2008-06

A decision framework for enhancing Mobile Ad Hoc Network stability and security

Orwat, Mark E.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/48127

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

A DECISION FRAMEWORK FOR ENHANCING MOBILE AD HOC NETWORK STABILITY AND SECURITY

by

Mark E. Orwat

June 2008

Dissertation Supervisor: Cynthia E. Irvine

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Dissertation

4. TITLE AND SUBTITLE: A Decision Framework for Enhancing Mobile Ad Hoc Network Stability and Security	**5. FUNDING NUMBERS**
6. AUTHOR(S) LTC Mark E. Orwat	
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.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

One of today's most significant technical challenges is the ability to empirically measure the security status and capabilities of information systems. The lack of security metrics in general and the inability to uniformly combine different dimensions of security information prevents decision-makers from having a macro-level view of system security. The purpose of this dissertation is to develop a conceptual decision framework to address this shortcoming and to apply the approach to a current information system problem: the resource management of Mobile Ad Hoc Networks (MANETs). This framework, called the MANET Distributed Functions Ontology Management Mechanism (MMM), leverages the benefits of ontologies, Value Focused Thinking, and a specialized network flow optimization model in order to craft a holistic view of the configuration and security of an information system (e.g., a Mobile Ad Hoc Network). The resulting decision making capability allows for a better connected, more secure network of communications devices. Ultimately, this research contributes to the provision of a dynamic mobile ad hoc network capability to the warfighter and the first responder with increased network stability, secure and persistent communications, and continuous operations.

14. SUBJECT TERMS Security and Protection; Measurement Techniques; Network Management; Portable Devices; Decision Support; Reliability, Availability and Serviceability	**15. NUMBER OF PAGES** 174
	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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A DECISION FRAMEWORK FOR ENHANCING MOBILE AD HOC NETWORK STABILITY AND SECURITY

Mark E. Orwat
Lieutenant Colonel, United States Army
B.S., United States Military Academy at West Point, 1991
M.S., Massachusetts Institute of Technology, 2001

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author:
Mark E. Orwat

Approved by:

Cynthia E. Irvine
Professor of Computer Science
Dissertation Supervisor

Gurminder Singh
Professor of Computer Science

Kyle Y. Lin
Professor of Operations Research

Theodore D. Huffmire
Professor of Computer Science

Timothy E. Levin
Professor of Computer Science

Approved by:
Peter Denning, Chair, Department of Computer Science

Approved by:
Doug Moses, Associate Provost for Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

One of today's most significant technical challenges is the ability to empirically measure the security status and capabilities of information systems. The lack of security metrics in general and the inability to uniformly combine different dimensions of security information prevents decision-makers from having a macro-level view of system security. The purpose of this dissertation is to develop a conceptual decision framework to address this shortcoming and to apply the approach to a current information system problem: the resource management of Mobile Ad Hoc Networks (MANETs). This framework, called the MANET Distributed Functions Ontology Management Mechanism (MMM), leverages the benefits of ontologies, Value Focused Thinking, and a specialized network flow optimization model in order to craft a holistic view of the configuration and security of an information system (e.g., a Mobile Ad Hoc Network). The resulting decision making capability allows for a better connected, more secure network of communications devices. Ultimately, this research contributes to the provision of a dynamic mobile ad hoc network capability to the warfighter and the first responder with increased network stability, secure and persistent communications, and continuous operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Success

To laugh often and much;
To win the respect of intelligent people and the affection of children;
To earn the appreciation of honest critics
and endure the betrayal of false friends;
To appreciate beauty, to find the best in others;

To leave the world a bit better, whether by a healthy child, a garden patch
or a redeemed social condition;
To know even one life has breathed easier because you have lived.
This is to have succeeded.

Bessie Stanley, 1905

My wife, Celeste, provides me with strength, love, friendship, and support in the face of the uncertainty that a military career brings. She makes life exciting and fun. My two daughters, Tessa and Natalie, energize me with their playful smiles and unconditional love. My parents, Edwin and Christine, gave me the tools for success in life and continue to impart their wisdom, love, and support.

Professor Cynthia Irvine devoted countless hours to my intellectual development during my journey towards a Ph.D. She is professional, dedicated, and engaging. I attribute my improved ability to think critically to the time that she spent mentoring me, challenging me, and editing my work. I truly value the opportunity that I had to study under her mentorship.

Professor Tim Levin consistently offered his time and expertise throughout my time at NPS. Watching and listening to him reason about research problems made my own thought process much clearer. He has a love of knowledge, which I wish to emulate.

My dissertation committee members: Professor Gurminder Singh, Professor Kyle Lin, and Professor Ted Huffmire, always opened their doors to me and freely contributed their expertise in innumerable ways.

Professor Alexandra Newman from the Colorado School of Mines became both a mentor and a friend through her time and assistance with my work. She is an incredibly intelligent, precise, and hard-working person. Her unconditional assistance was instrumental to my success.

The Naval Postgraduate School and Monterey, California, was an excellent place to study, learn, and grow. I must formally thank the United States Army for giving me the time to pursue a Ph.D., the National Security Agency for funding my attendance at NPS through the Information Assurance Scholarship Program, and both the NSF and DARPA for funding my research.

This material is based upon work supported by the National Science Foundation, under grant number CNS-0430566, with support from DARPA ATO. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or of DARPA ATO.

I. INTRODUCTION

A. GENERAL OVERVIEW / MOTIVATION OF THE PROBLEM

Nothing is more difficult, and therefore more precious,
than to be able to decide.

Napoleon Bonaparte

The widespread adoption of handheld communications devices has both motivated and enabled technologies that facilitate ad hoc mobile communications. Mobile Ad Hoc Networks (MANETs) provide the basis for communications without a fixed or pre-existing infrastructure. The ultimate goal of MANET network designers is to provide a self-protecting, “dynamic, self-forming, and self-healing network” for devices on the move [34]. MANET technology is useful to organizations such as tactical military units and disaster response teams, both of which have a critical need to communicate even when fixed networks and central services are unavailable [22].

A high priority United States military communication acquisition program currently being fielded is the Joint Tactical Radio System (JTRS). This radio set will be “software-reprogrammable, multi-band/multi-mode capable, *mobile ad hoc network capable*, and provide simultaneous voice, data, and video communications” [62]. By mandating that all the services (Army, Navy, Air Force, Marines) use this tactical radio system, the military is highlighting the great importance of MANETs in tactical communications. The United States Special Operations Command (USSOCOM) was an early adopter of Mobile Ad hoc Network (MANET) technology in order to leverage the ability to provide persistent communications in the face of high mobility and a lack of a fixed infrastructure. Harris Corporation, a large manufacturer of MANET-capable tactical radios, has built 50,000 handheld radios in response to the Army’s requests, with a production rate of 200 per day [113]. The MANET-capable devices being shipped, however, lack the ability to dynamically manage the network responsibilities required by the MANET.

Ideally, soldiers and first responders could deploy to a hostile, unsecure, or undefined location that lacks a fixed network and conduct secure, persistent communications with each other using a MANET that provides stability through dynamic reconfiguration. The MANET would reconfigure itself as the physical topology changes via a device and context-aware, security-based decision process that migrates functional responsibilities in a transparent fashion. This transparent reconfiguration would ensure near optimal resource usage among the devices, network stability, and minimal operational confusion and disruption.

To maintain persistent, secure communication and connectivity, the network must be able to dynamically adjust its physical and logical configuration, routing procedures, the distribution of functionality among the devices (e.g., cluster-head, content portal, security services, printer services, etc.), and the network security posture. As the context of the network changes and the devices consume resources, these same decisions must periodically be revisited to ensure that the goals of the network continue to be met.

However, maintaining a MANET at its optimal performance level is difficult. For example, changes in a MANET's physical network topology can affect the logical network topology. Physical changes in the network topology may be caused by devices moving in and out of the transmission ranges of their neighboring devices as well as devices "dying" due to the depletion of their limited resources [52]. If connectivity among MANET devices is broken, the logical topologies (e.g., connectivity maps, routing tables) can change frequently, causing communication difficulties that may disrupt the organization's operations. Additionally, stability may be adversely affected by poor reconfiguration choices such as the assignment of network management functions to compromised or under-provisioned nodes which could disrupt the functionality, efficiency, and security of the inter-device communications.

Current MANET implementation technology does not meet these ideal goals. The two manufacturers of the JTRS radio, Thales Communications, Inc. and Harris Corporation, both implement a MANET management decision-making process that lacks the flexibility to provide persistent communication in the face of high-tempo maneuver warfare and first-responder activity. Neither solution provides the required dynamic stability, information assurance, and communications availability. Thales's MANET solution uses a flat hierarchical, intra-zone routing scheme with a pre-determined, permanently-assigned gateway node for inter-zone communication. The solution does not take into account the energy-saving advantages of aggregating localized traffic through a cluster-head [96]. Harris's MANET solution requires that all decision-making be accomplished prior to network deployment. A Master, or Point-of-Contact, is programmed a priori. The Master can listen to all network traffic and send control messages to all devices in the MANET. A back-up Point-of-Contact may be configured ahead of time to allow for contingencies such as the Master losing connectivity or becoming disabled, e.g., due to the depletion of battery power [113]. The assignment is not modifiable in the event that the backup device is disabled.

Both of these current government-purchased MANET solutions rely on configuration decisions made before the network is deployed. Neither is able to react to a dynamic change in the device or network context, with the exception of the back-up Point-of-Contact. During the normal conduct of a fluid, highly mobile operation, we could expect these MANETs to suffer from a lack of network stability, exposure to adversaries, and an inability to provide persistent communications.

In the research literature numerous methods to facilitate dynamic stability within a MANET (see Chapter II, B for a summary) have been proposed. These methods are not sufficiently developed to deploy into actual MANET capable devices. They do not provide a holistic picture of the component devices of the network to the MANET management decision-making process due to three major shortcomings. First, they do not address the input and normalization of device characteristics into the decision-making process. Second, the selection methods are not able to combine characteristics with dissimilar units into a meaningful decision. Third, the methods do not incorporate security factors into the decision-making process. A decision process for the allocation of MANET resources that is aware of network context changes, security attributes, and device resource usage would contribute to increased network stability [52].

To compound this problem, effectively measuring the security of information systems is extremely difficult. Such measurement is one of the eight information security (INFOSEC) technical hard problems identified by the INFOSEC Research Council (IRC) [55]. A lack of security metrics and an inability to combine multi-dimensional metrics into a single measure of the security for a system prevents decision-makers from having a macro-level view of security [55], or from using security as a tool for effective network management [73].

We propose an approach to security measurement and MANET management decision-making that exploits tools from both the Computer Science and the Operations Research fields. This framework leverages the benefits of *Value Focused Thinking* and a specialized *network optimization model* in order to craft a holistic view of the configuration and security of a large system (e.g., a MANET). Ultimately, this can contribute to the provision of a MANET capability to the warfighter and the first responder that allows for dynamic network stability, secure and persistent communications, and continuous operations.

B. STATEMENT OF THE PROBLEM

As discussed in Section A, MANETs are comprised of mobile, resource-constrained, physically unsecure communications devices. To provide persistent communications in the face of rapid changes in device connectivity, MANETs require *dynamic stability*, or the ability of a MANET to maintain its *ad hoc* virtual organizational structure as the underlying resources change and the physical topology varies [52].

Current approaches to MANET management decision-making do not consider device security factors, in part due to an inability to quantify and integrate security-related measures. The result is less fidelity in the individual device assessment that the decision-making process relies on. Without a decision procedure that is security aware, insecure or under-provisioned devices may be selected to perform MANET functions, resulting in premature organizational changes and decreased network stability. Additionally, the approaches are not automated and reduce the flexibility and efficient resource usage of the component devices that are assigned functions.

C. THESIS STATEMENT

A MANET management process based on an ontological organization of network decision factors and device security characteristics can provide a decision framework for efficient, effective connectivity and security of inter-device communications.

D. CONTRIBUTIONS OF THIS RESEARCH

In general, this research addresses the INFOSEC Research Council's hard problem of security measurement and improves the ability to manage the resources of a Mobile Ad Hoc Network. There are three significant contributions to our work.

First, we present a new method for quantifying and incorporating security factors into the measurement of information systems security including a Value Focused Thinking (VFT) based process for the incorporation of subjective factors.

Second, we enhance MANET decision making by incorporating the new method into a framework that provides stability and security to mobile networks. We develop a new conceptual framework to better manage network resources including the first domain ontology of MANET decision factors and the first combination of Value Focused Thinking (VFT) and a Network Flow Optimization Model for MANET decision making. The framework addresses the entirety of the management process to include the collection, normalization, composition, and comparison of network characteristics. We apply VFT in order to structure multiple competing objectives, reduce decision subjectivity, and incorporate qualitative decision factors. The use of our specialized network flow model bolsters the *availability* of communications links by optimizing the device and link characteristics important to availability as well as the direct connectivity of the device in relation to its neighboring devices. Two important consequences result: better energy efficiency and higher link reliability. The framework's decision optimization process reinforces connectivity among the MANET devices and directly contributes to resource availability, network stability, and network security. The decision framework is modular; any of the individual components may be used separately from the others.

Third, we provide a worked example and an initial prototype of the new framework as a basis for the validation of our approach.

E. OVERVIEW OF DISSERTATION

To orient the reader to this dissertation document, we provide an outline by chapter. Chapters I, II, and III are introductory, Chapters IV, V, and VI describe the principal components of the decision framework, and Chapters VII and VIII present framework validation and application, conclusions, and future work.

Chapter I, the Introduction, motivates the research problem in a discussion of MANETs and security measurement. We clearly state the problem statement, thesis statement, and the three main contributions of this research. Last, we provide this roadmap to the remainder of the document. Chapter II presents the background information on MANET technology that is applied in the decision framework. Additionally, we assess related work pertinent to our research problem, including current approaches to MANET management, MANET security, and general security measurement. Chapter III gives a view of the decision framework at a high level of abstraction. First, a description of the operational concepts provides context for the rest of the discussion. Second, a figure depicting our operational vision of the framework puts the subsequent component chapters into perspective.

Chapter IV describes the first component of the decision framework, the MANET Distributed Functions Ontology. This component serves to collect, normalize, and organize the decision data that enters the decision process. Chapter V presents the second component, the Value Focused Thinking decision analysis component. This component aids in structuring the decision problem, as well as quantifying and combining the relevant decision factors in a meaningful manner. Chapter VI describes the specialized network flow model component, which is based upon minimum cost flow optimization. The three component chapters have similar structure, with component-specific introductory, background, and related work sections. A common thread focused on a five device MANET serves to both demonstrate the methodology of the component as well as relate the component to the overarching framework.

Chapter VII, Decision Framework Application and Validation, shows how the framework may be applied in a more complex MANET with a higher number of devices and communications links. This chapter also presents a validation of the conceptual model that underlies the decision framework. Chapter VIII provides conclusions that we derive from our research as well as recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DECISION FRAMEWORK BACKGROUND AND RELATED WORK

Before presenting the decision framework, we provide background information on the unique nature of Mobile Ad Hoc Networks and the management of component devices. We address two major influences on MANET operations: decision-making and optimization. Additionally, we assess related work addressing current approaches to MANET management, MANET security, and general security measurement.

A. MOBILE AD HOC NETWORKS (MANETS)

Following the invention of the two-way radio and the advent of communication without stationary interconnecting wires, the next step was to organize “a set of mobile, radio-equipped nodes” into a communication network [7]. Early networks included the PacketRadio (PRNET) [64], the Advanced Mobile Phone Service (AMPS) [36], and Battlefield Information Distribution (BID) [85]. However, these networks were organized around fixed relaying stations or static controllers. Baker and Ephremides described an architecture based upon the varying connectivity and the changing topology of the High Frequency (HF) Intra-Task Force communication network. This network was required to adapt to the inherent mobility of Navy ships as they attempted to communicate at sea. This ground breaking work has transformed into what we presently call Mobile Ad hoc Networks (MANETs) [7].

Generally, there are two types of ad hoc networks: sensor networks and MANETs. Sensor networks are designed to collect information about an object or area and relay that information back to a central collection point. MANETs are deployed with the purpose of allowing *communication* between devices on the move.

A MANET is an autonomous, mobile, wireless communication network that is not dependent on a fixed infrastructure [25]. A MANET is *self-forming*, in that the deployed devices take a peer-to-peer approach in the formation of their own network routing infrastructure. Devices that are within range of each other establish a network association without human intervention [22]. Continuous movement leads to varying connectivity among the devices, which results in network topology changes. For a MANET to be *self-healing*, the network must automatically reorganize itself when devices join or leave, without impacting the operation of the other participating devices [22]. For a MANET to be *self-protecting*, the devices must safeguard the information flowing throughout the network against unauthorized access in accordance with the overarching security policy [5]. Self-protection is extremely challenging due to the lack of physical security for the mobile devices and the vulnerability of the medium to eavesdropping and jamming. To enable MANET communication, devices cannot rely on a fixed infrastructure. Each device must have the ability to transmit to, receive from, and route messages on behalf of other devices.

MANET devices have limitations in terms of capabilities and resources such as transmission range, battery power, available memory, and computing power. As such, decision-making and optimization greatly influence MANET operations.

The first influence on MANET operations is decision-making. To compensate for the lack of a fixed infrastructure, devices in a MANET must cooperate in making decisions that enhance their ability to communicate. Networked devices must rely on their peers to pass messages and to gain services that the component devices require in the day-to-day operation of the MANET. Decisions made for the collective good of the network are made in areas such as network clustering (the grouping of devices) and cluster-head selection [123], routing protocol selection [91][61][92], and the assignment of distributed functions. Table 1 lists and defines some of the functions that MANET component devices may require in the everyday operation of the network. The list has been compiled from domain knowledge.

Content Portal	Acts as the focal point for the search, viewing, and download of content hosted on personal servers
Cluster-head	Makes routing decisions on behalf of network
User-specified Contact Node	The device where a specific user is logged into the system
Lightweight Certificate Authority	(also called trust authority) manages the security certificates on behalf of the network
MANET Rally Point	Serves as an assembly point if network communications irreparably break down
Web Services Gateway	Provides web access to network devices that cannot connect
Long-range Communications Service Provider	Provides capability to transmit messages over large distances
Printer Service Provider	Provides printer access to network devices without the ability to print
Photographic Service Provider	Provides the capability to take photos to nodes that are not camera-enabled or that require a photo of a specific item outside of their location
Cross-domain Gateway	Serves as the communications link between MANETs at two different classification levels
Multilevel Secure Connection Node	Provides the maximum reachability to other MANETs of different security classification domains
Policy Enforcement/Policy Decision Point	(e.g., for RADaC architectures) makes access control, authorization, authentication, and other security decisions related to the secure management of the MANET and its resources

Table 1 Summary of MANET Distributed Functions

MANET decision-making does not end with providing the network with its initial organization. As stated earlier, the randomness of device movement and the unpredictability of the wireless medium make the network topology susceptible to rapid, unpredictable connectivity and topological changes. Device attributes may also vary widely as the devices use their already-constrained internal resources to conduct routing and other tasks required to keep the MANET functional.

The second influence driving MANET operations is optimization. In the ideal case, a decision made for the collective good of the MANET has to be efficient in order to best conserve the scarce resources that exist among the networked devices. The quality and the optimality of every MANET decision rely on the quality of the underlying input parameters to the decision-making process. The data are often hard to collect and combine within a coherent decision process due to the heterogeneity of the device and network characteristics.

Further hampering the quality of decisions is the fact that security factors are rarely incorporated, resulting in a decision that may be optimal for performance, but not optimal or even highly risky for secure communications. One notable exception to date has been the inclusion of the "trustworthiness" of a public key infrastructure (PKI) scheme-based certificate in MANET decision-making [26].

B. ASSESSMENT OF RELATED WORK

In this section, we describe other research applicable to the MANET management decision-making process. The first part details approaches to cluster-head selection, the most studied MANET distributed function. The second part addresses the integration of security into MANET operations, to include the selection of trust authorities which are also known as lightweight certificate authorities. The third part discusses related work in security measurement that is not specific to the MANET context.

1. MANET Management Approaches

The primary issue in MANET research is the efficient routing of message traffic between two participating devices [123]. In a network with limited resources, routing schemes must minimize communication overhead (e.g., the number of control messages transmitted for administrative purposes). An area of active research focuses on hierarchical network routing architectures as a way to improve the practical performance of existing routing algorithms. A common ad hoc hierarchical structure consists of groups of networked devices, called *clusters*. The clustering of devices improves the quality of service for large-scale networks [123].

In clustering approaches, the cluster is built around an elected *cluster-head*, or local coordinating node [53]. Even approaches that are classified as non-cluster-head based utilize a cluster-head during the initial formation of clusters [78]. We may classify the fourteen prominent clustering schemes as single metric and multiple metric [123][53].

Single metric selection is the most common approach to cluster-head selection. Algorithms use various individual metrics such as: (1) unique identification (ID) number [7], (2) connectivity (a measure of a device's node degree, or the number of direct connections that a device has with its neighbors) [19][48] , (3) mobility (a measure of a device's speed relative to its neighbors) [41][8] , (4) energy-efficiency (a measure of the duration that a device has served as cluster-head) [4], and (5) load-balancing (a measure of the optimal number of nodes that a cluster-head can handle, based upon the medium access control protocol used) [4]. To select a cluster-head, all of the devices in the MANET are rank-ordered according to their respective values for the specified single metric. The algorithms choose the highest ranked device. The shortcoming of a single metric approach is that the cluster-head choice is optimized for the chosen metric, but not for any of the other aspects of the complex MANET. If the context of the MANET changes (e.g., energy-efficiency becomes more critical than connectivity), the initial choice of cluster-head may lead to poor network performance [53].

