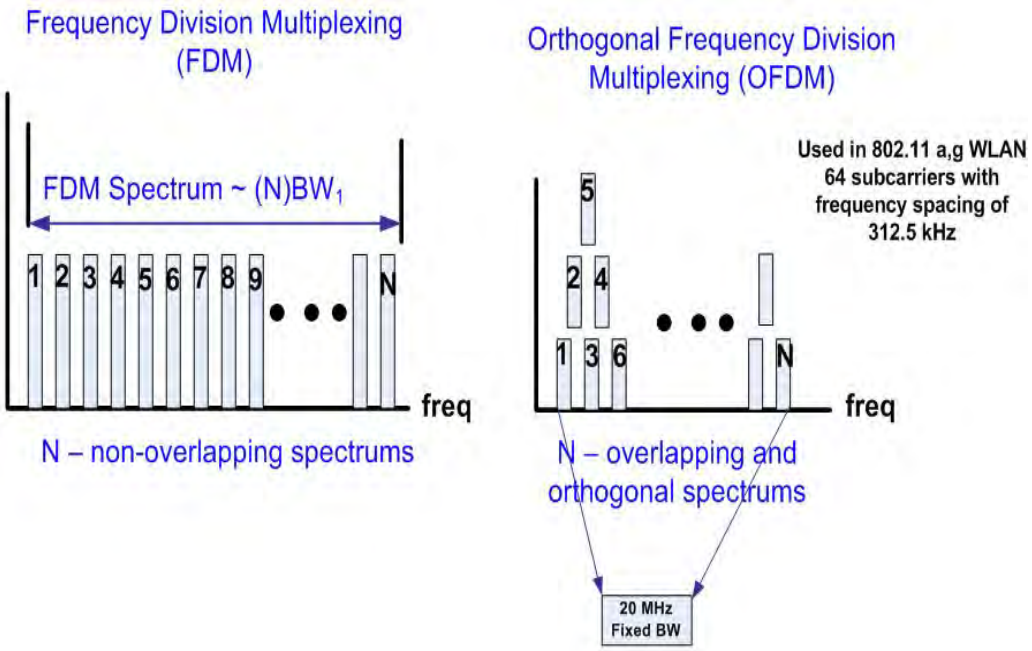

Figure 12. Comparison FDM and OFDM (From [36])

Through advanced signal processing in the receiver using an Inverse Fast Fourier Transform algorithm, it is possible to detect the OFDM subscriber signals [36]. In order to prevent intersymbol inference, a guard band or time is built into the OFDM symbols carried by each sub-carrier. This guard time is created by a process called cyclic-prefix that ensures that the symbols in the bit stream will not interfere with each another [1]. To achieve a high data rate, the OFDM is combined with modulation-techniques like quadrature phase shift keying (QPSK) or quadrature amplitude modulation (QAM). An advantage with OFDM is that it can manage transmission in spite of bad conditions for propagation, and it is resistant to fading and multipath. Additional OFDM capabilities include the capability to use some of the available sub-carrier channels to sample the condition of the wireless channel and the ability (although not often used) to adjust the modulation techniques of the sub-carriers to improve their performance.

E. CAPABILITIES AND SHORTFALLS

After the initial analysis of different technologies, the following conclusion can be made:

The technology for ad hoc networking by using a MANET can provide a flexible communications solution. MANETs do not require any infrastructure, which makes this particular system extremely mobile. The development within JTRS shows that it is possible to produce waveforms such as the Wideband Networking Waveform (WNW) with sufficient capacity providing a bandwidth up to 12.1 Mbps. There are some issues with ad hoc networking though; for example, the management process for ad hoc networking is complex. Today's technology requires a large flow of information overhead to keep track of all nodes for routing and other parameters needed for controlling the network. Another issue with ad hoc networking is area coverage. If the tactical force needs to cover a large operational area, the units need to spread out, which will probably have effects on connectivity and capacity in the network. There is also a risk that some nodes will have increased mobility because they need to act as relays between other nodes.

Infrastructure-based technologies such as 3G and 4G can also provide an interesting communication solution. The most common system used today, 3G will provide a bandwidth that is in the lower level of what is required. The upcoming technology of 4G will more than satisfy today's required bandwidth for a tactical force. The idea of a centralized infrastructure-based communications, such as 3G and 4G, will have both advantages and disadvantages. One advantage is that a centralized system will be easy to manage. In a centralized system, there will be a more straight-forward approach for routing and other flows of information needed to control the network. A disadvantage with an infrastructure-based system will be vulnerability. The whole communications solution will depend on the base stations that form the backbone. The base stations have to be protected in order to ensure functionality in a military tactical scenario. Both 3G and 4G require a number of base stations for building the network. In comparison between these two technologies, 4G will need more base stations to cover the same area as a 3G system.

IV. ANALYSIS THROUGH MODELING AND SIMULATION

A. INTRODUCTION

The purpose of this chapter is to analyze the possible technologies for tactical communication solutions. The different communication technologies are analyzed through modeling against an operational/tactical scenario. Initially, the modeling was made for tactical solutions based on the radio transmission that is commonly used in today's tactical systems. This network served as a reference or baseline for performance. Thereafter, tactical solutions were based on ad hoc networking and 3G/UMTS-technology. The solutions are the performance compared to the reference system. The results of the analysis are used for evaluation in the next chapter.

B. JOINT COMMUNICATION SIMULATION SYSTEM

In this thesis project, Joint Communication Simulation System (JCSS) was chosen as the software to model and simulate the different technologies for wireless communications. The JCSS software is based on the well-known OPNET software that is commonly used for developing and validating networks in commercial applications. JCSS provides features that are easily tailored and adapted for military use. When developing the networks for this thesis project the Department for Information Systems Agency (DISA) in Arlington, Virginia together with the OPNET's headquarters in Bethesda, Maryland provided a significant level of support. DISA provided JCSS training to the author and simulated network developments. OPNET provided exceptional support in debugging these networks models, and they also provided subject matter expertise while the UMTS network was under development. In cooperation with both DISA and OPNET the following models were created as a part of this thesis project.

- SINCGARS Network
- Mobile Ad hoc Network (MANET)
- 3G/UMTS Network

These three models were developed specifically for this thesis project and were adapted in architecture to be used for a land force of battalion size.

The experience gained from using JCSS/OPNET is that the software worked well for measuring the networks according to the stated goals and objectives of this research. When properly used, these software tools can provide a sufficient simulation for military networks operating in a field environment.

C. TACTICAL FORCE AND SCENARIO SETUP

The operational/tactical scenario chosen for the analysis is a generic Peace Support Operation (PSO). The terrain for the scenario is fictitious and was chosen to provide the most realistic input possible for wave propagation calculations within the simulation software. The tactical force will be configured to simulate the Maneuver Battalion within the Nordic Battle Group 2011 (NBG11) and the Maneuver Battalion will conduct operations within an Area of Responsibility (AOR) that correlates to cover a 500-km^2 requirement [19].

The Maneuver Battalion within NBG11 consists of the following sub-units [37]:

– 1 Battalion Headquarters

– 2 Mechanized Companies

– 1 Air Assault Squadron

– 1 Combat Support Company

– 1 Logistics Company

As applied to these simulations, NBG11 will be deployed to support an ongoing UN-operation. Since there has been tension between the two warring factions, NBG11 in their peacekeeping mission will separate the two principal opponents in order to ensure security for the civilians who live and work in the area. The Maneuver battalion within NBG11 and all of its resources will be responsible for the main part of the AOR. Each subordinated company will be responsible for their individual positions of the AOR, ensuring security for civilians by conducting mobile surveillance operations and

patrolling. The subordinated companies will be prepared to quickly mobilize support for other units within the whole AOR when needed.

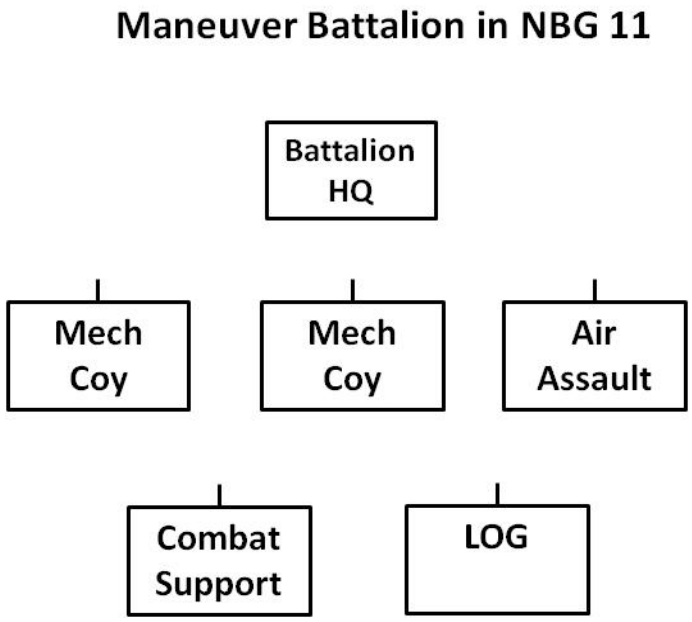

Figure 13. Maneuver battalion within NBG11

D. SCENARIOS

In order to realistically evaluate different wireless technologies, the networks will be analyzed through three individual scenarios. When building the tactical communication solutions for the three scenarios, the hierarchy for each network has been intentionally made flat. A flat hierarchy will enhance full transparency between the highest and the lowest level in the tactical force. The MANET solution was not divided in different subnets for different companies. If the MANET were divided in subnets, the comparison between a MANET and an infrastructure-based system would not be balanced and the subnet dividing will also decrease the ability for end-to-end communication between the highest and the lowest level in the tactical force.

1. Scenario 1: Surveillance

In the first scenario, the battalion will conduct surveillance in the given AOR. The battalion consists of one Battalion Commander, three Company Commanders and nine patrols. All units will be spread out in the entire battalion area and conduct surveillance from fixed positions. Communications that have the highest priority are the links between the Battalion Commander and the three Company Commanders.

2. Scenario 2: Movement within AOR

In the second scenario, an incident happens within the AOR, which requires units to move to this location in order to secure the incident area. The place for the incident is arbitrarily located in the southwest corner of the AOR. Three patrols, together with a Company Commander, will move to the incident location. Communications that have the highest priority are the link to the patrol that is closest to the incident and the link to the Company Commander that is assigned command and control responsibility for the operation.

3. Scenario 3: Extended AOR

In the third scenario, there is a risk that hostile actions can occur in the area south of the deployed battalion. In order to act against this potential threat, the AOR will be extended, and three patrols and one Company Commander will move south in order to secure and cover this area. Communications that have the highest priority are the links to the two patrols that first enter the extended AOR and the link to the Company Commander that is assigned to monitor the extension of the AOR.

E. MODELING OVERVIEW

1.1 SINCGARS Network, Scenario 1, surveillance

1.2 SINCGARS Network, Scenario 2, movement within AOR

1.3 SINCGARS Network, Scenario 3, extended AOR

2.1 MANET, Scenario 1, surveillance

2.2 MANET, Scenario 2, movement within AOR

2.3 MANET, Scenario 3, extended AOR

3.1 Infrastructure Based UMTS Network, Scenario 1, surveillance

3.2 Infrastructure Based UMTS Network, Scenario 2, movement within AOR

3.3 Infrastructure Based UMTS Network, Scenario 3, extended AOR

F. SINCGARS NETWORK MODELING

Model Network 1 is a SINCGARS broadcasting network based on the AN-PSC 5A radio. The SINCGARS network communications are based on the following parameters. See Table 1.

