



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**THE TACTICAL NETWORK OPERATIONS  
COMMUNICATION COORDINATOR  
IN MOBILE UAV NETWORKS**

by

Kristina S. Jeoun

June 2004

Thesis Advisor:  
Second Reader:

Alex Bordetsky  
Russell Gottfried

**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 June 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: The Tactical Network Operations Communication Coordinator in Mobile UAV Networks			5. FUNDING NUMBERS	
6. AUTHOR(S) Kristina Jeoun			8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			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.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words)				
<p>Warfare planners and tacticians are seeking ways to leverage information technology to gain advantage on the battlefield. With the advent of Internet technologies, complex systems are becoming more networked, and access to information is more critical than ever. The increasing utilization of special operations forces in ad hoc, dynamic operations poses a need for adaptable communications to support the unit. Effective communication within the unit and critical information exchange with the command center affect the overall outcome of the mission. An adaptive, mobile network with UAV relays is well-suited to support the ad hoc nature of special operations.</p> <p>The area of research for this thesis is the role of the tactical network operations communication coordinator in mobile UAV networks. The coordinator's purpose is to oversee the management and status of the network and provide feedback to network participants, thus resulting in an effective and well-functioning environment. The tactical network coordinator is an important and integral part of network operations by establishing what is known as network awareness. This thesis will be a model for sharing network awareness, and it will explore the potential benefits of incorporating network performance as a planning objective rather than a constraint.</p>				
14. SUBJECT TERMS Mobile networks, network management, UAV, special operations forces, network awareness			15. NUMBER OF PAGES 69	
			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 UL	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**THE TACTICAL NETWORK OPERATIONS  
COMMUNICATION COORDINATOR IN MOBILE UAV NETWORKS**

Kristina S. Jeoun  
First Lieutenant, United States Air Force  
B.A., University of Colorado, 2002

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2004**

Author: Kristina S. Jeoun

Approved by: Alexander Bordetsky  
Thesis Advisor

Russell Gottfried  
Second Reader

Dan C. Boger  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Warfare planners and tacticians are seeking ways to leverage information technology to gain advantage on the battlefield. With the advent of Internet technologies, complex systems are becoming more networked, and access to information is more critical than ever. The increasing utilization of special operations forces in ad hoc, dynamic operations poses a need for adaptable communications to support the unit. Effective communication within the unit and critical information exchange with the command center affect the overall outcome of the mission. An adaptive, mobile network with UAV relays is well-suited to support the ad hoc nature of special operations.

The area of research for this thesis is the role of the tactical network operations communication coordinator in mobile UAV networks. The coordinator's purpose is to oversee the management and status of the network and provide feedback to network participants, thus resulting in an effective and well-functioning environment. The tactical network coordinator is an important and integral part of network operations by establishing what is known as network awareness. This thesis will be a model for sharing network awareness, and it will explore the potential benefits of incorporating network performance as a planning objective rather than a constraint.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	HISTORY OF COMPLEX AND DYNAMIC SPECIAL OPERATIONS.....	4
1.	Vietnam.....	4
2.	Operation Enduring Freedom (OEF) .....	5
B.	TECHNOLOGY & RESOURCES.....	5
C.	ENVIRONMENT.....	7
D.	STRATEGY.....	8
II.	THE TACTICAL NETWORK OPERATIONS COMMUNICATION COORDINATOR MODEL.....	11
A.	NOC MANAGEMENT .....	11
B.	THE INFERENCE PROCESS .....	12
1.	DSS Input Grid.....	12
a.	<i>Performance Management</i> .....	12
b.	<i>Fault Management</i> .....	13
c.	<i>Configuration Management</i> .....	15
2.	Situational Awareness .....	16
C.	THE KNOWLEDGE ACQUISITION PROCESS.....	17
1.	Knowledge Base Evaluation.....	18
2.	Network Awareness.....	19
D.	TNOCC MODEL.....	21
E.	OTHER ROLES AND RESPONSIBILITIES.....	22
1.	NOC Plan of Operation and Coordination .....	23
2.	Network Data Collection.....	23
3.	Personnel Training .....	23
F.	TNOCC MEASURES OF EFFECTIVENESS .....	24
G.	NETWORK CONSTRAINTS .....	25
1.	Bandwidth .....	25
2.	Signal Range.....	26
3.	Number of Nodes.....	26
4.	Enemy Defense .....	26
5.	Environment.....	27
6.	Time .....	27
7.	Operational Ramifications .....	27
III.	EXPERIMENTAL ANALYSIS OF THE TNOCC AT STAN 6.....	29
A.	STAN 6 EXPERIMENT OVERVIEW .....	29
1.	Long-Haul Air Network w/ UAV Relay .....	29
2.	Long-Haul Ground Network/OFDM 802.16.....	30
3.	Mesh Sensor Cell Network.....	31
B.	RESOURCES AND TOOLS.....	32

1.	SolarWinds Network Performance Tool™ .....	33
2.	AirMagnet™ .....	33
3.	OPNET Modeler and ACE™ .....	33
C.	TNOCC MODEL AT STAN 6 .....	34
1.	Inference Process Inputs .....	34
a.	<i>Performance Management</i> .....	34
b.	<i>Configuration Management</i> .....	36
c.	<i>Fault Management</i> .....	37
2.	Knowledge Base Comparison .....	38
D.	ANALYSIS OF TNOCC ACTIONS.....	39
1.	UAV Airborne Network Example .....	39
2.	Mesh Networking Example .....	41
V.	CONCLUSION .....	45
A.	SUMMARY .....	45
B.	RECOMMENDATION FOR FURTHER RESEARCH.....	47
C.	CONCLUSIONS .....	47
	APPENDIX: LIST OF ACRONYMS.....	49
	LIST OF REFERENCES.....	51
	INITIAL DISTRIBUTION LIST .....	53

## LIST OF FIGURES

Figure 1.	UAV Network Structure .....	7
Figure 2.	Inference Process Model.....	17
Figure 3.	Knowledge Acquisition Process Model.....	19
Figure 4.	Complete TNOCC Model.....	22
Figure 5.	UAV Network Diagram (Courtesy of Captain Trey Blacklock) .....	30
Figure 6.	OFDM Network Diagram (Blacklock).....	31
Figure 7.	Mesh Network Diagram (Blacklock).....	32
Figure 8.	Bandwidth Gauges™ .....	35
Figure 9.	SNMP Real-Time Graph™ .....	35
Figure 10.	IP Network Browser™ .....	36
Figure 11.	Routing Table .....	37
Figure 12.	SolarWinds Network Monitor™ .....	38
Figure 13.	UAV Input Before Action.....	40
Figure 14.	UAV Input After Action.....	41
Figure 15.	Overhead Shot of Tacticomp Configuration.....	42
Figure 16.	192.168.1.217 Tacticomp w/ No Connectivity .....	43
Figure 17.	192.168.1.217 Tacticomp w/ Connectivity .....	44

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	TNOCC MOEs.....	46
----------	-----------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

Thank you Dr. Bordetsky for involving me in the STAN experiments. I learned a lot about the NOC from the experience. I admire and respect the passion you have in your research. Thank you for your wisdom, positive attitude, and kindness.

LCDR Gottfried, thank you for your patience with me throughout this entire process. Your drive for excellence is unwavering, your pursuit for knowledge inexhaustible. Thank you for your encouragement and your guidance. You gave me a wider perspective and an appreciation for the operational side of the network.

Thanks to the GIGA team, especially LCDR Eric Bach, LT Ryan Blazeovich, and Axel Schumann for your help during STAN. Thank you Captain Trey Blacklock for creating the network diagrams.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

“War is a product of its age. The tools and tactics of how we fight have always evolved along with technology.” (Alberts) Today, warfare planners and tacticians are seeking ways to leverage information technology to gain advantage on the battlefield. With the advent of Internet technologies, complex systems are becoming more networked and connected, and access to information is more critical than ever. Although the advantages of an interconnected world are numerous, the U.S. military is wary of the impact of a networked enemy. Recent history has proven that most adversaries could not contend with the United States in a major, conventional war, as evidenced in the Persian Gulf War in 1991. Instead, they have chosen to wage more unconventional forms of conflict like guerrilla warfare and terrorism.

The way these adversaries fight is characterized by the term netwar, in which they use and depend on network forms of organization, doctrine, strategy, and communication. (Arquilla) The enemies are no longer necessarily hierarchical nation-states; they may be both subnational and transnational in scope with decentralized and dispersed decision making. So far, this type of enemy has had a major impact and has proven to be an ongoing challenge for the U.S. military. (Arquilla) Unclear threats from undefined transnational groups can strike against a dominant military power by finding vulnerabilities, as witnessed by the United States on September 11, 2001.

To combat this networked threat of adversaries, the U.S. military is changing the way it organizes and fights. A fundamental shift from platform-centric warfare to network-centric warfare (NCW) is transforming the military into a more lethal force “by networking sensors, decision makers, and shooters to achieve shared awareness.” (Alberts) Combat power is realized when the right entities have the correct type of information at a precise moment. NCW attempts to utilize the advances in information technology to better link the knowledgeable entities in the battlespace to achieve combat power. (Alberts)

One key component of NCW is the utilization of special operations forces (SOF). US Special Operations Command (USSOCOM) defines special operations as the use of small units in direct or indirect military actions that are focused on strategic or operational objectives, requiring units to combine specialized personnel, equipment, training or tactics that exceed the routine capabilities of conventional forces. (JP 3-05) Unconventional warfare (UW) is one of the principal missions of SOF, and it is defined as those operations conducted by indigenous or surrogate forces that are organized, trained, equipped, supported, or directed by an external source. (Adams) Examples of UW include guerrilla warfare, covert, or clandestine operations as well as humanitarian efforts, complex emergencies, insurgency and counterinsurgency, and some forms of subversion, sabotage, and similar activities.

While the missions listed above are explicit, how SOF coordinate and execute is not as straightforward. Using the U.S. Army Special Forces A-Team as a prime example, the basic SOF team structure breaks down as follows. An officer leads the twelve-man team, a warrant officer is second in command, and the remaining NCOs are trained in five functional areas: weapons, engineering/demolitions, medicine, communications, and operations/intelligence. ([www.specialoperations.com](http://www.specialoperations.com)) Despite the specialized skills of particular members, the entire team is cross-trained in the required areas to perform different types of special operations.

The dynamic nature of SOF missions requires a highly adaptive, ad hoc organization and mindset to carry out tasks across the entire spectrum of conflict. The SOF team is successful because it relies on small unit proficiency to apply skills with adaptability, improvisation, innovation, and self-reliance. (JP 3-05) Effectiveness of the unit depends on contingency planning, rehearsal, flexibility, and command and control (C2).

The C2 organization structure of the SOF depends on specific objectives, security requirements, and the operational environment. (JP 3-05) At the top level, depending on the SOF chain of command, the unit may be placed under

the theater special operations command, joint special operations task force, or other component commanders of a joint force. At the tactical level, the tactical operations center (TOC) directly oversees and guides the mission requirements of the SOF operation.

The ability for the SOF to communicate within the team and to the TOC is essential because the accuracy and timeliness of information flows directly affect the performance of the team. Essential information includes force disposition, mission status, surveillance and reconnaissance data, unexpected occurrences, and changes to the plan, which are relayed back to the command center. The communication network that supports the C2 system is congruent to the ad hoc nature of the SOF and aligns with its tasks and activities. The network is adaptable to the changing needs and circumstances characteristic of SOF operations. It supports the dynamic unit and empowers the soldier to accomplish the mission more easily and effectively.

A solution for the communication requirements to enable C2 is the utilization of mobile wireless networks with UAV relays to increase the effectiveness of a SOF unit. The network operations center (NOC) facilitates the communication channels between the TOC and SOF by managing and controlling the information systems in the network.

The C2 system can be collectively viewed as an organization in the sense that it takes input from the surrounding environment, subjects it to a transformation process, and produces some type of output to fulfill the particular mission. The performance of the SOF is shaped by the interplay of many social and technical factors that influence the input and transformation processes that result in the output. (The Congruence Model) To increase and/or optimize the performance of the organization, it is necessary to fully understand the behavioral processes and performance issues that govern the C2 structure. However, the dynamics of the organization are complex, and it may be helpful to decompose the system into manageable parts.

The remainder of this chapter focuses on four main categories of input that affect the C2 system of the SOF and ultimately affect the mission and outcome: history, technology and resources, environment, and strategy.

## **A. HISTORY OF COMPLEX AND DYNAMIC SPECIAL OPERATIONS**

### **1. Vietnam**

In mid 1970, U.S. intelligence revealed the presence of as many as fifty prisoners-of-war (POW) in a small compound at Sontay in North Vietnam. (Vandenbroucke) By that time, more than fourteen hundred U.S. servicemen were classified POW or missing in action (MIA) in Southeast Asia. The issue was a growing concern for the National Command Authority (NCA). The idea of a rescue mission presented itself as a timely opportunity to alleviate concerns and bring the POWs home.

A complex plan was forged by top-level special operations leaders involving handpicked personnel from a number of organizations that typically had not operated together, including Air Force Special Operations Forces, Army Special Forces, the Defense Intelligence Agency (DIA), as well as members from the Central Intelligence Agency (CIA). Despite months of preparation, extensive contingency planning, and numerous rehearsals, the rescue forces arrived to an empty camp and a fruitless end.

As it turns out, while the execution date drew near, questions arose over intelligence regarding the presence of any POWs in the camp. But the mission remained a “go” because of the possibility and the hope that the POWs were still there. Despite continuous communication between the command post in South Vietnam and the raiders at every stage of the operation, there was inadequate reconnaissance and intelligence feed for the command post to relay to the SOF. As a result, one helicopter crew mistakenly landed at the wrong location, and the other crew landed at the empty compound.