Multiple metric selection approaches provide a more accurate, holistic picture of the complexity of a MANET and its constituent devices [53]. Two distinct multiple metric approaches have been developed and differ in the use of optimization during the selection process. The first approach applies a combination of several different metrics using a weighted, linear sum [17][42][116]. A well known example is the Weighted Clustering Algorithm (WCA) [17]. WCA considers four factors: the ideal node degree, the transmission power, the mobility, and the battery power of the devices. WCA relies on proxy metrics, or ways to indirectly measure a characteristic, for both transmission power and battery power. Transmission power is represented by the sum of the distances to all of its neighbors while battery power is represented as the cumulative time that a node acts as cluster-head. The proxy measures are all created such that a minimum value is preferred (e.g., a device with a lower cumulative time as cluster-head had higher battery power). WCA uses proxies due to an inability to collect actual metric values and an inability to combine dissimilar metrics in a meaningful way. WCA does not include a methodology for determining the weights that are assigned to the linear combination of metrics. A cluster-head selection is highly sensitive to the weights used in the function, yet WCA depends on a random determination [53]. The devices are rank-ordered according to the combined weights, and the algorithm chooses the smallest combined weight as the cluster-head, since the minimum measurement value is best. In subsequent work, a genetic algorithm was used to optimize the network topology [116]. In this case, the *number* of clusters and, correspondingly, the number of cluster-heads, are minimized; the cluster-head selection itself is not optimized.

The second multiple-metric approach combines metrics using an evolutionary algorithm [53]. The Stability-based Multi-objective Clustering Algorithm considers three factors: degree difference (a measure of the number of direct connections that a device has with its stable neighbors), power consumption (a measure of the distances to its stable neighbors), and node lifetime (and estimate of battery energy to power consumption). The algorithm defines two neighbors as *relatively stable* if the average distance between two devices is less than their transmission distance over a time window that is fixed for all analysis [53]. This stability argument takes into account the relative difference in mobility between two neighboring nodes, but does not actually include a metric based on mobility. An additional proxy metric is the power consumption. The combination of the three factors occurs in the evolutionary optimization phase of the algorithm. The evolutionary algorithm optimizes all three factors simultaneously and produces a set of "compromised" solutions (also known as pareto-optimal solutions), instead of a single optimal solution [53]. To produce a single globally-optimal solution, the individual factors would have to be combined using a single weighted vector sum, as in the first multiple metric approach [43].

The existing multiple metric selection approaches do not consider the collection and normalization of metric values and resort to carefully crafted proxy metrics in order to allow for the combination of dissimilar metrics. Lastly, the algorithms do not assign weights in a methodical manner.

Figure 1 summarizes the cluster-head selection approaches in a continuum. We list the previously mentioned approaches as well our contribution, a selection method based upon multiple metric linear optimization.

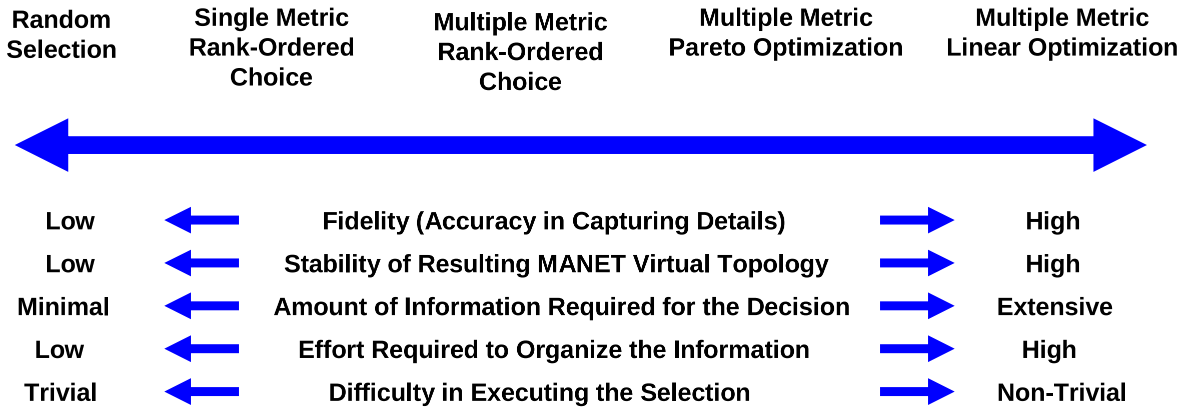

Random Selection
Single Metric Rank-Ordered Choice
Multiple Metric Rank-Ordered Choice
Multiple Metric Pareto Optimization
Multiple Metric Linear Optimization
Low
Fidelity (Accuracy in Capturing Details)
High
Low
Stability of Resulting MANET Virtual Topology
High
Minimal
Amount of Information Required for the Decision
Extensive
Low
Effort Required to Organize the Information
High
Trivial
Difficulty in Executing the Selection
Non-Trivial

Figure 1 MANET Cluster-Head Selection Continuum

Currently, the principal shortcoming in both single and multiple metric MANET management approaches is the inability to solve the metric composition problem. When we introduce security considerations into MANET management, the composition problem is even more challenging due to the categorical nature of many of the security factors.

2. MANET Security

The clustering algorithms evaluated in [123] assume that the participating devices in the MANET are not malicious. A *malicious* device may intercept traffic, corrupt messages, or intentionally decrease the lifetime of the other devices through the depletion of their resources. A malicious device chosen as cluster-head can do even more damage than a similarly malicious participant node to the ability of a MANET to communicate [26].

Much of the MANET security research has been on securing routing protocols [1][121][101]. The approach used is typically limited to the application of cryptography certificates into a symmetric or lightweight public key infrastructure (PKI) scheme. As a system for certificate management, Trust Authorities (TAs) may be selected from the devices within the MANET [98]. The proposed TA selection algorithm is a multiple metric approach, with the addition of a “quality factor” metric that describes one device’s “belief” that a second device is qualified to be a TA [98]. The algorithm does not address the metric composition problem.

Trust-based cluster-head selection algorithms attempt to reduce the possibility of the selection of a malicious device as the cluster’s controller [26]. The algorithm calculates a “trust level” for each device in the MANET using a multiple metric approach. The metrics reflect the trustworthiness of a device, based upon network events such as data packets “dumped and not retransmitted” and “unique addresses have been spoofed” [26]. The trust level is based on observed performance with respect to a trust standard, rather than an innate device-specific trust quality. Each device in the MANET has a calculated trust value that is stored in a trust table. A rank-ordered choice from the trust level values determines the cluster-head [26].

3. Security Measurement

In the computer security field, researchers are working on ways to measure the security of a system by crafting new metrics and creating measurement frameworks that have the ability to adapt to meet potential changes in overall security needs.

One such framework redefines the notions of “security” and “dependability” such that these objectives can be readily combined [63]. The proposed model describes a computer system in terms of preventative measures (related to input into the system) and behavioral methods (output). The framework is qualitative, focusing on the relationships between security terms at the expense of quantification. The model is not specific about how to actually measure and weight the two new system attributes and does not address the metric composition problem [63].

Another framework [120] describes both the qualitative and quantitative aspects of security measurement, with a focus on the process. The framework uses a decomposition method to create low-level, measurable security attributes from high-level security properties. The attributes are combined using a set of logical relations and composite rules that must be created for each individual system. The research provides an approach to weighting the attributes that incorporates a measure of decision-maker consistency. Stated future work includes: (1) the need for increased granularity in the decomposition of the system to include component interactions, (2) the creation of models that better aggregate the low-level measures, and (3) the development of automated tools for data gathering [120]. In addition, the framework does not integrate non-security functionality (e.g., component available memory), thus a holistic picture of the system is not possible. Researchers do not explicitly provide a capability to combine dissimilar attributes. The framework demonstrates a process for obtaining a final security "score" for a system, but does not show how to apply the security measurement into a useful decision-making processes with optimization in mind [120]. This framework is not responsive to varying security needs [68].

The framework in [68] provides a method of evaluating the effectiveness of a resource management system (RMS) in terms of how well the network scheduler assigns application requests to system resources. The resultant objective function may be incorporated in the resource scheduling decision-making. The Flexible Integrated System Capability (FISC) ratio combines attributes such as request priorities and deadlines, Quality of Service (QoS), and security. The framework allows for *variant security*, or the ability to adjust security services within an allowed range depending on the situational context of the distributed network [68]. Follow on work introduced an additional quality representing security to the standard QoS dimensions, known as Quality of Protection (QoP) or Quality of Security Services (QoSS) [58][73]. Researchers have described components of the security vector, and have further refined the ability of a system to vary, or tune, security mechanisms and services within predetermined ranges to allow for a flexible security policy based on the network situation [68][58][73]. The framework provides a qualitative method for incorporating the various factors into a cost benefit function. A procedure for assigning the weightings within the function is not described, in that the weights are dictated by the scheduling policy [58].

This ends our discussion of the background required to understand the decision framework, as well as our assessment of closely related work. We now present the context that defines our problem space in the form of two Concepts of the Operation (CONOPs) and describe the operational vision of our framework at a high level of abstraction.

III. HIGH LEVEL VIEW OF THE DECISION FRAMEWORK

In this chapter, we describe both the concept of the operation and the operational vision of the decision framework at a high level. The concept of the operation firmly establishes the context within which we frame our problem. We give the operational vision at a high level of abstraction before describing in detail each individual component of the decision framework in subsequent chapters.

A. CONCEPT OF THE OPERATION

> *More so than at the operational level of warfare, the tactical level requires C4I[1] technologies that are untethered from fixed architectures. The tactical level requires mobile command posts and communications networks that can support a corps in the attack.*
>
> *LTG W. Wallace* [119]

Senior military leaders see the value of networks that are flexible enough to adapt to the operational mobility inherent in both warfare and disaster response. Mobile Ad Hoc Networks (MANETs) have the potential to provide connectivity between commanders, key leaders, and coordination staffs without the reliance on a fixed communication infrastructure.

We expect that our decision framework is applicable to a wide variety of fields outside of MANET-specific technology. Elements of the framework may be applied to situations requiring improved decision-making, optimization, and security measurement. However, we have set our framework in the context of MANETs in order to demonstrate the usefulness of the research. We illustrate and validate our approach to MANET management decision-making with two specific concepts of operation (CONOPS): a military special operations unit conducting split team operations, and a military corps commander on the attack.

[1] The acronym C4I mentioned in the quote stands for Command, Control, Communications, Computers and Intelligence.

United States military special operations units are typically small in size, and rely on covertness and mobility to operate deep within hostile territory. These units have been the first elements of the military to adopt MANET technologies to enhance their communication on the move. Our first CONOP involves an Army Special Forces unit operating in an unsecure, high risk area. The 12 members are operating in “split teams” (teams of six) in order to reduce the size of their footprint and to minimize the chance of compromise. There are two MANET-capable handhelds per split team, one with the element leader and one with the communications expert, for a total of four. An Air Force controller providing coordination for air support holds a fifth handheld. The controller is co-located with one of the split teams. The mode of transportation may be dismounted or vehicular, with mobility up to a small wheeled vehicle (e.g., the High Mobility Multi-purpose Wheeled Vehicle, the HMMWV), approximately 60 miles per hour.

In regards to transmission ranges, the distances over which MANET-capable devices can communicate will vary due to the network communication standard used, the device power and antenna characteristics, and obstructions. Short range, low throughput technologies such as ZigBee and Bluetooth operate at very close distances (5 to 10 meters). 802.x standards allow for longer range communications, see Figure 2. In this CONOP, the units use a MANET-capable Joint Tactical Radio System (JTRS), such as the Falcon III AN/PRC-152 manufactured by the Harris Corporation and the AN/PRC-148 manufactured by Thales Communications, Inc. [46][109]. For data transmission, a user connects a handheld to the radio, which acts as a wireless modem for the terminal and produces longer transmission ranges over UHF (up to three kilometers) [46].

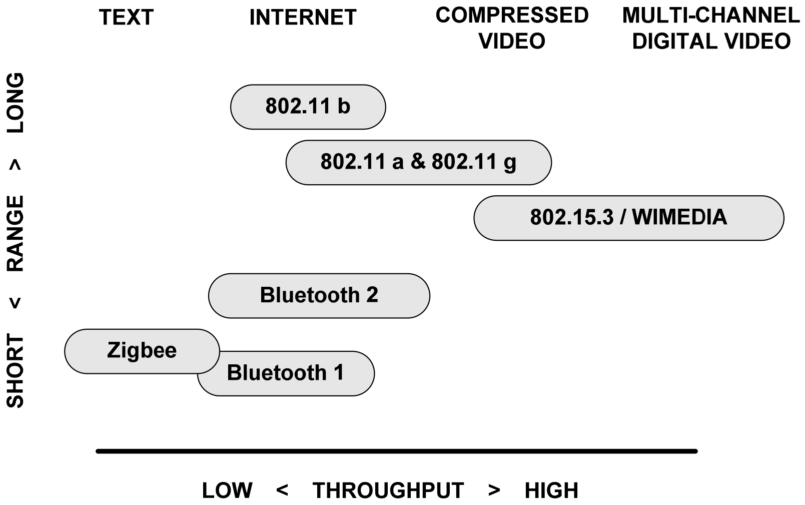


Figure 2 Current and Prospective MANET Communications Standards [50]

For the special operations unit conducting split team operations, the device transmission overlay is in Figure 3. A circle represents the transmission coverage of the enclosed device. If a device is within the transmission range of another, then communication connectivity exists. The connectivity between devices and the element grouping is shown in Figure 4. The resulting MANET topology is illustrated in Figure 5. We revisit this scenario, CONOP #1, throughout the development of the decision framework in order to provide a source of requirements as well as a way to demonstrate the methodology through a check against realistic conditions. We call this thread the "detailed example."

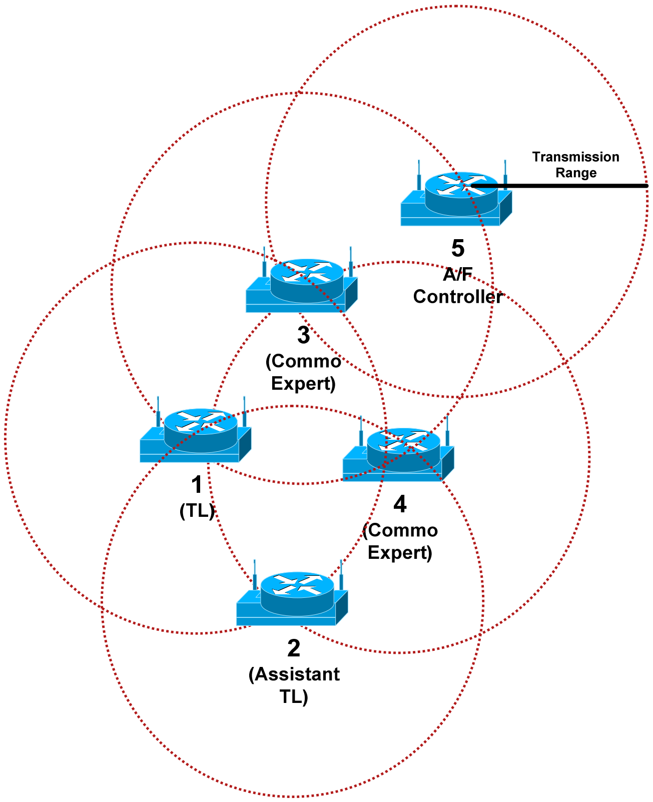


Figure 3 CONOP #1: Device Transmission Overlay

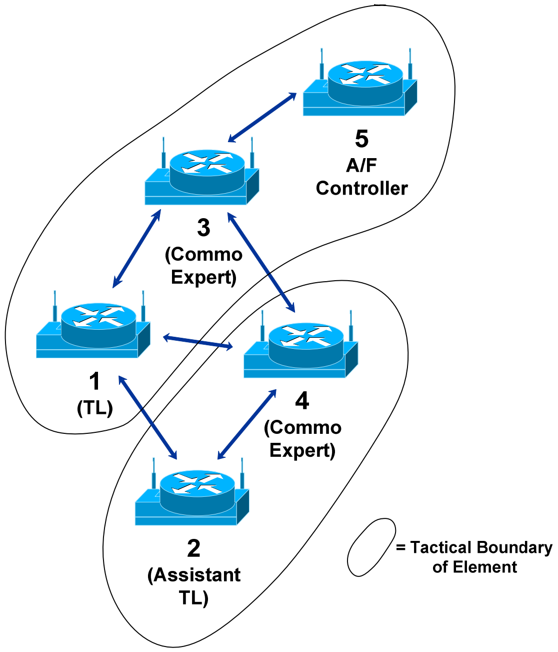


Figure 4 CONOP #1: Element (Split-Team) Overlay

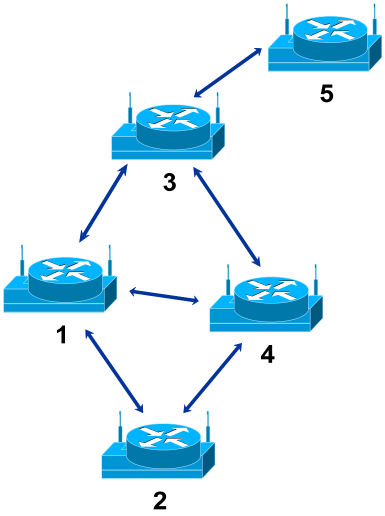


Figure 5 CONOP #1: MANET Topology

The second CONOP involves an Army corps commander and his subordinate leaders and staff officers. A United States Army corps is made up of between 20,000 and 40,000 soldiers. The corps has two to five maneuver divisions and five separate specialty brigades (fires, medical, military intelligence, engineering, and sustainment). The corps commander is a Lieutenant General with eight principal staff advisors. The staff is managed by an officer who serves as a chief of staff. Lastly, there is a senior non-commissioned officer who advises the corps commander. There are other elements such as coalition and joint (e.g., Navy, Air Force, Marines) forces that provide key leaders and liaisons to the corps. For CONOP #2, we crafted a scenario with 30 devices. The mode of transportation may be dismounted or vehicular, with mobility up to the speed of a small wheeled vehicle (e.g., the High Mobility Multi-purpose Wheeled Vehicle, the HMMWV).

The choice of 30 devices provides a more complex scenario than that in CONOP #1. Even though MANETs may total hundreds of devices, operational considerations, transmission ranges, and medium access protocols (MAC) impact the total number of devices that may be effectively grouped together with a cluster-head. Operationally, the commander requires a minimal number of key leaders in order to be most effective as a supervisor and to limit operational confusion. Organization theory suggests that some levels of management can efficiently supervise only three to eight subordinates, while others can supervise up to thirty employees [29]. Based on the discussion of transmission ranges above, it is not realistic that all of the elements under the control of the corps will be within communication range of the commander. A corps occupies an area in excess of three kilometers. Lastly, the MAC protocol used limits the number of devices that are directly connected to each other in order to minimize message collisions [17]. For instance, Bluetooth employs a master-slave model where a master can only handle up to seven slaves [17]. For these reasons, the decision to use a second CONOP with a MANET of 30 devices is realistic. Figure 6 represents the MANET topology by showing the component devices and their corresponding connectivity.

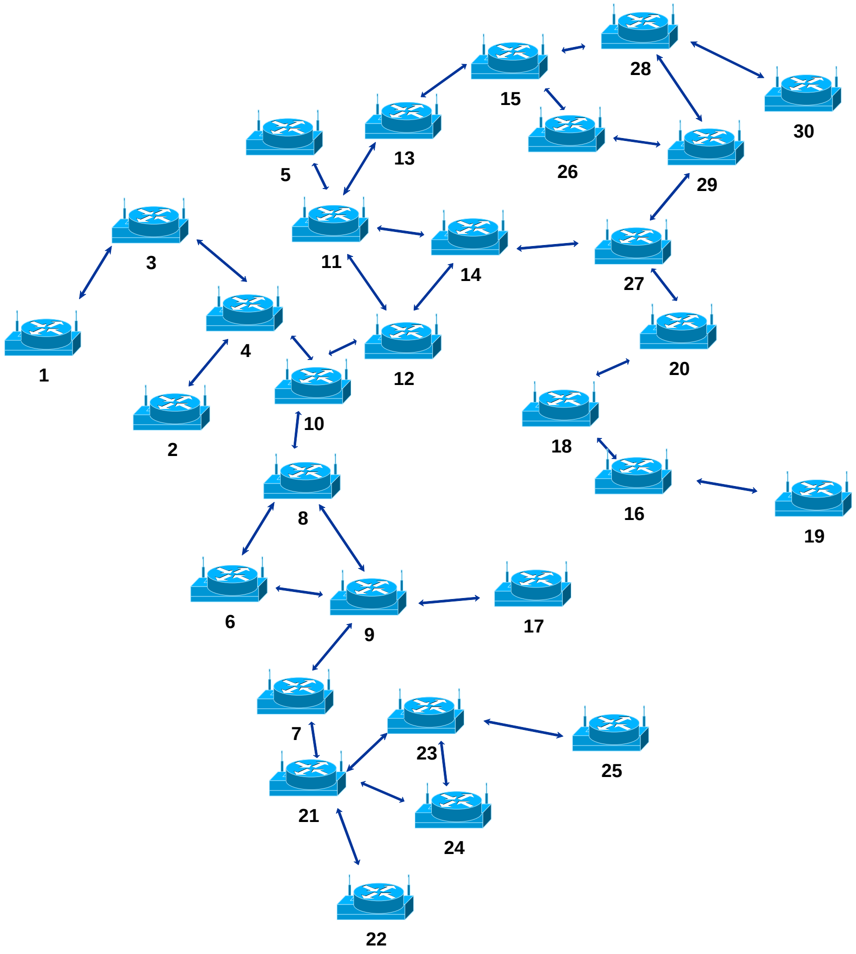


Figure 6 CONOP #2: MANET Topology

As suggested earlier, although the CONOPS described above are military-specific, we may apply the framework to other scenarios depicting governmental agencies, first-response units, and civilian social networks[2].