SINCGARS Network	
Frequency range	30-89 MHz
Output power	20 W
Modulation/Spread Spectrum	FM/FHSS
Simulated traffic in the network	IER:s (Information Exchange Requirements) of 64 kbps sent every 100 s. Protocol UDP

Table 1. Data for SINCGARS Network model

1. SINCGARS Network, Scenario 1: Surveillance

Network overview

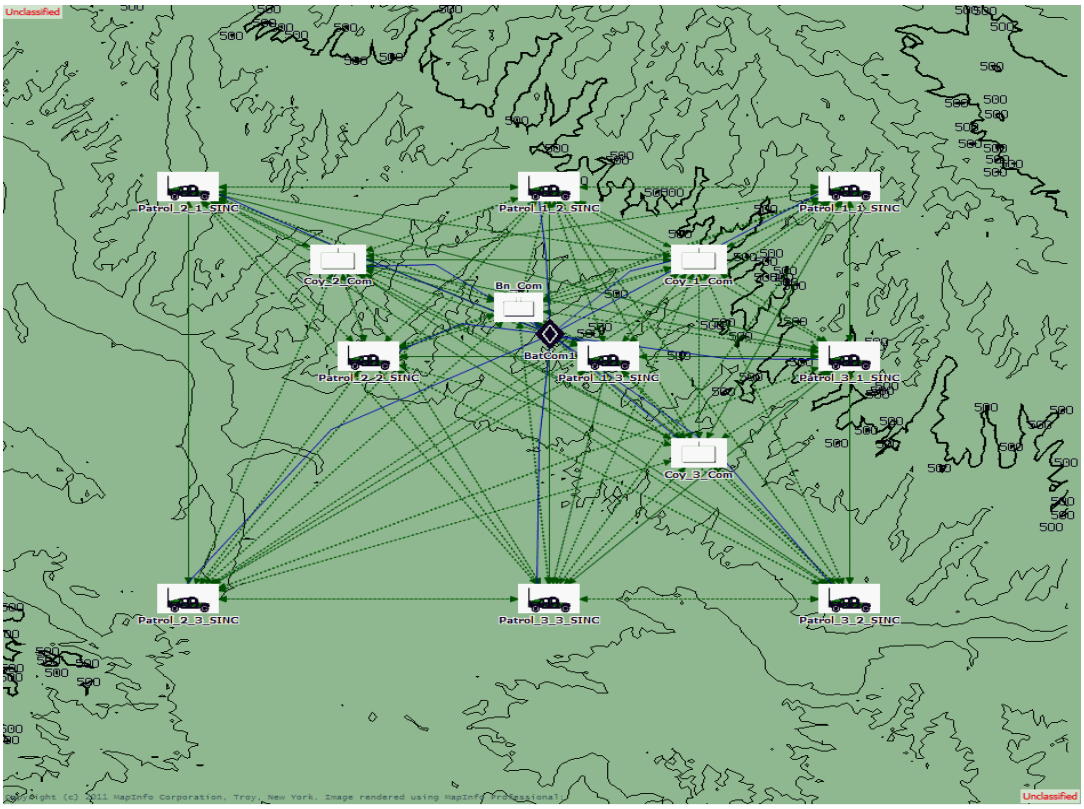

Figure 14. 1.1 SINCGARS Network, Scenario 1: Surveillance

Simulation parameters

The simulation time for 1.1 SINCGARS Network, Scenario 1, surveillance was set to 60 minutes. Traffic was simulated by sending IERs between the 13 nodes during the simulation time. The tactical force covers an area of 24 km * 21 km, which is equal to approximately 500 km^2. The 13 nodes are stationary and do not move in this scenario. Communications with the highest priority in this scenario are the links between the Battalion Commander and the three Company Commanders.

Results

Overall IER average completion rate: 96%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.96034	0.97152	0.00694

Table 2. Overall throughput for the 1.1 SINCGARS Network, Scenario 1, surveillance

Performance for communications with the highest priority:

Battalion Commander to Commanders Company 1, Company 2 and Company 3

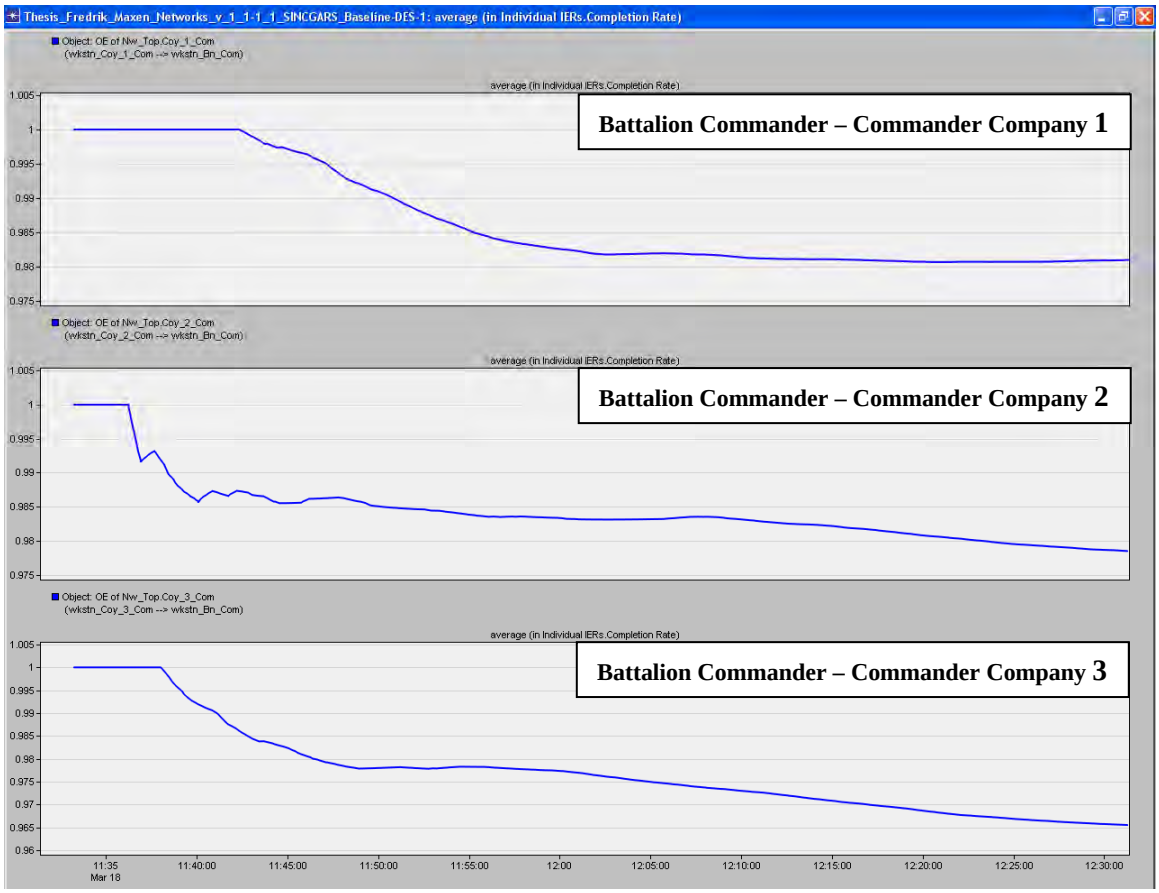

Figure 15. Throughput between nodes with high priority in 1.1 SINCGARS Network, Scenario 1, surveillance

Comments

The simulation result for the 1.1 SINCGARS Network, Scenario 1, surveillance, shows that there is a high throughput of IERs in the network. The result correlates with what should be expected for a frequency-hopping network with regular combat net broadcast technology. A SINCGARS network should be able to connect all nodes in an

area of 500 km^2 but the data rate is assumed to be lower compared to what should be expected for more modern modulation technologies.

2. SINCGARS Network, Scenario 2, Movement within AOR

Network overview

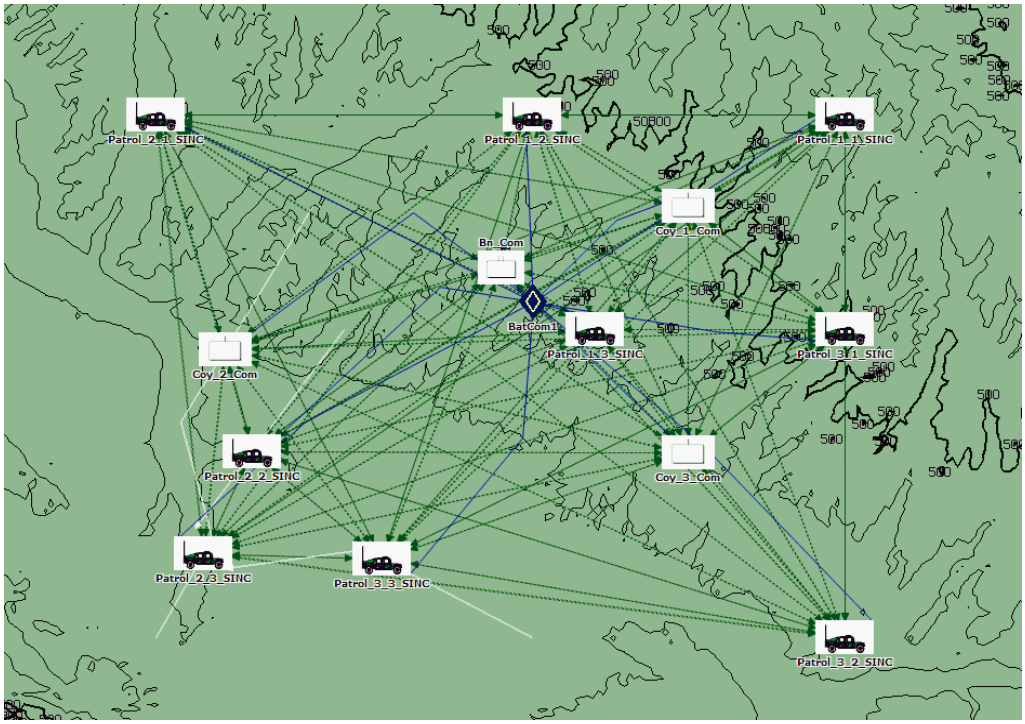

Figure 16. 1.2 SINCGARS Network, scenario 2, movement within AOR

Simulation parameters

The simulation time for 1.2 SINCGARS Network, Scenario 2, movement within AOR, was set to 60 minutes. Traffic was simulated by sending IERs between the 13 nodes during the simulation time. The tactical force covers an area of 24 km * 21 km, which is equal to approximately 500 km^2. Four of the units within the tactical force will move towards a location in the southwest part of the AOR where an incident has occurred. The other nine units within the tactical force will be stationary. Communications with the highest priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 2, Patrol 2.3, and Patrol 3.3.

Result

Overall IER average completion rate: 91%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.90992	0.92222	0.00641

Table 3. Overall throughput for the 1.2 SINCGARS Network, Scenario 2, movement within AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 2, Patrol 2-3, and Patrol 3-3

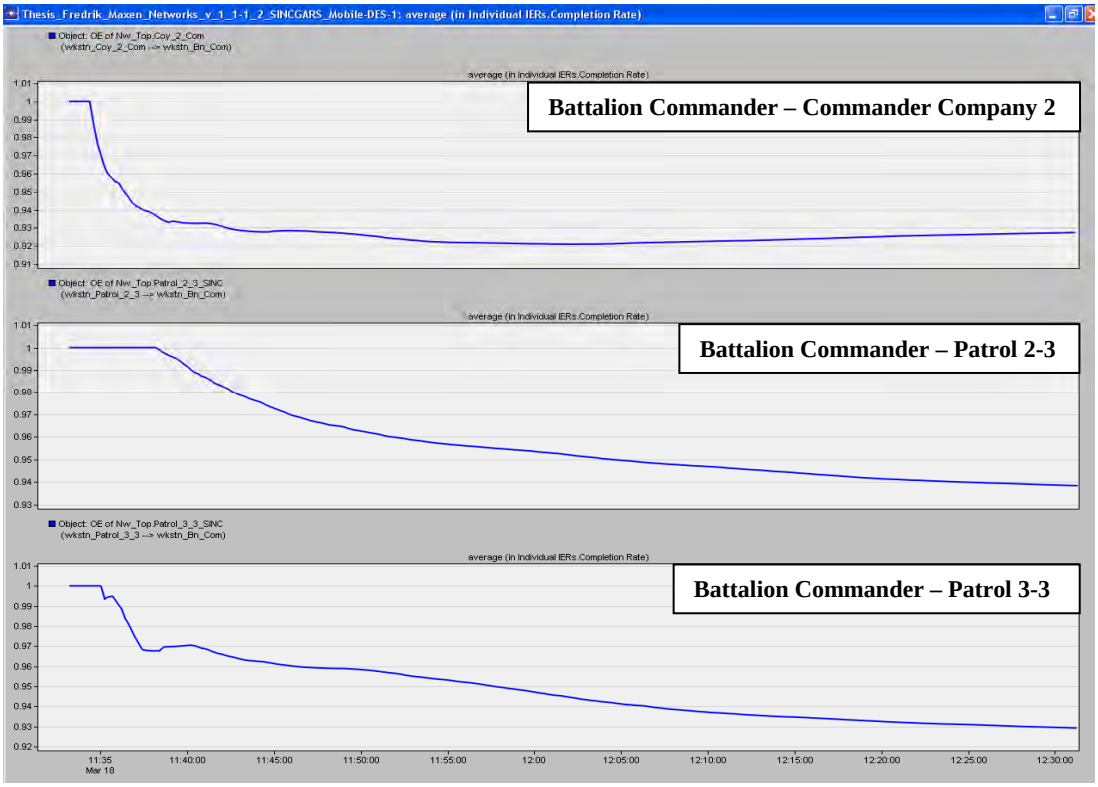

Figure 17. Throughput between nodes with high priority in 1.2 SINCGARS Network, Scenario 2, movement within AOR

Comments

The throughput of IERs decreased slightly in 1.2 SINCGARS Network, Scenario 2, movement within AOR, compared to scenario 1, from 96% to 91%. The overall

throughput should still be considered as delivering an acceptable level. Since the movement of nodes will create interference in some of the transmissions of IERs, the result is expected.