The Sontay operation was unsuccessful due to uncertainty and doubt in the intelligence input received at the command center. In the decision-making process, the commanders and tactical planners examined the situation and

executed the rescue mission with considerable risk. Sontay is a good example of the unforeseen changes that occur in special operations and the need for better data-capturing technology and mobile communication networks to support the ad hoc environment.

## **2. Operation Enduring Freedom (OEF)**

In response to the World Trade Center attacks, the US military organized and conducted missions against terrorist training camps in Afghanistan to topple the Taliban and prevent al Qaeda from being able to operate the camps. Their missions included locating and capturing Taliban terrorists, designating terrorist camps for attack by US aircraft, assisting indigenous anti-Taliban forces, and performing clandestine reconnaissance missions. (Gresham) The land's countryside and mountainous terrain significantly complicated military operations, especially for conventional forces, as evidenced by the Soviets in the 1970's and 1980's. When US Special Forces took action during OEF, Afghans, such as the Northern Alliance, proved to be valuable partners.

The Army SF teams known as Operational Detachment Alphas (ODAs or A-teams) deployed to Afghanistan and operated with CIA operatives and Afghan warlords. Members of the Northern Alliance were eager to defeat the Taliban, and their efforts aided the A-teams in finding targets for the bombers and fighters overhead. At times, the SOF found themselves in bizarre situations "where one minute they might be watching a cavalry charge by AK-47-wielding Afghans against Taliban tanks, and the next calling in a JDAM strike from horseback." (Gresham, 2003) One soldier recalls the moment when an Afghan warlord approached on horseback as a scene from "Lawrence of Arabia."

In the mountainous terrain of Afghanistan, the SOF proved to be a significant asset in ground operations because they were able to adapt to an unfamiliar and harsh environment and cope with uncertain circumstances.

## **B. TECHNOLOGY & RESOURCES**

A wireless network that incorporates UAVs is mobile. This characteristic is what makes UAV networks so attractive to SOF units. The ad hoc nature of

SOF means that they move from place to place, and they must have mobile communication technology available to support their efforts anywhere.

For aerial reconnaissance missions, UAVs act as a relay station between the SOF and NOC to observe what is happening on the other side of the “hill”. If there are terrestrial obstacles in the way, UAVs can overcome the barriers more easily than the SOF. UAVs provide better resolution of objects and bypass the potential danger of getting too close. The mobility of the network also allows it to intercept adversary vehicles and maneuver away from attack.

The configuration of the UAV network is a tree-structured wide area network (WAN). Figure 1 represents the nodal connectivity in the network. At the bottom of the hierarchy are ground sensors and mobile ground units. The next level up incorporates the low flying UAVs that act as wireless bridges between the ground nodes. At the top of the hierarchy are the high flying UAVs that act as a top-level router and transmission relay back to the NOC. The long-haul wireless technology is 802.11, and the network is self-healing which indicates that all the nodes can communicate with each other.

With respect to use application, the network supports multipoint video streaming of airborne and ground sensors as well as digital voice, audio, and data communication between the SOF and NOC. The reach of the long-haul wireless technology allows the low flying UAVs to be approximately 10 miles from the SOF. With multiple UAVs, the scalability of the network can be increased, and the SOF unit can venture further away from the NOC. To be responsive, it is essential that the network provides asynchronous transfer, high bandwidth, minimal delay, and flexibility.

Other network resources for the SOF include GPS, PDAs, maps, and radios. But one of the most important resources for the SOF is the NOC because it directs and controls the UAV network that either hinders or improves the operation.

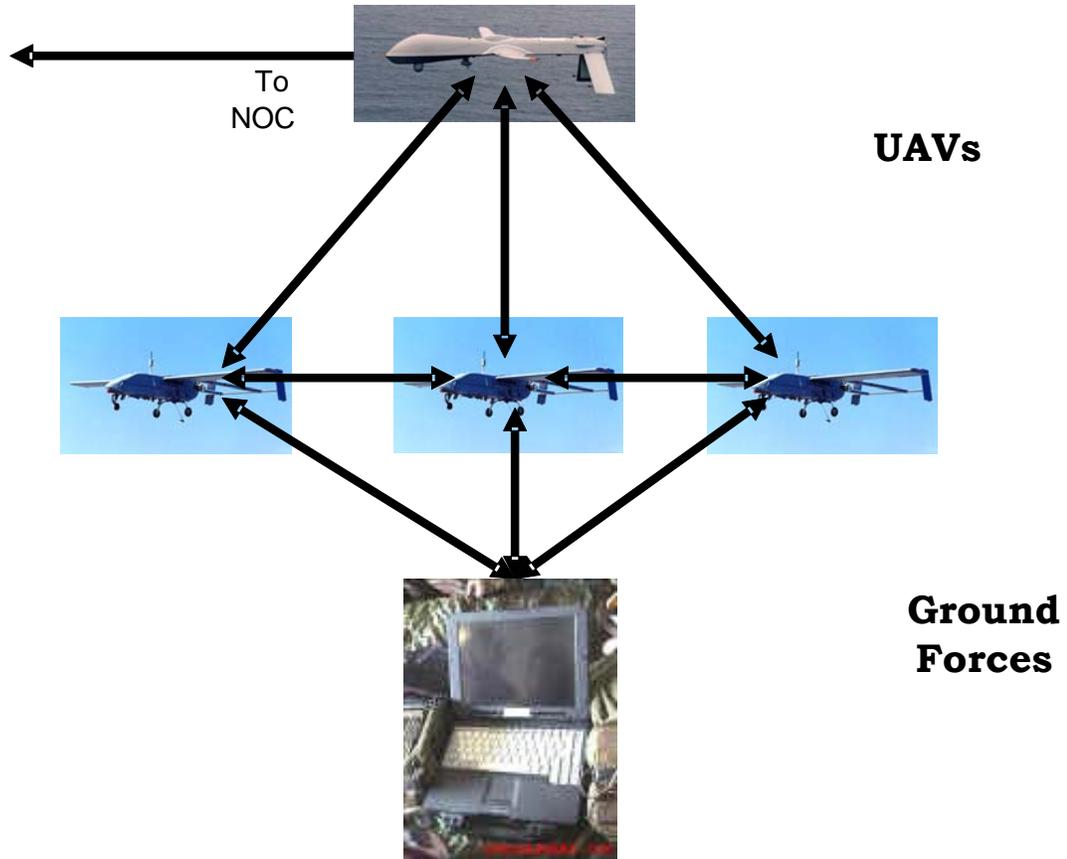


Figure 1. UAV Network Structure

**C. ENVIRONMENT**

The UAV and SOF network exists and is influenced by the surrounding environment, which differs from mission to mission. Specifically in this case, the environment encompasses terrain, weather, and enemy forces-- each potentially having a major impact on the network and mission. These environmental forces can affect the SOF and the network in three ways: by imposing demands, by placing constraints, and by providing opportunities for the two.

A SOF unit can be deployed anywhere, which has different terrain and weather implications on the unit and network. The terrain, especially in a mountainous area, may constrain the line-of-sight required for connectivity between the UAVs and ground units. The terrain then demands reconfiguration of the network-- movement of applicable nodes-- to adapt to the area. The same

constraints apply to weather conditions, which may ground UAVs and also decrease network performance. Conversely, a flat terrain better accommodates a far-reaching network and enables better connectivity.

The presence of enemy forces also hinders the performance of the network and mission. High on the priority list is to protect network assets, including UAVs and ground soldiers, from enemy attack. Movement of UAVs and SOF is limited by where the enemy forces are located, so the network adjusts to avoid the disruption.

It is important to note that there is a network performance balancing act when considering the terrain and enemy opposition. Although a preferred flat terrain optimizes network connectivity, the operational consequences are greater because assets are more vulnerable to attack. In the opposite environment, the network would suffer, but the operational consequences decrease. Because mission success depends on a strong network and protection of assets, careful planning and balancing is required.

#### **D. STRATEGY**

The effectiveness and success of SOF missions is ultimately the number one goal for tactical commanders and network operators. The history of SOF operations has shown a need for adaptable and mobile wireless networks to support the SOF mission. The U.S. military has within its grasp the most advanced technology to serve this purpose. However, a balance is necessary between the objectives of the NOC and the objectives of the mission. It would be nice to optimize network performance but not at the expense of the mission.

The tactical network operations communication coordinator (TNOCC) is the key to achieving this balance. The remainder of this study examines the TNOCC and the effect of actions taken on the network to improve network performance and SOF mission effectiveness. The study addresses questions regarding network performance and the coordinator. It specifies how the role of the tactical network coordinator improves network operations. Chapter II discusses why network awareness is important for mobile networking, and how

the tactical network coordinator contributes to network awareness. Chapter III looks at metrics for the tactical network coordinator and characteristics of factors that influence this performance, as observed during live operations.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. THE TACTICAL NETWORK OPERATIONS COMMUNICATION COORDINATOR MODEL**

It is vital for Special Forces to have the ability to communicate effectively and transmit critical data to the tactical operations center (TOC). The TOC has control of the SOF unit, so they remain in contact with the soldiers to manage the operation. An adaptive, mobile network with small UAV relays is well-suited to support the communication channels between the SOF and the TOC for a number of reasons. The mobility of UAVs enables the SOF to be flexible in its movements, autonomous to a certain degree from the TOC, and dynamic in its actions while supporting the SOF's needs. The management of a mobile UAV wireless network occurs primarily at the NOC. The focus of the NOC is to provide, manage, and improve these communication channels.

### **A. NOC MANAGEMENT**

The goal of the NOC is to enable communications by running and controlling the network environment to help fulfill the SOF mission at hand. This study proposes the role of the TNOCC (aka, the facilitator), who manages the NOC and coordinates efforts and resources to make decisions pertaining to network operations. The NOC is the basic unit of management in a grid, or network-based operations center (Bordetsky, Dolk), and the facilitator is the key player for the coordination of NOC management. The facilitator is faced with the challenge of maintaining a robust network to effectively support special operations to ultimately fulfill the tactical mission at hand.

This chapter analyzes the role of the facilitator and the impact on network operations. To help define the roles and responsibilities of the facilitator, this model illustrates the different facets of input, including the measures of performance (MOPs) of the input, available to the facilitator and how to convert it into actions improving the network and supporting the SOF operator. Communication between the facilitator and the SOF operator creates a feedback loop, an important component of the model. The feedback relationship depends on the knowledge base of each party, which varies and depends on the

knowledge experience of network operations. After defining the facilitator's roles and responsibilities, this chapter lays out the necessary resources and tools characteristic of the operational setting and the factors that constrain network management. After discussing those aspects, the chapter concludes by discussing the facilitator's measures of effectiveness (MOEs).

## **B. THE INFERENCE PROCESS**

Before introducing the model of the facilitator, the processes that govern the facilitator's ability to manage the NOC require definition. The first process is called the inference process, in which the facilitator garners the inputs describing the network operations to make a recommendation or take some action to maintain or improve the health of the network. It is assumed that the network technology used in the model is functioning properly and the data captured by the sensors and presented in the NOC is accurate of the environment.

### **1. DSS Input Grid**

The facilitator's inputs are presented on a grid decision support system (DSS) displayed in the NOC. The input that the facilitator receives from the grid system can be categorized into defined clusters of information. There are five main categories in the network management system: performance, configuration, fault, security, and accounting. (Subramanian) The last two categories are not covered by this study. The clusters in the NOC represent only performance management, configuration management, and fault management. In a military-oriented NOC that supports a network tailored for SOF missions, the DSS presents to the facilitator the types of information to make an informed decision about the network and as a result, the mission.

#### ***a. Performance Management***

The actions of the facilitator have a direct impact on network performance. Because the goal of the NOC is to support the SOF with an adaptable, mobile network, it is important to measure the network's performance as well as the facilitator's effectiveness. A network that shows high measures of

performance indicates a robust and stable one with strong connectivity and mobility. Its performance is the result of actions taken by the NOC to optimize network activity.

Performance management concerns the optimum health of the network, which aims to maximize the bandwidth efficiency of throughput while minimizing latency and packet loss. Throughput is the lifeline of the network. It is the data rate in packets per second of transmission, whether the application is audio, voice, or video data. The throughput of every network device is computed through the data layer, also known as layer two of the OSI network model. (Subramanian)

Network monitoring tools are used to scan a particular subnet to capture all of the devices in the network and monitor the throughput and other MOPs flowing through each device. Specific software tools are discussed in Chapter III.

Throughput is a function of the available bandwidth and depends on other application transmissions taking place at the same time. Bandwidth represents the data capacity of the network. The maximum amount of bandwidth limits the size and speed of data flow and varies depending on the transmission medium. For the wireless 802.11b network, 11 Mbps is the maximum bandwidth capacity.

In the NOC, the DSS reveals network statistics on traffic flow, network availability, and network delay. The NOC monitors traffic data to aid in detecting trends and planning future needs. Performance data on network availability and delay helps the facilitator fine tune the network to ensure connectivity to critical nodes. This is also referred to as link management. The result of performance management is increased reliability and improved response time of the network.

***b. Fault Management***

Fault management, also known as troubleshooting, involves the handling of problems that may arise during network operations. The NOC's task

is to keep abreast of network performance measures to identify the problem and resolve the situation, minimizing the consequences. Two MOPs that indicate problematic nodes in the network are latency and packet loss.

Latency is a measure of the delay as packets travel through the network. High latency, around or above 50 ms, is acceptable but not ideal because the packets are still arriving at their destination but with significant delay. When packets begin to drop off the network, the data is retransmitted, which takes more time and adds to network traffic. The loss of application packets during transmission also degrades the signal quality. Reasons for packet loss include link failure, high network congestion, and misrouting of packets.