Now that we have described the context of our MANET, we present a high level overview of the decision framework by discussing our operational vision.

B. OPERATIONAL VISION OF THE DECISION FRAMEWORK

In this section, we describe the operational vision of the MANET management decision framework at a very high level of abstraction. Chapter IV contains a more thorough explanation. Conceptually, the framework relies on the message traffic originating from the networked devices as input into a decision mechanism, which selects a device to perform the required MANET distributed function. The MANET Distributed Functions Ontology (MDFO) Management Mechanism (MMM) consists of a translator (1), the ontological database with function matching and inference capability (2 and 3), and the decision-making process (4), depicted in Figure 7. An important piece of the framework is the MANET Distributed Functions Ontology (MDFO), which supports the entire framework. The MDFO allows us to organize, normalize, and infer decision data. We describe the ontological knowledge structure in Chapter IV.

[2] A social network is a social structure made up of individuals or organizations that are linked together by interests and connections. This "social cohesion" is gaining in popularity due to the improvements in mobile smart phone technology [80].

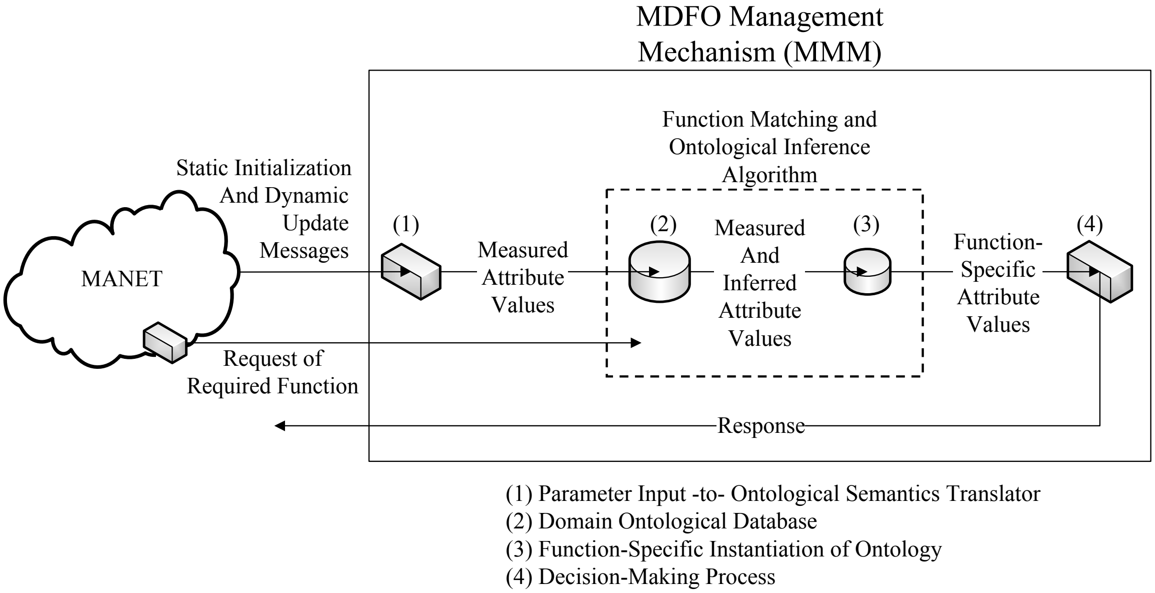


Figure 7 Operational Vision of the MANET Management Decision Framework

The translator (1) and the ontological database (2 and 3) serve to refine the decision data into an accurate, minimal set of attributes and values that feed into the decision-making process (4). The decision-making process (4) has two components, Value Focused Thinking Decision Analysis and Node Choice Optimization. The first component analyzes the decision data and assigns a value representative of both the device characteristics and the MANET priorities to a relative entity consisting of two devices and the communication link that they share. The second component produces a node choice by optimizing both the overall network strength value and the MANET device connectivity.

We now depart from the high level of abstraction in order to describe the MANET Distributed Functions Ontology (MDFO) Management Mechanism (MMM) by component in Chapters IV to VI.

IV. THE MANET DISTRIBUTED FUNCTIONS ONTOLOGY (MDFO)

The first component of the MANET Distributed Functions Ontology (MDFO) Management Mechanism (MMM) is the ontology itself. We provide an introduction to the component as well as a discussion of pertinent background information and related work. We then explain the MDFO to include the ontological classes and the class interactions. Finally, we present a detailed example that incorporates the MDFO.

A. INTRODUCTION

Mobile Ad hoc Networks (MANETs) rely on dynamic configuration decisions to efficiently operate in a rapidly changing environment of limited resources. The ability of a MANET to make decisions that accurately reflect the real environment depends on the quality of the input to those decisions. However, collecting and processing of the multitudinous factors related to the operation of a MANET is a significant challenge. Equally significant in current approaches to dynamic MANET management is the lack of consideration given to security factors. We show how our ontology of MANET attributes including device security and performance characteristics can be leveraged to efficiently and effectively make dynamic configuration decisions for managing a MANET. Finally, our proposed organizing structure facilitates automated decision processes.

The *MANET Distributed Functions Ontology (MDFO)* that we describe in this chapter is used to structure MANET performance and security information. We present an associated "operational vision" for its integration into MANET operations in Chapter III with a more detailed view of the mechanism in Section E of this chapter. This ontology enhances the MANET decision processes in three ways: it gives us the ability to normalize parameters into common terms, it allows us to make inferences should values be unavailable or inconsistent, and it provides a canonical means to incorporate network and device security. These benefits directly lead to more accurate and secure MANET functional decisions as well as more efficient network operations.

There are two major contributions of this work. First, the ontological organization and structuring of MANET decision support data will make it easier to automate future decision algorithms. Secondly, the *MANET Distributed Functions Ontology* provides a much needed foundation for incorporating security factors as a means to enhance the decision processes of MANETs [89].

In Section B, we give additional background information about ontologies. Section C discusses related work. Section D describes the structure of our ontology as well as provides a descriptive fragment of a typical entry. Section E provides additional detail about the operational vision reflecting the integration of the ontology into MANET operations. Finally, Section F provides a detailed example based on the realistic MANET scenario outlined in Chapter III. The example shows the powerful potential of an ontological approach to secure MANET management.

B. BACKGROUND ON ONTOLOGIES

The term *ontology*, rooted in philosophy, describes the study of existence. Computer science (originally the artificial intelligence community) later adopted the term ontology to mean “a theory of a modeled world” and “a component of knowledge systems” [44]. Thus, besides the philosophical connotation of ontologies, there are pragmatic reasons for their use. Ontology, as an engineering tool, may be further defined by its use. The tool may provide the “representational machinery with which to instantiate domain models in knowledge bases,” allow the querying of knowledge-based services, and represent the results from these queries [44].

The use of ontologies has become much more widespread since the World Wide Web Consortium (W3C) included the concept as an explicit layer in the standards stack for the futuristic *semantic web* [10]. The semantic web uses ontologies to specify standard conceptual vocabularies. This approach makes data exchange easier and knowledge databases more accessible throughout the World Wide Web. W3C is leveraging the ability of ontologies to normalize data into consistent terms and to provide inference from data due to linkages between common terms. The linkages are manifested as relationship rules among objects.

Within an ontological framework, *classes* are abstract groups, sets, or collections of objects. *Objects* are the basic individual items in the domain. *Attributes* are properties, or characteristics that objects can have and share. *Relations* are ways that objects may interact with each other. Ontologies are different from taxonomies, which do not incorporate the *relations* concept. A relation is an attribute whose value is another object in the ontology. Ontological relationships can specify arbitrarily complex rules about the attributes of the related objects, whereas a taxonomy has only the “is-a” relation. The set of relations taken as a whole fully describes the semantics of the domain [44].

C. RELATED WORK

Chapter II describes current research related to the introduction of security aspects into MANETs. This related work section outlines the integration of ontologies into computer science (CS).

Much of the research currently focused on ontologies is in the creation of knowledge systems for inclusion as accessible content in the future semantic web. Top-level ontologies are being created for every conceivable domain in order to start establishing common terminology and to facilitate natural language processing and artificial intelligence. An example of a non-computer science ontology is the Stanford Wine Ontology, which relates wine grape type, wines, and wineries [86]. An example of a CS-specific ontology is the information security ontology. The application of this proposed ontology is limited to creating a common language among security researchers and to the processing of natural language data sources [97]. Creators of these ontologies are building various general ontological databases in preparation for the expected deployment of the semantic web [10]. A challenge of this wide-spread research is to carefully define linkages between domain-specific ontologies to maintain the consistency of the root (all-encompassing) ontology.

The integration of ontologies into actual network operations is rare. One of the few examples is in network management and control, where researchers use an ontological approach to perform configuration tasks in a network [23]. In their architecture, the system collects Simple Network Management Protocol (SNMP)-based configuration messages and converts their content into ontological semantics. The system develops a current state of the network based on the input and suggests, through inference, relevant configuration changes. Finally, an export mechanism distributes the new network configuration plan to network devices for re-configuration [23].

Now that we have presented background information and related work, we describe the ontology in detail.

D. THE MANET DISTRIBUTED FUNCTIONS ONTOLOGY

The domain of the MANET Distributed Functions Ontology (MDFO) is the functions or services that may be provided by component devices on behalf of other devices within a MANET. Before we describe the intricacies of the MDFO, we look at how our ontology potentially extends the root ontology provided by existing ontologies. An example conceptual organization of this extension is presented in Figure 8.

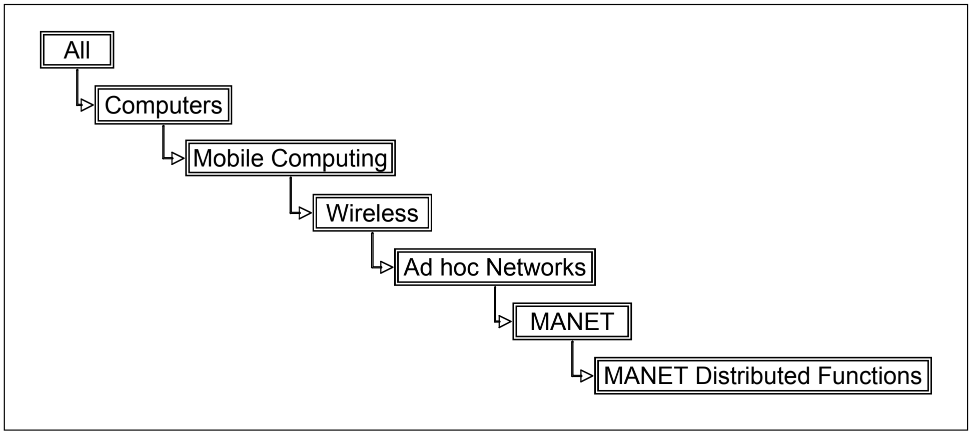


Figure 8 Conceptual Organization of Extended Ontologies

This figure shows at an abstract level the potential linkages between our ontology and others that may occur. The top tier (root) of this hypothetical hierarchy is shown as the “All” ontology, which encompasses all of the ontologies in existence. The linkages reflected in the figure show either an “is-a” relationship or a meronymy “part-of” relationship. Thus, the MDFO is “part-of” the MANET ontology, which “is-an” object in the Ad hoc Network ontology, etc.

In the *MANET Distributed Functions Ontology*, there are three major classes. Each class comprises one or more objects; each object has one or more attributes; and each attribute may take the form of a complex data type with one or more values.

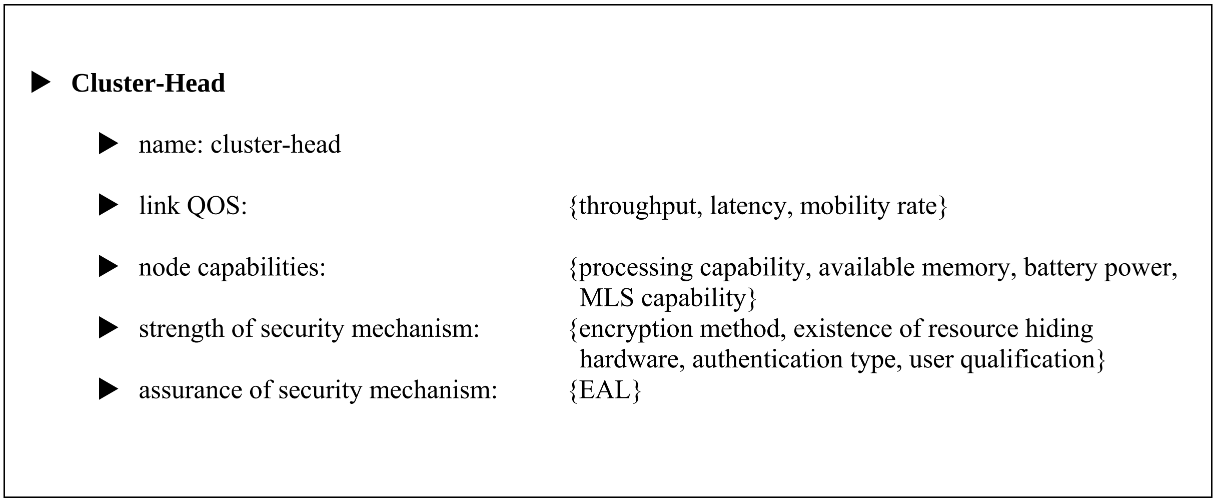
The *MANET Function* class (**Class I**) defines all distributed functions or services that a device in the MANET might need to perform on behalf of the network, along with their assigned minimal set of parameters. The *Network Component Profile* class (**Class II**) is the class of all devices connected to the MANET. Every device lists the entire set of possible parameters along with their measured levels observed before and during network operation. The *Parameter* class (**Class III**) specifies the entire set of parameters and their allowable measured levels or ranges for the MANET Function and Network Component Profile classes.

A list of the *MANET Function* Class objects (function names) is shown in Figure 9. We formally defined the functions in Table 1.

- Content Portal
- Cluster-head
- User-specified Contact Node
- Lightweight Certificate Authority
- MANET Rally Point
- Web Services Gateway
- Long-range Communications Service Provider
- Printer Service Provider
- Photographic Service Provider
- Cross-domain Gateway
- Multilevel Secure Connection Node
- Policy Enforcement/Policy Decision Point

Figure 9 The *MANET Functions* Class

If we open one of the objects within the *MANET Function* Class from Figure 9, the relationship between the functions and the parameters becomes quite clear. In the fragment of Class I shown in Figure 10, a specified function (here, the Cluster-head) has an assigned minimal set of parameters that are considered critical to the categories listed as "object attributes."



- **Cluster-Head**
    - name: cluster-head
    - link QOS: {throughput, latency, mobility rate}
    - node capabilities: {processing capability, available memory, battery power, MLS capability}
    - strength of security mechanism: {encryption method, existence of resource hiding hardware, authentication type, user qualification}
    - assurance of security mechanism: {EAL}

Figure 10 Fragment of the *MANET Function* Class

For the Cluster-Head, certain parameters are intrinsic to the device (e.g., processing capability, MLS capability, authentication type), while others will change during operation and are dynamic (e.g., battery power, mobility rate). This fact will impact the way that we utilize the MDFO.

The *Network Component Profile* class contains all of the devices connected to the MANET as "objects." A fragment of Class II is shown in Figure 11.

- **Device 1499965**
  - name: device 1499965
  - connections: {longrange, wifi, bluetooth}
  - bandwidth: {11 Mbps}
  - mobility rate: {10 mph}
  - clock speed: {33 MHz}
  - available memory: {50 MB}
  - authentication type: {biometric}

Figure 11 Fragment of the *Network Component Profile* Class

Device 1499965 has the intrinsic and dynamic parameters given, with the measured levels located within the braces. For every possible performance and security parameter, there is a separate object attribute in this class.

With respect to the "attribute value types" in this ontology, the types differ according to the anticipated input. Figure 11 has examples of a string type ({biometric}), a number type ({11}), and an enumerated type ({longrange, wifi, bluetooth}).

Lastly, the *Parameter* class is organized by category (e.g., Link QOS), see Figure 12. The entire set of parameters, independent of distributed function, is specified along with a range of allowable measured levels. Class III allows us to check the validity of input data.

▶ **Link QOS**

▶ name: link QOS	
▶ throughput:	{0, 248 Mbps}
▶ latency:	{1, 500 ms}
▶ mobility rate:	{0, 250 mph}
▶ jitter:	{0, 50 ms}
▶ Mean Opinion Score (MOS):	{0, 5}

Figure 12 Fragment of the *Parameter* Class

As discussed earlier, the power of an ontology comes from the semantic links between its classes. The links allow for the ability to infer and interpolate among the objects in the ontology. In the next section, we discuss the integration of the ontology into actual MANET operations.

E. INTEGRATING THE ONTOLOGY INTO AN OPERATIONAL MANET

In Chapter III, we give a high level introduction to the operational vision of the decision framework. We duplicate the framework diagram in Figure 13 to allow for easier reference as we explain the integration of the ontology and the linkages between the classes of the MANET Distributed Functions Ontology.

The MDFO can serve as the basis for MANET decision-making and optimization and correspondingly both control and facilitate the conduct of MANET operations. The actual ontology, the MDFO, is an abstraction that guides the construction of the operational "ontological database."

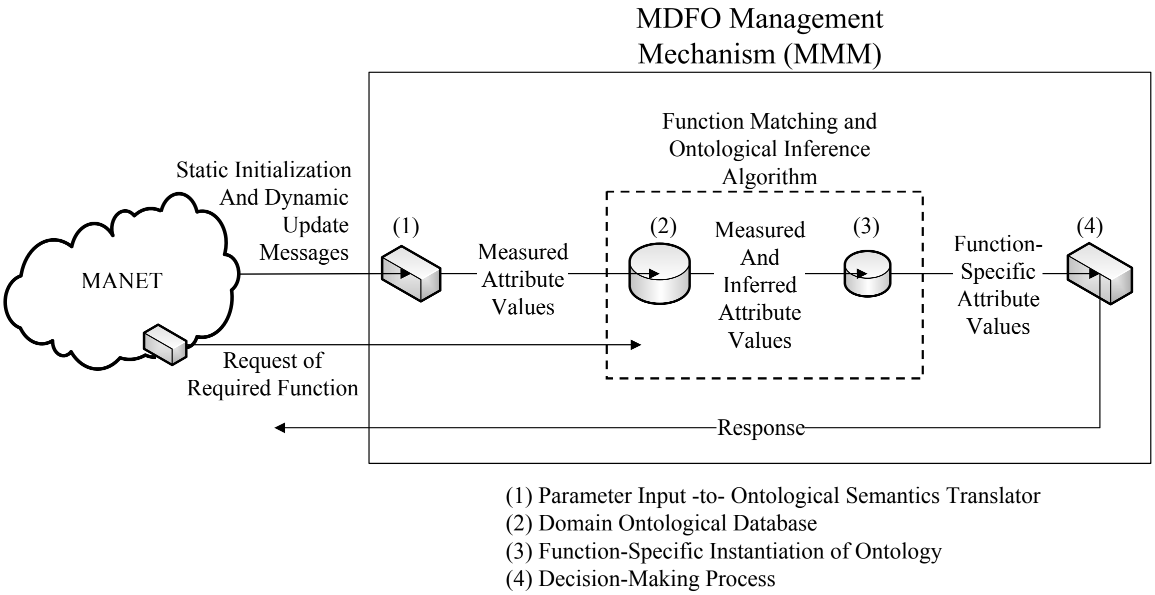

MDFO Management Mechanism (MMM)
Function Matching and Ontological Inference Algorithm
Static Initialization And Dynamic Update Messages
MANET
(1)
Measured Attribute Values
(2)
Measured And Inferred Attribute Values
(3)
Function-Specific Attribute Values
(4)
Request of Required Function
Response
(1) Parameter Input -to- Ontological Semantics Translator
(2) Domain Ontological Database
(3) Function-Specific Instantiation of Ontology
(4) Decision-Making Process

Figure 13 Operational Vision of the MANET Management Decision Framework

The MDFO Management Mechanism (MMM) is made up of a translator, the ontological database with function matching and inference capability, and the decision-making process. The translator is a mechanism for converting the information collected from the various messages circling the network, into the semantics of the ontology. The output of translation mechanism populates a database that is representative of the MDFO with both static and dynamic information about the devices within the MANET. The dynamic parameters will continue to be updated as MANET operations occur. When a function or service is required, a user or device may send a query to the MDFO. The ontology mechanism will instantiate (or take a subset of) the relevant portion of the ontology based on the service required, and an inference or interpolation may occur as needed. The inference may be required if parameters are not known or if the existing value is deemed to be outdated (e.g., when coupled with a timestamp) or unreasonable. The function-specific instantiation will then be available as input to a subsequent decision-making process.