3. SINCGARS Network, Scenario 3, Extended AOR

Network overview

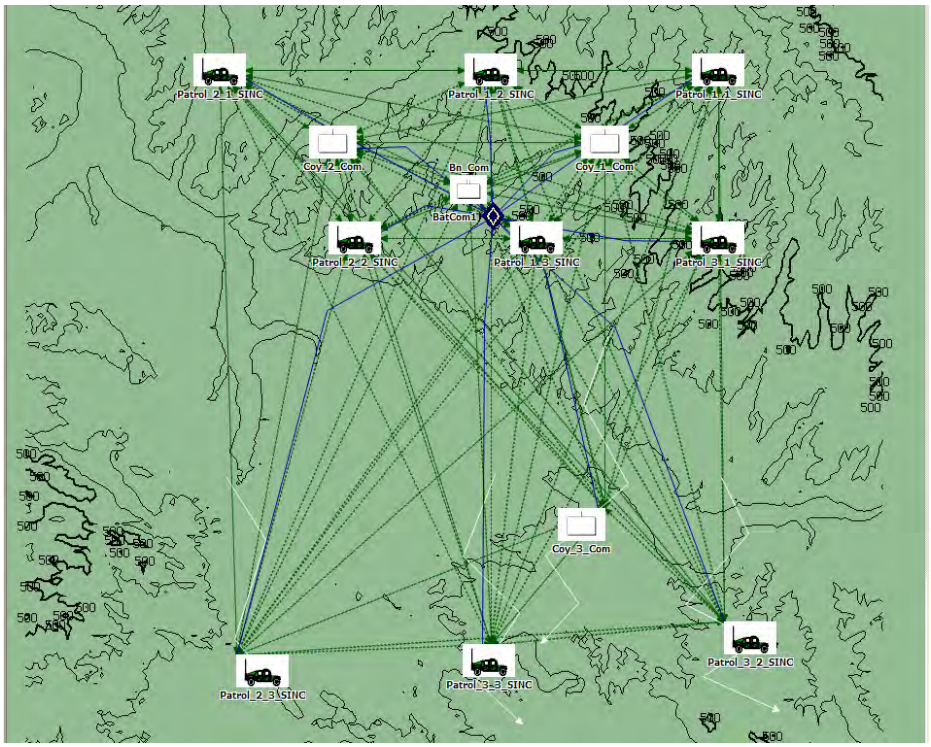

Figure 18. 1.3 SINCGARS Network, Scenario 3, extended AOR

Simulation parameters

The simulation time for 1.3 SINCGARS Network, Scenario 3, extended AOR, was set to 60 minutes. Traffic was simulated by sending IERs between the 13 nodes during the simulation time. The tactical force covers initially an area of 24 km * 21 km, which is equal to approximately 500 km^2. Due to hostile actions outside the initial AOR, four of the units within the tactical force have to move south. The tactical force will, after this movement, cover an area of 24 km * 27 km, which is equal to approximately 650 km^2. The other nine units within the tactical force will be stationary. Communications

with the highest priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 3, Patrol 2.3, and Patrol 3.2.

Result

Overall IER average completion rate: 79%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.79098	0.80208	0.00694

Table 4. Overall throughput for the 1.3 SINCGARS Network, Scenario 3, extended AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 3, Patrol 2-3, and Patrol 3-2

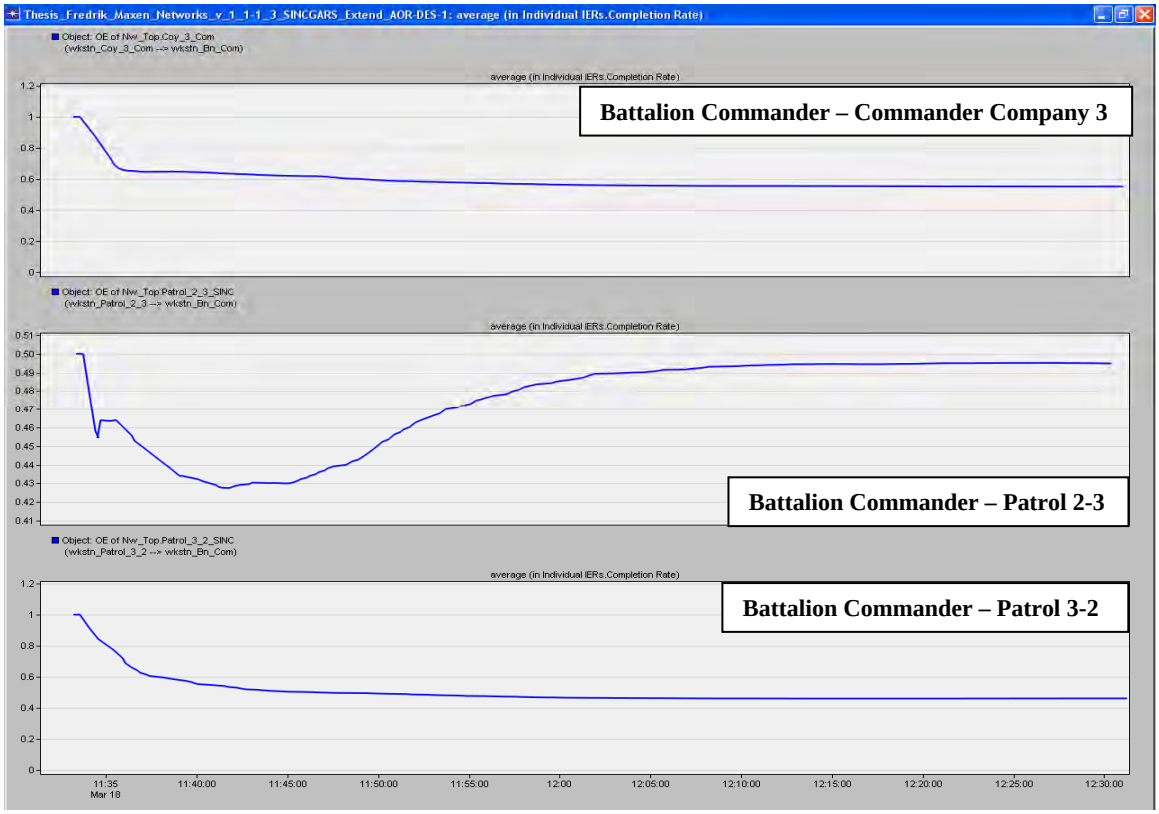

Figure 19. Throughput between nodes with high priority in 1.3 SINCGARS Network, Scenario 3, extended AOR

Comments

The throughput of IERs significantly decreased in 1.3 SINCGARS Network, Scenario 3, extended AOR, from 96% in scenario 1 to 79% in this scenario. The throughput of IERs to the nodes that move south has greatly decreased. The decreased throughput in extended coverage area of scenario 3 shows that the links between nodes in a regular broadcasting network will be greatly degraded when the ranges approach the limit for connectivity.

G. MANET NETWORK MODELING

Model Network 2 will be based on Mobile Ad Hoc Networking (MANET) technology.

MANET Network	
Frequency range	2.4 GHz
Output power	20 W
Modulation/Spread Spectrum/Routing	OFDM/OLSR Ad-Hoc routing protocol
Simulated traffic in the network	IER:s (Information Exchange Requirements) of 64 kbps sent every 100 s. Protocol UDP

Table 5. Data for MANET Network model

1. MANET, Scenario 1, Surveillance

Network overview

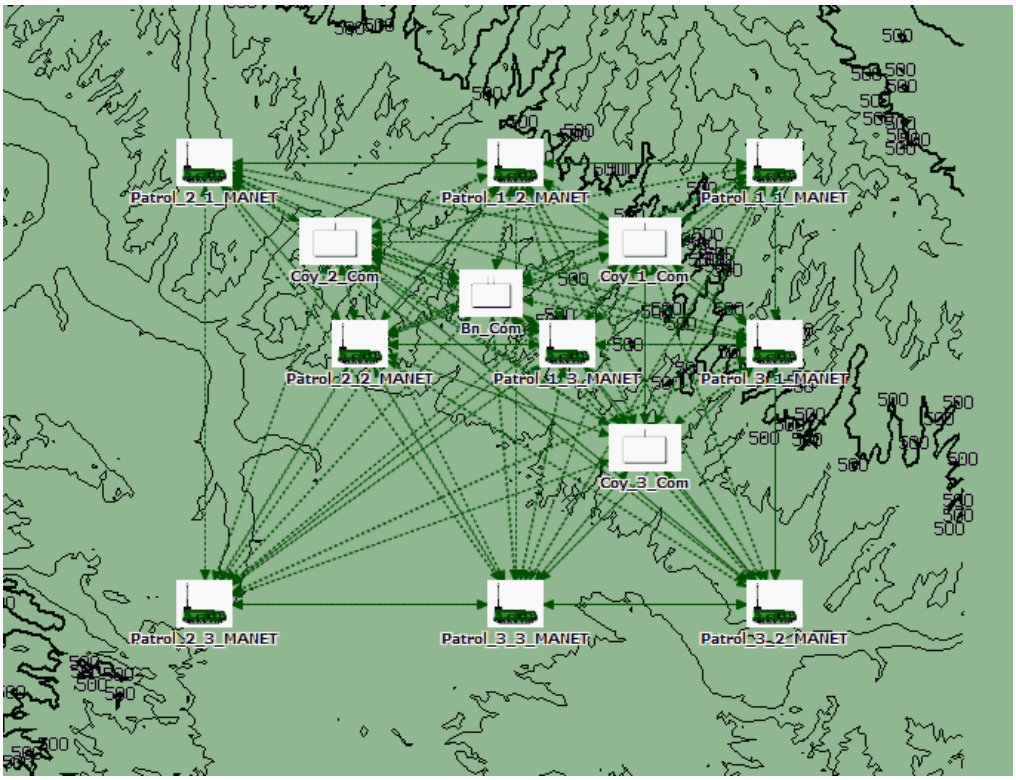

Figure 20. 2.1 MANET, Scenario 1, surveillance

Simulation parameters

The simulation time for 2.1 MANET, Scenario 1, surveillance, was set to 60 minutes. Traffic was simulated by sending IERs between the 13 nodes during the simulation time. The tactical force covers an area of 24 km * 21 km, which is equal to approximately 500 km^2. The 13 nodes are stationary and do not move in this scenario. Communications with the highest priority in this scenario are the links between the Battalion Commander and the three Company Commanders.

Results

Overall IER average completion rate: 99%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.98646	0.99359	0.00641

Table 6. Overall throughput for the 2.1 MANET, Scenario 1, surveillance

Performance for communications with the highest priority:

Battalion Commander to Commanders Company 1, Company 2 and Company 3

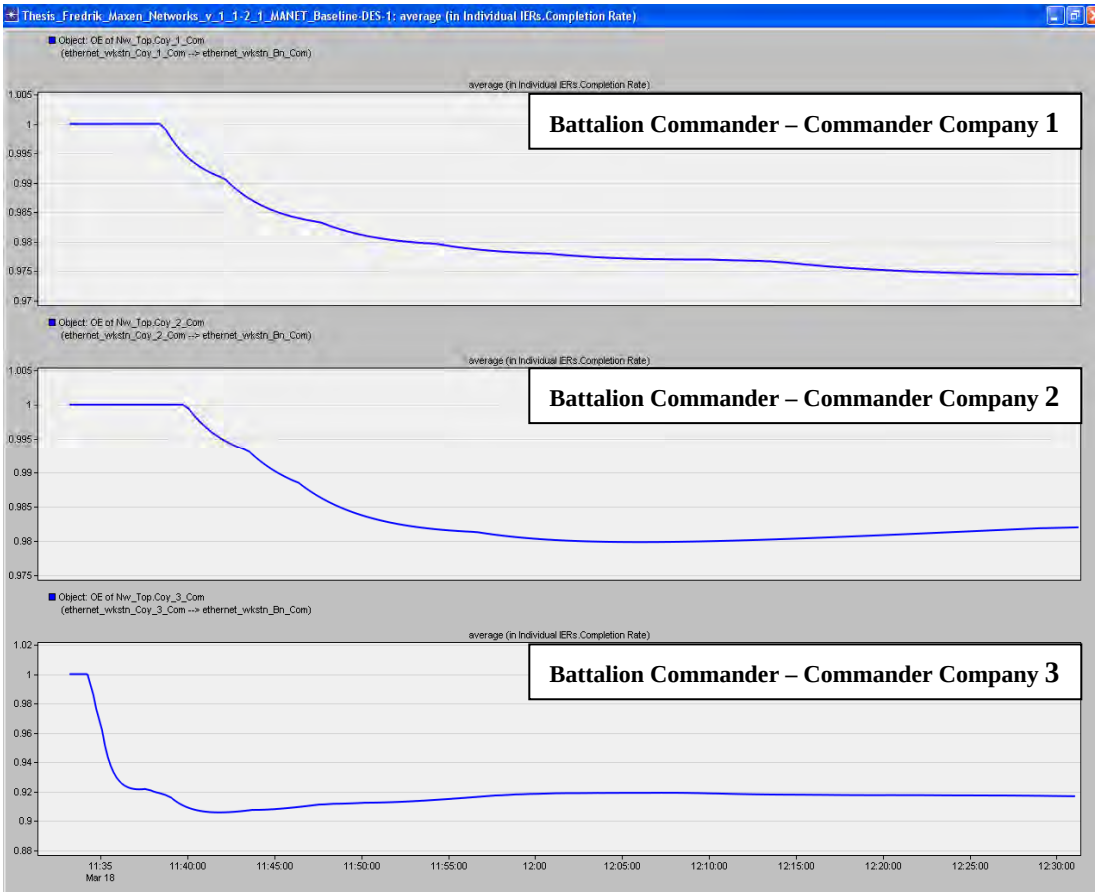

Figure 21. Throughput between nodes with high priority in 2.1 MANET, Scenario 1, surveillance

Comments

The overall throughput for IERs for 2.1 MANET, Scenario 1, surveillance, is very high with an average completion rate of 99%. According to the high throughput, it seems that there is a high connectivity between the nodes in the network. In comparison with the SINCGARS network for the same scenario, the throughput is even higher.