Jitter is a MOP to describe the network when it experiences significant delay and high packet loss. It is a problem with voice and video applications because of the choppy effect of the timing of the delivery of packets to the end system. Jitter can be removed by using a buffer to collect the packets and then feed them smoothly to the end system.

Fault management also addresses the operational availability of each node and how it affects the quality of the network. The operational availability of a node is divided into the time it is up and down in the network; they add up to 100%. The percentage of time that a node is up is influenced by many factors such as bandwidth capacity, signal strength, distance from NOC, and weather. The facilitator strives for increased up time of each node to increase network performance.

To counter node problems, the facilitator should take preventative actions. Familiarity with common network problem scenarios and remedies better prepares the NOC to deal with such problems and mitigate hazards to the SOF. Tracking down the causes behind network aggravations is another preventative action.

In the fault management information cluster, the DSS grid displays indications of failure as well as traffic pattern and performance. The NOC

monitors the health of the network, so it is important to know the time a node goes down, where it is located, why it drops off, and how to resolve the problem. The NOC conducts the troubleshooting process in order to flag common network problems and take preparatory and preventative actions.

**c. Configuration Management**

Configuration management reflects the dynamic configuration and status of the network and its components. This cluster of information reveals the topology of the network including the physical location, mobility, routing configuration, and effective design of the nodes in the network. Changes to the network configuration are also displayed. The facilitator should establish a design plan of the network configuration to best support mission objectives.

When troubleshooting, the facilitator can reconfigure or shift network assets to increase network performance and connectivity. For example, when throughput numbers begin to drop and latency and packet loss begin to rise, the facilitator can pinpoint the weak nodes and direct them to a new position. Real-time monitoring shows if the MOPs recovered to better network health.

It is important to note that the NOC's objectives for the network's MOPs are not mutually exclusive. The facilitator's objective may be to increase the throughput of nodes by placing many of them closer to a transmitting receiver, but the result may be increased packet loss due to the increased number of collisions. Also, increasing the number of nodes in the network might remove some traffic burden, so latency and packet loss drop, but the new nodes might capacitate the available bandwidth. Using the DSS, the facilitator's task is to prioritize which MOPs are most critical to the operation and take actions to achieve MOP objectives.

The facilitator does not have the first-hand look at the data coming in from the outside network. Operators at the DSS terminals monitor the clusters of information and filter out the appropriate data that the facilitator needs to make

an informed decision. At times, there may be too much information, and it is up to the operators to filter through the data and present the significant information.

There may be times when the facilitator takes action without the preferred amount or type of network data input. Despite factors such as unforeseen changes to mission requirements, enemy presence, weather, and other factors that the facilitator cannot control, communication supported within the NOC is under control. Effective feedback between the facilitator and the DSS operators creates a collaborative environment that ensures the correct information is channeled to the appropriate party.

## **2. Situational Awareness**

The inference process allows the facilitator to create an accurate situational awareness (SA) picture of the tactical network. SA consists of completeness, accuracy, and timeliness of the input received from the DSS grid. Real-time ability to monitor the network components and understand the state of the networking system is critical for effective management. In a high-paced operation, the facilitator demands complete and accurate understanding of the network environment in order to make good decisions in a limited timeframe.

To achieve SA, the facilitator performs the following tasks: 1) maintain an accurate view of critical node locations and the surrounding environment, 2) identify problems or potential problems that might hinder network performance and mission success, 3) recognize a need for action and decision-making, 4) note deviations in the network and mission, and 5) maintain awareness of the tasks performed and the effects/results. (Shrestha) Figure 2 models the DSS categories of input operated at the NOC and the situational awareness picture of the network created between the facilitator and DSS operators.

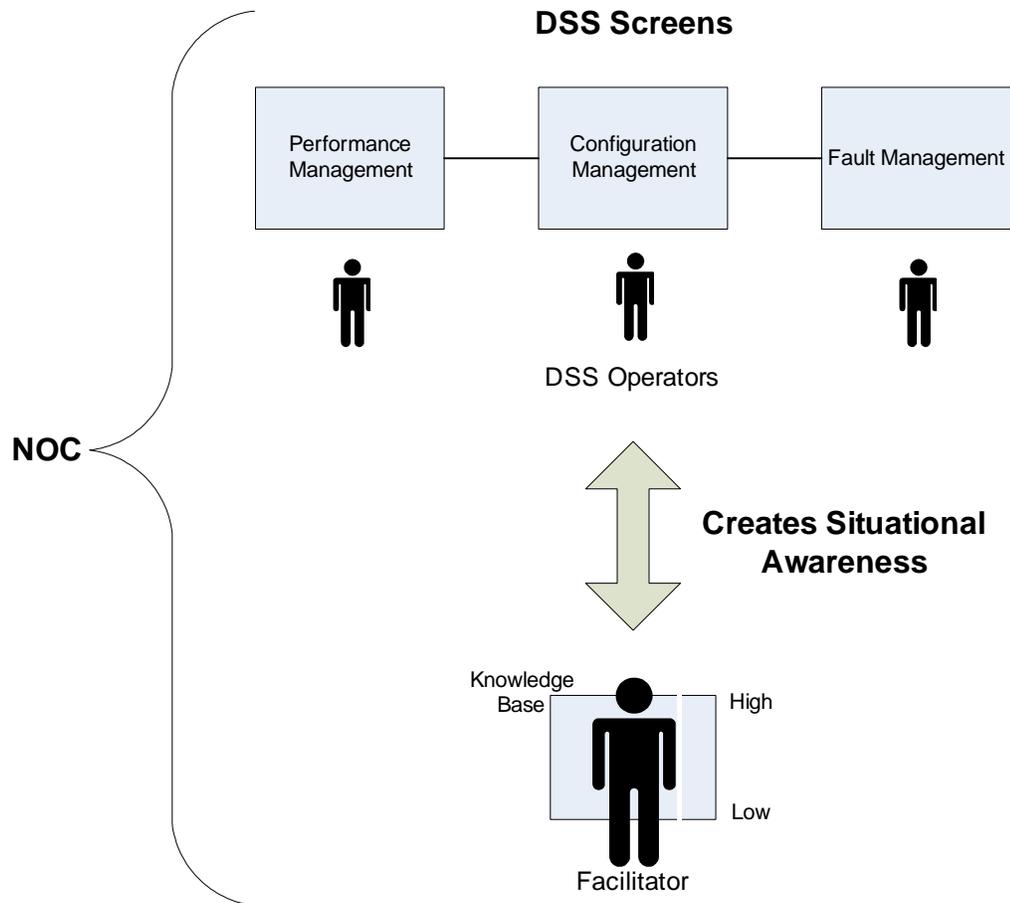


Figure 2. Inference Process Model

### C. THE KNOWLEDGE ACQUISITION PROCESS

A key assumption of this model is that the facilitator has the appropriate knowledge and skills to run the NOC. This knowledge base encompasses the ability to manage and control the network as well as to recommend or take the corrective actions necessary during network operations. However, even if warfighters are as knowledgeable in the area of networking, the primary focus of these forces is to operate tactically. More likely, however, the unit undergoes light network training, enough to operate a tablet PC or handheld sensor, and they are by no means experts in network operations.

The focus of SOF training is to successfully complete the operation. It is not reasonable for a SOF unit to focus on network management, much less is it feasible to deploy with bulky network monitoring equipment or the technicians necessary to operate the equipment. This is the primary rationale for a facilitator.

The individual enables and supports the communication channels among the troops and the TOC, who execute dynamic missions of national importance.

### **1. Knowledge Base Evaluation**

In the knowledge acquisition process, the facilitator acquires the level of the knowledge base of the SOF operator at the user end of the network and upgrades his knowledge base accordingly to best support the operator. The knowledge evaluation is a swift process, almost instantaneous, as the facilitator reflects on the operator's knowledge base and determines the level and frequency of feedback required for the operator.

Compared to the high knowledge base of the facilitator, the SOF operator usually has a low knowledge base. A person's knowledge base does not rest on experience and training alone, but it also factors on the availability and accessibility of networking tools. The NOC houses an abundance of monitoring and decision-support systems for the facilitator vice a limited amount of equipment (i.e., a handheld tactical component) that the SOF operator can carry.

Circumstances may arise when the facilitator's knowledge base is insufficient to resolve every networking problem, uncover every anomaly, or answer every SOF request. If the input feeding the facilitator's inference process is inadequate to meet certain demands, the facilitator can look to other knowledge pools. For instance, feedback from the TOC can address questions pertaining to the SOF mission and how network actions may affect it. Communication with other networking experts not present in the NOC can give the facilitator a different perspective into an issue.

Additionally, an operation may dictate the NOC to coordinate with other communications assets within the operational theater. The NOC can gain valuable insight from other operation centers including their facilitator's processes, their means of coordination, and their communication mechanisms with the SOF unit. Figure 3 depicts the relationships and information flows among the NOC, the operators, and other theater communications assets.

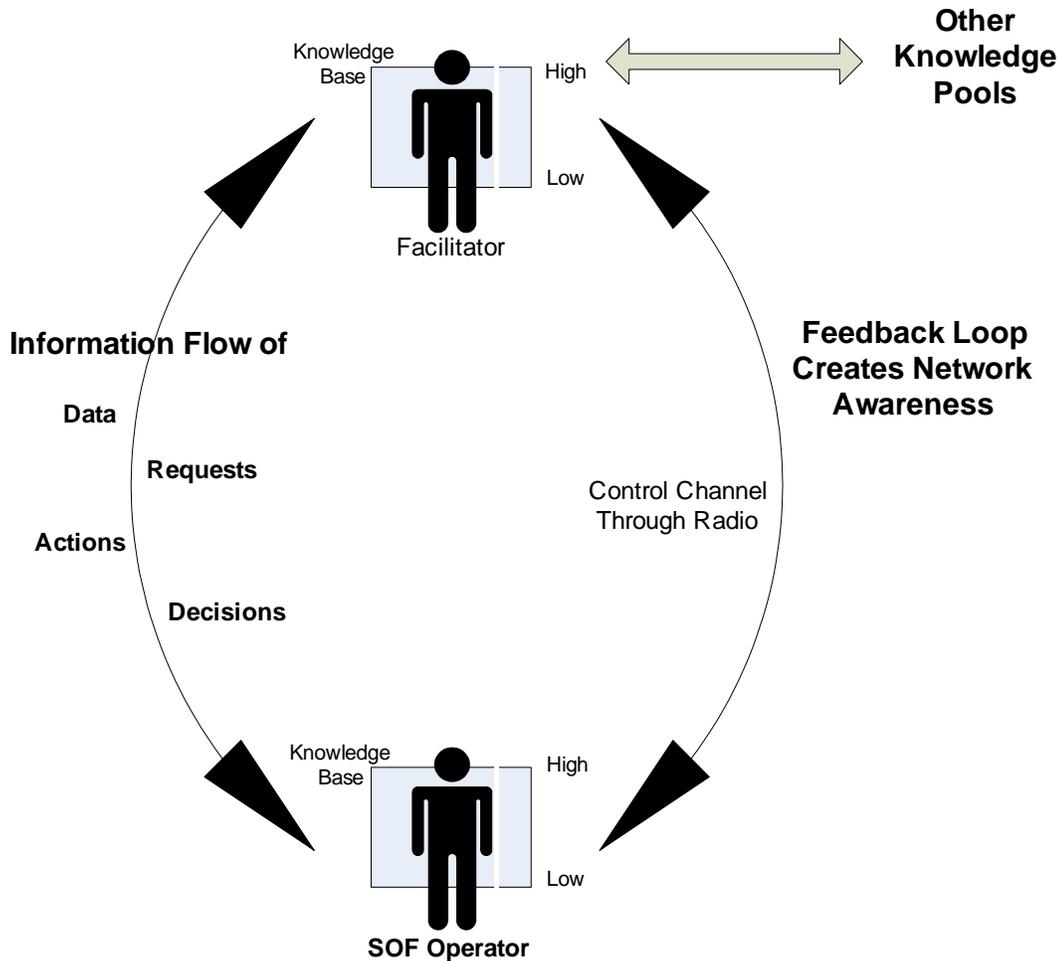


Figure 3. Knowledge Acquisition Process Model

## 2. Network Awareness

The TNOCC oversees the management and current status of the network and provides feedback to all of the participants on the network, in an effort to establish an effective and well-functioning environment. This capability is essential to maintain what is known as network awareness. Network awareness refers to the effects of operational feedback provided to the SOF and back to the facilitator, and how this feedback on the status of the network will enable users to self-organize their behavior. (Bordetsky, Bourakov) The facilitator also promotes collaboration between all the players in the NOC to create a group decision support environment. Integration of this type of support in network operations improves performance and maintainability of the network.

Network awareness refers to the effects of operational feedback provided to the SOF operators and back to the facilitator, and how this feedback on the status of the network enables users to self-organize their behavior. (Bordetsky et al) Depending on the knowledge base of the operator, the frequency of communication between the two parties varies. A SOF operator with a low knowledge base requires more guidance and feedback from the NOC. Even with a higher knowledge base, the facilitator might require a period of adjustment with the SOF operator until the feedback loop becomes more efficient. A steep learning curve suggests that as the feedback loop “tightens”, indicating increased network awareness, the frequency of communication calls drops because the calls are more effective and productive.

To demonstrate a scenario for network awareness, consider a SOF unit tasked with a surveillance mission to place sensors in enemy territory. The area of action is far from the command center, requiring an airborne asset like a UAV to relay the data back to headquarters. The network requires end-to-end line-of-sight (LOS) with the UAV. The NOC needs real-time feedback from the SOF unit on their LOS status with the UAV. The SOF can report back to the facilitator any information about the terrain or other factors that might affect the video feed to the TOC. As they progress through the area of operations, SOF requires continuous feedback on the quality and strength of each sensor’s connectivity. The facilitator is tasked with the placement of sensors and the UAV to increase network performance but without hindering the safety of the mission. For instance, the UAV needs to fly high enough to maintain LOS but away from enemy detection. The sensors need to be placed close to enemy action but at the same time without compromising the safety of the SOF unit.