To further explain the integration of the MDFO into MANET operations, it helps to look from the standpoint of the linkages between classes of the abstraction-level ontology. We summarize the three classes below.

Class I: *MANET Function*

Objects: function names

Attributes: categories {**Values** = parameters (partial listing)}

Class II: *Network Component Profile*

Objects: device identification (IDs)

Attributes: parameters (full listing) {**Values** = measured levels}

Class III: *Parameter*

Objects: categories

Attributes: parameters {**Values** = measured level allowable range}

In the operation of the MANET (per Figure 13), the parameters in the ontology are assigned measured levels. Classes I and III are pre-established to reflect the actual configuration of the MANET and its individual devices, but expandable as needed. In Class II, the static (intrinsic) measured levels of a portion of the parameters will also be pre-established. The dynamic measured levels (measurements or metrics extracted from the MANET context and normalized in the translator) are entered into Class II during operations, per object (device ID) and attribute (parameters). The dynamic measured levels in Class II are then checked against the allowable measured levels in Class III, where allowable ranges are defined for input data accuracy.

When a function or service is required in the conduct of MANET operations, a user or a device inputs a request. The MMM references Class I to find the minimum set of parameters related to the desired function, and then references Class II to assign values for those parameters for each device ID involved in the request. Within the Function Matching and Ontological Inference Algorithm, if either the distributed function or the complete attribute values do not exist in the MDFO, the inference rules are applied to complete the decision data and facilitate the creation of the instantiation.

The flow chart in Figure 14 shows the logical flow of MANET operations in the MMM. The parallelograms represent input, the rectangles represent processing, the diamonds represent decisions, and circles are on-page continuations (i.e., a visual "go to"), here, from the left column of the figure to the right.

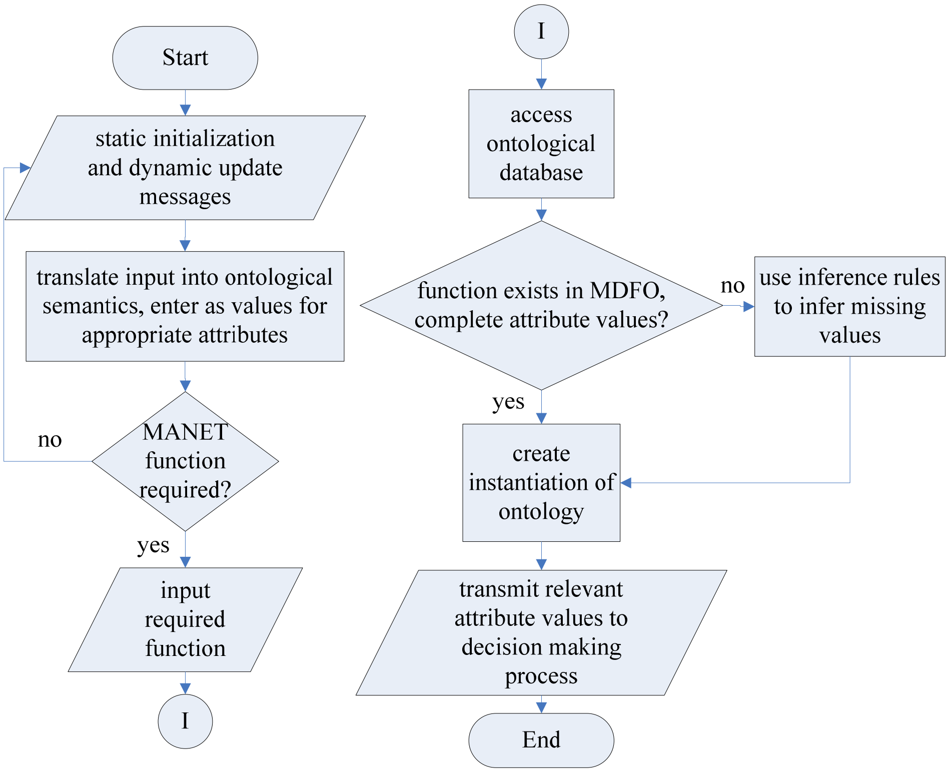

Start
static initialization and dynamic update messages
translate input into ontological semantics, enter as values for appropriate attributes
MANET function required?
no
yes
input required function
I
I
access ontological database
function exists in MDFO, complete attribute values?
no
use inference rules to infer missing values
yes
create instantiation of ontology
transmit relevant attribute values to decision making process
End

Figure 14 Flow Chart of the Operational Vision

The next section provides a detailed example to show how the *MANET Distributed Functions Ontology* may be integrated into an operational MANET.

F. DETAILED EXAMPLE

We use a realistic scenario involving five heterogeneous, MANET-capable devices in the context of CONOP #1 (see Figure 15) to illustrate the operational vision described in Section E and to demonstrate the value of integrating the *MANET Distributed Functions Ontology* into the context of a MANET implementation. The devices are the individual network components of the ontology. Each device is shown to have a lightweight router, due to the requirement that every node must be able to participate in message passing. The axes are used to give a measure of the device locations.

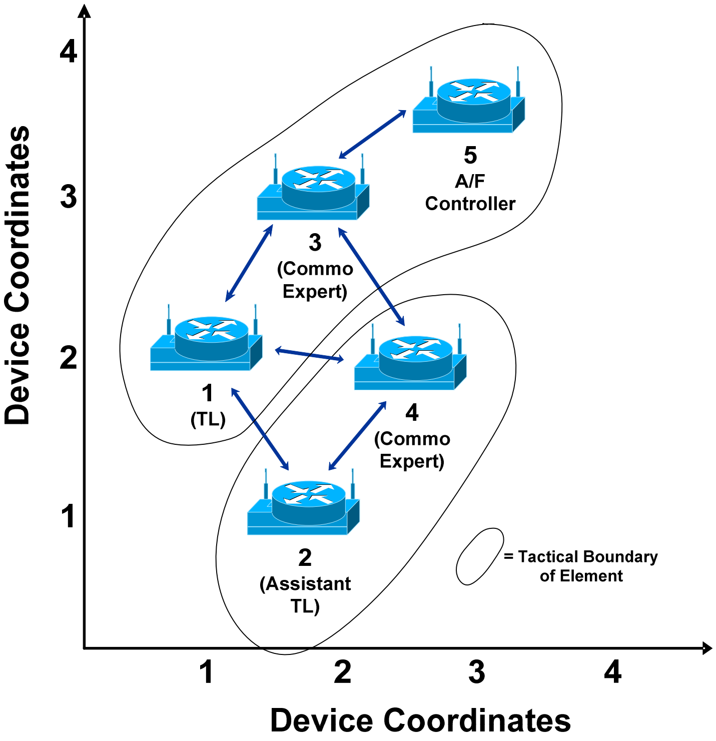


Figure 15 CONOP #1: MANET Topology

A sampling of the device characteristics appears in Table 2.

	Device 1	**Device 2**	**Device 3**	**Device 4**	**Device 5**
Process. Capability	500 MIPS	500 MIPS	800 MIPS	600 MIPS	1200 MIPS
Trust Zone					
MTM	w/ secure coprocessor	w/ secure coprocessor		enabled	w/ PKI smartcard
Total Memory	128 MB	256 MB	2048 MB	512 MB	2048 MB
Available Memory	64 MB	64 MB	1250 MB	128 MB	1250 MB
Power and battery (internet usage)	5.0 hours battery	5.0 hours battery	9.0 hours battery	7.5 hours battery	15.0 hours battery
Location	(1, 2)	(2,1)	unknown	(3, 2)	(3, 4)
Mobility rate	23 mph	2 mph	15 mph	2 mph	10 mph
Controls		lightweight PKI server			
Activated Capability	Firewall	Camera			Camera
Inactive Capability			Long-range communications	Printer	Long-range communications
Throughput	1 2 (2 Mbps) 1 3 (4 Mbps) 1 4 (2 Mbps)	2 1 (2 Mbps) 2 4 (3 Mbps)	3 1 (4 Mbps) 3 4 (7 Mbps) 3 5 (25 Mbps)	4 1 (2 Mbps) 4 2 (3 Mbps) 4 3 (7 Mbps)	5 3 (25 Mbps)
Latency	1 2 (100 ms) 1 3 (50 ms) 1 4 (100 ms)	2 1 (100 ms) 2 4 (100 ms)	3 1 (50 ms) 3 4 (50 ms) 3 5 (35 ms)	4 1 (100 ms) 4 2 (100 ms) 4 3 (50 ms)	5 3 (35 ms)
Physical Distance of Links	1 2 (350 m) 1 3 (350 m) 1 4 (500 m)	2 1 (350 m) 2 4 (350 m)	3 1 (350 m) 3 4 (350 m) 3 5 (350 m)	4 1 (500 m) 4 2 (350 m) 4 3 (350 m)	5 3 (350 m)
MLS Capability	Dedicated Mode	Dedicated Mode	Multilevel Mode	System High Mode	Multilevel Mode
Authentication	2-factor w/ biometric reader	2-factor w/ biometric reader	Password	Password	2-factor w/out biometric reader
Encryption	NSA Type 1	NSA Type 1	NSA Type 4	NSA Type 4	NSA Type 1
Current session level	SECRET	SECRET	SECRET	SECRET	SECRET
EAL	6	6	1	1	3
User Qualification	Commander	Commander	Senior Operator	Senior Operator	Junior Operator
Site	Secure operations center	Field	Open terminal (café)	Field	Field

Table 2 CONOP #1 Device and Link Characteristics

As is apparent, the MANET device information characteristics are disorganized and unwieldy. Additionally, the dynamic parameters listed above may change frequently during operation of the MANET.

1. MDFO Management Mechanism (MMM)

MMM may reside in a dedicated node, or may be assigned as would be a "cluster-head" (i.e., to the node best suited for that responsibility in terms of processing, storage, and security characteristics), or it may be distributed. To guarantee the integrity of information, this mechanism may reside in a protected system such as a Mobile Trusted Module (MTM) [117].

There are a few common ontological tools available to researchers, such as Stanford's Protégé [94], that show promise for holding data based upon the ontological model. Protégé allows users to build and populate ontologies. Additionally, the tool may be extended with a Java-based application programming interface to allow applications to access, use, and display ontologies. The current version of Protégé has yet to be extended to actual integrated network operations like the MDFO proposed in this paper. As a result of the lack of scalability of the ontological tools and resource limitations in the MANET nodes, and depending on the size of the MANET, a commercial lightweight database management system may need to be created to implement the MDFO Management Mechanism [65].

2. Initialization and Update of Static Attributes

Before any operations, the domain ontological database (shown in Figure 13) is initialized, filling an operational representation (e.g., the lightweight database management system) of Classes I and III and the static attributes of Class II. Static attributes for this detailed example (Table 2) partially include processor capability, presence of resource hiding hardware, total memory, capabilities, authentication, encryption, and the Common Criteria Evaluated Assurance Level (EAL) assigned to the device. The static attributes are not expected to vary as the MANET devices communicate.

The initialization of static (intrinsic) values occurs prior to the operational deployment of the MANET. Should a device be allowed to enter the MANET after initialization, that device transmits its static information to the MMM through a network management protocol (e.g., at the router level). For example, to represent the *external* *assurance and functional evaluation level*, a device may transmit a binary representation of the Common Criteria Evaluated Assurance Level (EAL) assigned to the device.

During operation, Class II dynamic attributes are collected, updating the device characteristics. Dynamic values can be collected by the MMM via passive listening, through polling of individual devices, or by receiving network management messages sent by devices that are new or have changed. The translator has to extract the parameter value and normalize it into terms consistent with the MDFO. The translator strips the layered header information from the obtained message and reads the data reflecting the input value. The translator will normalize the value into the correct form. In this detailed example, if the MMM receives a message containing a device's Mobility Rate in miles per hour, it will convert the value to meters per second as required. Dynamic attributes from our detailed example (Table 2) partially include the available memory, battery power, and mobility rate.

3. Processing of Requests

When a distributed function is required during network operations, a user or a device sends a request to perform an operation to the MMM. For this detailed example, we use the "cluster-head" described in Table 1. A cluster-head is a MANET distributed function that makes routing decisions on behalf of the network. This function is assigned to one of the nodes, which acts as a central controller. An example distributed function request would be encapsulated with protocol-dependent information in the header and trailer:

```
<header> cluster-head <trailer>
```

The query for the cluster-head initiates the function matching and inference algorithm within the MMM. The request is matched to the respective object(s) in Class I of the ontology. The Class I object "cluster-head" contains information on which parameters are critical for this specific function. Each object (MANET device) in Class II is then instantiated to reflect only the critical parameters. The instantiation is temporarily stored outside of the ontology. In this example, the Class II object "Device 3" is instantiated. Because the total memory is not as critical for a cluster-head as those parameters stated as attributes in Class I, it is not applicable (N/A) in the instantiation of this class. A fragment of the object "Device 3" is below.

```
name : {device 3}
mobility rate : {150} m/s
~~total memory : {2048} MB~~    # N/A
authentication : {password}
```

The parameter values are evaluated for completeness and checked for accuracy against the value ranges in Class III. If there are missing or inaccurate values, they may be collected by the MMM as outlined in Section F, 2, or they may be inferred from the existing data when possible through the use of a set of inference rules. For example, if "location" is an important parameter, Device 3's location ("unknown") may be inferred. We know that the device has attribute "site" with a value "open terminal (café)". We could access a remote (not located within the MDFO) semantic ontology of cafés that have attributes of location, and *infer* the actual location of the device that way. An alternative is to *interpolate* the information based on the link directions to the neighboring devices of known location.

As an additional example of potential inference rules, certain security related parameters may be inferred. If we know the characteristics of the hardware (secure coprocessor, TPM enabled, etc.) or the external evaluation level, we might infer that the overall security posture of the device is high, and, with reasonable confidence, assign the device high values for the remaining security parameters. Other non-MDFO ontologies may be tapped to assist with this inference action.

The output of the process is the function-specific attribute values. This output is the minimal set of values required to characterize a node's ability to perform the specific function (in this example, the cluster-head). Devices 1 through 5 would have a measured or inferred value for each of the attributes listed in Figure 10. A partial subset for Device 3 follows.

```
name : {device 3}
mobility rate : {150} m/s
authentication : {password}
```

The minimal set of parameters for the devices in the MANET may then be fed into a decision-process and the device most capable of providing the cluster-head service may be selected.

This ends our discussion of the first component of the MMM. The output of this component informs the second component, the Value Focused Thinking (VFT) Decision Analysis. We discuss the VFT Decision Analysis in detail in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTRODUCING SECURITY FACTORS INTO MANET MANAGEMENT USING VALUE FOCUSED THINKING (VFT)

The second component of the MANET Distributed Functions Ontology (MDFO) Management Mechanism (MMM) is the Value Focused Thinking (VFT) Decision Analysis. We provide an introduction to VFT as well as a discussion of background and related work. We then explain the qualitative and the quantitative models developed for MANET distributed functions. Finally, we continue the detailed example from Chapter IV by applying VFT to our CONOP.

A. INTRODUCTION

Effectively measuring the security of information systems is one of the eight information security (INFOSEC) technical hard problems identified by the INFOSEC Research Council (IRC) [55]. A lack of security metrics and an inability to combine multi-dimensional metrics into a single measure of the security of a system prevents decision-makers from having a macro-level view of security [55]. We propose integrating aspects of *Value Focused Thinking* (VFT) into security measurement in order to craft a holistic view of the security of a large system.

Decision analysts within the operations research community utilize VFT to assimilate decision-maker and user input, to incorporate dissimilar measures into decisions, and to provide structure to decision-making by combining factors in a way that is meaningful to the user. We leverage all of these benefits as well as introduce a way to modulate the security of a system based on the user's current posture.

The VFT approach is an integral part of our MANET decision-making framework. The MANET Distributed Functions Ontology (MDFO) developed in Chapter IV supports a wide range of analysis. Specifically, the ontology yields the minimal attributes required for a device to provide a given function in the MANET, along with device measurements. This input feeds into the MANET Management Mechanism (MMM) Decision-Making Process described in Chapter IV, D. The decision component includes *Value Focused Thinking* (VFT) *Decision Analysis* and *Node Choice Optimization* functions, see Figure 16. We describe the VFT Decision Analysis in this Chapter.

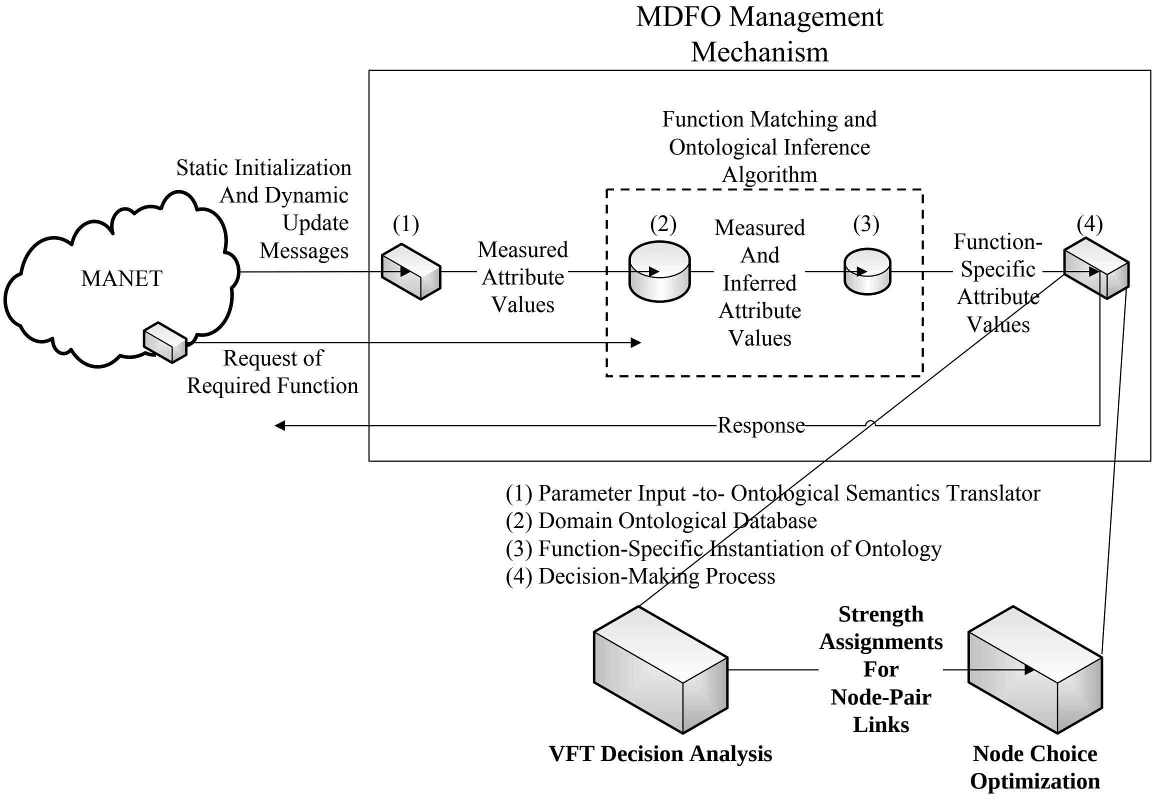


Figure 16 Expanding the Decision-Making Process

VFT Decision Analysis is centered on evaluating the *strength of the node-pair links* across the devices of the MANET. A *node-pair link* is an entity consisting of two MANET devices (“nodes”) and the single channel (“link”) that allows them to communicate. In a MANET formed from N devices, there could potentially be $(N-1)!$ node-pair links. We use the node to node link as the fundamental component of analysis rather than the node itself because the underlying purpose of a MANET is to communicate, and communication channel factors help to characterize the node connectivity. The isolated device characteristics are necessary for determining its suitability to perform a function, however, the device’s relationships to its neighbors is determined not only by the characteristics of the node itself but by the characteristics of the neighbor as well. The analysis of links ultimately leads to the selection of nodes by way of a node's association with the sum attributes of its direct links. A similar model, called the Barbell Model, exists in the area of capital allocation [74].

To properly evaluate "strength," we must manage the tradeoffs between non-security functionality and security of each node-pair link. VFT Analysis gives us the ability to handle these competing objectives. The approach involves decomposing the overall objective (strength of the node-pair link) into other sub-objectives, and ultimately, measureable attributes. The attributes that result from this structured approach are utilized in the determination of the minimal set of attributes in the output of the ontology. The VFT process also enables us to meaningfully combine dissimilar factors in an additive way through its use of value functions [67]. Dissimilar factors include measures with differing units as well as those that are non-quantifiable (e.g., categorically measured). Many computer security attributes are categorical in nature and are difficult to incorporate into decision problems. The strength assignments for the node-pair links are the output of the VFT analysis, which become the input to the *Node Choice Optimization* described in Chapter VI.

The integration of the Value Focused Thinking approach into the MANET management decision process affords four major contributions. First, VFT gives us a structured way to reason about the decision problem as well as a method of accommodating multiple, competing objectives (tradeoffs). The subjectivity inherent in decision-making is controlled in a way that is transparent, defensible, and auditable. Second, VFT allows us to integrate non-quantifiable factors into a decision process in a structured, meaningful way that is also justifiable. Third, the output of the rigorous VFT Decision Analysis directly and succinctly informs the other framework components (MDFO and Node Choice Optimization) through its attribute set determination and its strength assignments, all of which is defensible. Finally, the use of VFT enables the ability to "tune," or give emphasis to, either security or non-security functionality factors in accordance with the context in which the MANET devices are operating.