2. MANET, Scenario 2, Movement within AOR

Network overview

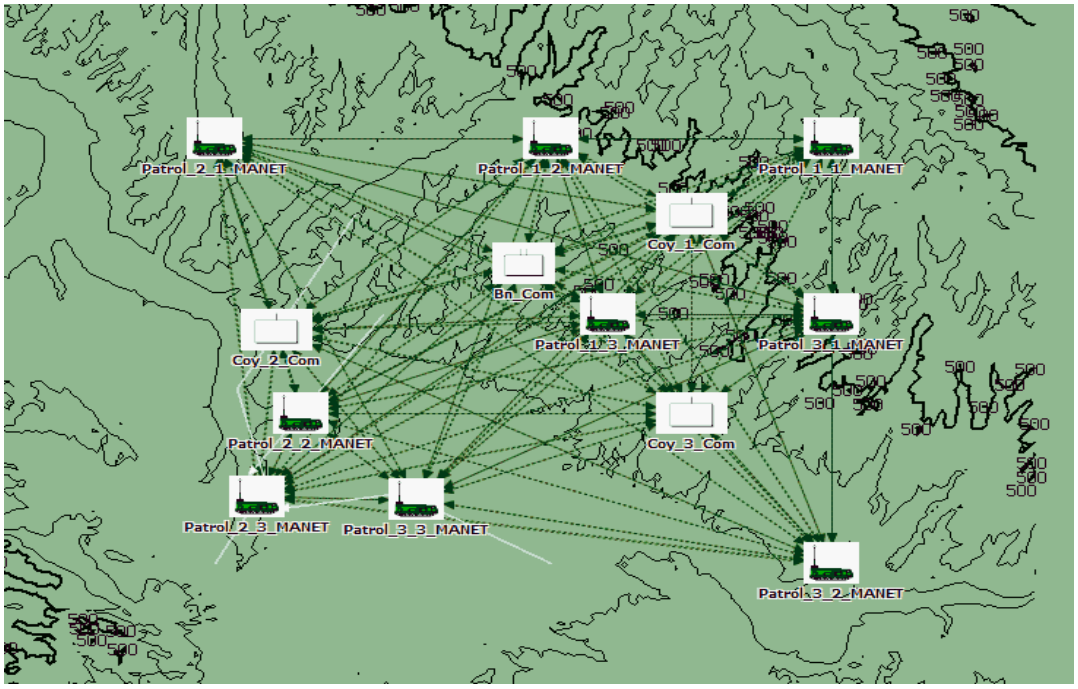

Figure 22. 2.2 MANET, Scenario 2, movement within AOR

Simulation parameters

The simulation time for 2.2 MANET, Scenario 2, movement within AOR, was set to 60 minutes. Traffic was simulated by sending IERs between the 13 nodes during the simulation time. The tactical force covers an area of 24 km * 21 km, which is equal to approximately 500 km^2. Four of the units within the tactical force will move towards a location in the southwest part of the AOR where an incident has occurred. The other nine units within the tactical force will be stationary. Communications with the highest

priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 2, Patrol 2.3, and Patrol 3.3.

Results

Overall IER average completion rate: 99%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.98731	0.98893	0.00641

Table 7. Overall throughput for the 2.2 MANET, Scenario 2, movement within AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 2, Patrol 2-3, and Patrol 3-3

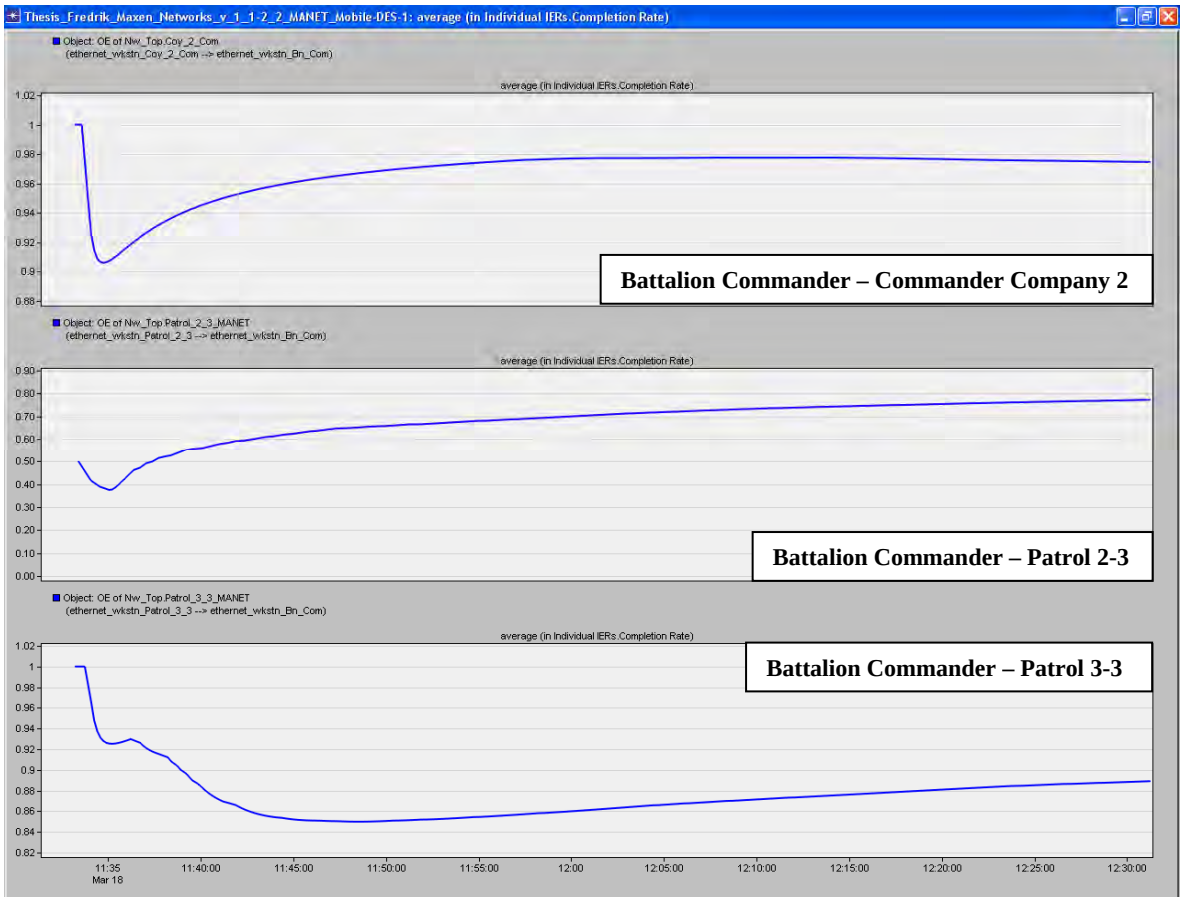

Figure 23. Throughput between nodes with high priority in 2.2 MANET, Scenario 2, movement within AOR

Comments

The throughput of IERs remains on a high level for the 2.2 MANET, Scenario 2, movement within AOR. In comparison, when the nodes were fixed, the movement of nodes did not affect the connectivity or throughput. In comparison to the SINCGARS network in the same scenario, there is noticeable difference in level of throughput.

3. MANET, Scenario 3, Extended AOR

Network overview

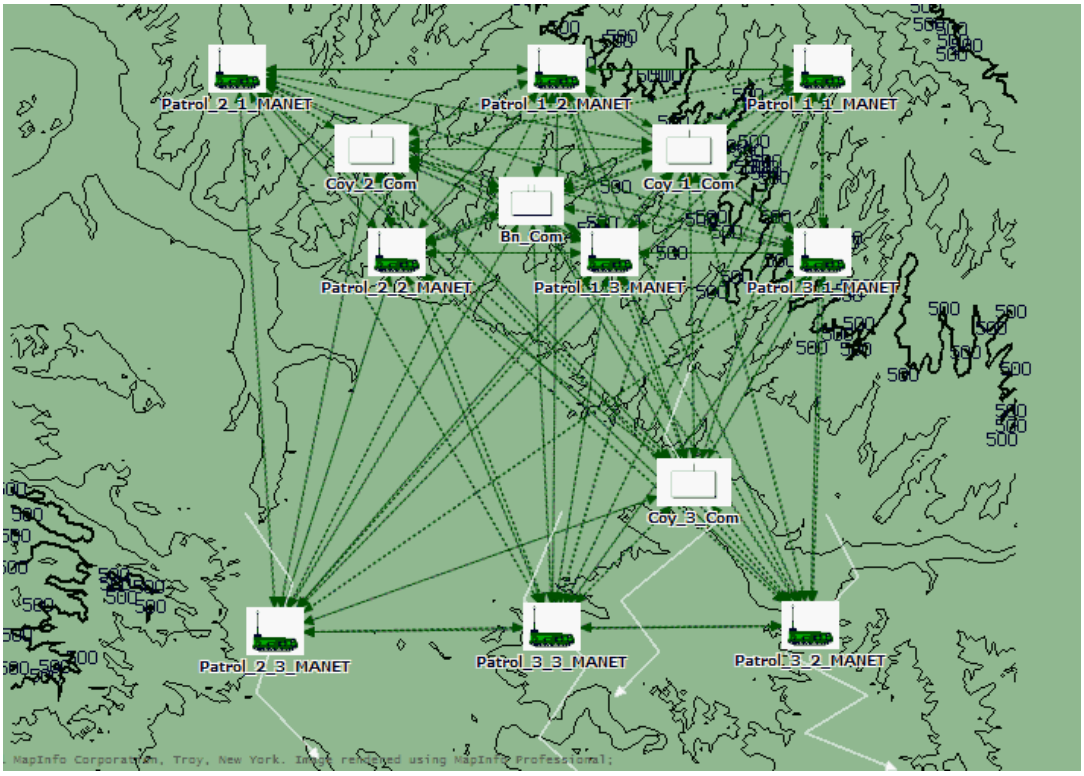

Figure 24. 2.3 MANET, Scenario 3, extended AOR

Simulation parameters

The simulation time for 2.3 MANET, Scenario 3, extended AOR, was set to 60 minutes. Traffic was simulated by sending IER's between the 13 nodes during the simulation time. The tactical force covers initially an area of 24 km * 21 km, which is equal to approximately 500 km^2. Due to hostile actions outside the initial AOR, four of the units within the tactical force have to move south. The tactical force will, after this

movement, cover an area of 24 km * 27 km, which is equal to approximately 650 km^2. The other nine units within the tactical force will be stationary. Communications with the highest priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 3, Patrol 2.3, and Patrol 3.2.