Operational success is closely correlated with the quality of information exchange between the TOC and SOF. The NOC manages this communication flow. Facilitator feedback to the SOF operator is a management and control mechanism of the network. Network awareness includes not only feedback messages exchanged between the two parties but also an awareness of the facilitator’s intentions pertaining to the network. If each party share the same

understanding, network operations run more smoothly, and the forces better understand how network performance is key to supporting mission success.

#### **D. TNOCC MODEL**

By combining the inference and the knowledge acquisition components together, we have a complete descriptive model of the facilitator's effort to share network awareness. The model shows that the facilitator is responsible for the coordination of many tasks inside and outside the NOC. The facilitator is challenged with managing the NOC effectively, which means monitoring the necessary aspects of the network to provide the right type of feedback to the SOF.

The full model represents a balancing act between the inference process and the knowledge acquisition process. The DSS screens provide the network input, and the facilitator determines if the input is sufficient to relay to the SOF. If the unit requires additional or different information, the facilitator adjusts the inference process to monitor what the SOF requires. The knowledge acquisition process is also dynamic as the facilitator offers more or less feedback depending what information is available from the NOC. Figure 4 diagrams the full system of the facilitator.

## Model of Tactical Network Operations Communication Coordinator

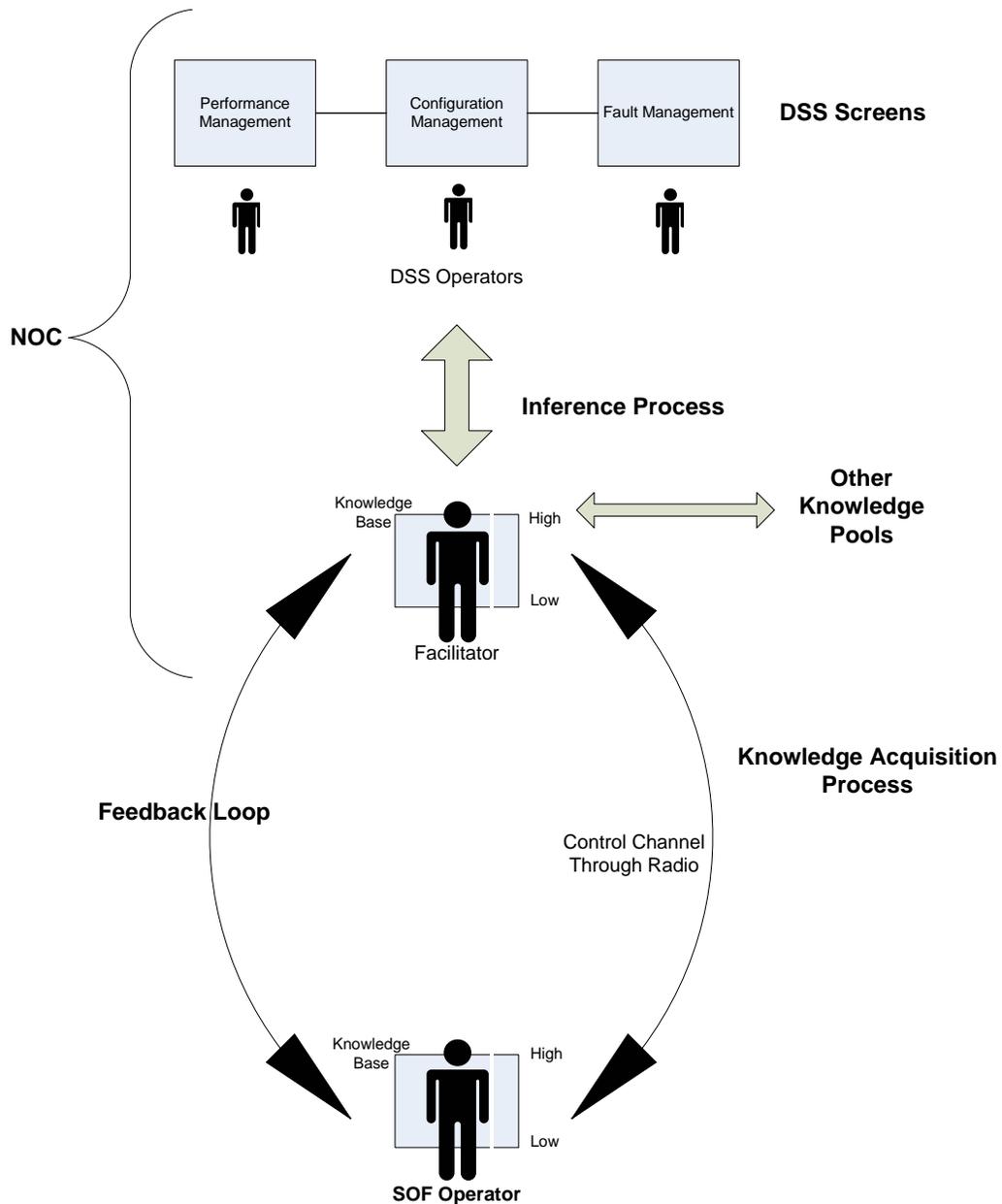


Figure 4. Complete TNOCC Model

### E. OTHER ROLES AND RESPONSIBILITIES

The network coordinator manages the network by executing the necessary tasks to run the system. Part of the facilitator's responsibility is to have a thorough knowledge of network operations including a strong background of the technology, its functions and capabilities. The coordinator has an

operational understanding of the SOF mission and the network's role in that mission. The network supports the mission by enabling communication and data transfer on demand, among the SOF and the TOC. The facilitator attempts to optimize the network's capabilities but within the boundaries of the mission requirements. Effective management entails much more than ensuring the network is up and running; it also involves the following tasks.

### **1. NOC Plan of Operation and Coordination**

An important responsibility for the facilitator is to create a network operations plan that describes the SOF mission and outlines how the NOC supports it. A working relationship is established within the TOC to ensure full synchronization with respect to mission objectives. The NOC objectives and how to accomplish them are also written in the plan. The facilitator sets forth throughput/utilization goals for the network as well as the means of coordination within the NOC. Maintaining awareness of operational ramifications of network actions taken to improve performance constrains the facilitator to a degree but ensures that actions do not hinder the mission.

### **2. Network Data Collection**

Capturing data from experimental network models and simulations and live operational scenarios provide valuable insight into network operations. The facilitator collects data not only to examine the current state of a network but also to input the data into other models and simulate different network topologies to test for improved performance in future operations. Analyzing the data for quantitative measures of performance can identify problem areas. For example, if there is substantial delay in a network, capturing the packet transfer between the nodes reveals which node is the bottleneck. A different node configuration could be tested to resolve the delay.

### **3. Personnel Training**

A major responsibility for the facilitator is to prepare and train the NOC team with the tools used to monitor network performance. The DSS operators have the first-hand look at the network data coming into the NOC. They need the knowledge to recognize what the data means, so they can distinguish which data

is important to relay to the facilitator and which data can be overlooked. The collaborative environment in the NOC is only effective when everyone is aware of their responsibility and they are expertly trained in that area. A DSS operator has a narrow view of the network, but that view is sufficient because there are many other operators that have a different look into the network. The facilitator holds the overall picture of the network and makes decisions about the network by pulling information from the operators.

#### **F. TNOCC MEASURES OF EFFECTIVENESS**

In the military, it is important to measure the effectiveness of a combat-ready unit or a logistics support group. Qualitative and quantitative measures must be in place to gain some perspective into the readiness and effectiveness of a unit. Inspections play a key role in this task. Similarly, the network coordinator's actions require measurement to determine whether this role indeed has a positive impact on network operations and performance.

The management of network operations rests largely with the facilitator, so the effectiveness of the individual can be correlated to the total operational availability of the network. The availability of individual nodes or the combined availability of all the nodes divided by the total operation time can be viewed as a measure of the facilitator's influence. The probability that a node is available and healthy depends on the facilitator's actions to improve the node's performance. For instance, the facilitator can place the node in a new location for increased signal strength or amplify the receiving antenna at the NOC. These actions increase the operational availability of the network, and a network characterized by healthy and stable nodes indicates strong management and coordination.

Wireless networks are volatile, so when an asset drops off the network, the reason could be due to poor signal area, signal range, physical breakdown of the asset, environmental barriers, or even combat attrition. The time it takes the facilitator to respond to a downed node and resolve the situation is measurable. The more quickly the facilitator can bring up the downed nodes and maintain connectivity, the higher the effectiveness. How quickly the facilitator can take corrective actions depends on the network monitoring tools sensing the problem,

what type of problem it is-- a common or unique situation--, if the facilitator has the operational insight required to fix the problem, and if the resources are available. The facilitator's response time to meet any type of requirement is measurable. The requirement could be to add an asset to the network or reconfigure the existing network topology to adapt to the SOF's needs.

Another factor in the facilitator's effectiveness is the preparation and planning of the network. Planning time can be days, weeks, or months in advance of the actual operation, but longer planning time does not necessarily equate to better performance. It is more important that the planning is productive and comprehensive. For example, the facilitator sets aside enough planning time to set NOC objectives and requirements, choose the proper monitoring tools, train the NOC team, clarify their responsibilities, and coordinate with the TOC.

The level of coordination between the NOC and the TOC is also a critical qualitative measure. Coordination meetings are held to lay out mission and network objectives, establish communication channels, alleviate concerns, and resolve conflicting interests. This coordination ensures that both parties are on the same playing field with respect to how the network serves the SOF unit. Less coordination is required with the SOF because their objectives are set by the TOC.

## **G. NETWORK CONSTRAINTS**

Maximizing network performance would be an easy task with unlimited resources, bottomless bandwidth capacity, and flat terrain. But the real world presents a different set of issues that constrain the network. The following constraints influence the decision-making process of the network coordinator and the actions taken to manage the network.

### **1. Bandwidth**

The network is constrained by the total amount of bandwidth available to the nodes. The bandwidth capacity depends on the type of wireless technology utilized and the number of nodes transmitting data at the same time. The facilitator has the responsibility of managing the bandwidth availability and utilization for the specific nodes required by the SOF. This means determining

which nodes are vital for mission accomplishment at specific points in the operation and providing adequate bandwidth for communication and data transmission. The facilitator's knowledge of what file types the SOF receive and transmit at certain times in the mission ensures the SOF has adequate bandwidth to operate.

## **2. Signal Range**

The signal strength of the network is constrained by the distance between the SOF/ground sensors and the UAV relays to the NOC. Wireless technologies transmit to a certain range, determined by the type of technology (802.11b, 802.16, etc.). Signal strength past the range drops off dramatically; however, the signal can be amplified by an antenna. When incorporating UAVs into the network, the flying altitude also constrains the signal strength. 802.11b and 802.16 require LOS between assets, so the UAVs are limited as to where they can fly. To increase the signal reach of the network, additional UAV relays can be incorporated to increase the mobility and coverage of the network.

## **3. Number of Nodes**

The number of assets in the network determines the signal strength and reach of the network. Increasing the number of assets in the configuration may increase the signal and reach, but asset availability and necessity should be taken into account. The mission dictates the number of nodes required for mission success. If the SOF needs to travel lightly, they cannot be burdened with bulky sensor equipment that hinders their movement. The facilitator decides on the suitable number and type of equipment that still provides ad hoc network support.

## **4. Enemy Defense**

The presence of enemy forces affects the network configuration by influencing where the SOF can place sensors and where the UAVs can fly. Feedback from the SOF informing the facilitator that sensor placement is not achievable due to enemy forces near the location presents a problem. The power of a mobile network allows for quick recovery because the facilitator can change the configuration by placing the sensor in a different location and

adjusting other assets to support the new configuration. The facilitator also takes into account the attrition of assets and has contingency plans set to replace the assets. Appropriate encryption of the data transmitting across the wireless channels is necessary for protection.

#### **5. Environment**

The terrain presents sensor placement and LOS issues for the UAVs. Weather may degrade and/or prevent signal connectivity. The date of the Sontay mission was restricted to two windows of time due to weather conditions. The SOF required clear skies and moonlight to safely fly the helicopters to the camp and better communicate with the command center.

#### **6. Time**

The tasks in a SOF mission are typically constrained by time issues. The facilitator is aware of the time constraints involved in the mission and adjusts in a timely manner. The SOF at Sontay had a limited amount of time to conduct the rescue, so mission support was challenged with providing the necessary resources with timeliness and accuracy.

#### **7. Operational Ramifications**

The facilitator is aware of the consequences of actions on the SOF mission. For example, flying a UAV at a higher altitude results in better signal quality, but the UAV may be more susceptible to attack. Also, reconfiguration of the network topology may involve moving a ground sensor close to enemy location, which might compromise the safety of the SOF unit.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. EXPERIMENTAL ANALYSIS OF THE TNOCC AT STAN 6**

#### **A. STAN 6 EXPERIMENT OVERVIEW**

The Surveillance and Target Acquisition Network (STAN) program at the Naval Postgraduate School is an ongoing research effort to explore the technologies of mobile, UAV networks in support of special operations forces (SOF) in combat. (Manuel) A collaborative effort of NPS departments, military units, contractors, and laboratories develop a series of models and demonstrations to enhance the SOF warfighting capabilities with UAV support. The purpose of STAN is to test various network configurations, including the incorporation of state of the art technology, and measure the network performance and effectiveness in special operations.