In Section B, we give additional background information about Value Focused Thinking. Section C describes the Qualitative VFT Model and Section D the Quantitative VFT Model for the MANET node-pair link strength assessment. Section E continues the detailed example we initially developed in Chapter IV, Section F outlines related work, and Section G provides conclusions and future work.

B. BACKGROUND ON VALUE FOCUSED THINKING

A decision may be defined as “a position or opinion or judgment reached after consideration” [122]. Naturally, all decision processes contain elements of subjectivity. In fact, the mere inclusion or exclusion of an attribute in a decision requires subjective judgment. A very effective way to inject defensible subjectivity is with Value Focused Thinking. VFT is a way to balance “judgments about uncertainties” with a decision-maker’s “preferences for possible outcomes” [67].

Multi-objective Analysis, also known as Value Focused Thinking (VFT), was first presented by Keeney and Raiffa in 1976 [67]. VFT is designed to enable a decision entity to make tradeoffs between competing objectives in a structured fashion. In the VFT approach, emphasis is placed upon what a decision-maker, customer, or subject matter expert values in making the decision. The opposite, more common approach is an alternative-based approach, where the focus is on studying a predetermined set of choices, or alternatives [67]. In an alternative-based approach, if a decision context is extremely complex, alternatives outside of the predetermined set may be missed, even though they may potentially result in a better outcome. The VFT approach focuses on structuring the decision problem as a well-defined hierarchy of *fundamental objectives*. A fundamental objective expresses what the decision-maker values, or finds most important, in the decision context.

Essentially, the VFT approach is about determining [69]:

(1) What is important (the fundamental objectives)

(2) A way to measure how well the alternatives support the important objectives (the attributes or measures of effectiveness)

These two elements form a structured list known as an *objective hierarchy*. An objective hierarchy is the resulting product of a thorough *qualitative analysis*. A qualitative analysis begins with a comprehensive study of the decision context using two primary sources: document reviews and interviews. The top-most fundamental objective is created and decomposed into sub-objectives and measureable attributes. The fundamental objectives and attributes are typically illustrated in a hierarchical tree-like structure or an affinity diagram. A tier consists of all those objectives or attributes that lie on the same level away from the top-most fundamental objective (the root). A well constructed hierarchy is considered the most essential part of VFT, in that it is the foundation upon which a meaningful result is based [67]. The objective hierarchy must meet certain properties in order for it to be considered "well-defined," which allows for an effective application of the VFT methodology. These properties include [69]:

- Completeness - at each tier of the hierarchy, the objectives or attributes should collectively include everything that is required to evaluate the decision alternatives ("collectively exhaustive")
- Non-redundancy - no two objectives in the same tier should overlap ("mutually exclusive")
- Decomposability or Independence - the levels of attainment of multiple objectives in the same tier should not depend on each other
- Operability - elements of the hierarchy should be understandable to the interested audience
- Small size - a hierarchy with fewer elements is easier to communicate to an interested audience, and requires fewer attributes to ultimately measure

The *quantitative analysis* component to VFT consists of two major parts. The first part is the development of *value functions* for each of the attributes created during the qualitative model development. A value function assigns a *preference value* (or a measure of the degree to which an objective is achieved by a given alternative) to every attribute. Value functions may be used for both natural and constructed attributes. Natural attributes (measurements and metrics that have common use and interpretation by everyone) may be measured in units such as dollars, meters, and miles per hour. Constructed attributes (measurements and metrics that are specific only to a given decision context) are often measured categorically in dimensions such as high/medium/low. Through the assignment of a meaningful preference value to attributes within the context of a decision, a decision entity may then combine the factors into a single value [67].

The second part of quantitative analysis is the combination of attribute preference values in such a way as to reflect the tradeoffs inherent in the decision as well as the objectives that the decision-maker values. Various methods exist to allow for the structured estimation of the relative importance of each attribute in the decision.

C. RELATED WORK

The use of Value Focused Thinking has largely been confined to a small sub-discipline within the Operations Research (OR) field. A recent, successful application of Value Focused Decision Analysis to a real world problem occurred during the Department of Defense's analysis for the Base Realignment and Closure (BRAC) decisions. Researchers had to quantify important considerations such as "power projection for joint operations" and "enhance soldier and family well-being" in order to better compare base closure alternatives. Operations researchers successfully used the VFT approach to "ensure that the Army had a technically sound, repeatable, and auditable method to determine military value" [37]. VFT is increasingly being used in business-related decision making [82].

There are very few examples of the VFT approach extending into information technology. A group of OR researchers included this approach in their methodology for the analysis of information assurance (IA) strategies, with the fundamental objective: "select the best IA strategy." This work focused on IA from an organizational perspective, including tradeoffs in the operation of an information system, the needs of the organization, and the costs and best practices of current information systems [45].

A second information technology-related research effort incorporates VFT in examining the organizational impact of mobile technology on a publishing company. This work also focuses at a very high, policy-driven level. Tradeoffs are made in the working process used at the company, the internal communication and knowledge sharing, and the impact on sales and marketing [103].

We now explain the development of the qualitative model using the VFT techniques.

D. INFORMAL QUALITATIVE VFT MODEL OF THE MANET NODE-PAIR LINK STRENGTH ASSESSMENT

The qualitative model begins with the identification of the top-tier fundamental objective. We conduct this VFT Decision Analysis in order to assign an assessment of *strength* to each member of the set of Node-Pair Links, from which the selection of the most suitable node may be eventually made. As stated earlier, a node-pair link is an entity consisting of two MANET devices ("nodes") and the channel ("link") that allows them to communicate. Due to the specific nature of the output of this process, we define the top-tier fundamental objective to maximize the *Strength of the Node-Pair Link: Cluster-head* (Figure 17). The distributed function listed (e.g., "cluster-head") will vary in accordance with the requirements of the MANET.

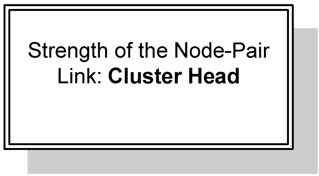
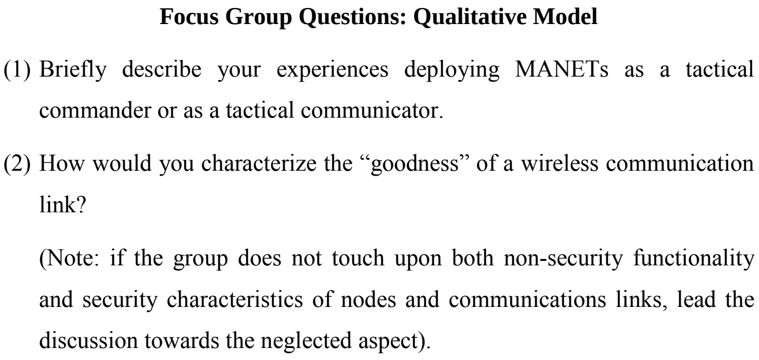


Figure 17 Top-Tier Fundamental Objective

Decomposing this top-tier objective into sub-objectives and, ultimately, measurable attributes, involves a degree of subjectivity. We control these sources of subjectivity by using the structured, defendable, auditable methodology of VFT [69]. To assist with the technical decisions involved in the development of the objective hierarchy, we require expertise and study in the areas of MANET wireless communications and computer security. Extensive literature review, subject matter expert interviews, and a focus group session helped in the development of the Qualitative Model.

The insight gained from technical experts and from a focus group centered on the important characteristics of a wireless communication channel. Focus groups are useful because group members tend to provide meaningful responses as well as generate new thoughts that are stimulated from other participants [35]. We tasked the group with the purpose of determining the objectives and factors important to successful MANET communications. The focus group consisted of experienced military commanders and communicators. The group's questions included an introductory, or "warm-up" question, followed by a research question related to the Qualitative Model, see Figure 18. We discuss the focus group questions related to the Quantitative Model in Section E.



Focus Group Questions: Qualitative Model

(1) Briefly describe your experiences deploying MANETs as a tactical commander or as a tactical communicator.

(2) How would you characterize the "goodness" of a wireless communication link?

(Note: if the group does not touch upon both non-security functionality and security characteristics of nodes and communications links, lead the discussion towards the neglected aspect).

Figure 18 Focus Group Qualitative Questions

For the subsequent data analysis, we observed patterns or themes among the participants' responses and noted suggestions that we had not previously considered. The results of combining the input from the technical experts and the focus group are listed in Table 3.

Specialty	Suggested Objective
Wireless Communications	Provide specified Quality of Service on link (throughput, link fluctuation) Ensure link availability (intermittent behavior, battery power) Incorporate physically lightweight devices Use non-CPU intensive computing within devices Provide a large amount of device buffering on both sides of link Minimize the physical distance in the MANET (device proximity to other devices) Ensure availability by minimizing the existence of obstructions
Computer Security	Maintain integrity of the link (protection against information modification, confidentiality if needed, strong cryptography keying) Secure the links from unauthorized access and hacking Control who is holding the handheld Prevent jamming of the communication channel

Table 3 Subject Matter Expert and Focus Group Insight

These suggested objectives, along with a comprehensive document review, allow us to collect sufficient knowledge about the decision context for use throughout the VFT process.

The ideas in Table 3 reflect a dichotomy that is commonly seen in computer technologies. Often, an engineering tradeoff must be made between *non-security functionality* (what a technology can do for a user) and *security* (how well the technology protects the user's information). We take this tradeoff into account by decomposing our top-tier fundamental objective into two competing second tier objectives as shown in Figure 19.

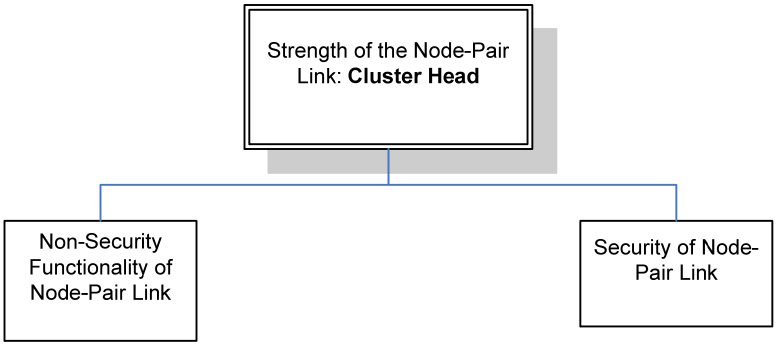

Strength of the Node-Pair Link: **Cluster Head**
Non-Security Functionality of Node-Pair Link
Security of Node-Pair Link

Figure 19 Second-Tier Objectives

Next, we focus on decomposing the "Security of Node-Pair Link" objective. From a security perspective, there are two approaches to evaluating security: strength of security mechanism and assurance of security mechanism [81]. Strength of mechanism describes the conceptual resistance to attack, assuming correct implementation, and is typically on a per-attribute basis. Assurance of mechanism describes the degree of confidence that a system component is built correctly, based upon evidence and analysis. An assurance assessment performed by a third party may take into account the attributes defining strength of mechanism, but in more of a collective fashion.

When considering strength of security mechanism, it is helpful to use the "CIA Triad" consisting of the three commonly held computer security requirements: confidentiality ("C," the concealment of information or resources), integrity ("I," the trustworthiness of data or resources, which includes both data integrity and origin integrity), and availability ("A," the ability to use the information or resource desired) [51]. The Venn diagram in Figure 20 reflects the fact that, depending on the security policy in place, these requirements may necessitate tradeoffs that depend on the overall network security objectives. A system that exhibits C, I, and A is in the portion of the Venn diagram that is labeled "Secure" with respect to all three policies. However, as these attributes are not binary, the exact position in this acceptable space will depend upon the tradeoffs in our qualitative model. Depending on the situation, the security policy may not require all three security requirements, and placement within the acceptable space may vary widely.

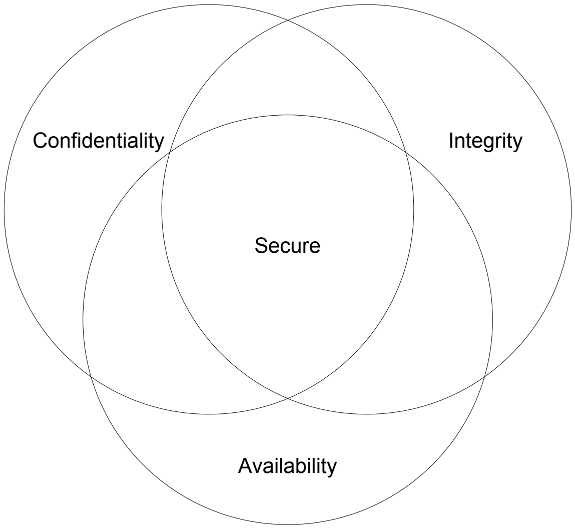


Figure 20 Computer security tradeoffs [93]

To reflect the strength of mechanism and assurance of mechanism, we decompose the *Security of Node-Pair Link* into a combined objective reflecting the confidentiality and the integrity of the node-pair link, and a separate attribute reflecting the assurance as shown in Figure 21. Note the convention of utilizing boxes for fundamental objectives and ovals for measureable attributes. We discuss the actual measurement of the attributes in Section E.

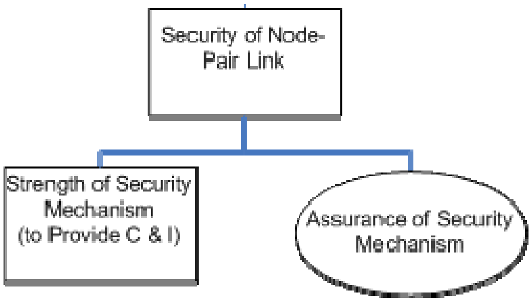

Security of Node-Pair Link
Strength of Security Mechanism (to Provide C & I)
Assurance of Security Mechanism

Figure 21 Third-Tier Objectives (Security)

Availability is assured within our decision framework in two ways. First, we include link quality factors in the decomposition of the *Non-Security Functionality of Node-Pair Link* objective. Second, we focus on availability through connectivity during the node choice optimization component in the next chapter.

Next, we focus on decomposing the "Non-Security Functionality of Node-Pair Link" objective. Both link communication attributes and node capability add value to the strength of a node-pair link. Quality of Service (QOS) is the ability to provide varying levels of performance to different applications or users in the event of limited network capacity [59][11][77]. The focus of QOS is on end-to-end communications as well as those characteristics most visible to the user [100]. When we look at two MANET nodes, it is useful to characterize the quality of the link by utilizing well established QOS metrics, including throughput, latency, jitter, and packet loss [59][11]. We have called the objective related to link communication *Provide Link Quality of Service*. Although the node characteristics naturally impact the link performance, there are capabilities provided in the nodes themselves that would allow the node-pair link to better perform a distributed function. As an example, a cluster-head may require additional memory in a node in order to store a large number of routing tables. The resulting decomposition of the Non-Security Functionality of Node-Pair Link is shown in Figure 22.

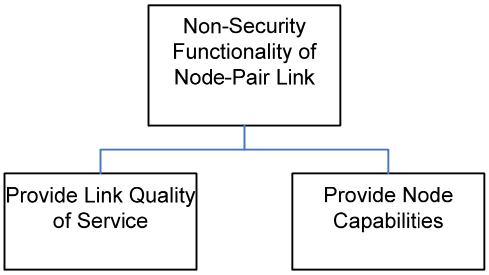

Non-Security Functionality of Node-Pair Link
Provide Link Quality of Service
Provide Node Capabilities

Figure 22 Third-Tier Objectives (Non-Security Functionality)

The final step in the development of the qualitative model is to decompose these objectives into *measureable* attributes. We have already done this with the Assurance of Security Mechanism attribute. The measure for this attribute may derive from a number of different external evaluation systems including the Trusted Computer System Evaluation Criteria (TCSEC) [31], the Common Criteria [81], and the Protection Level (PL) scheme [33]. The remaining branches of the objective hierarchy require one or more attributes that may be used to evaluate an alternative's impact on the decomposed (higher tier) objective. This is the point at which the objective hierarchies differ for the various

MANET distributed functions. An attribute central to one of the functions may not be as critical to another. For the cluster-head function, we include the following measureable attributes based upon interviews, the focus group, and literature review. The attributes are listed under their respective third-tier fundamental objective (in italics), all of which have been discussed previously.

- *Provide Link Quality of Service (QOS)*: We include two of the well established QOS metrics (throughput and latency), as well as an attribute peculiar to MANETs (mobility rate) that QOS literature does not address [59][11][16].
    - Throughput. The amount of data transferred from one device to another in a specified amount of time. Typically, throughput is less than bandwidth due to message protocol overhead. This rate at which information may be sent over a link directly impacts link QOS [32].
    - Latency. The amount of time it takes for a packet to move across a network connection. When there is high latency, users experience a delay in packet delivery, which in turn impacts the speed and capacity of their network [59].
    - Mobility rate. The faster the nodes are moving in relation to each other, the more likely that obstructions, interference, and decreased signal strength will occur [16]. This attribute is especially relevant given the mobile nature of MANET devices. Mobile devices are being embedded in vehicles, aircraft, and other fast moving objects to the detriment of link QOS.
- *Provide Node Capabilities*: We include attributes only to the extent that they are independent from their ability to support the link QOS attributes.
    - Processing capability. The number of instructions per second that the microprocessor is capable of processing. A larger number of

    instructions per second results in faster computing, which is important in distributed functions requiring many calculations.

  - Available memory. Within a computer system, memory is used to retain digital data for future computation. The memory could be collocated with the CPU chip, on the motherboard near the CPU, or external to the system (known as secondary storage). A distributed function such as the cluster-head may require the storage of data structures holding routing information. In our context, we are more concerned with the speed of data retrieval than with memory expenditure, so we distinguish between the different types of memory (e.g., cache, dynamic random access memory, flash).
  - Battery power. The ability of a device to participate in MANET functions and communications is dependent on the electrical energy that the device's battery is able to produce. Message transmission drains this energy due to antenna power requirements. Battery power is a finite resource, as once a mobile device runs out of power, a recharge operation must occur.
  - Multilevel Security (MLS) Capability. A MLS capability allows a device to process information that is classified at different security levels by using mechanisms designed to prevent a user session from accessing information that it is not authorized to view or modify. We suggest that a device with a MLS capability has increased network connectivity, as it may interact with devices of dissimilar classification levels under the right security conditions.

- *Strength of Security Mechanism (to Provide C & I)*: We include attributes that portray device's ability to support the communications policy with respect to both confidentiality and integrity during its participation in MANET communications.

- Encryption method. Encryption (the process of turning information into a form that is unreadable to only those possessing special knowledge, or a key) helps to address the two security requirements of confidentiality and integrity. The harder it is to break the cryptographic algorithm used to encrypt messages, the more secure the communication is from certain vulnerability attacks against confidentiality and integrity.

- Existence of resource hiding hardware. A device may incorporate a mechanism designed to store internal resources such as cryptographic keys in a way that obscures their presence from external observers [107][115][71]. This attribute receives attention in both the government (e.g., the Army requires "trusted computing" components in all of its systems) and in industry (e.g., Intel's ClassmatePC has a TPM) [72][57].

- Authentication type. An authentication mechanism verifies the digital identity of the user prior to a session on a device. There are two different authentication concerns in a MANET, human user-to-device, and device-to-device. To characterize a device's ability to prevent an unauthorized user from accessing MANET resources, we focus on user-to-device authentication mechanisms. The higher the number of different authentication factors (methods of verifying identity), the higher the accuracy in verifying the user identity.

- User qualification. We suggest that the user of a device may be an indicator of how well the device's security mechanisms are being employed. We assess a user's level of responsibility and technical knowledge in the measurement of this attribute.

We show the final objective hierarchy for the Cluster-head distributed function in Figure 23. The boxes represent fundamental objectives and the ovals represent measureable attributes. This hierarchy represents our Qualitative VFT Model of the MANET Node-Pair Link Strength Assessment.