Results

Overall IER average completion rate: 97%

Statistic	Average	Maximum	Minimum
Total Data IERs Completion Rate	0.97419	0.98130	0.00641

Table 8. Overall throughput for the 2.3 MANET, Scenario 3, extended AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 3, Patrol 2-3, and Patrol 3-2

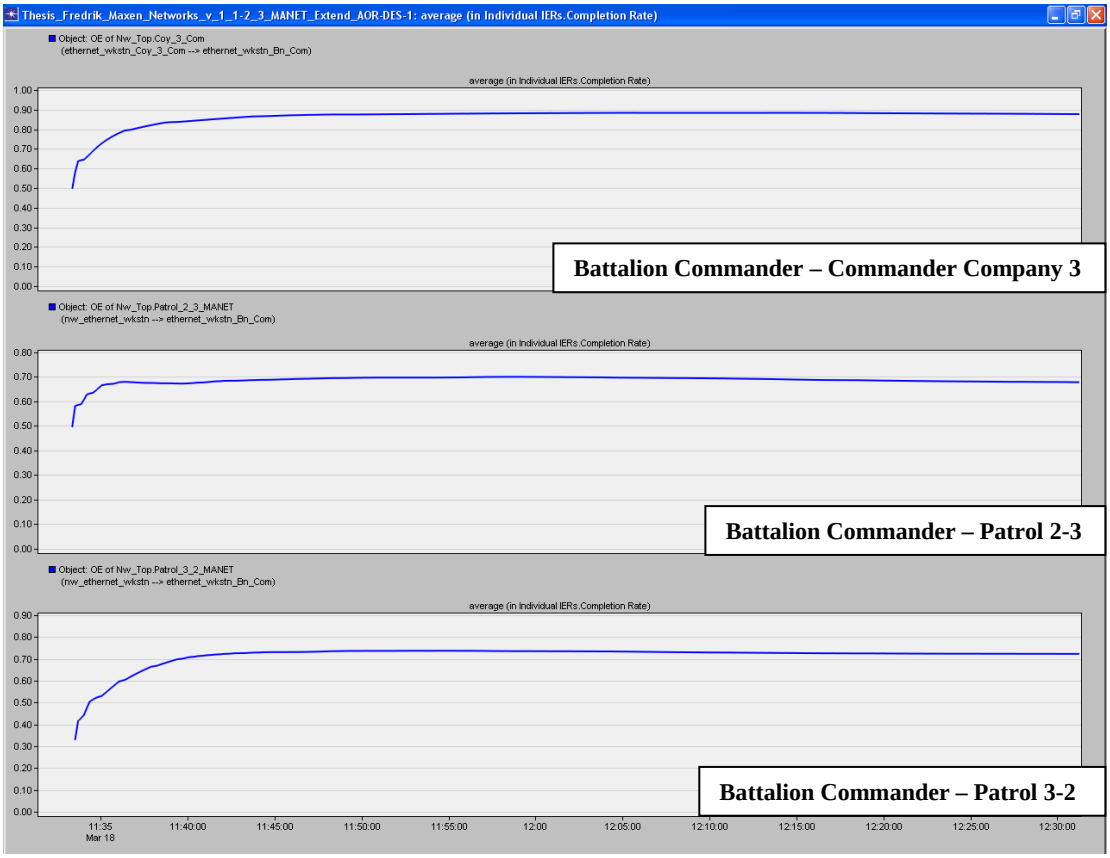

Figure 25. Throughput between nodes with high priority in 2.3 MANET, Scenario 3, extended AOR

Comments

There are two major observations identified in 2.3 MANET, Scenario 3, extended AOR. The first observation is a decreased localized throughput to the nodes that acts in the added area. The second observation is that the overall throughput remains, on average, relatively high compared to the SINCGARS network in the same scenario. It seems that the MANET technology, where nodes act as relays between each other, will have an impact associated to the overall performance.

H. UMTS NETWORK MODELING

Network 3 will be based on civilian cellular technology. This network is built on 3G/UMTS with an infrastructure based on towers. The backbone is formed by one base station and two repeaters on towers where the 3G subscribers are connected.

UMTS Network	
Frequency range	1.9-2.1 GHz
Output power	Base-station: 20 W; Subscribers: 0.5 W
Modulation/Spread Spectrum	CDMA/DSSS
Communication Protocol	IP/TCP
Simulated traffic in the network	FTP using IP/TCP. Sending and receiving traffic (measured in bytes/sec)

Table 9. Data for UMTS Network model

1. UMTS Network, Scenario 1, Surveillance

Network overview

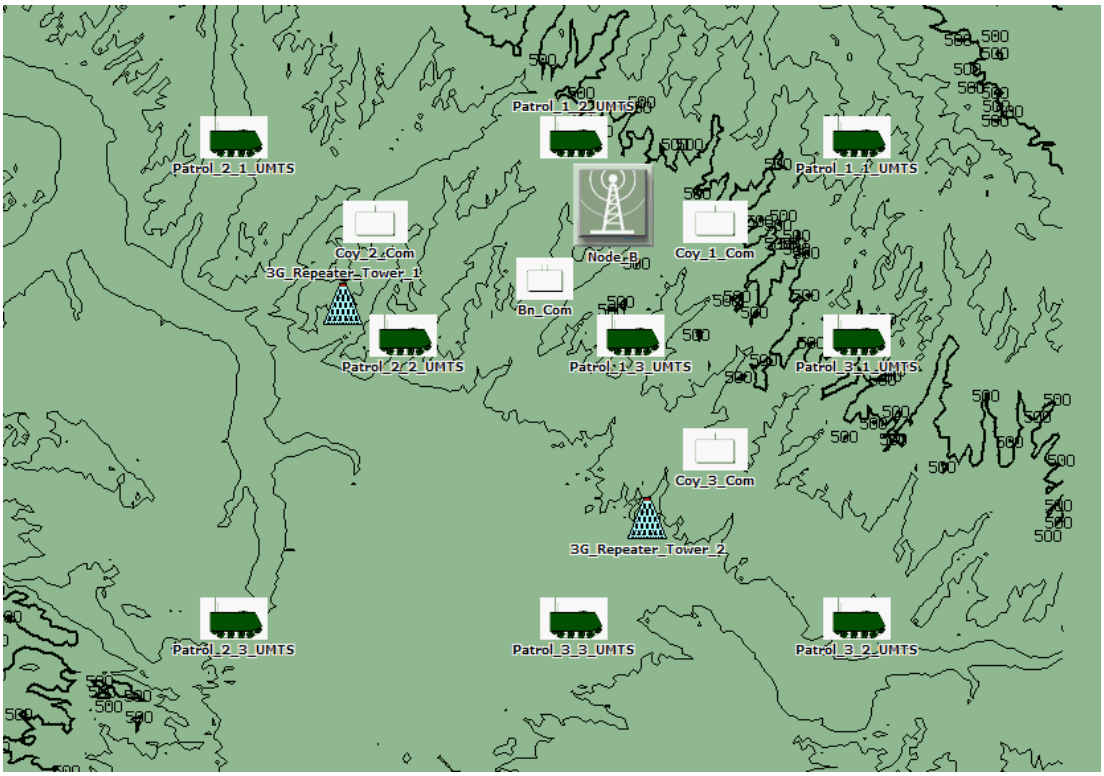

Figure 26. 3.1 UMTS Network, Scenario 1, surveillance

Simulation parameters

The simulation time for 3.1 UMTS Network, Scenario 1, surveillance, was set to 60 minutes. Traffic was simulated by transmitting packets between the 13 nodes using FTP during the simulation time. The tactical force covers an area of 24 km * 21 km which is equal to approximately 500 km^2. The 13 nodes are stationary and do not move in this scenario. Communications with the highest priority in this scenario are the links between the Battalion Commander and the three Company Commanders.

Results

Overall performance:

Statistic	Average	Maximum	Minimum
Ftp Traffic Received (bytes/sec)	3,833.2	5,083.1	0.0
Ftp Traffic Sent (bytes/sec)	3,863.2	5,016.0	0.0

Table 10. Overall throughput for the 3.1 UMTS Network, Scenario 1, surveillance

Performance for communications with the highest priority:

Battalion Commander to Commanders Company 1, Company 2 and Company 3.

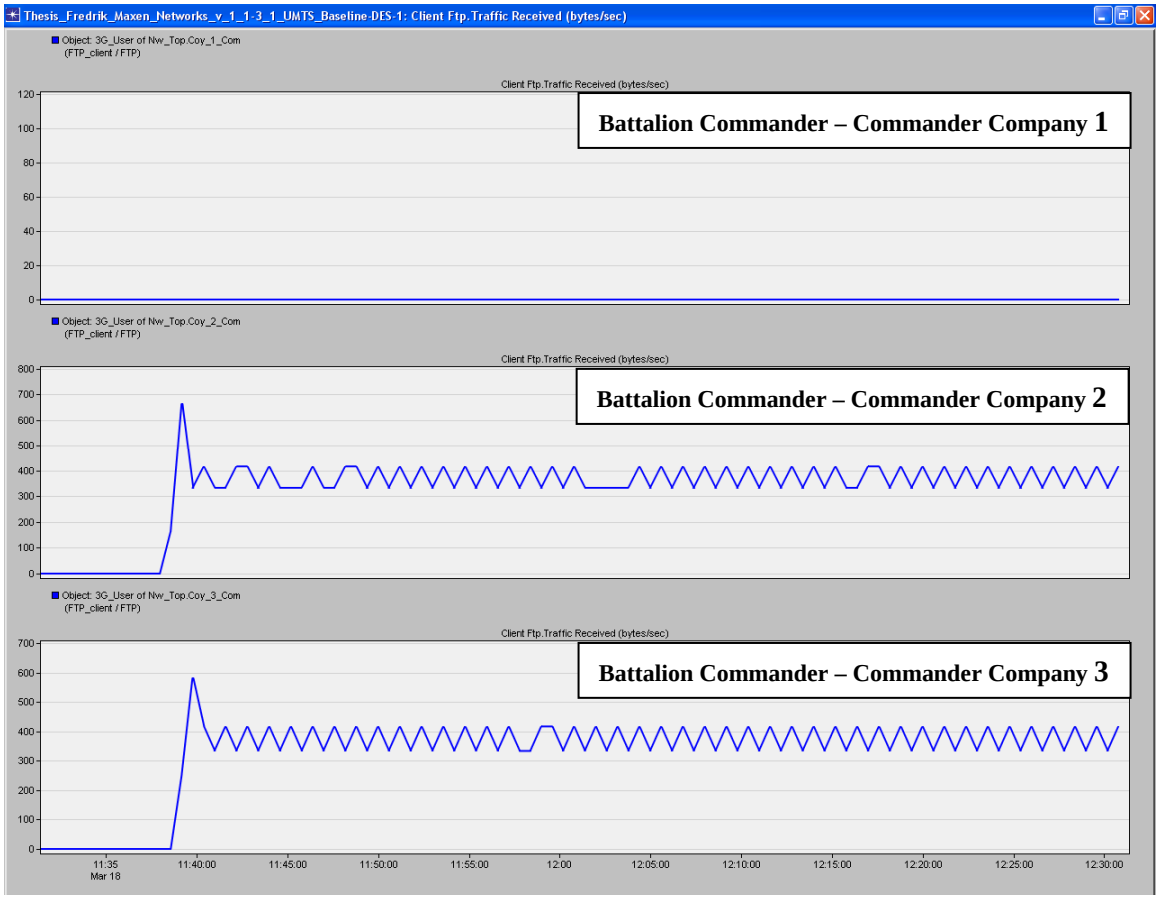

Figure 27. Throughput between nodes with high priority in 3.1 UMTS Network, Scenario 1, surveillance

Comments

The throughput is on average considered to be relatively high in the 3.1 UMTS Network, Scenario 1, surveillance. When discussing data rate with subject matter experts at OPNET, a realistic value for data rate is 400 kbps in a UMTS network. In the simulation for Scenario 1, one of the priority links did not get any throughput at all. When moving the node away from the UMTS base station, the link could be re-established. The observation was that the node initially was interfered with by other nodes when it was too close to the base station. The identified interference issue was discussed and confirmed by subject matter experts at OPNET.

2. UMTS Network, Scenario 2, Movement within AOR

Network overview

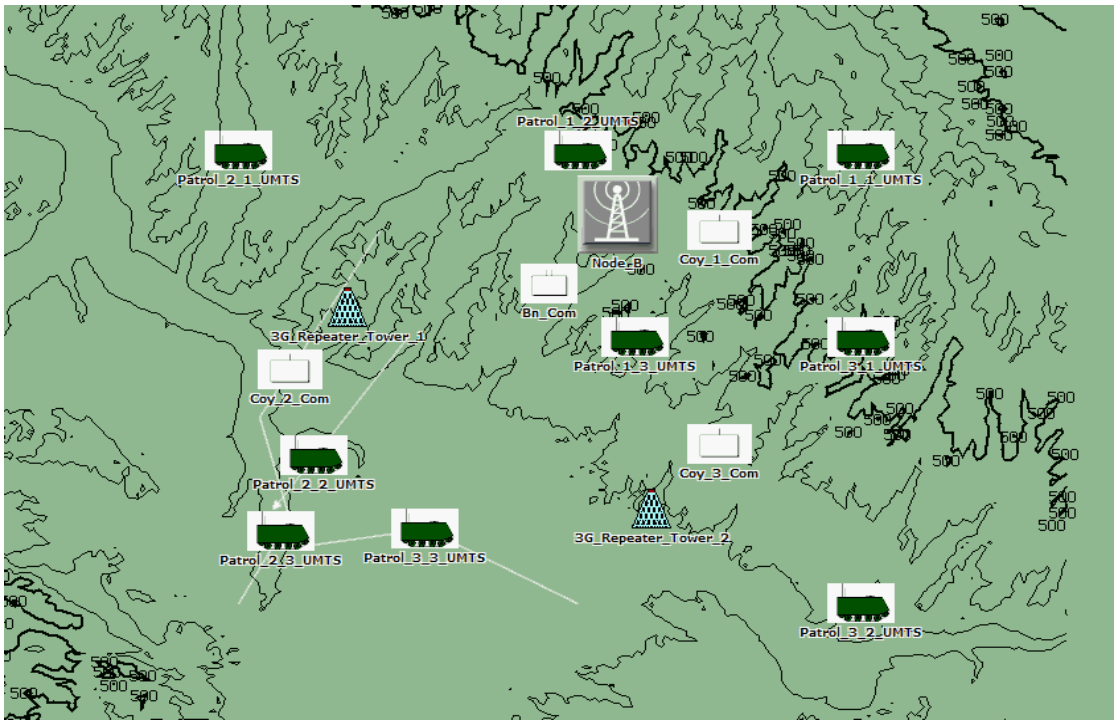

Figure 28. 3.2 UMTS Network, Scenario 2, movement within AOR

Simulation parameters

The simulation time for 3.2 UMTS Network, Scenario 2, movement within AOR, was set to 60 minutes. Traffic was simulated by transmitting packets between the 13 nodes using FTP during the simulation time. The tactical force covers an area of 24 km * 21 km, which is equal to approximately 500 km^2. Four of the units within the tactical force will move towards a location in the southwest part of the AOR where an incident has occurred. The other nine units within the tactical force will be stationary. Communications with the highest priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 2, Patrol 2.3, and Patrol 3.3.