The first STAN demonstration was conducted in July 2003 with successive occurrences every few months. The most recent episode was STAN 6 held in May 2004 at Camp Roberts, CA. The focus of STAN 6 is on the self-forming/self-healing multi-path wireless network comprised of three main network configurations monitored by the NOC. STAN provides an opportunity to observe the facilitator's processes and the effect on network operations.

##### **1. Long-Haul Air Network w/ UAV Relay**

The airborne network consists of three main components: an ARIES autonomous underwater vehicle (AUV), a TERN UAV, and a K2 antenna situated at a smaller command post near the NOC. The TERN UAV acts as a wireless 802.11b network relay point between the ARIES AUV and the NOC. (Figure 5) As the TERN UAV circles above, the K2 antenna head manually follows its flight pattern and logs its GPS coordinates. The data is transferred to a laptop at the command post through a radio network. The purpose of the long-haul airborne network is to test the connectivity and stability of the network utilizing an aerial node at various distances and heights from the ARIES AUV and NOC.

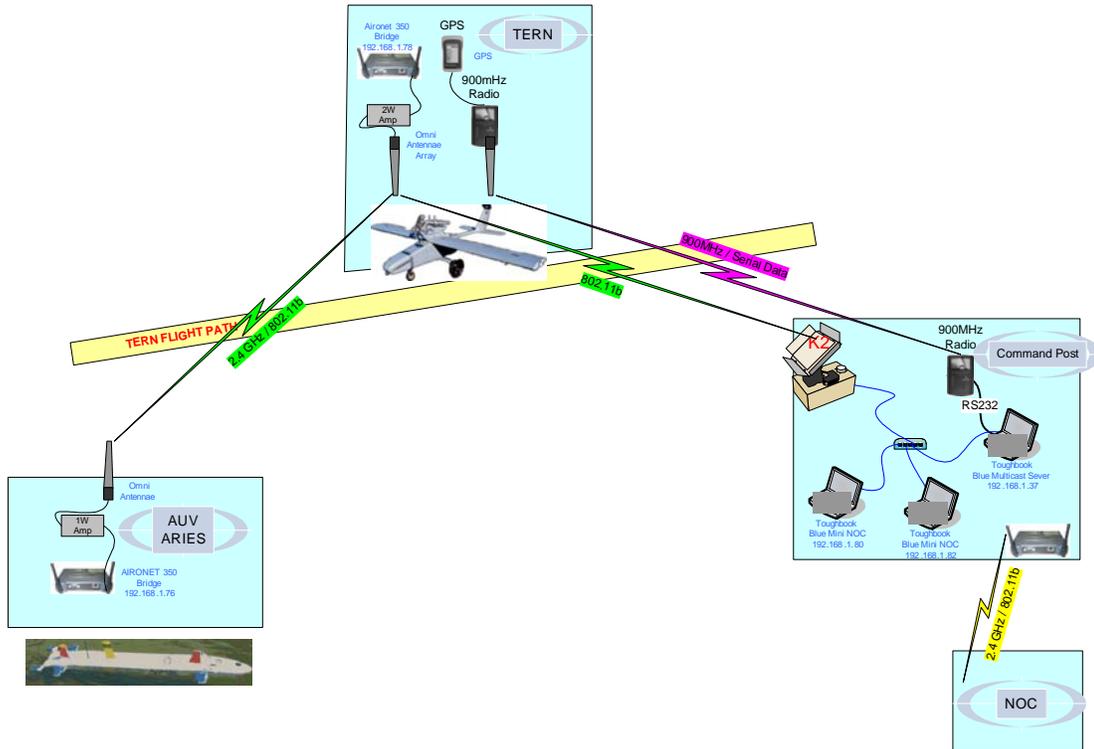


Figure 5. UAV Network Diagram (Courtesy of Captain Trey Blacklock)

**2. Long-Haul Ground Network/OFDM 802.16**

For the first time at STAN, the 802.16, an oscillating frequency division medium (OFDM) technology, is brought into the demonstration. Compared to 802.11b, OFDM is a more robust technology that increases the range and power of the network. The goal is to test the feasibility of the OFDM link with three relay points up to 20 km away from the NOC using non-LOS connectivity. (Figure 6)

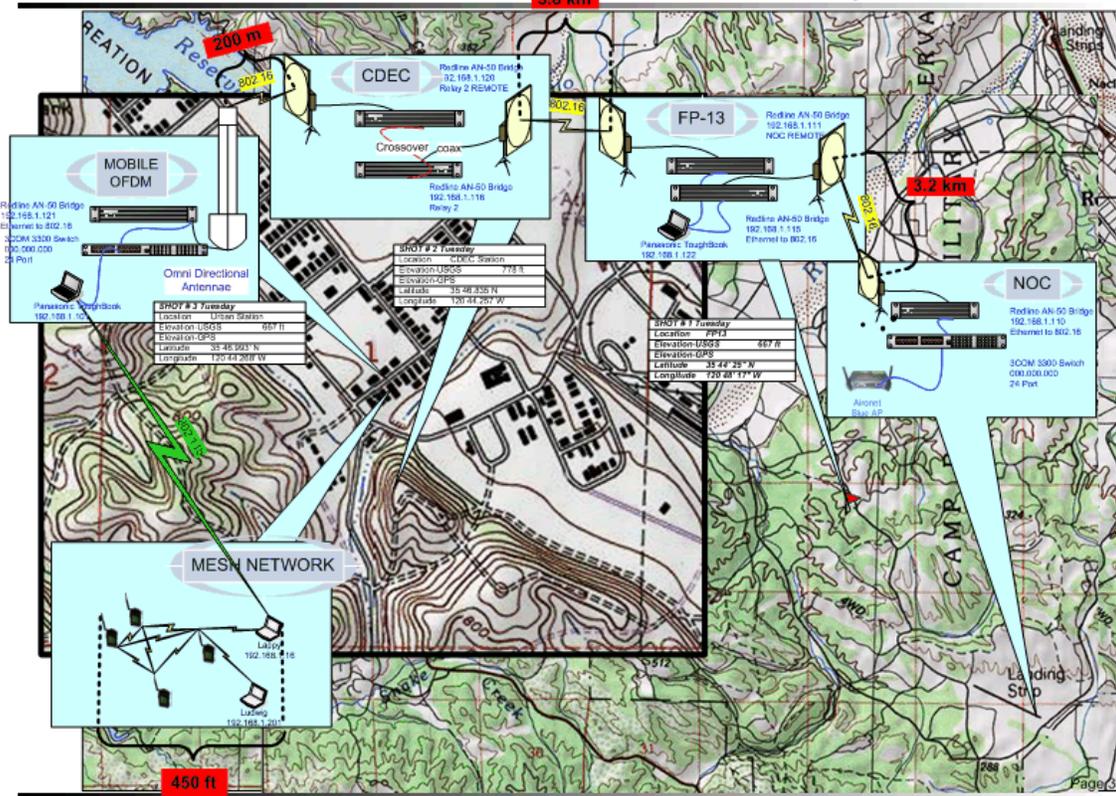


Figure 6. OFDM Network Diagram (Blacklock)

### 3. Mesh Sensor Cell Network

The sensor cell cluster consists of Tacticomps (aka rugged PDAs) and laptops configured in a mesh networking environment. The idea behind mesh technology is that each node in the network can serve as an access point, so communication can be routed through any accessible or nearby node to reach back to the NOC. Figure 7 diagrams the sensor cell cluster. The objectives of the mesh network at STAN 6 are to test the stability and feasibility of different meshing protocols and integrate the sensor cell over the OFDM backbone link to the NOC.

## STAN 6 Mesh Network / Sensor Cell Cluster Detail

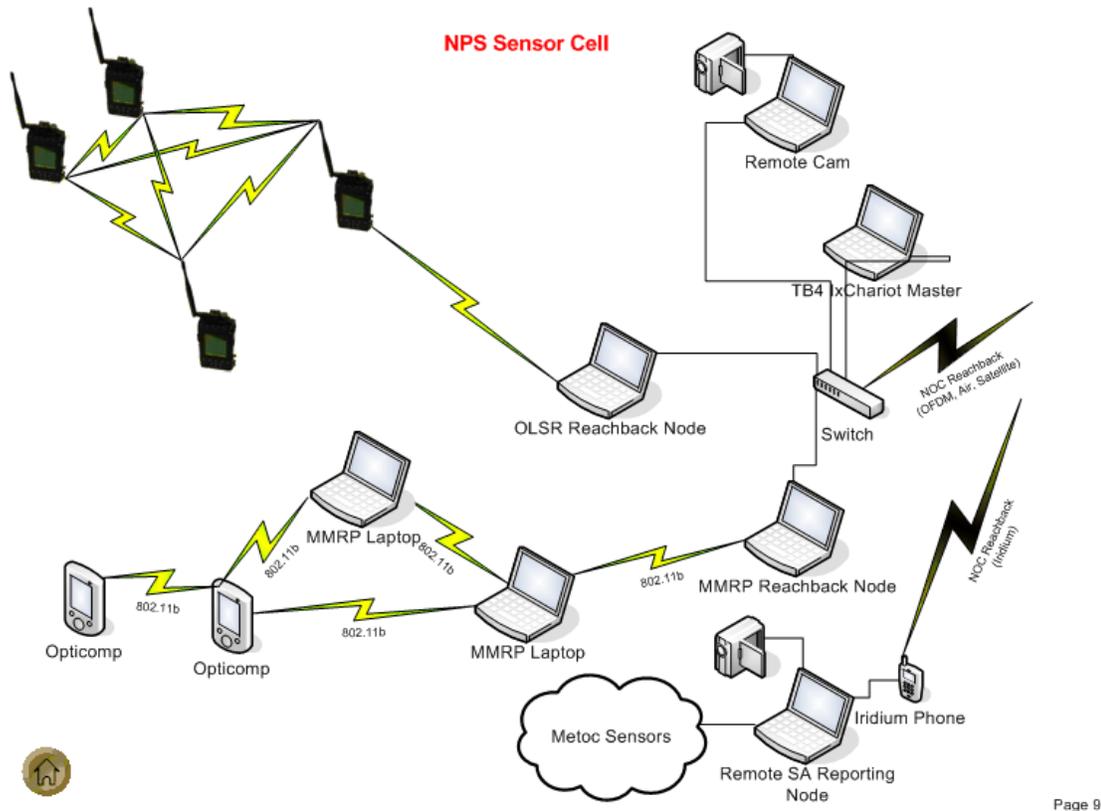


Figure 7. Mesh Network Diagram (Blacklock)

### B. RESOURCES AND TOOLS

The network coordinator has a toolset of resources that aid in network management and decision-making. Many NOCs use the simple network management protocol (SNMP) to manage network activity. (Subramanian) This automated method involves SNMP software agents in each network device. The SNMP agents act as servers. On the client side, software programs like SolarWinds Network Management™ and HP OpenView™ make up what is known as the console manager. The applications request information from the agents to obtain knowledge about which nodes in the network are active. It is the facilitator's responsibility to manage the client side. The following sections detail the various software tools used by the NOC and the facilitator at STAN 6.

### **1. SolarWinds Network Performance Tool™**

The SolarWinds Network Management™ software managed bandwidth performance and is primarily used for data-link management. The DSS screens show the real-time statistics of the active nodes in the network in a web browser view. The Network Performance Monitor™ collects data from routers, switches, servers, and any other SNMP-enabled devices. The IP Network Browser™ displays the IP address of each node in the specified subnet. The SNMP Sweep™ tool pulls device information from the SNMP agent.

### **2. AirMagnet™**

To monitor the network layer, the AirMagnet™ software, installed on desktops and laptops in the NOC, operates in stealth mode in order to “listen” for network packets. AirMagnet™ detects new access points in the 802.11b network and provides information about the node including manufacturer, MAC address, and SSID. The Network Summary View™ provides a simultaneous and detailed view of all the nodes in the 14 channels of the 802.11b network. The Channel Bandwidth Monitor™ detects channel interference, poor RF signals, and low transmission rates. A key component of AirMagnet™ is the performance management alerts that warned against wireless conditions that can cause performance problems. Examples of these conditions are hidden node problems, excessive roaming, and overloaded access points.

### **3. OPNET Modeler and ACE™**

The performance of networked applications depends on complex interactions between applications, servers, and networks. The OPNET Application Characterization Environment™ (ACE) is a toolset of techniques to better understand the environment and improve application performance troubleshooting. To diagnose end-to-end performance problems, OPNET ACE™ provides the capability to capture application traces of the packet exchange between the nodes in the network. ACE™ collects application statistics including processing delays, network delays, response times, and number of application messages. The software allows the NOC to view the application transaction flow at the level of the application layer as well as the network layer. The application

behavior is graphically displayed in a number of intuitive and in-depth diagrams. OPNET™ then applies expert knowledge to the captured application data for automated troubleshooting. The techniques in ACE™ help to identify and diagnose end-to-end performance issues including potential bottlenecks that slowed the network down. The analysis helps to answer if it is the network or the application that cause the problem. After diagnosis, OPNET™ provides fine-tuning recommendations for the network. It is a powerful tool to evaluate bandwidth, protocol settings, application behavior, server speed, and network congestion to derive solutions for increased network performance.

### **C. TNOCC MODEL AT STAN 6**

The week-long experimentation provides much insight into the roles and responsibilities of the facilitator and the effect of his actions on the network. The facilitator's model described in Chapter II is implemented and explored at STAN 6.

#### **1. Inference Process Inputs**

At STAN 6, the facilitator's inputs come from many tools that monitor the health of the network and help to identify any problems. The set-up at the NOC is comprised of a grid structure of monitors displaying different types of information. The primary software tool used by the NOC is the SolarWinds Network Performance Monitoring Tool™ to observe the three main categories of information displayed on the NOC monitors: performance, configuration, and fault management of the network.