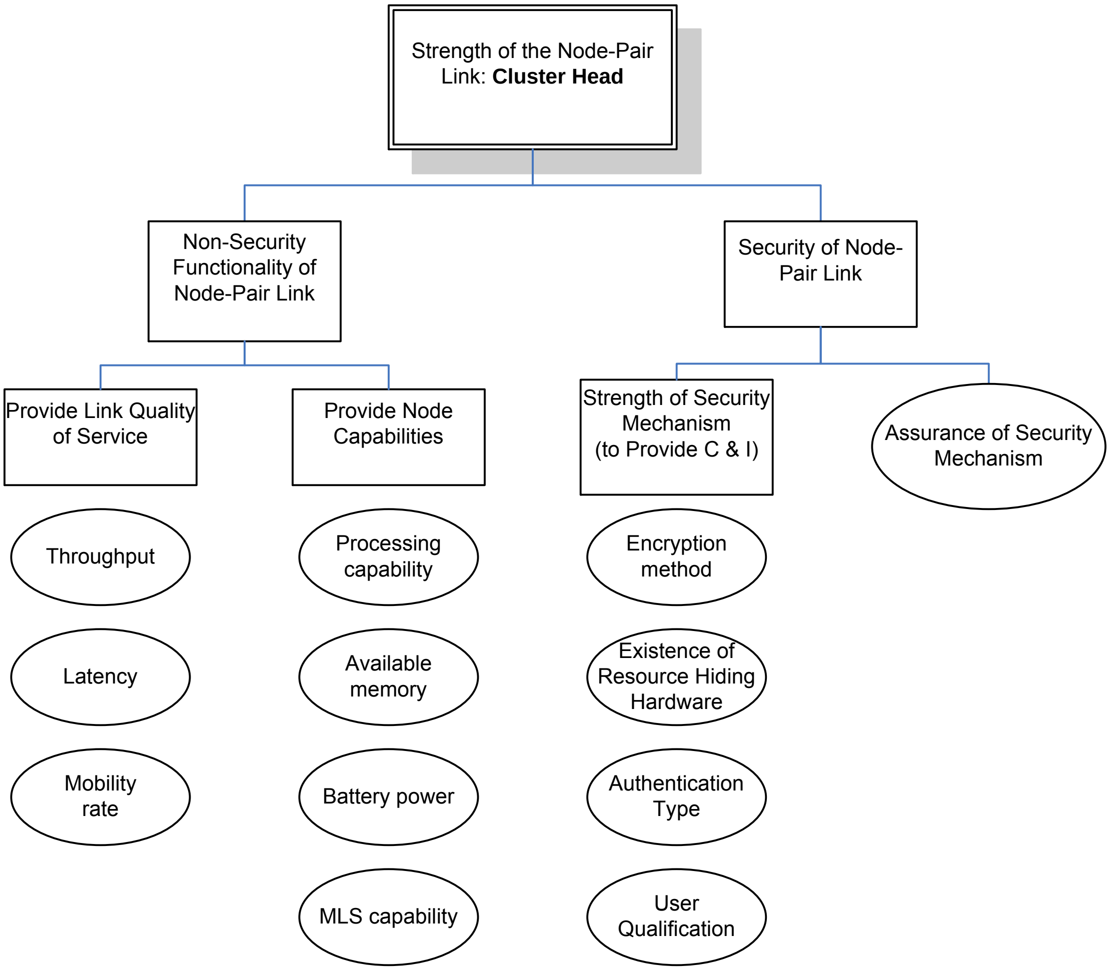

Strength of the Node-Pair Link: **Cluster Head**
Non-Security Functionality of Node-Pair Link
Security of Node-Pair Link
Provide Link Quality of Service
Provide Node Capabilities
Strength of Security Mechanism (to Provide C & I)
Assurance of Security Mechanism
Throughput
Latency
Mobility rate
Processing capability
Available memory
Battery power
MLS capability
Encryption method
Existence of Resource Hiding Hardware
Authentication Type
User Qualification

Figure 23 Objective Hierarchy for the Cluster-head Distributed Function

This final objective hierarchy informs the next component of the VFT process, the Quantitative Analysis.

E. QUANTITATIVE VFT MODEL OF THE MANET NODE-PAIR LINK STRENGTH ASSESSMENT

The qualitative model described in Section D provides the measureable attributes used to characterize the strength of a node-pair link. The value functions for each of these individual attributes (known as *single attribute value functions*) are central to the quantitative model. In fact, the resulting validity of the VFT Decision Analysis has more to do with the accuracy of these value functions than with the weighting scheme employed when combining the measures [69].

In the development of the quantitative model, we add additional focus group input based on the questions listed in Figure 24. The first question serves as a transition to the quantitative research. The subsequent questions assist in the crafting of value functions and preference value composition.

Focus Group Questions: Quantitative Model

(1) What do you know about the use of a cluster head in a MANET?

(2) The context is a ground-based MANET with a requirement for a cluster head. For the following factor:____

- what is an appropriate measure for the factor
- what are realistic minimum and maximum measurement levels for the measure
- what "value" should be assigned to the intervals between the measurement levels

Repeat this for every factor introduced by the focus group in (2).

(3) For the factors we have discussed, rate their contribution to device strength (High / Low) or function (High / Low) as appropriate.

Repeat this for every factor introduced by the focus group in (2).

Figure 24 Focus Group Quantitative Questions

As stated earlier, a value function assigns a preference value (a measure of the degree to which a given alternative achieves an objective) to every attribute. The methodology for constructing the single attribute value functions is twofold. First, we decide *how to measure* the attribute (e.g., Node Pair Mobility Rate in miles per hour) to include the range (minimum and maximum of possible scores) of its measured level. Second, we assign a *return to scale*. Used in economic theory for production functions, a return to scale is a property that analyzes the changes in output following a proportional change in its inputs [108]. When used in VFT Analysis, value functions measure the returns to scale ("preference values") of the measured levels. For example, if we "prefer" an increase in Mobility Rate from 0 miles per hour (mph) to 2 mph more than an increase from 2 mph to 10 mph, we would assign a higher preference value for that input increment. To define the returns to scale, we use the method presented in [37]. A second method, known as the ARGUS Method, has also been applied to the determination of returns to scale [30].

As the returns to scale are defined, the value functions must be either monotonically increasing or monotonically decreasing in order to allow for the eventual summation of the entire set of attributes. A monotonically increasing function means that higher measurement levels (scores) are preferred over lower ones, while a monotonically decreasing function means that lower levels are preferred over higher levels [69].

Value functions may be continuous or discrete and can take a number of different forms (e.g., linear, concave, convex, or s-curve). All of these forms may be increasing or decreasing. Our quantitative model uses discrete value functions. Our approach is to assume a *piecewise linear function*. A piecewise linear function may be mathematically defined as:

f is a piecewise linear function if and only if:
$\left(x_{1,}x_2\right)$ can be partitioned into a finite number of sub-intervals,
s.t. on each sub-interval, i, f is equal to a linear function
$f\left(x\right)=a_i x+b_i$

Figure 25 shows a piecewise linear function approximating a continuous function.

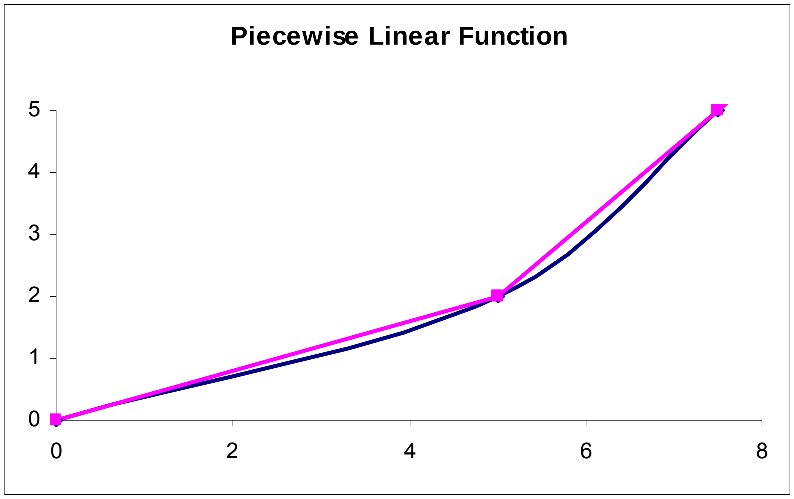


Figure 25 Piecewise Linear Function

For each of the twelve attributes specific to the Cluster-head function, we now explain the measurement levels and the value functions reflecting the returns to scale.

For the platform-driven attributes of processing capability, available memory, and battery power, we investigated the specifications for current military and civilian handheld communications devices.

Military communications devices assessed include the Falcon III AN/PRC-152 manufactured by the Harris Corporation and the AN/PRC-148 manufactured by Thales Communications, Inc. Both of these devices are heavily utilized by ground forces, are Joint Tactical Radio System (JTRS) software capable, and are MANET capable. See Figure 26 [46][109].

 AN/PRC-152	 AN/PRC-148

Figure 26 Military Handheld Radios

A user connects a handheld to the radio via a serial interface cable. The radio acts as a wireless modem for the terminal using either point to point or broadcast connections. The radio can act as an intranetworking or gateway node to exchange voice and user data [95]. The configuration is depicted in Figure 27.

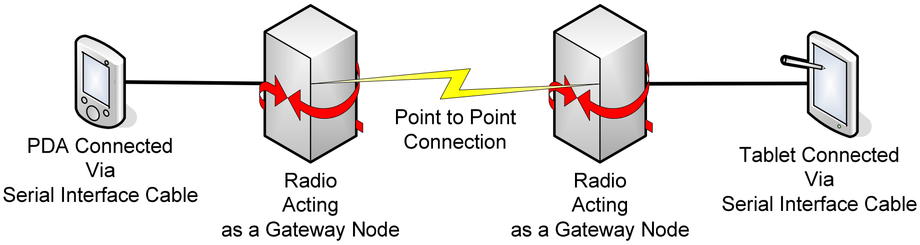


Figure 27 Radio Configuration

The limiting factor for participation in MANET communications are the radios themselves, thus it is important to consider the platform characteristics of these MANET-capable radios.

Civilian communications devices assessed included two currently popular smartphones (the BlackBerry 9000 and the iPhone) as well as a handheld computer (the OQO Model 01+). See Figure 28 [110][12][6][49][111].

 Blackberry 9000	 IPhone	 OQO Model 01+

Figure 28 Civilian Smartphones and Handheld Computers

Although the smartphones typically communicate through the public switched telephone network, they may also communicate by a point to point or broadcast connection using Wifi or Bluetooth interfaces (Figure 29). The OQO handheld communicates via the internet, but may also be configured for Wifi or Bluetooth communication.

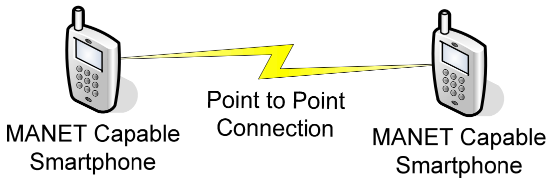


Figure 29 Smartphone Configuration

The assessment of these devices includes attributes and measurements from the product specification and allows us to see the general measured levels reached in this technology, circa 2008. As we develop the value functions, we consider the capabilities of a device as deployed within the limitations of our operational MANET context (see Chapter III).

The value function generation for the twelve measureable attributes follows. Note that we model all attributes as monotonically increasing, piecewise linear value functions except both the latency and the mobility rate, which are monotonically decreasing. We represent the measurement levels of categorical attributes (e.g., encryption method) as a bar chart. Additionally, we have previously defined each of the attributes in Section D.

- *Throughput*: High throughput results in better link quality because more information is able to be transmitted over the medium. We consider throughput to be a better gauge of link quality than bandwidth, which is a higher theoretical rate seldom realized due to factors such as overhead requirements and channel inconsistencies. We prefer high throughput. The measure is in megabits per second (Mbps), and is assigned to the link itself. Most currently popular devices support Wi-Fi (wireless networking). Standards include 802.11b (with a realistic throughput of 4.3 Mbps with a maximum throughput of 11 Mbps) and 802.11g (19 Mbps/ 54 Mbps). Other Wi-Fi standards for consideration include Legacy Wi-Fi (0.9 Mbps/ 2 Mbps), 802.11a (23 Mbps/ 54 Mbps), and the newer standards of 802.11n (74 Mbps/ 248 Mbps) and 802.11y (23 Mbps/ 54 Mbps **Error! Reference source not found.**. Another factor to consider is that the throughput for an Army brigade communications link is typically 3.088 Mbps [32]. We set the maximum measurement level at 74 Mbps, a realistic throughput using 802.11n. If there is no throughput, the preference value is 0. We show the throughput value function in Figure 30.

Attribute	Throughput	
Mbps (assigned to the link)	Mbps	Preference Value
	0	0
	2	2
	4	4
	11	7
	54	9
	74	10

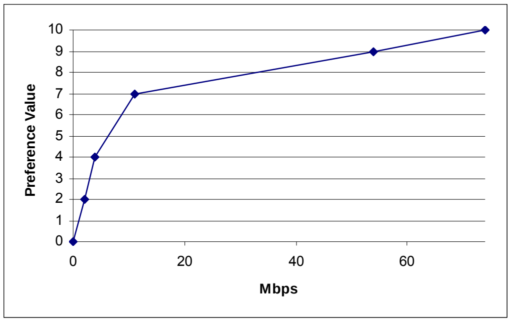


Figure 30 Throughput Value Function

- *Latency*: Latency is a measure of the delay in transmitting a message through a communications channel. Network users observe latency as a decrease in network speed (the rate at which uploads and downloads of information occur). Latency is orthogonal to throughout, in that an increase in latency coincides with a decrease in throughput. Latency may be measured as either one-way delay or round-trip delay. We use round-trip delay as the measurement level because it is more common in QOS literature [11][77]. In computer network administration, Ping tests and Traceroute determine round-trip delay in a network connection by sending a test packet to a remote destination and timing its return. We prefer low latency. The measure is in milliseconds (ms), and is assigned to the link itself. The telephone industry rule of thumb is that a human can tolerate a latency of 100 ms before his conversation breaks down [20]. DSL and cable connections typically have a latency of 25 ms, while satellite connections have a long delay of 250 ms [20]. We set the maximum measurement level at 250 ms. If there is no latency, the preference value is 10. We show the latency value function in Figure 31.

Attribute	**Latency**	
ms (assigned to the link)	milliseconds	Preference Value
	0	10
	25	7
	100	2
	250	1

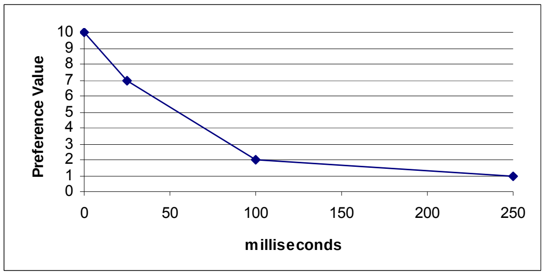


Figure 31		Latency Value Function

- *Mobility Rate*: High mobility typically results in intermittent link connectivity, potentially due to exceeding device communications distance limitations and signal degradation due to terrain obstructions. We prefer low mobility. The measure is in miles per hour (mph), and is a relative value between the devices of the Node-Pair Link. We assume the worst case, in that both devices are moving in opposite directions. Thus, the measured level is the summation of the two device mobility rates. The maximum mobility rate is 120 mph, or twice the speed of a military vehicle (the HMMWV) moving tactically at 60 mph [70]. A soldier carrying a load of 35 pounds can move at a sustained pace of 5 mph. We set the maximum measurement level to 120 mph. If the devices are both stationary, the preference value is 10. We show the mobility rate value function in Figure 32.

Attribute	**Mobility Rate**	
miles / hour (relative)	miles / hour	Preference Value
	0	10
	2	9
	10	6
	25	4
	50	1
	120	0

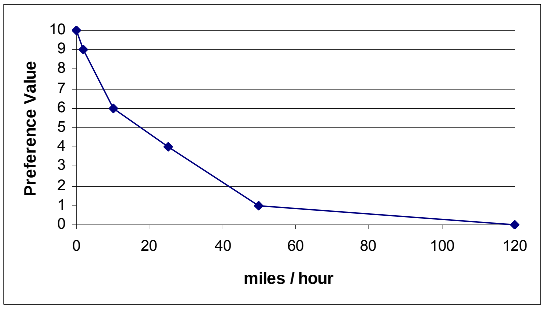


Figure 32 Mobility Rate Value Function

- *Processing Capability*: As stated earlier, a higher number of instructions per second results in faster computing, which is important in distributed functions requiring many calculations. "Instructions per second" is calculated using the microprocessor's frequency and its cycles per instruction (the number of clock cycles required for a microprocessor to execute an instruction). The calculation does not take into account the impact of memory hierarchy on processor performance [3]. We prefer high processing capability. The measure is in millions of instructions per second (MIPS). The measured level is the greatest lower bound (GLB) of the processing capability of the two devices in the Node-Pair Link. Looking at the devices studied, the Blackberry has an Intel XScale PXA270 processor (624 MHz, 800 MIPS), the iPhone has an ARM 1173 processor (620 MHz, 740 MIPS), the OQO has a Transmeta Crusoe TM5800 processor (1.0 GHz, 1,000 MIPS), and Intel's Itanium processor (1.0 GHz, 1200 MIPS) [75]. Intel's latest Core 2 Micro-architecture improves upon the processor's use of available clock cycles and power and returns to lower clock speeds [56]. We set the maximum measurement level to 1,200 MIPS. If the device has a processing capability below 500 MIPS, the preference value is 1. We show the processing capability value function in Figure 33.

Attribute	Processing Capability	
MIPS (GLB of 2 nodes)	MIPS	Preference Value
	500	1
	700	7
	800	8
	1200	10

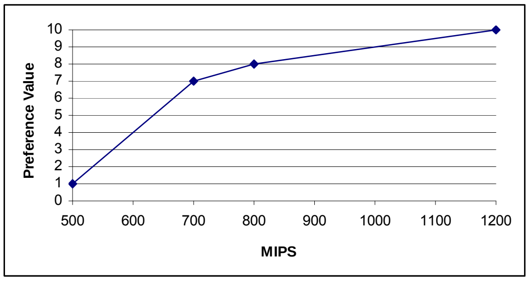


Figure 33 Processing Capability Value Function

- *Available Memory*: Greater available memory typically results in better node-pair capability because data such as computational results, keys, routing tables, and messages may be stored for efficient retrieval. Relevant types of memory include cache, dynamic random access memory (DRAM), and secondary storage such as flash memory. However, the focus of our attribute is on the amount of available memory, not the type. We discuss the types of memory for the sake of completeness. The measure is in mega bytes (MB). The measured level is the higher available memory of the two devices in the Node-Pair Link. Looking at the devices studied, the Blackberry has 1,000 MB of primary memory, the iPhone has 128 MB of RAM (if sysctl() is used, there is evidence of memory partitioning with 117 MB of physical memory and 11MB reserved for the graphics chip), and the OQO has 512 MB of DDR RAM [49]. We use these memory numbers as measurement levels since they are all on-board, or close to the CPU. Each device has secondary storage (e.g., the iPhone has 4,000 MB and 8,000 MB flash memory capability, the OQO has a 30,000 MB shock-mounted hard drive). However, in a military setting, a mobile handheld should have the capability to destroy its memory quickly (zero out sensitive data) if attacked. Flash, for example, would need to be repeatedly written to until the memory is "blackened." Because writing to a secondary device is a relatively slow process, it is best to use RAM with a battery backup, from which sensitive information can be removed more easily [99]. We also allow for improvements in technology by setting the maximum measurement level to 2,000 MB. If neither device has any available memory, then the preference value is 0. We show the available memory value function in Figure 34.

Attribute	Available Memory	
MB (higher of 2 nodes)	MB	Preference Value
	0	0
	64	3
	128	5
	512	7
	1000	9
	2000	10

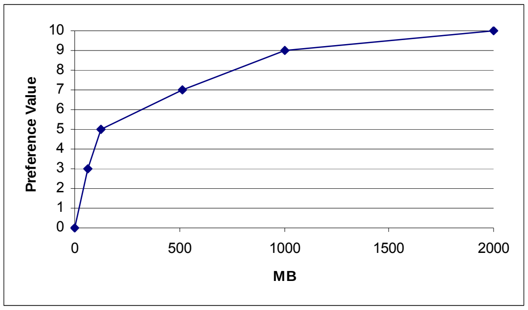


Figure 34 Available Memory Value Function

- *Battery Power*: Higher battery power typically results in better link quality because the device's antenna draws from the battery's electrical energy. Also, a device with higher battery power may be able to operate for a longer duration without undergoing a recharge operation. We prefer a higher amount of battery power. The measure is in hours of internet usage, a common gauge for civilian handheld specifications (versus watts of power output available). The measured level is the greatest lower bound (GLB) of the battery power of the two devices in the Node-Pair Link. Ten hours is typically the maximum of today's devices, but we expand the range to incorporate a 50% improvement in battery sources, to 15 hours. As batteries age, they tend to lose their ability to hold a charge. Because we use hours for this measure, this attribute will naturally reflect the battery inefficiency due to age factors. If both devices fall below one hour of battery power remaining, then the preference value is 1. We show the battery power value function in Figure 35.

Attribute	Battery Power	
hours (GLB of 2 nodes)	Hours	Preference Value
	1	1
	5	2
	7.5	4
	10	7
	12.5	9
	15	10

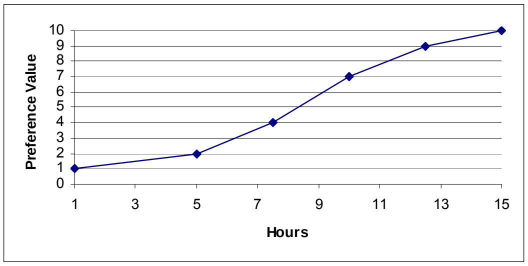


Figure 35 Battery Power Value Function

- *MLS (Multilevel Security) Capability*: For this attribute, we focus on the reachability aspect of MLS. A stronger MLS Capability typically results in better node-pair capability because the MLS device may have connectivity with a greater number of other devices (it may reach devices of different classifications as specified in the security policy). Reachability is important to the cluster-head's routing responsibilities. We prefer a strong MLS capability. The measure reflects a classification scheme of multi-user operating modes taken from within the defense community. There are 3 major operating modes [106]:
  - *dedicated mode* - all user sessions on a device have permission to access any of the data on that device. No built-in multilevel access control mechanisms are required as long as physical mechanisms prevent unauthorized users from accessing the system.
  - *system high mode* - all user sessions on a device have the correct sensitivity level to access any of the data on the device, but not all of the user sessions have a "need to know" for all of the data. The device must have a mechanism to restrict access of data to user sessions that do not need to know (e.g., file access mechanisms used in a typical multiuser system).
  - *multilevel mode* - not all user sessions on the device have sensitivity attributes that enable them to access all of the data stored on the device.