Results

Overall performance:

Statistic	Average	Maximum	Minimum
Ftp Traffic Received (bytes/sec)	3,926.2	5,249.8	0.0
Ftp Traffic Sent (bytes/sec)	3,975.4	5,337.1	0.0

Table 11. Overall throughput for the 3.2 UMTS Network, Scenario 2, movement within AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 2, Patrol 2-3, and Patrol 3-3.

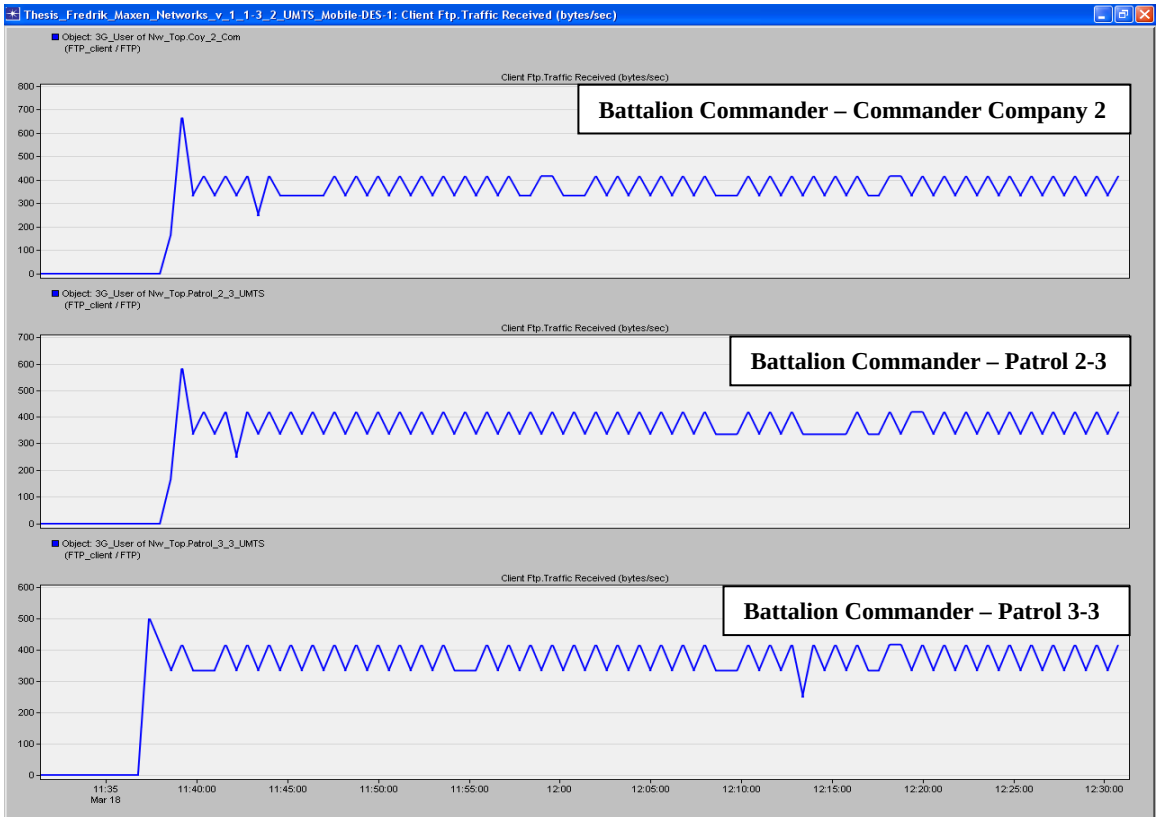

Figure 29. Throughput between nodes with high priority in 3.2 UMTS Network, Scenario 2, movement within AOR

Comments

The throughput for the 3.2 UMTS Network in Scenario 2, movement within AOR, remains high in an overall perspective. There is no interference from the base station to links with priority in this scenario. The interference that was identified for the UMTS network in the previous scenario 1 seems only to occur in a certain area and affects therefore only a few nodes.

3. UMTS Network, Scenario 3, Extended AOR

Network overview

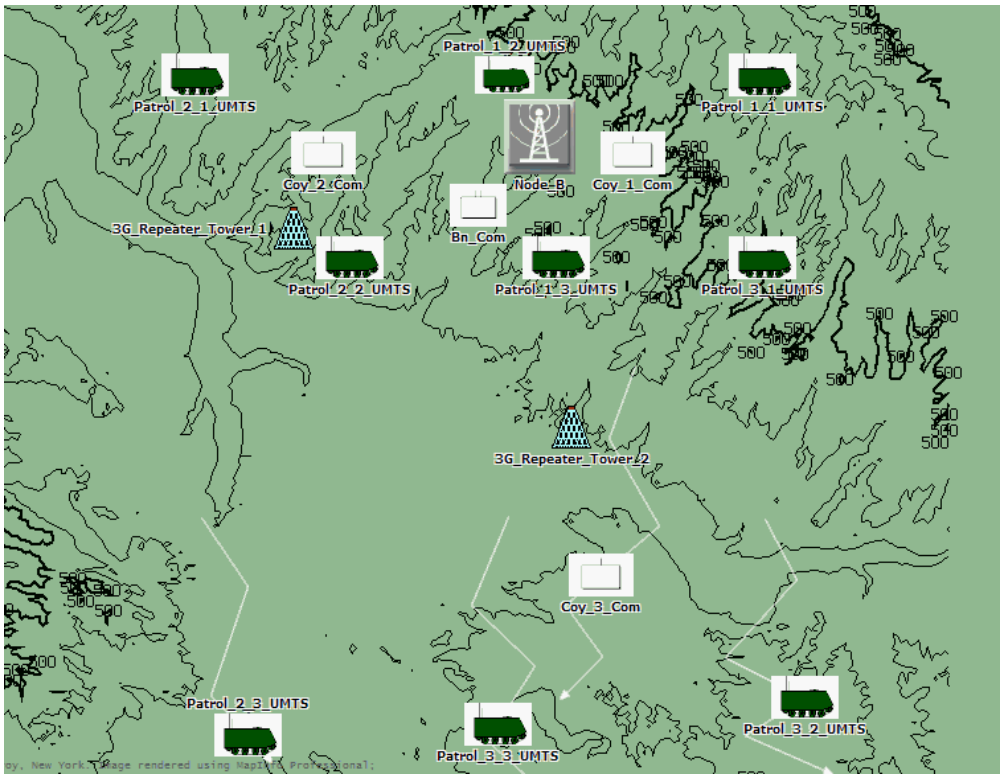

Figure 30. 3.3 UMTS Network, Scenario 3, extended AOR

Simulation parameters

The simulation time for 3.3 UMTS Network, Scenario 3, extended AOR, was set to 60 minutes. Traffic was simulated by transmitting packets between the 13 nodes using FTP during the simulation time. The tactical force covers initially an area of 24 km * 21 km, which is equal to approximately 500 km^2. Due to hostile actions outside the initial AOR, four of the units within the tactical force have to move south. The tactical force will after this movement, cover an area of 24 km * 27 km, which is equal to approximately 650 km^2. The other nine units within the tactical force will be stationary. Communications with the highest priority in this scenario are the links between the Battalion Commander and the moving units, which corresponds to the following nodes: Commander Company 3, Patrol 2.3, and Patrol 3.2.

Results

Overall performance:

Statistic	Average	Maximum	Minimum
Ftp Traffic Received (bytes/sec)	4,039.1	4,818.9	0.0
Ftp Traffic Sent (bytes/sec)	4,080.7	4,877.8	0.0

Table 12. Overall throughput for the 3.3 UMTS Network, Scenario 3, extended AOR

Performance for communications with the highest priority:

Battalion Commander to Commander Company 3, Patrol 2-3, and Patrol 3-2

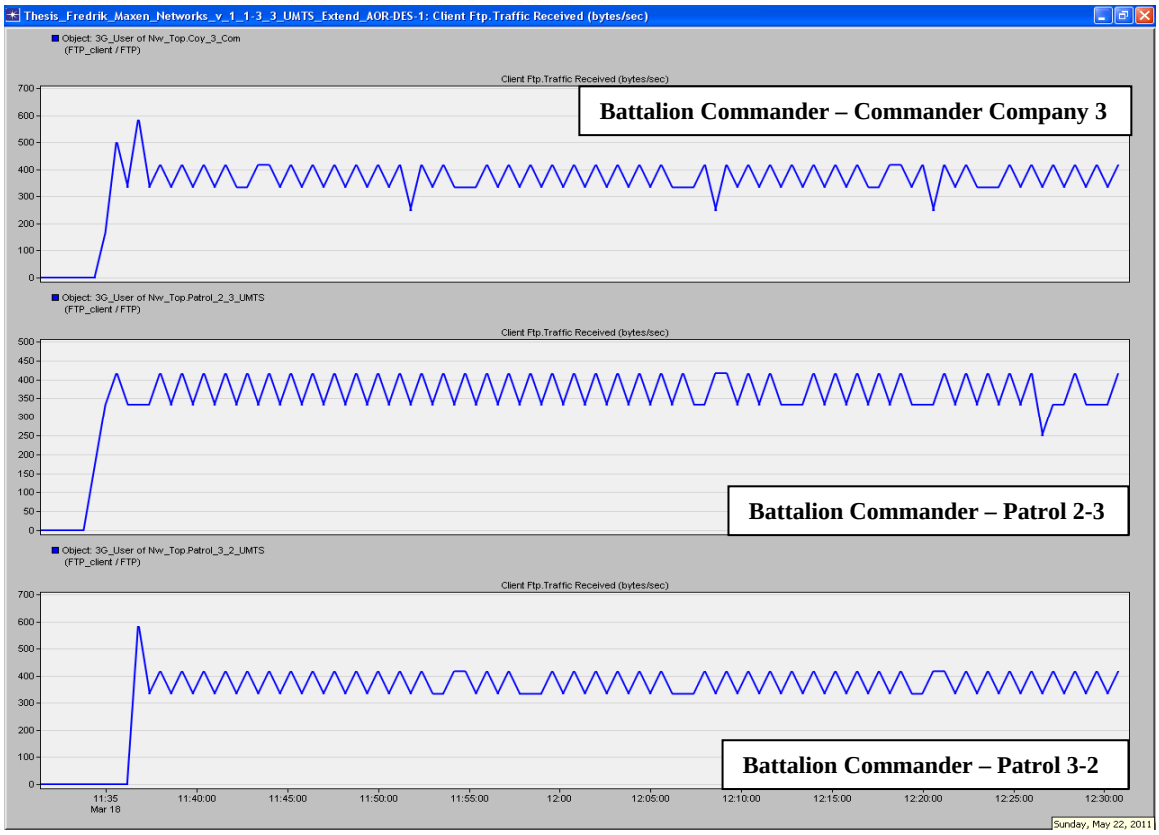

Figure 31. Throughput between nodes with high priority in 3.3 UMTS Network, Scenario 3, extended AOR

Comments

The overall throughput remains high also for the 3.3 UMTS Network, Scenario 3, extended AOR. There is no interference from the base station to links with priority as

occurred in scenario 1. An overall observation for the UMTS Network was that there seems to be a distinct limit for connectivity between the base station and a subscriber. In the SINCGARS and the MANET Networks, a graceful degradation occurs when the links between nodes are extended. A similar graceful degradation of throughput effect could not be observed in the UMTS Network.

I. OVERALL RESULTS FROM THE MODELING

After modeling the networks, the following summary can be accomplished for the various network approaches.

Comment: The throughput measurement is made by sending IERs in the MANET and the SINCGARS network. In the UMTS-model, the default measurement for throughput was done by transmitting data using FTP. Since there is a difference in the method of measurement between the networks, some uncertainties will occur when cross-comparing values for throughput. The tabulated results are therefore based on how each network performed to the different scenarios (see Table 13).

Scenario	SINCGARS	MANET	UMTS
1. Surveillance	Overall high throughput within the network.	Overall high throughput within the network.	Overall high throughput within the network. Interference related to power management occurred for some nodes.
2. Movement within AOR	A decrease in the overall throughput was observed. The overall throughput is still considered as acceptable.	Overall high throughput within the network, slightly decreased compared to the surveillance scenario.	Overall high throughput within the network. Small difference in throughput between links
3. Extended AOR	A significant decrease in the overall throughput was observed. Low throughput for nodes acting in the added area.	Decreased throughput for nodes acting in the added area. The overall throughput is still relatively high.	Overall high throughput within the network. Low ability for graceful degradation is assessed for a UMTS network.

Table 13. Overall results from the modeling

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMPARATIVE EVALUATION AND DISCUSSION OF THE TECHNOLOGIES

The purpose of this chapter is to discuss, compare and evaluate ad hoc networking versus existing infrastructure-based systems. In order to discuss, compare and evaluate these technologies, results from the modeling and simulation in Chapter IV were combined with the information gathered from literature studies in Chapters II and III.