##### ***a. Performance Management***

The performance of the network is an important quality because the NOC needs to know how well the network was operating. Throughput, bandwidth usage, and latency are the measures of performance captured to gauge the network, so actions can be taken to maintain the quality or improve it. Within the Solarwinds™ tool kit, the Bandwidth Gauges™ and SNMP Real-Time Graphs™ reveal real-time information on a specific node in the network. For example, Figure 8 is the Bandwidth Gauges™ for one of the main servers in the

NOC and a laptop attempting to reach back to the server. Figure 9 is a continuous throughput graph of the laptop.

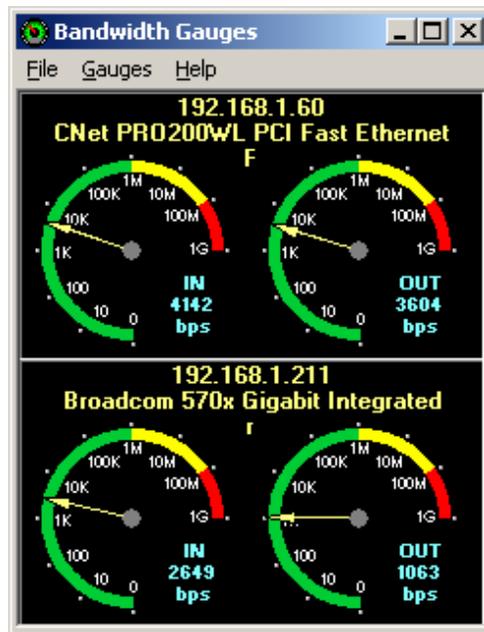


Figure 8. Bandwidth Gauges™

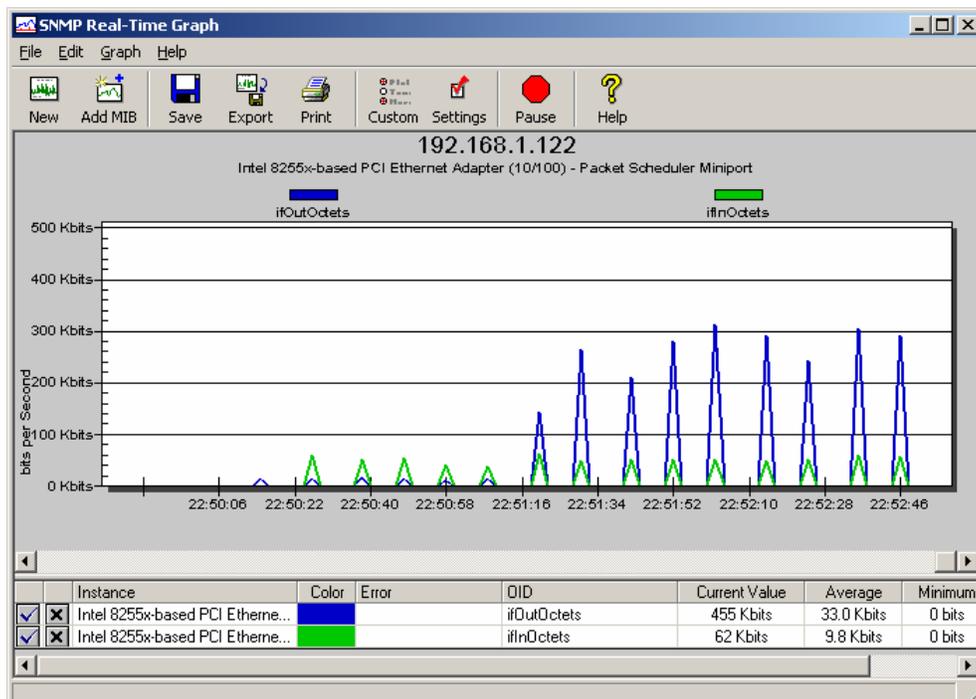


Figure 9. SNMP Real-Time Graph™

## b. Configuration Management

To get a sense of the overall network configuration and status, the IP Network Browser™ scans the subnet to capture a real-time picture of which nodes are in the network. (Figure 10)

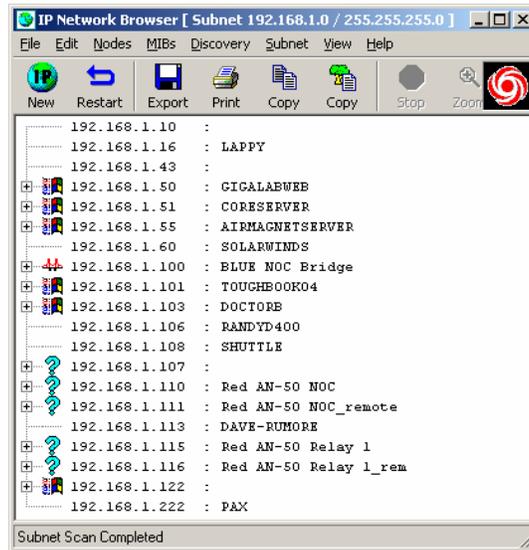


Figure 10. IP Network Browser™

Within the IP Network Browser™, the SNMP-enabled devices, which have plus sign list boxes, can be opened to reveal system description, MIB information, and routing tables. The routing tables are especially important in mesh networking, which allows the NOC to view the available nodes a device could route to and its “next hop” in the mesh network. (Figure 11)

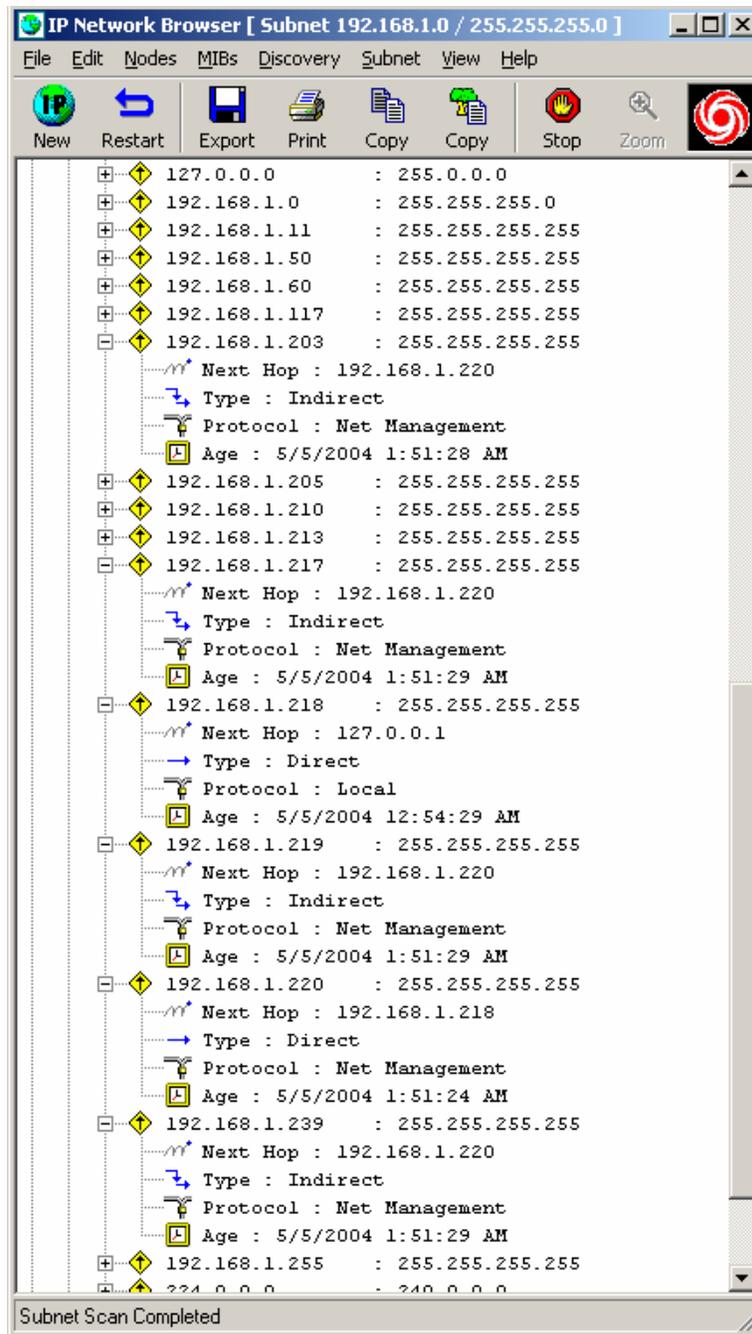


Figure 11. Routing Table

**c. Fault Management**

After scanning the subnet, the IP numbers of the nodes are manually added to the SolarWinds Network Monitor™ that dynamically updates the status of a node as it drops in and out of the network. (Figure 12)

Node	Response Time	Packet Loss	Status	Since last change
192.168.1.100 BLUE NETOPSCENTER AP	0 ms	0 %	Node Up	50 minutes
192.168.1.110 RED AN-50 NOC	2 ms	0 %	Node Up	38 hours, 29 minutes
192.168.1.10 AMSENSOR1	0 ms	0 %	Node Up	51 minutes
192.168.1.111 RED AN-50 NOC REMOTE	2 ms	0 %	Node Up	4 hours, 12 minutes
192.168.1.115 Red AN-50 Relay	2 ms	0 %	Node Up	3 hours, 20 minutes
192.168.1.43 AIRDEFENSE	0 ms	0 %	Node Up	2 hours, 27 minutes
192.168.1.122 TOUGHBOOK01 (FP13)	0 ms	0 %	Node Up	2 hours, 6 minutes
192.168.1.116 Red AN-50 Relay 1_rem	14 ms	0 %	Node Up	1 hour, 9 minutes
192.168.1.113 REDLINE LAPTOP-RUMORE	no response	5 %	Request Timed Out	16 minutes
192.168.1.121 Red AN-50 Relay2_remo	3 ms	0 %	Node Up	16 minutes
192.168.1.120 Red AN-50 Relay 2	3 ms	0 %	Node Up	28 minutes
192.168.1.11 LUDWIG (MESH GATEWAY)	1 ms	0 %	Node Up	16 minutes
192.168.1.203 Tacticomp 1	61 ms	0 %	Node Up	6 minutes
192.168.1.219 tacticomp 2	80 ms	0 %	Node Up	6 minutes
192.168.1.220 tacticomp 3	1001 ms	0 %	Node Up	6 minutes
192.168.1.239 tacticomp 4	39 ms	0 %	Node Up	6 minutes
192.168.1.122 NOC LAPTOP3	28 ms	4 %	Node Up	6 minutes
192.168.1.101 RED TOUGHBOOK 04	1 ms	0 %	Node Up	13 minutes
192.168.1.117 (D2W9ZZ11)	19 ms	0 %	Node Up	6 minutes
192.168.1.210 STAN-X300	4 ms	43 %	Node Up	2 minutes
192.168.1.213 LLDRLAPTOP	19 ms	50 %	Node Up	2 minutes
192.168.1.218 DELLINTEGRATED	no response	100 %	Request Timed Out	8 minutes
192.168.1.114 REDLINE LAPTOP-DON	no response	100 %	Request Timed Out	3 hours, 35 minutes
192.168.1.201 LUDWIG	no response	100 %	Request Timed Out	20 hours, 27 minutes
192.168.1.211 X-300 WIRED	no response	100 %	Request Timed Out	39 hours, 41 minutes
192.168.1.215 TOUGHBOOK5	no response	100 %	Request Timed Out	38 hours, 13 minutes

Figure 12. SolarWinds Network Monitor™

## 2. Knowledge Base Comparison

The facilitator’s model in Chapter II applies to a real operational setting where the knowledge base of the facilitator is high and the knowledge base of the SOF operator is relatively low. However, this situation is not always the case as there may be technical field operators or the technology can make up for the lack of knowledge in the field.

In the case of the STAN 6 experiments, it is important to note that the knowledge base of the field operators is very high as they are primarily running the experiments. They take on a surrogate facilitator role in the field because they have the knowledge to guide the experiments and take the necessary actions to boost network performance and resolve difficulties. For the purposes of analyzing the functions of the facilitator, we are assuming the actions taken by the field operators are usually taken by the facilitator in the NOC during a SOF mission.

## **D. ANALYSIS OF TNOCC ACTIONS**

### **1. UAV Airborne Network Example**

One of the major objectives at STAN 6 is to test the long-haul airborne network from the NOC to the ARIES AUV in Lake Nacimiento, approximately 12 km away. The TERN UAV acts as a LOS relay between the two locations. Reach back from the ARIES AUV to the TERN UAV to the NOC is through a wireless 802.11b network. GPS data on the TERN UAV feeds through a 900 MHz radio network back to the NOC, which is displayed on a laptop. In addition to the performance, configuration, and fault input available to the facilitator, the GPS input is vital to knowing the location of the UAV.

Connectivity from the NOC to the UAV is strong and stable due to clear LOS. However, the LOS between the ARIES AUV and the TERN UAV remains a problem. Feedback from the NOC operators informs the facilitator that as the TERN circles its flight path, the ARIES connection is consistently lost in the same arc of the path. Using maps and GPS to determine where the UAV is flying, the facilitator realizes that the lost connectivity is due to a large hill obstructing the LOS between the ARIES AUV and the TERN UAV. Figure 13 is the fault management view of the network as it informs the facilitator that the ARIES AUV node can not reach back to the NOC.

The SolarWinds Network Monitor™ is the fault management view of the airborne network. (Figure 13) It shows that the bridge and CPU in the ARIES AUV are both down. The performance management graph pertains to the throughput in and out of the TERN UAV. The top line in the graph shows that data is flowing out of the aerial node to the NOC because a connection is established between the two. But there is no connection between the ARIES and TERN, which is indicated by the bottom line showing negligent throughput coming into the TERN.