The device must have an access control mechanism that enforces MLS restrictions as well as mechanisms to enforce multiuser file access restrictions.

The measured level is the weaker of the two devices' MLS capabilities in the Node-Pair Link. We prefer a stronger MLS capability. Despite its more complex security mechanisms, a device with a multilevel mode capability may hold data of different sensitivities and allow for greater reachability to devices in different security classes. As a result, the maximum measurement level is multilevel mode. If either device has no mechanism in place to prevent unauthorized access, the preference value is 0. We show the MLS capability value function in Figure 36.

Attribute	**MLS Capability**	
Multi-User Operating Modes (weaker of 2 nodes)	MLS Capability	Preference Value
no mechanism to prevent unauthorized access	0	0
dedicated mode	1	2
system high mode	2	6
multilevel mode	3	10

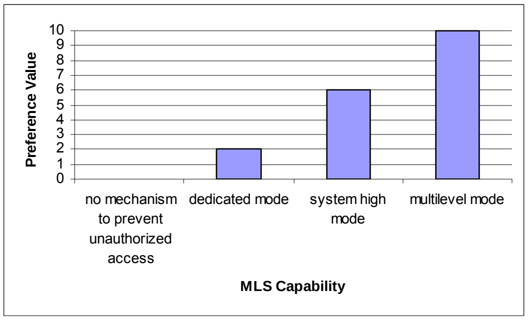


Figure 36 MLS Capability Value Function

- *Encryption Method*: A strong encryption method typically results in better Node-Pair Link security because a higher rated encryption algorithm better protects against vulnerability attacks on the confidentiality and integrity of transmitted information. We prefer a stronger encryption method. The measure incorporates the National Security Agency's (NSA) encryption classification scheme [104]:
    - NSA Type 1 Encryption is a system-based evaluation of classified and controlled cryptographic items. Algorithms used in NSA-approved Type 1 encryption systems include the Advance Encryption Standard (AES) and Skipjack.

- NSA Type 2 Encryption is also a system-based evaluation, but the cryptographic items may not be used for classified information. Type 2 encryption contains NSA-approved encryption algorithms such as Cordoba.
- NSA Type 3 Encryption is algorithm-based, with many of the provably stronger encryption algorithms included (e.g., AES, 3DES). These algorithms are appropriate for sensitive, unclassified information on non-national security systems.
- NSA Type 4 Encryption is algorithm-based, with notably weaker (defined as "broken") encryption algorithms. These algorithms cannot be used on classified information, and are exportable.

The NSA Encryption classification scheme is a proper measure because it not only takes into account the strength of the encryption algorithm, but also includes strength of encryption frameworks such as public key cryptography, symmetric key cryptography, and Elliptical Curve Cryptography (ECC). ECC has a great potential for use in mobile devices because it is a secure, lightweight encryption scheme. The military's JTRS radios use NSA Type 1 endorsed encryption. If devices within a deployed MANET use different encryption schemes, an interoperability problem exists. The MANET itself may require mechanisms to handle the segmentation of the network due to the differing encryption schemes. The measured level is the greater lower bound (GLB) of the encryption category of the two nodes. The maximum measurement level is Type 1 encryption. If the devices of the node-pair do not employ encryption, the preference value is 0. We show the encryption method value function in Figure 37.

Attribute	Encryption Method	
Type (GLB of 2 nodes)	Encryption Method	Preference Value
None	0	0
NSA Type 4 encryption algorithm	1	1
NSA Type 3 encryption algorithm	2	4
NSA Type 2 encryption system	3	8
NSA Type 1 encryption system	4	10

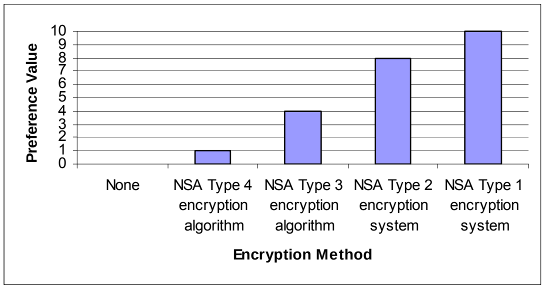


Figure 37 Encryption Method Value Function

- *Existence of Resource-Hiding Hardware*: The stronger the type of resource-hiding hardware utilized, the better the Node-Pair Link security due to the fact that secrets such as keys may be protected from unauthorized disclosure and secure ("hidden") computation may occur. These resource-hiding capabilities serve to increase the protection of a system against confidentiality and integrity attacks. We prefer a stronger implementation of resource-hiding hardware. The measure incorporates five categories, three of which follow the *Mobile Trusted Module* (MTM) architecture. The MTM specification is derived from the *Trusted Platform Module* (TPM), but has applicability to lightweight, mobile devices [107][115]. The specification itself outlines standards for the API level and format, but does not specify implementation in order to give a system designer flexibility in the hardware level. Chip makers create the lowest level of services defined in the specifications. They incorporate the specification either as discrete silicon chips, chipsets, or system-on-a-chip [118]. The higher measurement levels include MTM enabled with a secure processor (e.g., XOM, AEGIS, VSCOP), MTM enabled with a secure co-processor (also referred to as a micro-controller, e.g., tamper-resistant crypto modules such as IBM's 4758, the Chinese-made Hengzhi Security Chip being put into Lenovo PC's, and Intel's Southbridge chipset being used in some TPM implementations), and MTM enabled with PKI Smartcard (e.g., the IBM Embedded Security System Chip, a public key smartcard). A device may also be Trusted Zone Enabled (e.g., Juniper Networks makes a Netscreen Hardware Firewall that utilizes trusted and untrusted zones) [83]. The measured level is the existence of the capability in either node. If the devices of the node-pair do not have resource-hiding hardware, then the preference value is 0. We show the existence of resource hiding hardware value function in Figure 38.

Attribute	**Existence of Resource-Hiding Hardware**	
Trust Zone / MTM Enabled (capability exists in either node)	Resource-Hiding Hardware	Preference Value
None	0	0
Trusted Zone Enabled	1	2
MTM enabled with PKI smartcard	2	6
MTM enabled with secure coprocessor (micro-controller)	3	8
MTM enabled with secure processor	4	10

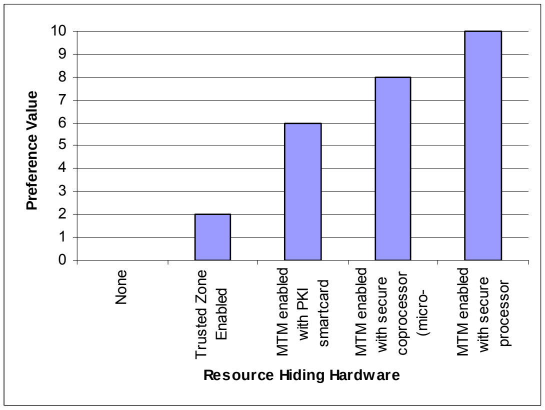


Figure 38 Existence of Resource Hiding Hardware Value Function

- *Authentication Type*: The stronger the authentication type and the greater the number of authentication factors used, the better the Node-Pair Link security since the probability of a correct user identification is increased. Authentication protects the origin integrity of data. We prefer a stronger authentication type. The measure incorporates six measurement levels, all with various combinations of the primary authentication methods: information known only to the user (e.g., password), an item in the user's possession (e.g., token or key), and an intrinsic physical or behavioral trait specific to the user (e.g., biometric). The measured level is greater lower bound (GLB) of the authentication type of the two nodes. Currently, passwords are the most widely used authentication mechanism, and there is interest in two factor authentication for smartphones including Smartphone Security v7.3 and RSA SecurID Software Token 2.2 [112]. The maximum measurement level is three-factor authentication, which would also include a biometric. If the devices have a single password authentication scheme, the preference value is 1. We show the authentication type value function in Figure 39.

Attribute	**Authentication Type**	
n-factor authentication (GLB of 2 nodes)	n-Factor Authentication	Preference Value
pwd	1	1
token	2	2
bio	3	5
two-factor authentication without bio	4	6
two-factor authentication with bio	5	8
three-factor authentication with bio	6	10

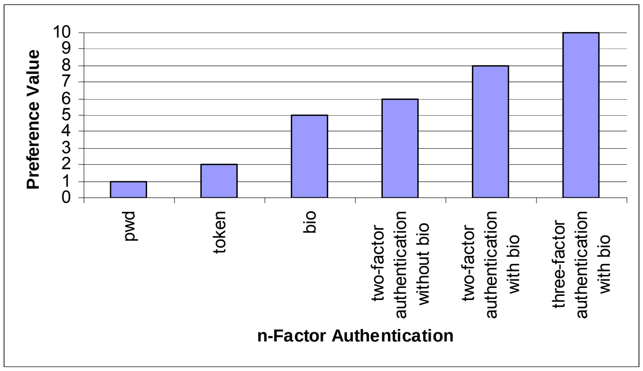


Figure 39 Authentication Type Value Function

- *User Qualification*: We suggest that a higher level of user responsibility and technical knowledge is an indicator that a device is configured in a secure fashion, so the resulting Node-Pair Link security is higher. User qualification helps in ensuring the integrity of information. We prefer a higher classification of user qualification. The measure incorporates five measurement levels. In the military, a high level manager has increased responsibility, more technical expertise, and the ability to obtain immediate technical support. An administrator of a network is the technical expert for the device and the network. We define a senior operator as more experienced with technology than a junior operator. The measured level is that of the node with the lower ranking. The maximum measurement level is the commander or high level manager. If one of the devices has an unknown user, the preference value is 0. We show the user qualification value function in Figure 40.

Attribute	**User Qualification**	
user qualification (of lower ranking node)	User Qualification	Preference Value
unknown	0	0
junior operator	1	2
senior operator	2	6
administrator	3	9
commander or manager	4	10

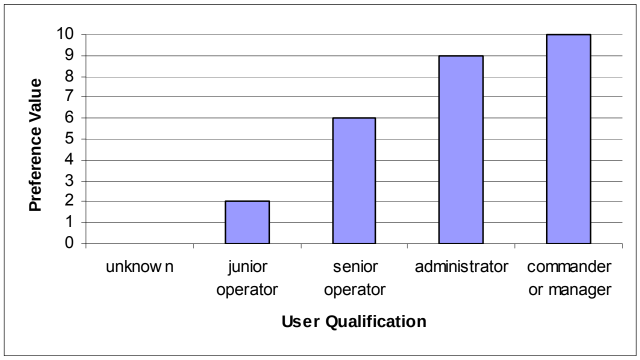


Figure 40 User Qualification Value Function

- *Assurance of Security Mechanism*: A high assurance of security mechanism means that a system component (e.g., a firewall) is built with rigor, based upon evidence and analysis. A third-party rigorous assessment provides a collective, holistic view of the component's security. Examples of external evaluation systems include the Trusted Computer System Evaluation Criteria (TCSEC) [31], the Common Criteria [81], and the Protection Level (PL) [33]. We prefer high assurance of mechanism. As a measure, we have chosen the current standard of the Common Criteria, with its numerical rating system of the Evaluation Assurance Level (EAL). The EAL rating scheme goes from unrated up to an EAL of 7. The measured level is the greater lower bound (GLB) of the rating of the two devices. Currently, the highest evaluated mobile platform is the Blackberry, which is rated at a 2+ [12]. Since the establishment of the National Information Assurance Partnership (NIAP) in 1997 (the organization that manages the Common Criteria process), there have been 3 out of a total of 127 evaluated systems in the EAL 5 to EAL 7 range [9]. In our measurement levels, we allow for both technical growth and for an increase in the number of commercial vendors willing to spend the time and expense to have their products rated in the Common Criteria system. The maximum measurement level is an EAL rating of 7. If a device is unrated or has a rating of 1, the preference value is 0. We show the assurance of security mechanism value function in Figure 41.

Attribute	Assurance of Security Mechanism	
EAL (GLB of 2 nodes)	EAL	Preference Value
	1	0
	2	3
	3	4
	4	5
	6	8
	7	10

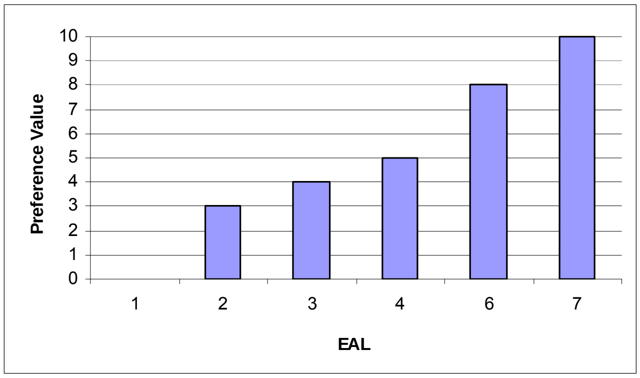
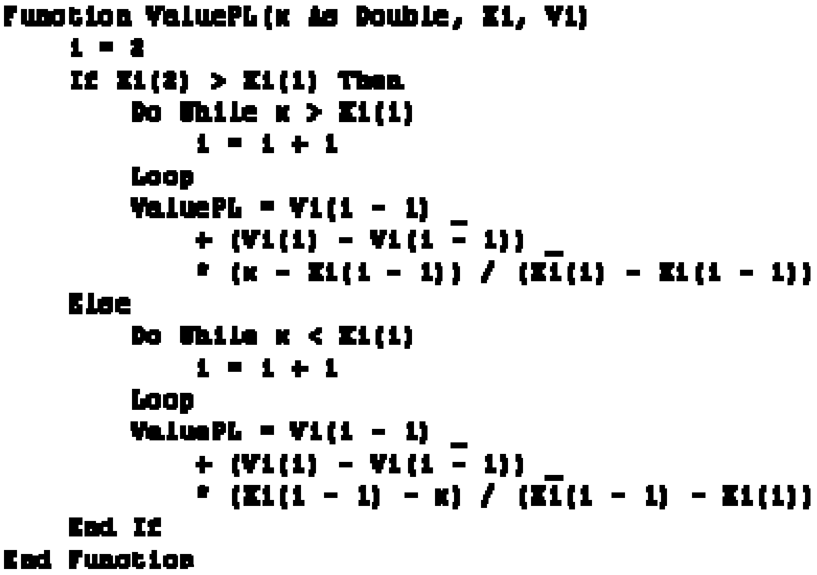


Figure 41 Assurance of Security Mechanism Value Function

The purpose of the twelve value functions developed above is to convert between the measured levels of a device for a given attribute and the preference value created from decision-maker input. As a first step towards an automated means of conducting this conversion, we enter the twelve value functions into an Excel spreadsheet. Given a measured level for an attribute, a Visual Basic Macro performs the preference value assignment by iterating through the piecewise linear function's sub-intervals, see Figure 42. An underscore (_) represents a continuation to the next line.



```
Function ValuePL(x As Double, Xi, Vi)
    i = 2
    If Xi(2) > Xi(1) Then
        Do While x > Xi(i)
            i = i + 1
        Loop
        ValuePL = Vi(i - 1) _
            + (Vi(i) - Vi(i - 1)) _
            * (x - Xi(i - 1)) / (Xi(i) - Xi(i - 1))
    Else
        Do While x < Xi(i)
            i = i + 1
        Loop
        ValuePL = Vi(i - 1) _
            + (Vi(i) - Vi(i - 1)) _
            * (Xi(i - 1) - x) / (Xi(i - 1) - Xi(i))
    End If
End Function
```

Figure 42 Preference Value Assignment Visual Basic Macro [69]

The Macro in Figure 42 contains a single function, the Value Piecewise Linear function. ValuePL( ) takes 3 arguments (x, X_i, V_i) as input.

x = the measured level of the attribute
X_i = the attribute measurement levels (x-axis)
V_i = the preference values (y-axis)
(i = a counter that allows iteration through the segments)

The "If" part of the function is for monotonically increasing value functions while the "Else" part is for monotonically decreasing functions. The "Do While" loop iterates through the straight line segments of the piecewise linear function and identifies the segment in which the measured value (x) falls. The "ValuePL" equation calculates the preference value using the equation for the identified segment.

The end result is a preference value assignment for each of the attributes for a given Node-Pair Link. Through the assignment of a meaningful preference value to attributes within the context of the decision, the decision entity may then combine the factors into a single value [67].

The second part of quantitative analysis is to combine the attribute preference values in such a way as to reflect the decision tradeoffs and the decision-maker's objectives. We call this *preference value composition*. We use the swing-weight matrix technique for the structured weighting of the relative importance of each attribute in the decision. The utility function that combines the individual attributes with respect to each alternative node-pair link consists of an additive function, as described below.

i = the index of the individual attribute being considered, up to n attributes
(for this example, $i = \{1,...,12\}$)
x = the node-pair link being evaluated
$v_i(x)$ = the individual attribute (i) preference value assignment
for the evaluated node-pair link (x)
w_i = the relative weight assigned to the individual attribute (i)
$v(x)$ = the preference value assignment for the node-pair link being evaluated (x)

The Preference Value Composition Function:

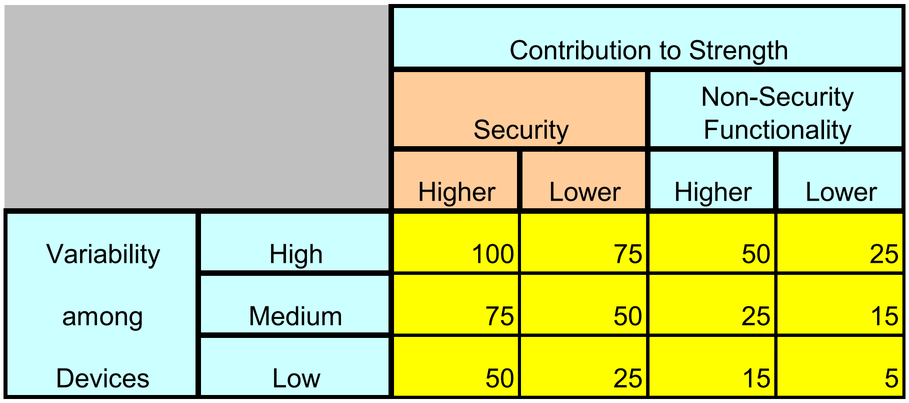
$$v(x) = \sum_{i=1}^{n} w_i v_i(x)$$

The weights across all of the individual attributes (i) must sum to 1:

$$\sum_{i=1}^{n} w_i = 1$$

This overall preference value assignment, $v(x)$, is specific for a given node-pair link. This preference value represents the *Strength of the Node-Pair Link*.

The final source of subjectivity that we must control is in the assignments of the weights (w_i). To make a meaningful, defendable, and auditable weight assignment based on decision-maker input, we use the Swing Weight Matrix Method. This approach was first developed for use in the U.S. Army's Base Realignment and Closure (BRAC) analysis [37], to better assess and explain attribute weights. The matrix is central to our ability to make the trade-offs between the multiple, competing objectives identified in our qualitative analysis. We use the weight matrix shown in Figure 43 for our VFT Decision Analysis.



		Contribution to Strength			
		Security		Non-Security Functionality	
		Higher	Lower	Higher	Lower
Variability among Devices	High	100	75	50	25
	Medium	75	50	25	15
	Low	50	25	15	5

Figure 43 Assigning Attribute Weights

The Swing Weight Matrix Method defines two factors that impact attribute weighting: *importance* and *variation*. The technique follows four steps [37]:

(1) Define the importance and variance dimensions

We define the importance dimension as the extent to which an attribute contributes to strength (our top-tier fundamental objective). In a normal MANET mode of operation where time is not critical, devices may implement all security mechanisms and adhere to all security policy, even if there is some loss of non-security functionality. We rank contributions to security higher in importance than the non-security related functionality in our function assignment decision. The security-related attributes are in the first two columns and the non-security functionality-related attributes are in the right two columns of the matrix.

We define the variance dimension as the extent to which an attribute changes in measured level across the node-pair links throughout the MANET. In highly uniform MANETs where the devices are purchased from the same vendor and have similar characteristics, there is low variability among many of node-pair links. Factors that change during run time (e.g., battery power and available memory) may have high variance across the devices. Military networks are often highly uniform.

The matrix shown in Figure 43 reflects an increasing contribution to strength from right to left and a decreasing variability among devices from top to bottom.

(2) Place the measures in the matrix

After defining the matrix, we place the attributes into the matrix. Decision-maker and focus group discussion is important in this step. We assess an attribute based on both importance and variability. Comparisons across attributes also help to order the attributes. The end product of this step is the matrix with our 12 attributes placed in appropriate cells, Figure 44.

		Contribution to Strength			
		Security		Non-Security Functionality	
		Higher	Lower	Higher	Lower
Variability among Devices	High	Encrypt	Authent	ThruPut BtryPwr	Latency MobRate
	Medium	Assur	UserQual	ProcCap AvlMem	
	Low	RsrcHide			MLS Cap

Figure 44 Attribute Placement into the Swing Matrix

(3) Assess the swing weights

Next, we assign a swing weight, f_i, to all the matrix cells. In all weighting techniques, it is important to guarantee the proper range of weights between the highest and lowest weighted attribute [37]. To ensure that we have significant variability between the preference values assigned to the individual node-pair links, we vary the swing weights from 5 to 100 with steps of varying sizes (100, 75, 50, 25, 15, and 5). The highest swing weight (f_1 = 100) is in the upper left cell, the lower weight in the bottom right cell.