A. CAPACITY

> *The maximum theoretical rate at which data can be reliably transmitted over a given communication path, or channel, under given conditions is referred to as the channel capacity.* [38]

According to the modeling and simulation performed in this thesis, the result shows that a MANET, in general, can provide good throughput. An ad hoc network can be assessed to perform at a data rate to approximately 1 Mbps.

The throughput that can be provided in a UMTS network should also be considered as high. The modeling and simulation shows that it is possible to achieve a data rate exceeding 400 kbps between a base station and a node. This level for the data rate in a UMTS network was also confirmed by a subject matter expert at OPNET [39].

When comparing MANET to UMTS, it seems that a higher data rate can be provided in the MANET. In a further perspective, a future 4G system can be expected to provide a data rate that will equal, or even exceed, what can be achieved with a MANET solution. The modulation form Orthogonal Frequency Division Multiplexing (OFDM), which can provide a high data rate and handle many different types of users, is the preferred standard method for handling both 4G networks as well as in next-generation waveform development for military ad hoc networking such as the Wideband Networking Waveform (WNW).

B. MOBILITY AND FLEXIBILITY

In this thesis project, the ability to move units within a given Area of Responsibility (AOR), maintaining a sufficient channel capacity, is referred to as mobility.

In terms of providing a mobile and flexible network for a tactical force, both a MANET and an infrastructure-based system such as a UMTS network can obtain an acceptable solution. A MANET does not need to deploy towers and base stations, and can therefore provide an extremely flexible solution which can be rapidly deployed. Data rates are generally acceptable, and expected to improve in future implementations.

According to the modeling and simulation in this thesis, a MANET supported a tactical movement within the required AOR without causing any significant decrease in the required throughput. When extending the AOR, as was observed in the simulations, there will be a significant throughput decrease to the nodes that act in the far extremes of the covered area. This phenomenon conforms to the basic idea for an ad hoc network. Since all nodes act as relay elements between each other, there have to be a certain amount of nodes covering the whole area in order to establish reliable connectivity between all nodes. Therefore, nodes have to be equally distributed throughout the AOR in order to establish good connectivity between nodes.

A network based on UMTS technology requires significant and extensive infrastructure. This means that prior to the point in time when the network can first be used, an initialization phase has to be conducted, where base stations and towers are deployed and checked out. This resource requirement decreases the ability for the tactical force to immediately act when entering an AOR. Since one of the most important abilities in maneuver warfare is to maintain the initiative, this time delay can prove to be a severe limitation when using infrastructure-based systems. When the infrastructure is in-place, an UMTS network can be expected to provide valuable flexibility for the nodes that move within the AOR. When extending the AOR and nodes reach the extreme limits for their

transmission range, the connectivity rapidly decreases. In a scenario where the AOR needs to be extended, new base stations must be deployed. Alternatively, one could possibly regroup already deployed base stations.

When comparing the two technologies, a MANET solution seems—from the author's perspective—to provide the best flexibility and mobility for a tactical force. If the AOR is extended to the limits of the transmission range, it will certainly adversely affect the flexibility. Some nodes have to remain in certain positions in order to act as relays between other nodes. An infrastructure-based system requires a period of time to deploy all towers and base stations before the network can be used by the tactical force. When the infrastructure for a UMTS network is well in place, this solution can be expected to provide a sufficient flexibility within the AOR.

From the author's perspective, a combination of the two technologies could give the best support for both flexibility and mobility. A wireless system that is based on ad hoc networking, but enforced with some additional base stations, would give a solution that provides a high level of performance in terms of flexibility and mobility.

C. ROBUSTNESS

In this thesis project, *robustness* is referred to as the ability to maintain a sufficient channel capacity, under given conditions, when a communications system is affected by external factors such as jamming and physical manipulation.

When conducting the modeling and simulation of the network technologies in this thesis project, it was not possible to test the simulations in a jammed environment. For example, when attempting to jam in the MANET simulation, the jammer did not provide the simulations for the expected effect and for the UMTS there was no jamming model available. The UMTS network uses CDMA as modulation in combination with a direct sequence spread-spectrum technique. With this configuration, the assumption that can be made for the UMTS network is that the modulation used provides some level of protection in terms of resistance against jamming. There is a risk though that those different nodes can interfere with each other since they all use the same frequency and PN sequence. This can cause network nodes to unintentionally jam each other. The power

management function in a distributed UMTS network is important in order to balance the output power and adequately support all nodes. If this is not done properly, the nodes will interfere with each other.

Since it was not possible to simulate a relevant jamming scenario, the modeling and simulation effort could not provide a robustness result showing how the MANET responded to a jammed environment. Information about how ad hoc networking waveforms, such as Wideband Networking Waveform, respond to jamming has not been publicly released, and is therefore unavailable. The assumption made is that modern waveforms for ad hoc networking developed today contain some type of spread-spectrum technique that establishes a level of resistance against jamming. There are too many uncertainties to compare ad hoc networking versus infrastructure-based system in terms of resistance against jamming; therefore, no distinct conclusion can be made at this time.

Network security is another important issue when discussing vulnerabilities in different types of technologies. The information that is required by the tactical force can be affected in the security aspects of availability, integrity and confidentiality.

In ad hoc networking, all nodes have equal status, which means that the hierarchy for the level of security will be flat across the network. Every node will have equal vulnerability and therefore must be provided with the same level of security. If one node is compromised, the information in the network can be affected in almost all security aspects. Information can be denied and therefore not available for authorized users. Data can be manipulated and modified to affect the integrity of the information. Sensitive information can be revealed and thus, for example, affect the confidentiality of an operation. An ad hoc network therefore needs the presence of strong security mechanisms for the entire network. The first layer of protection should be to establish physical protection for the nodes to form a baseline for the overall protection of the network. In the next layer of protection, an Intrusion Detection/Prevention System (IDS/IPS) should be implemented in order to deny an intruder wireless access to the network.

An infrastructure-based system like UMTS is more centralized, and the vulnerability and the level of security will therefore not be equal across the entire network. The most vulnerable network elements will be the base stations. Because of their importance, the base stations in the network must be provided with especially strong physical protection. This means the tactical force resources have to be submitted to protect the base stations continuously. Similar to an ad hoc networking system, an infrastructure-based system must also be provided with IDS/IPS. However, due to the centralized hierarchy in an infrastructure-based system, the protection against wireless intrusion is probably less complex compared to a MANET.

D. INTEROPERABILITY

> *Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.* [40]

The term *interoperability* has to be discussed from a broad perspective in order to take all aspects into consideration. In this thesis, the focus is on discussing the technical interoperability when comparing ad hoc networking versus infrastructure-based system.

One of the objectives of the JTRS project in the United States and the GTRS project in Sweden was to develop a unified and "joint" approach for future wireless communications. Earlier developments had a "stove-piped" approach, where the Army, the Navy and the Air Force developed their own systems. This lack of cooperation between services resulted in limited interoperability, even between forces within the same nation. The mainstream plan for developing tactical wireless communications systems that most Western countries follow today is the software defined radio (SDR) approach with similar projects as JTRS and GTRS. These facts impact the perspective of interoperability. When most countries focus their development based on military exclusive SDR, it would be hard, in terms of interoperability, to go in any other direction and procure infrastructure-based civilian systems. In the framework of these military SDR-based projects, many countries develop waveforms that will support ad hoc networking, similar to the American Wideband Networking Waveform. At the same time,

the aspect of interoperability is more complex. Just because many countries have a similar approach and cooperate in SDR projects does not guarantee interoperability. There are many actors in this domain, some of them with strong economic and financial interests. It can be complicated to get all these actors to agree on standards and on their choice of technologies to ensure interoperability objectives are met.

Since infrastructure-based systems are mainly developed for civilian networks and communications solutions, the interoperability with military systems is limited. Within the perspective of interoperability looking into today's Peace Support Operations, there are many civilian actors that do not have exclusive military communications. The common base for cooperation and coordination between civilian actors and military forces could be an infrastructure-based system similar to the UMTS network used in this thesis project. Since cellular phone systems like 3G are so common in today's society, and almost everybody is comfortable with this technology, there will be much common use and a resulting short startup time for training people.

Comparing the ad hoc networking versus infrastructure-based systems in the perspective of interoperability, the ad hoc networking will be preferred. The SDR-based projects are the mainstream path for developing wireless communication for military use today. The author assumes that the standards used in civilian networks such as 3G and 4G can be implemented in the waveforms developed for JTRS and GTRS. A military force could then, in a Peace Support Operation, easily and conveniently switch to a 3G or 4G waveform if needed.

E. COST AND ECONOMY

Cost is a major factor to be considered when studying different tactical network solutions. In this thesis project, the cost perspectivewas not chosen to be the primary focus. However, the cost perspective is still a real-life issue and is therefore discussed. In order to make a comparison between ad hoc networking and infrastructure-based systems costs, information was gathered from the Swedish GTRS project and the Ericsson QuicLink system. When comparing these two, the results show that buying an infrastructure-based system like QuicLink seems to be a solution that is much less

expensive than procuring the Software Defined Radios through GTRS. The main reason GTRS is more expensive is that the development cost is included in the total cost. When comparing systems through an economic analysis, in a GTRS perspective, it is hard to set the limit of what should be included in the calculation of cost. As previously mentioned, the greatest impact of the cost calculation is most likely the cost for development, which is extremely difficult to characterize. When buying an existing system like QuicLink, the development cost will be shared between many actors. Since a system like QuicLink is based on existing 3G/UMTS technology, most of the development cost has already been funded. In contrast, when developing a unique military system like the JTRS or the GTRS, the cost for developing the system will not be shared by so many actors; most likely the sole actor will end up being the military community alone.

In this thesis project, the author chose not to present any specific figures for the different communications solutions due to the complexity of which factors should be considered for calculating cost. The conclusion can still be made that it is much more expensive to develop a unique military software-defined radio system than it is to buy an existing civilian infrastructure-based communication system like QuicLink. This conclusion is based only on the initial development and procurement costs for a new communication system. No consideration was made for long-term sustainability according to maintenance and upgrades that would be involved for an existing system.

Different technologies, in terms of mobility and flexibility, were previously discussed in this chapter. An infrastructure-based system has some limitations when it comes to mobility and flexibility, and requires a period of time to be operationally deployed. When the system is in place and operating, it can provide the PSO force a sufficient tactical solution. Earlier experiences from PSOs, for example in Kosovo, show that some operations can be very static and there is no need to move units over large areas. In the later part of the Kosovo operation, there has been a great increase of nonmilitary actors within the AOR who also need communications. In this type of scenario, which is more static, an infrastructure-based system like QuicLink could prove to be a cost-efficient communication solution. Another need for communications, which was not taken into consideration, is for management and welfare. To manage bases and

camps in an AOR requires communication. Soldiers who, for the moment, are not performing operations-related duty have to be provided with communications for morale and welfare. Communications for welfare and communications for managing camps and bases require no unique or sophisticated tactical abilities, so an infrastructure-based system could prove to be a highly cost-efficient and suitable solution.

Developing a military-exclusive communication system from scratch is costly. This high expense is due to the need for the military to be leaders in the field, with a state-of-the-art systems that will satisfy all the unique and critical requirements the forces need to perform at the top of their ability on the battlefield.

VI. CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER RESEARCH

A. ANSWERS TO THE RESEARCH QUESTIONS

1. Primary Research Question

From a Swedish perspective, what are the key success factors for a tactical communications solution for a land-based battalion?

To answer this question, the perspective must come from the basic principles for command and control in the Swedish Armed Forces, and how we want to conduct operations. The ruling principle for command and control in the Swedish Armed Forces is maneuver warfare. The key elements in maneuver warfare are initiative, tempo, and command and control by using mission-type tactics or directive control. A tactical communication solution must therefore support the commander and his/her tactical force and adapt to the basic principle of maneuver warfare. The key success factors for the tactical communication solution are the following.

– Provide a sufficient capacity for voice, text, data, pictures and video.

– Provide sufficient mobility and flexibility in order to meet the commanders need for keeping the initiative in any battlefield environment

– Provide sufficient adaptability in order to meet the requirements for interoperability with different actors, both military and nonmilitary. A tactical communications system should also be adaptable in terms of upward compatibility with new emerging technologies.

2. Subsidiary Research Questions

What are the key requirements for a tactical communications system?

This thesis research identified the following key requirements based on a tactical force of battalion size.

- Ability to connect up to 140 nodes
- Provide a minimum data rate at 1 Mbps
- Sustained operational capability (even during degraded service due to operations in hostile environment such as jamming, HPM and EMP)
- Upward compatible with new /emerging technologies
- Adaptable/flexible
  – Applications
  – Environment
  – Existing/available resources

How does ad hoc networking compare to civilian infrastructure-based technologies?