The screen shot is taken when the hill obstructs the LOS between the ARIES and TERN. After assessing the network situation, the facilitator makes a decision to fly the UAV higher, so the hill is no longer in the way. If there is

uncertainty about how high the UAV should fly, the pilot can test its flight path one full revolution to see if the connectivity is stable.

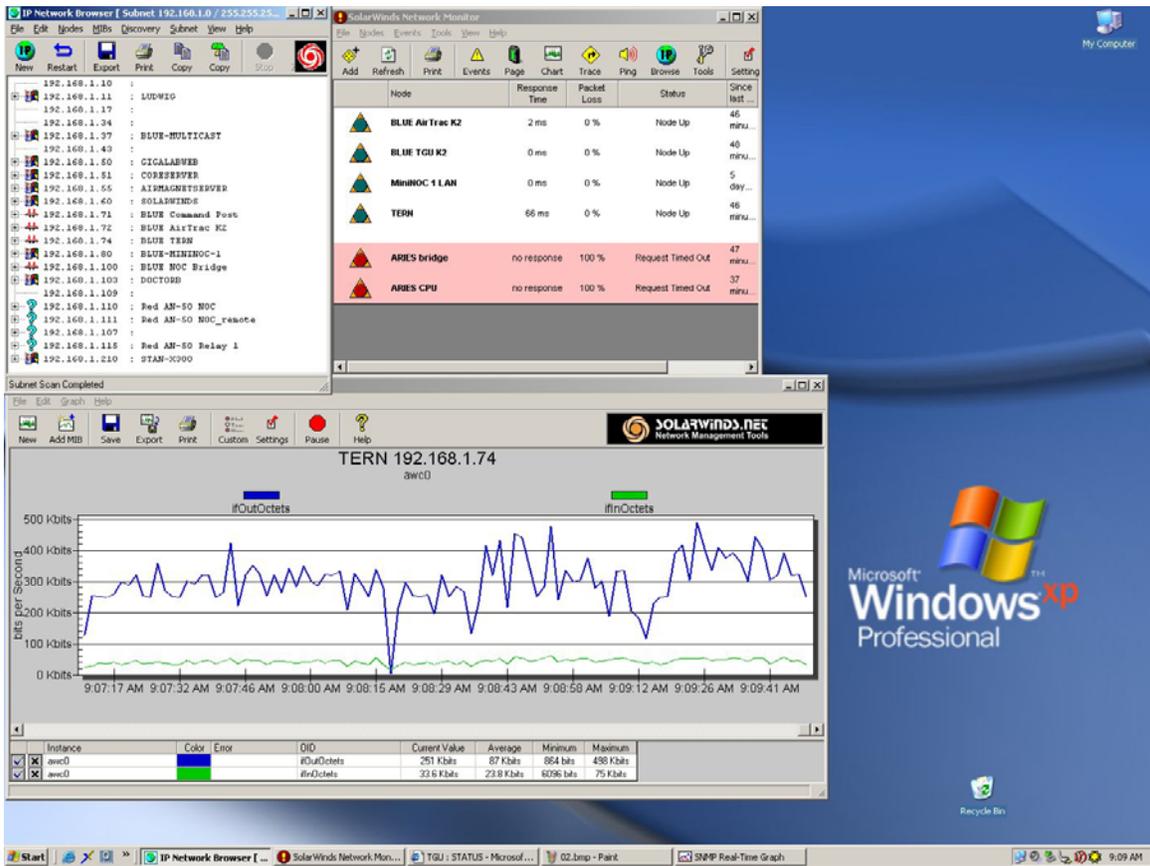


Figure 13. UAV Input Before Action

The network monitor shows that the ARIES is reestablished with minimal packet loss. Reach back to the NOC is tested with a file transfer originating from the ARIES. The performance management graph shows that the throughput lines in and out of the TERN UAV are virtually identical, which indicates that the file transfer is successful. (Figure 14)

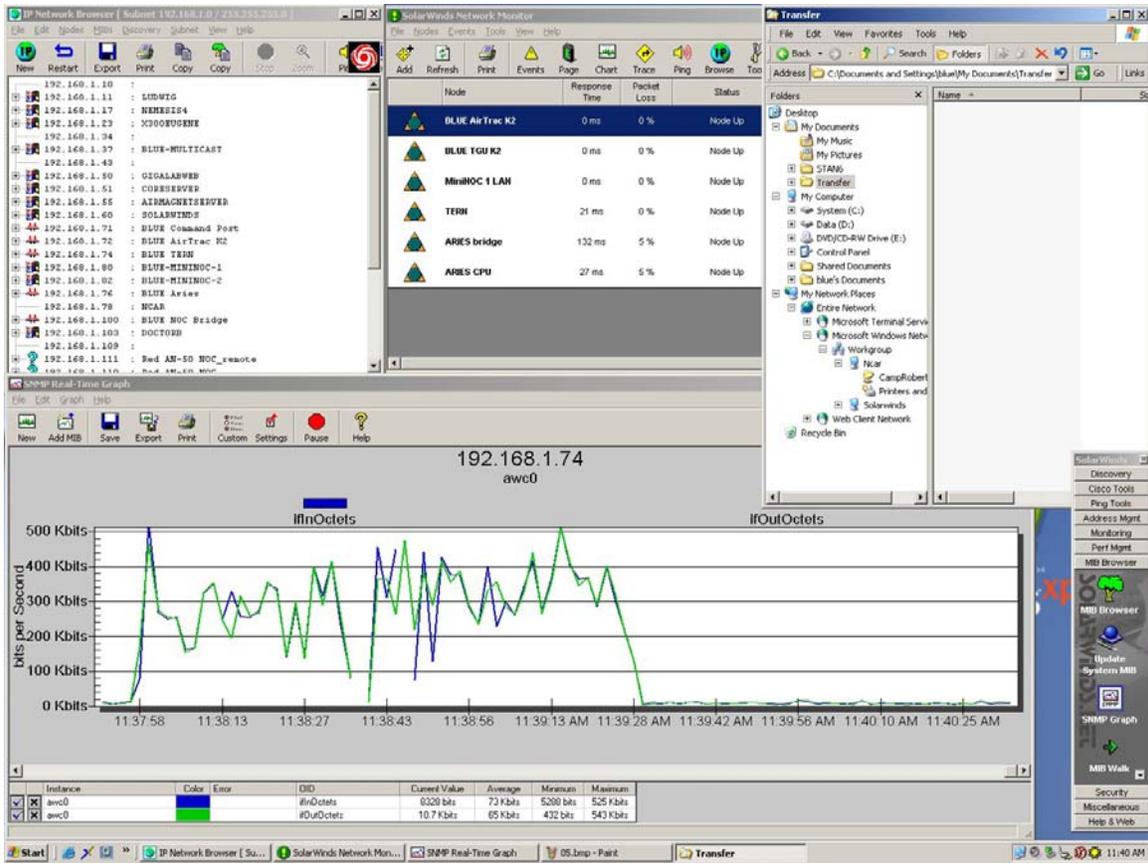


Figure 14. UAV Input After Action

## 2. Mesh Networking Example

In a mesh networking environment, the health of each node is vital because each individual Tacticomp serves as a routing point for reach back to the NOC. The remote team is dependent on the NOC and the facilitator for their status in the network and guidance on where to move for optimum performance. In the specific example, a team of Tacticomps is scattered in an urban environment while a designated vehicle with the gateway laptop inside it drives in a circular motion around the area picking up a network connection from various Tacticomps. (Figure 15) Reach back to the NOC comes from an individual Tacticomp to the gateway laptop in the vehicle to the OFDM antenna on the hill overlooking the urban area. From the hill, the link travels on the OFDM backbone to Firing Point (FP) 13 and then to the NOC. (Figure 6)

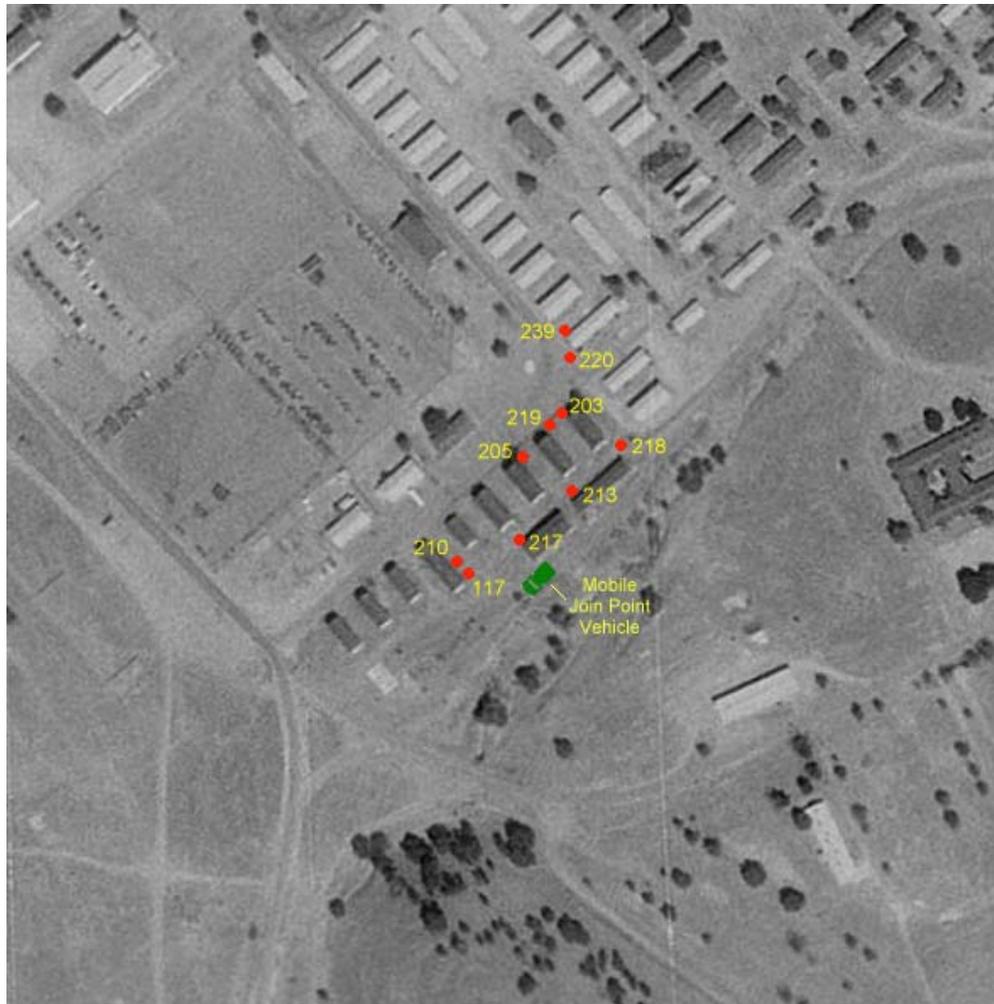


Figure 15. Overhead Shot of Tacticomp Configuration

The scenario is an example of a SOF unit that needs connectivity to the NOC to transmit data, whether it is video feed from a reconnaissance mission or coordinates of the enemy location. Sending the information reliably and safely to the TOC is critical to the operation. The experiment at STAN demonstrates the viability and stability of the Tacticomps in the urban environment. It is the role of the facilitator to monitor the health of each Tacticomp and recommend reconfiguration of the Tacticomps or movement of the vehicle to acquire reach back to the NOC.

Figure 16 shows the data collection of the 192.168.1.217 Tacticomp when the vehicle is at the farthest point away from the Tacticomp. As the vehicle is making its loop down past the 192.168.1.218 Tacticomp, there is little to no

connectivity. Congestion and weak antenna strength are suspected contributors to the low signal strength. The fault management view indicates to the NOC facilitator that there is no signal, and that information is then relayed to the local facilitator in the field.

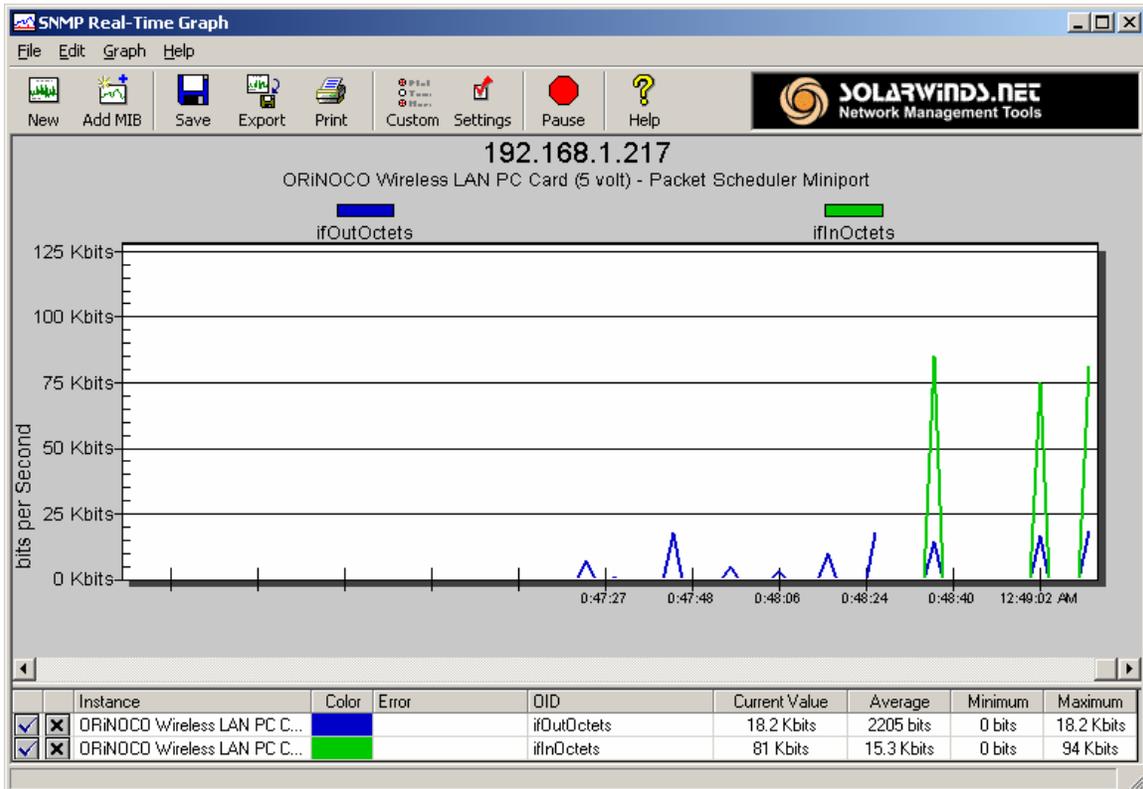


Figure 16. 192.168.1.217 Tacticomp w/ No Connectivity

Feedback to the vehicle driver directs him to locations with better mesh connectivity based on SolarWinds Network Monitor™. As the vehicle moves closer to the 192.168.1.217 Tacticomp, the signal strength increases, and reach back to the NOC is achieved. Figure 17 displays the increased throughput.