This thesis research shows that both ad hoc networking and infrastructure-based systems can serve as the baseline technology in a tactical wireless communication solution. The ad hoc networking in general is identified as the technology that best satisfies requirements, because the characteristics of the ad hoc networking technology make it highly flexible and mobile. An infrastructure-based system can also be seen as a cost-efficient alternative that can be useful in a more static battlefield.

In this thesis project, the comparison between ad hoc networking versus infrastructure-based systems was based on simulations in JCSS/OPNET. The author would like to emphasize that the conclusions made are therefore based on results from these simulations and not from real-life, full-scale tests with hardware.

What recommendations from this study can be made to the Swedish Armed Forces for developing wireless communications systems beyond the ongoing Software Defined Radio Program (GTRS)?

The path already taken by the Swedish Armed Forces—to develop software-defined radios with ad hoc networking capabilities—seems to be the right choice of technology for now and in the near future.

Since much of the development of modern military communication technology goes hand-in-hand with civilian sector developments, there are many similarities. Technologies developed for civilian use will be picked up in the future and used in military applications. An example is the Orthogonal Frequency Division Multiplexing (OFDM) used in 4G systems. Due to its capacity for high data rate, it is also used for modern military ad hoc networking waveforms such as the Wideband Networking Waveform (WNW). Therefore, it should be an ongoing process for development of military communication systems to benchmark against and look into the civilian developments in communications technology.

Developing a military-exclusive communication system is costly. At the same time, a battlefield environment can, in a worst-case scenario, have unique characteristics that require certain abilities for a communications system. The cost of developing military-exclusive communication capability is the price the military has to pay to be at the leading edge. Hopefully, these investments can pay off by making our fighting forces even more efficient on the battlefield.

B. CONCLUSIONS

In this thesis project, the focus has been on comparing ad hoc networking systems with modern infrastructure-based systems in order to determine which system options will be the best technology for future tactical wireless communications solutions for the Swedish Armed Forces.

As the first step in the thesis project, an analysis was accomplished concerning the requirements the Swedish Armed Forces have on their tactical communication systems.

In this context, a study into relevant national doctrinal, strategic and operational, documents was undertaken in order to better define the key requirements for a tactical communications system. These key requirements are based on how the tactical commander needs to command and control subordinated units. The doctrinal principle for command and control in the Swedish Armed Forces is maneuver warfare where the key elements are:

– Initiative

– Tempo

– The use of mission type tactics or directive control

In order to meet the principles for command and control for maneuver warfare, a tactical communications system must be flexible and support high mobility. The principle of using mission-type tactics or directive control requires a high volume of information flow within the tactical communications system. In terms of battlefield services, the tactical communications system should provide a sufficient capacity for voice, text, data, pictures and video. To handle all mission operations, including surge requirements, the tactical communication system also has to be secure and robust, and sustain operational capability even when presented with threat environments such as jamming, HPM and EMP. In today's operations, the tactical force needs to cooperate with other services and with other units from different nations, thus requiring a high degree of interoperability. As previously mentioned, the tactical communication system needs to be flexible and adaptable. In an extended perspective of adaptability, a tactical system must also be upwardly compatible with emerging technologies.

In the next step of the thesis research accomplished in this work, the available technologies for ad hoc networking and infrastructure-based system were analyzed. In the framework of JTRS and GTRS, waveforms are commonly developed to provide ad hoc networking for software-defined radios. The Wideband Networking Waveform (WNW) within JTRS and the Tactical Data Radio System (TDRS) within GTRS are both proven examples of waveforms with ad hoc networking capabilities that will be released in the near future. For infrastructure-based systems, the analysis focused on systems based on

3rd Generation Universal Mobile Telecommunications System (3G/UMTS) technology. An interesting infrastructure-based system that is operational today is the Ericsson QuicLink. The upcoming 4th Generation Long Term Evolution (4G/LTE) technology is interesting, but information about 4G/LTE for field use is currently limited.

In the further analysis of ad hoc networking versus infrastructure-based systems, modeling and simulation scenarios were implemented using the software JCSS/OPNET. A tactical force of battalion size was modeled through three scenarios in the framework of a Peace Support Operation (PSO). When simulating ad hoc networking, a custom-made model in JCSS/OPNET was developed, since no model was released for either WNW or TDRS. When simulating an infrastructure-based system, a model based on 3G/UMTS was used. The result of the ad hoc networking simulation shows an overall high throughput for all three of these scenarios. The throughput decreased for the nodes furthest away when extending the communication to the limits of their intended coverage area. The result of the infrastructure-based system simulation shows a relatively high overall throughput in all scenarios. Some situations of interference were observed. This interference was caused primarily by operating components in the systems itself, which inadvertently jammed some of the subscribers. The location of the base stations for a distributed communications system is essential. This shows the importance of detailed planning when deploying an infrastructure-based system.

As a final step in this thesis project, ad hoc networking was compared to infrastructure-based systems. When analyzing the different technologies in terms of capacity, the two technologies seem to perform equally. Using 4G/LTE technology in future infrastructure-based system can be expected to provide a high data rate.

Analyzing the two technologies in terms of mobility and flexibility, the ad hoc networking is preferred. An infrastructure-based system needs a period of time to be established, which can affect the maneuverability if the operational tempo is high and requires large movements. On the other hand, if the operational scenario is more static, an infrastructure-based system can provide a feasible and robust solution that can provide sufficient flexibility within an AOR.

Most European countries follow the same path as Sweden, and develop software-defined radios in similar projects, like the Swedish GTRS. Many other countries also develop ad hoc networking waveforms that will be used in their SDRs. Cooperation between projects will hopefully create common standards to enhance technical interoperability. Today's PSO scenarios do not consist of military forces only. There will most likely be a significant number and types of nonmilitary actors in future PSOs that do not use military communications. These actors will use the existing infrastructure-based civilian communication systems in the AOR. This makes the term *interoperability* even more complex.

When looking into the cost aspect of the two technologies, the infrastructure-based system is in favor. It is a complex issue of what to include when calculating the cost for tactical communication system. The overall cost for SDRs within the GTRS project is high, because the cost for development is included in the calculation.

The general conclusion when comparing ad hoc networking versus infrastructure systems is that the ad hoc networking approach best satisfies the identified requirements. The ad hoc networking provides a level of mobility and flexibility, which is important when conducting operations in a maneuver warfare approach. Maneuver warfare is a high priority for Swedish forces based on doctrinal preferences. An infrastructure-based system will most likely provide a cost-efficient communication solution in an operational/tactical scenario that is more static. An optimal solution would be to take the best of two worlds and make a hybrid system. Adding infrastructure in the form of base stations to an ad hoc networking tactical communication will provide an even higher flexibility, and further increase the robustness in the system.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

In this thesis project, the focal point has been on the battalion level as the tactical force. For future research, it could be both valuable and interesting to lower the perspective view and study the possible military use of infrastructure-based communications within forces smaller than a battalion. It could also be interesting to look

into the details associated with possible use for infrastructure-based systems to interconnect and effectively pull information from sensors.

When the JCSS/OPNET models for WNW and TDRS are available, they could also be interesting for additional research. JCSS/OPNET is a useful tool to simulate communication solutions in different combat environments.

When conducting the modeling and simulation in JCSS/OPNET for this thesis project, the default settings for measurements required the use of inconsistent network approaches. For future research, it could be interesting to investigate whether it would be possible to modify the JCSS/OPNET models for the actual network approaches in order to achieve a better measurement correlation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] W. Stallings, *Wireless Communications & Networks – 2nd Edition*. Upper Saddle River: Pearson Prentice-Hall Publishing, 2005.

[2] "Joint Tactical Radio System Programmable, Modular Communications System," http://www.globalsecurity.org/military/systems/ground/jtrs.htm

[3] "JPEOJTRS, About the Enterprise," http://www.public.navy.mil/jpeojtrs/Pages/about.aspx

[4] "Joint Tactical Radio System, Ground Mobile Radios (JTRS GMR)," http://www.boeing.com/defense-space/ic/jtrs/docs/JTRS_GMR_overview.pdf

[5] "Airborne and Maritime / Fixed Station Joint Tactical Radio Systems (AMF JTRS)," http://www.lockheedmartin .com/products/amf-jtrs/

[6] "Joint Tactical Radio System (JTRS)," http://www.thalescomminc.com/jtrs.asp

[7] J. McHale, "FPGAs enable SDR applications," *Military & Aerospace Electronics*, October 2010.

[8] "GTRS – Common Tactical Radio System The Armed Forces´Perspective, " Presentation from the Swedish Armed Forces, Major Kjell Lantto.

[9] The Swedish Armed Forces, *Strategic development plan*, Stockholm: "Author", 2011.

[10] The European Union, *A Secure Europe In A Better World – European Security Strategy*, Brussels: Author, 2003.

[11] The European Union, *Draft Declaration on Strengthening*, Brussels: Author, 2008.

[12] The Swedish Armed Forces, *Military Strategic Doctrine*, Stockholm: Author, 2002.

[13] Carl von Clausewitz, *On War*. Stockholm: Bonnier, 1991.

[14] The Swedish Armed Forces, *Doctrine for Joint Operations*, Stockholm: Author, 2005.

[15] J. Boyd, *Patterns of Conflict*: Author, 1986.

[16] "Intro to Command and Control," class notes for CC3000, Naval Postgraduate School, December 2010.

[17] D. S. Fadok, *John Boyd and John Warden – Air Power's Quest for Strategic Paralysis*, Alabama: Author, 1995.

[18] The Swedish Armed Forces, *Procurement Document for GTRS*, Stockholm: Author, 2009.

[19] The Swedish Defence Materiel Administration (FMV), *Tactical Data Radio System (TDRS) – Specification*, Stockholm: Author, 2003.

[20] "JTRS SINCGARS Waveform Development Overview," http://www.assurancetechnology.com/SINCGARSover.asp

[21] R. North, N. Browne, L. Schiavone, *Joint Tactical Radio System – Connecting the GIG to the Tactical Edge*, San Diego: 2006. (Paper, Military Communications Conference Washington DC 23-25 Oct 2006).

[22] "Wideband Networking Waveform," http://www.nova-eng.com/Inside.asp?n=Services&p=WNW

[23] "Rifleman Moves Information Sharing to The Front of Operations," http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1745&zoneid=243

[24] "JTRS handheld, manpack, and mobile military radio versions enter government test phase," http://www.militaryaerospace.com/index/display/article-display/7272532471/articles/military-aerospace-electronics/online-news-2/2010/9/jtrs-handheld__manpack.html

[25] "TETRA," http://www.tetramou.com/tetramou.aspx?ID=6376

[26] R. Iovine, J. Bouis, *The FlexNet-Waveform in the International SDR Arena*, Rockwell Collins, 2009.

[27] O. Cengiz, *Adaptive, Tactical Mesh Networking: Control Base Manet Model*, NPS-Thesis, Monterey: 2010.

[28] K. Sarkar, *Ad Hoc Mobile Wireless Networks, Principles, Protocols and Applications*, Boca Raton: 2008.

[29] Mobile Ad Hoc Network, Figure: http://www.freepatentsonline.com/7006453.html

[30] E. Osman, *Control-Based Mobile Ad hoc Networks (CBMANET)*, DARPA, 2006.

[31] OECD (DSTI/ICCP), *Development of Third-Generation Mobile Services in the OECD*, 2003.

[32] "Advanced Interdisciplinary Studies in Electrical and Computer Engineering," class notes for EO4911, Naval Postgraduate School, December 2010.

[33] T. S. Rappaport, *Wireless Communications, Principles and Practice – 2nd Edition*, Upper Saddle River: Pearson Prentice-Hall Publishing, 2009.

[34] Ericsson, *QuicLINK™ Communication Solution Description*, Kista: 2008.

[35] J. Govil, *4G Mobile Communication Systems: Turns, Trends and Transition*, Ann Arbor, MI, India: 2007.

[36] "Information Warfare Networks," class notes for IW3502, Naval Postgraduate School, May 2011.

[37] The Swedish Armed Forces, *Order of Battle for Nordic Battle Group 2011 (NBG11)*, Stockholm: Author, 2010.

[38] W. Stallings, *Data and Computer Communication –9th Edition*. Upper Saddle River: Pearson Prentice-Hall Publishing, 2011.

[39] Meeting at OPNET Bethesda April 2011: Alejandro Talavera, subject matter expert on UMTS.

[40] "Defense Acquisition Guidebook," https://acc.dau.mil/CommunityBrowser.aspx?id=334026

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Department of Information Sciences
   Monterey, California

4. Alex Bordetsky
   Department of Information Sciences
   Monterey, California

5. Lt. Col. Terry Smith
   Department of Information Sciences
   Monterey, California

6. Lt. Col. Fredrik Maxén
   Swedish Armed Forces
   Stockholm, Sweden

7. Steven Crum
   Department for Information Systems Agency
   Fort Meade, Maryland

8. Imran Umar
   Department for Information Systems Agency
   Fort Meade, Maryland

9. Chris Miller
   Department for Information Systems Agency
   Fort Meade, Maryland

10. Prasanna Sukumar
    OPNET
    Bethesda, Maryland

11. Varun Lalchandani
    OPNET
    Bethesda, Maryland

12. Alejandro Talavera
OPNET
Bethesda, Maryland