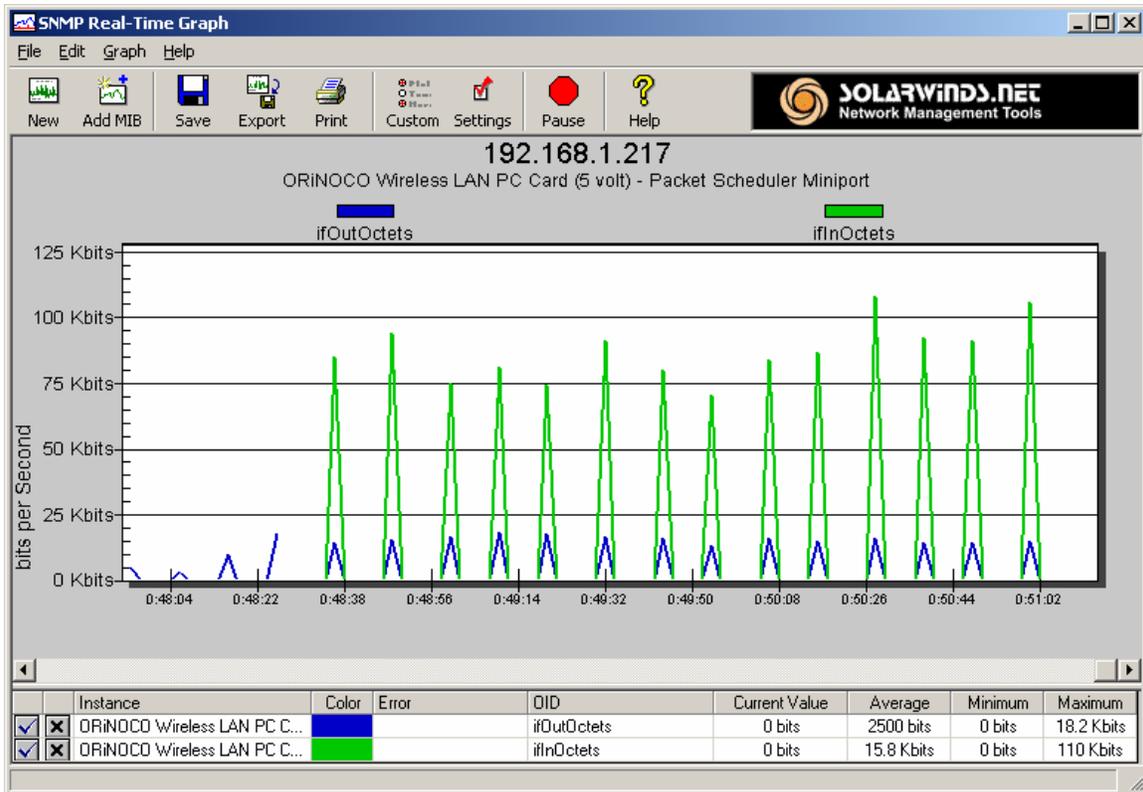


Figure 17. 192.168.1.217 Tacticomp w/ Connectivity

Analysis of the facilitator at STAN 6 shows the impact of his feedback on network operations. The focus of STAN 6 is more experimental with the technology that supports the SOF unit in the future than with the effects of the facilitator's actions in a real operational environment. At the experiments, the facilitator is able to provide feedback to the field operators on the performance metrics of the technology (i.e., throughput and latency). As the STAN program progresses and becomes more complex, the facilitator has more responsibility but also more opportunity to test his effectiveness on the network. The complexity requires the facilitator to consider additional factors that might constrain network performance and evaluate the operational consequences of decisions.

## V. CONCLUSION

### A. SUMMARY

The goal of the NOC is to enable communication channels for the SOF by running and controlling the network environment. The tactical network coordinator manages and coordinates efforts and resources in the NOC to create an environment that better supports decision-making. The facilitator is tasked with improving network performance but with the purpose to support SOF to ultimately fulfill the tactical mission.

A model of the facilitator describes the two processes that govern the ability to manage the NOC. The first process is the called the inference process, in which the facilitator garners the inputs describing network operations to make a recommendation or take action to maintain or improve the health of the network. Real-time network monitoring tools are available to the facilitator and provide input data concerning the performance, configuration, and fault aspects of the network. The inference process allows the facilitator to create an accurate SA picture of the tactical network.

In the knowledge acquisition process, the facilitator determines the level of networking knowledge of the SOF warfighter and provides the necessary level and frequency of feedback required for the SOF operator. The feedback loop created between the facilitator and the SOF operator creates network awareness, the effect of operational feedback and how it enables users to self-organize their behavior.

Network awareness is important for mobile networking because of the dynamic configuration of network assets. In a fixed network configuration, the nodes do not require significant attention because they are stationary. In an ad hoc network, the nodes are mobile in order to adapt to dynamic SOF missions. SOF operators with portable PDAs and mobile UAVs flying overhead require direction and feedback about their network health status in order to remain in the network and operate effectively.

To measure the effectiveness of the facilitator, Table 1 outlines the performance metrics that can be used to examine the individual.

Table 1. TNOCC MOEs

<b>MOE</b>	<b>Description</b>
Up time of network	<ul style="list-style-type: none"> <li>-Effectiveness of the facilitator is correlated to the total operational availability of the network</li> <li>-Probability that a node is up and healthy depends on facilitator's actions to improve node's performance</li> </ul>
Response time	<ul style="list-style-type: none"> <li>-Time to respond to a downed node and resolve the situation</li> <li>-The more quickly the facilitator can bring up the downed node and maintain connectivity, the higher the effectiveness</li> <li>-Response time to meet any type of requirement including adding assets and reconfiguring network topology</li> </ul>
Planning time	<ul style="list-style-type: none"> <li>-Planning time in days, weeks, or months in advance of the actual operation to set NOC objectives and requirements, choose proper monitoring tools, train the NOC team, clarify their responsibilities, and coordinate with the TOC</li> </ul>
Level of coordination	<ul style="list-style-type: none"> <li>-Level of coordination between NOC and TOC is a qualitative measure</li> <li>-Lay out mission and network objectives, establish communication channels, alleviate concerns, and resolve conflicting interests</li> </ul>

## **B. RECOMMENDATION FOR FURTHER RESEARCH**

Mobile networking that supports special operations is a new area of research. The wireless network technology is advancing at a rapid pace, and the U.S. military is attempting to take advantage of the possibilities that wireless communication offers. But the technology is only the first step; it is the management of these systems that enables Special Forces to be effective and successful. Further research of the tactical network coordinator is recommended in the following areas:

1. Detailed study of the facilitator's processes and contributions to network awareness
2. Experimental comparison of an unmanaged versus a managed network to measure the facilitator's effectiveness
3. More STAN experimental opportunities to examine the technology and the facilitator in an operational setting

## **C. CONCLUSIONS**

Success in special operations entails the management and coordination of mission requirements, training, logistics, communications, and other factors. Every aspect of the tactical operation requires the proper amount of attention to support it. Effectiveness of the operation is limited by its weakest aspect, which ultimately determines if the mission succeeds or fails. Network operations are one piece of the big picture, but without it or with poor communications support, the mission is at a loss. This study has introduced the tactical network operations communication coordinator, defined the individual's roles and responsibilities, modeled the processes that influence decision-making, and analyzed the impact of actions taken to improve network operations and support the SOF mission.

The facilitator contributes to network awareness by providing feedback to all of the participants on the network in an effort to establish an effective and well-functioning environment. Network awareness enables users in the NOC and in the field to self-organize their behavior. When the NOC team is aware and

skilled in their monitoring responsibilities, the input they relay to the facilitator results in effective feedback to the SOF. When the SOF is informed of their network status, they are free to perform their mission duties, acquiring additional feedback when needed.

Network awareness includes not only exchanged feedback messages but also an awareness of the facilitator's intentions pertaining to the network. If every party shares the same understanding, network operations run more smoothly, and the SOF better understand how network performance is key to supporting mission success. Integration of this type of support in network operations improves performance and maintainability of the network.

## APPENDIX: LIST OF ACRONYMS

ACE™	Application Characterization Environment™
AUV	Autonomous underwater vehicle
CIA	Central Intelligence Agency
DIA	Defense Intelligence Agency
DSS	Decision support system
GPS	Global positioning system
IP	Internet protocol
LOS	Line-of-sight
MOE	Measure of effectiveness
MOP	Measure of performance
NCA	National Command Authority
NCW	Network-centric warfare
NOC	Network operations center
OEF	Operation Enduring Freedom
OFDM	Oscillating frequency division medium
PC	Personal computer
PDA	Personal digital assistant
POW	Prisoners-of-war
RF	Radio frequency
SA	Situational awareness
SNMP	Simple network management protocol
SOF	Special operations forces
STAN	Surveillance and Target Acquisition Network
TNOCC	Tactical network operations communication coordinator
TOC	Tactical operations center
UAV	Unmanned aerial vehicle
UW	Unconventional warfare
USSOCOM	United States Special Operations Command

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

Adams, Thomas K. *US Special Operations Forces in Action: The Challenge of Unconventional Warfare*. London: Frank Cass Publishers, 1998.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series, February 2000.

Arquilla, John and David Ronfeldt. *The Advent of Netwar*. Rand, January 1996.

Bordetsky, Alex, Eugene Bourakov, Susan G. Hutchins, and William G. Kemple. "Network Awareness for Wireless Peer-to-Peer Collaborative Environments." Monterey, Naval Postgraduate School, 2003.

Bordetsky, Alex, Kevin Brown, and Leann Christianson. "Adaptive Management of QoS Requirements for Wireless Multimedia Communications." Netherlands: Kluwer Academic Publishers, 2003.

Bordetsky, Alex and Daniel Dolk. "Knowledge Management for Wireless Grid Operation Centers." Monterey: Naval Postgraduate School, 2003.

Bordetsky, Alex and Gloria Mark. "Memory-Based Feedback Controls to Support Groupware Coordination." Information Systems Research, December 2000.

Bruner, Edward F., Christopher Bolkcom, and Ronald O'Rourke. "Special Operations Forces in Operation Enduring Freedom: Background and Issues for Congress." Library of Congress, October 2001

"The Congruence Model: A Roadmap for Understanding Organizational Performance." Mercer Delta Consulting LLC, 1998.

Gerla, Mario, Xiaoyan Hong, and Kaixin Xu. *Landmark Routing in Ad Hoc Networks with Mobile Backbones*. Los Angeles: UCLA, Computer Science Department, 2001.

Gresham, John D. "Snake Eater's Ball: Operation Enduring Freedom." *A Tribute to Special Operations*. Tampa: Faircount LLC, 2003.

James, Gregory K. "Unmanned Aerial Vehicles and Special Operations: Future Directions." Monterey: Naval Postgraduate School, 2000.

Joint Publication 3-05. "Doctrine for Joint Special Operations." 17 April 1998.

Manuel, Chris. "Mission Statement." STAN Experiments Mission Statement. Monterey: Naval Postgraduate School, 2004.

McLaughlin, Lawrence W. "Defining Critical Technologies for Special Operations." Monterey: Naval Postgraduate School, 1999.

Shrestha, J. B., Prince, C., Baker, D. P. and Salas, E., (1995). *Understanding Situation Awareness: Concepts, Methods, and Training. Human/Technology Interaction in Complex Systems*. San Francisco: JAI Press, 1995.

Special Operations. Com. [www.specialoperations.com](http://www.specialoperations.com). Last accessed May 2004.

Subramanian, Mani. *Network Management: An Introduction to Principles and Practice*. Addison-Wesley, 2000.

Vandenbroucke, Lucien S. *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy*. "Raid to an Empty Camp." New York: Oxford University Press, 1993.

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dan C. Boger  
Naval Postgraduate School  
Monterey, California
4. Professor Alex Bordetsky  
Naval Postgraduate School  
Monterey, California
5. LCDR Russell Gottfried  
Naval Postgraduate School  
Monterey, California
6. Dave Netzer  
Naval Postgraduate School  
Monterey, California
7. CW2 Christopher Manuel  
Naval Postgraduate School  
Monterey, California
8. Academic Library  
Air Force Institute of Technology  
Wright-Patterson AFB, OH
9. Civilian Institution Programs  
Air Force Institute of Technology  
Wright-Patterson AFB, OH