(4) Calculate the global weights

We generate the relative weights assigned to each of the individual attributes (w_i) with a normalization function. The Normalized Global Weight Function looks like:

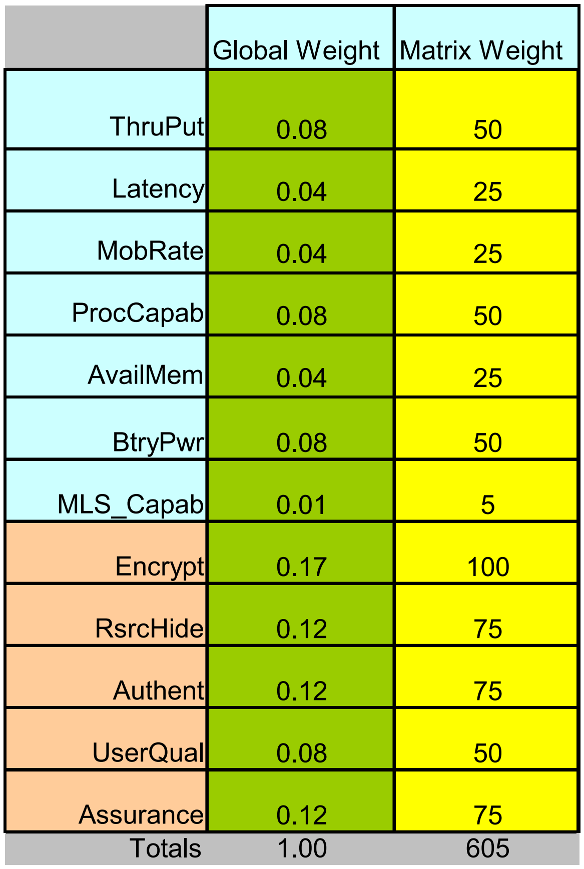
$$w_i = \frac{f_i}{\sum_{w_i}^{w_n} f_i}$$

$i =$ the index of the individual attribute being considered, up to n attributes here, $i = \{1, \ldots, 12\}$

$f_i =$ the matrix swing weight assigned to the individual attribute (i)

$w_i =$ the relative weight assigned to the individual attribute (i)

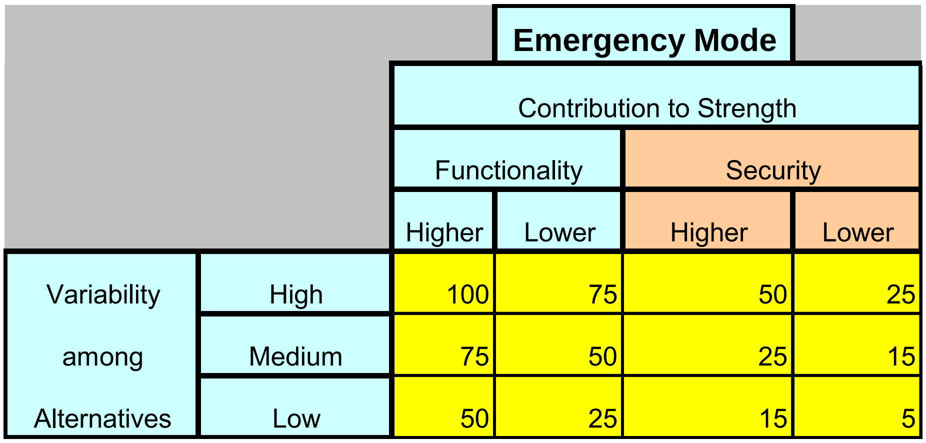
We list the resulting normalized global weights in Table 4. We use the resulting normalized global weights in the Preference Value Composition Function.



	Global Weight	Matrix Weight
ThruPut	0.08	50
Latency	0.04	25
MobRate	0.04	25
ProcCapab	0.08	50
AvailMem	0.04	25
BtryPwr	0.08	50
MLS_Capab	0.01	5
Encrypt	0.17	100
RsrcHide	0.12	75
Authent	0.12	75
UserQual	0.08	50
Assurance	0.12	75
Totals	1.00	605

Table 4 Weight Assignments in Normal Mode

An interesting feature that arises from the use of the Swing Weight Matrix Method is the ability to "tune security," or to reassess the importance of security to MANET function assignment. We have the ability to vary attribute weightings according to a given context. In our analysis above, we discussed a MANET operating in normal mode. When an emergency occurs and time is critical, we often must turn off some security in order to maximize non-security functionality. In an emergency context, decision-makers may change the importance dimension to reflect a higher priority on non-security functionality. The decision-makers may decide that the risk of unintended information disclosure or modification is acceptable in order to attend to the emergency. To show how to tune the weightings of our attributes, we alter the contribution of the attributes in the swing weight matrix by shifting non-security functionality to the left side of the matrix, where the assigned weightings are higher (Figure 45).



		Emergency Mode			
		Contribution to Strength			
		Functionality		Security	
		Higher	Lower	Higher	Lower
Variability among Alternatives	High	100	75	50	25
	Medium	75	50	25	15
	Low	50	25	15	5

Figure 45 Assigning Attribute Weights in Emergency Mode

This reweighting amounts to a shift in the decision-maker's emphasis and a corresponding change in the tradeoffs between objectives. The final Node-Pair Link strength ratings change, as those devices with higher functionality become preferred in the selection of a MANET function (e.g., Cluster-head).

The VFT Decision Analysis component of the framework described above is now applied to the detailed example.

F. DETAILED EXAMPLE

In this section, we resume our development of the detailed example in order to apply the VFT Decision Analysis component of our decision framework to a realistic scenario. We continue to make use of the first Concept of the Operation (CONOP #1): the five-device MANET. The network topology for this CONOP is shown again in Figure 46 for convenient reference.

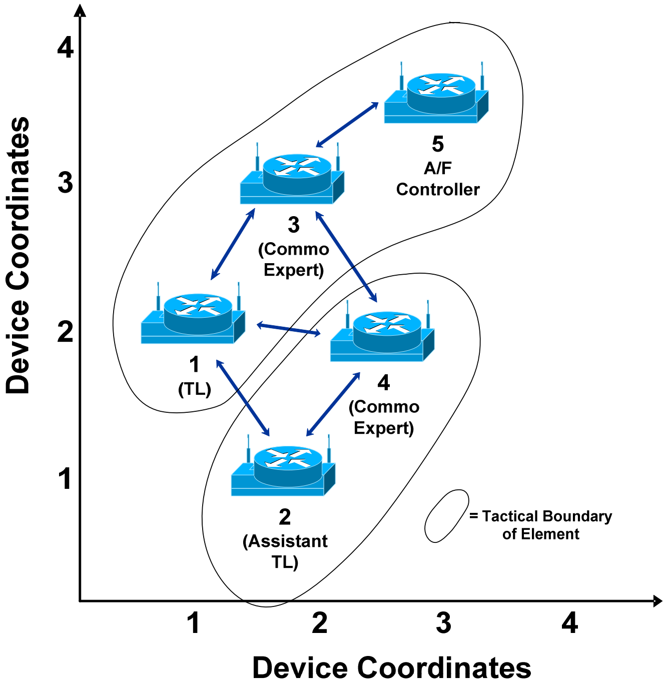


Figure 46 CONOP #1: MANET Topology

The output of the ontological component of the MDFO Management Module (MMM) is the minimal set of function-specific attribute values. This data set is the input of the VFT Decision Analysis. We demonstrate the qualitative analysis and the quantitative analysis of the VFT component of the MMM as applied to CONOP #1.

1. Qualitative Analysis

For CONOP #1, the top-tier fundamental objective mirrors the one in the qualitative analysis that we perform in Section V, D. The objective is to maximize the *Strength of the Node-Pair Link: Cluster-head*. As a result, the qualitative model is the same. The final objective hierarchy, which identifies fundamental objectives and attributes, is repeated in Figure 47.

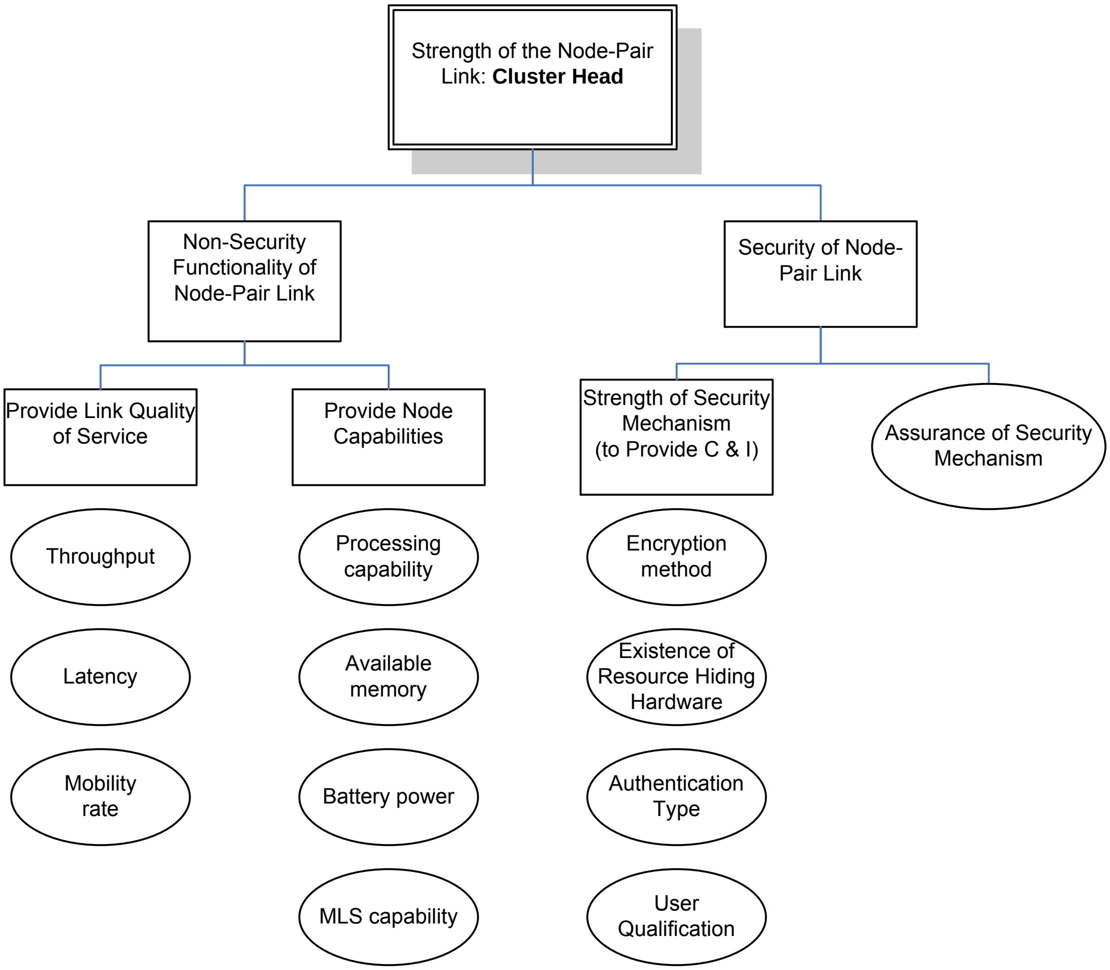
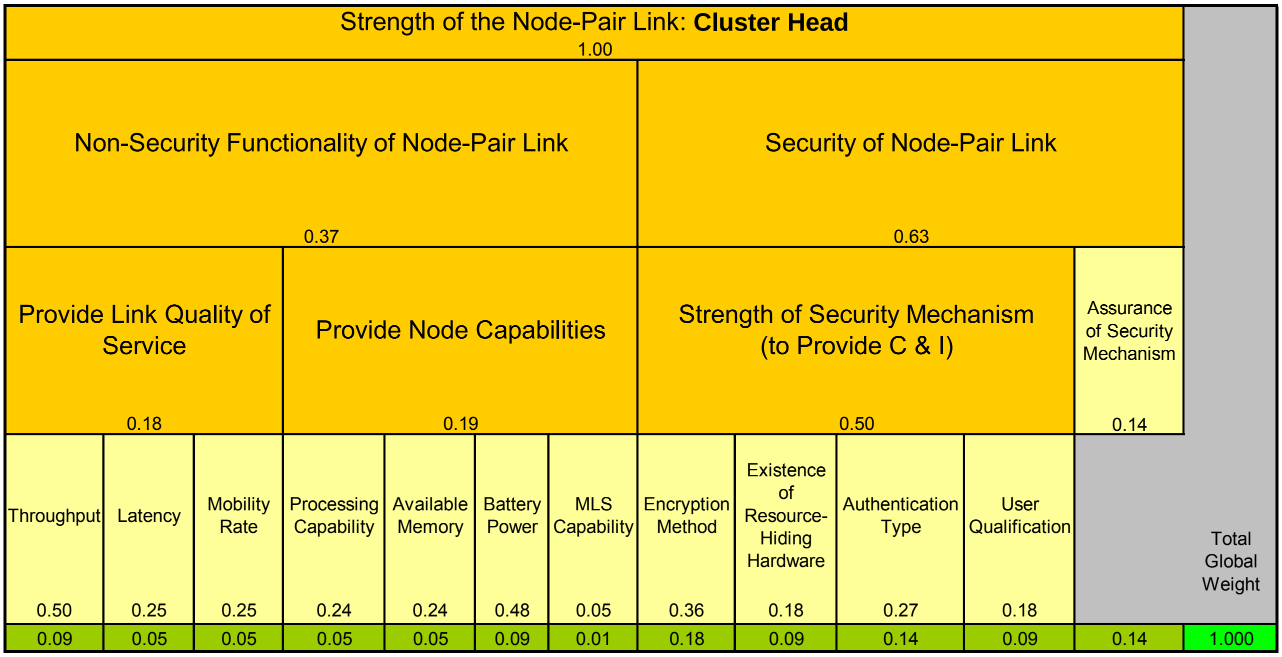

Strength of the Node-Pair Link: **Cluster Head**
Non-Security Functionality of Node-Pair Link
Security of Node-Pair Link
Provide Link Quality of Service
Provide Node Capabilities
Strength of Security Mechanism (to Provide C & I)
Assurance of Security Mechanism
Throughput
Latency
Mobility rate
Processing capability
Available memory
Battery power
MLS capability
Encryption method
Existence of Resource Hiding Hardware
Authentication Type
User Qualification

Figure 47 Objective Hierarchy for the Cluster-head Distributed Function

This final objective hierarchy informs the next component of the VFT process, the Quantitative Analysis.

2. Quantitative Analysis

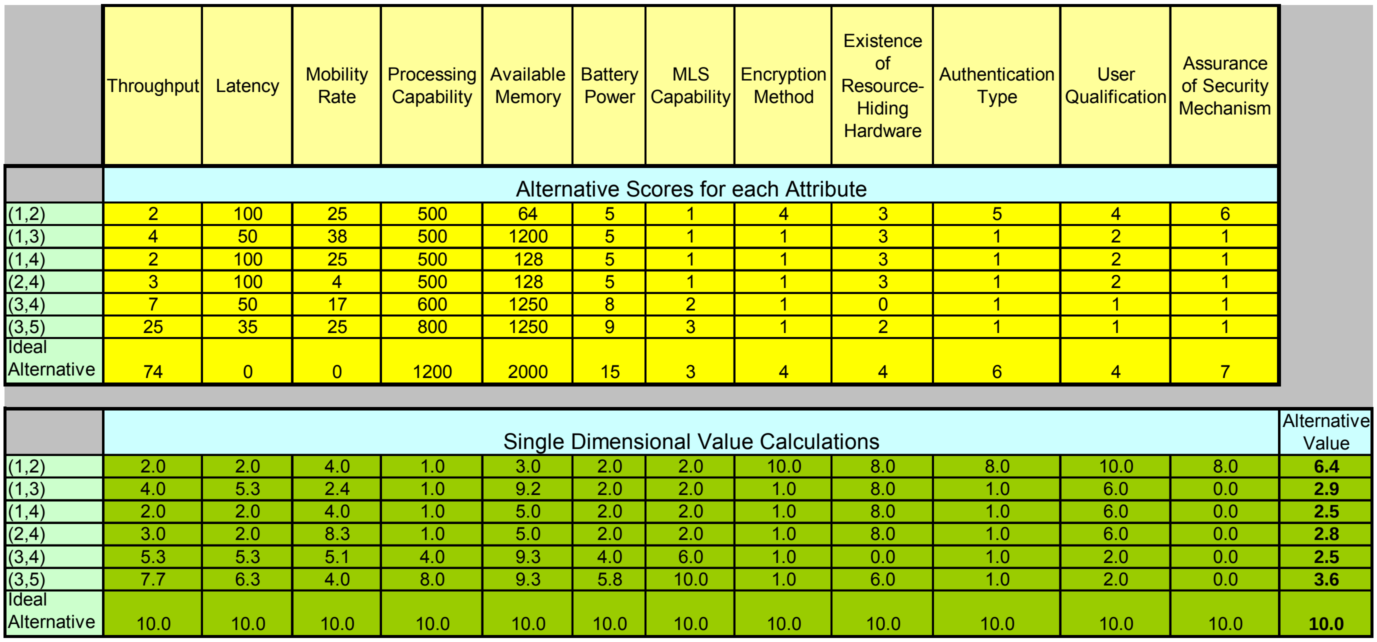
For this example, the practical application of the quantitative analysis is spreadsheet-based. The objective hierarchy developed above provides the headings for the Quantitative Model spreadsheet, see Figure 48. The top-level fundamental objective is in the upper portion of the fragment, followed by the second and the third tier objectives. Note that the darker shade represents fundamental objectives while the lighter shade represents the measurable attributes. The numbers beneath the objectives and the attributes indicate the local weights, or the weights with respect to the other elements of the same parent objective. The bottom row lists the global weights of the attributes with respect to the entire system. We discuss the weight vector generation later in this section. Note that the total global weight sums to 1.0.



<table>
<tr><td colspan="12">Strength of the Node-Pair Link: <b>Cluster Head</b>
1.00</td><td rowspan="4">Total
Global
Weight</td></tr>
<tr><td colspan="7">Non-Security Functionality of Node-Pair Link
0.37</td><td colspan="5">Security of Node-Pair Link
0.63</td></tr>
<tr><td colspan="3">Provide Link Quality of Service
0.18</td><td colspan="4">Provide Node Capabilities
0.19</td><td colspan="4">Strength of Security Mechanism (to Provide C & I)
0.50</td><td>Assurance of Security Mechanism
0.14</td></tr>
<tr><td>Throughput
0.50</td><td>Latency
0.25</td><td>Mobility Rate
0.25</td><td>Processing Capability
0.24</td><td>Available Memory
0.24</td><td>Battery Power
0.48</td><td>MLS Capability
0.05</td><td>Encryption Method
0.36</td><td>Existence of Resource-Hiding Hardware
0.18</td><td>Authentication Type
0.27</td><td>User Qualification
0.18</td><td></td></tr>
<tr><td>0.09</td><td>0.05</td><td>0.05</td><td>0.05</td><td>0.05</td><td>0.09</td><td>0.01</td><td>0.18</td><td>0.09</td><td>0.14</td><td>0.09</td><td>0.14</td><td>1.000</td></tr>
</table>

Figure 48 Fragment I of the Quantitative Model

The single attribute value functions shown in Section E are applicable to CONOP #1. The purpose of the value functions is to convert between the measured levels of a device for a given attribute and the preference value created from decision-maker input. The twelve value functions are positioned in the spreadsheet. We use the VB Macro described in Section E to find the value assignment from a given measured level for each of the attributes. Figure 49 is a fragment from the spreadsheet tool. The figure lists the MANET Node-Pair Links in the left column (for CONOP #1, there are six) and the measurable attributes in the top row. The upper matrix contains the actual measured levels that come from the ontology after conversion into the Node-Pair Link format. The Macro finds the appropriate preference value for the measured level ("scores") and the spreadsheet populates the lower matrix, which are the preference values.



	Throughput	Latency	Mobility Rate	Processing Capability	Available Memory	Battery Power	MLS Capability	Encryption Method	Existence of Resource-Hiding Hardware	Authentication Type	User Qualification	Assurance of Security Mechanism
	Alternative Scores for each Attribute											
(1,2)	2	100	25	500	64	5	1	4	3	5	4	6
(1,3)	4	50	38	500	1200	5	1	1	3	1	2	1
(1,4)	2	100	25	500	128	5	1	1	3	1	2	1
(2,4)	3	100	4	500	128	5	1	1	3	1	2	1
(3,4)	7	50	17	600	1250	8	2	1	0	1	1	1
(3,5)	25	35	25	800	1250	9	3	1	2	1	1	1
Ideal Alternative	74	0	0	1200	2000	15	3	4	4	6	4	7

	Single Dimensional Value Calculations												Alternative Value
(1,2)	2.0	2.0	4.0	1.0	3.0	2.0	2.0	10.0	8.0	8.0	10.0	8.0	**6.4**
(1,3)	4.0	5.3	2.4	1.0	9.2	2.0	2.0	1.0	8.0	1.0	6.0	0.0	**2.9**
(1,4)	2.0	2.0	4.0	1.0	5.0	2.0	2.0	1.0	8.0	1.0	6.0	0.0	**2.5**
(2,4)	3.0	2.0	8.3	1.0	5.0	2.0	2.0	1.0	8.0	1.0	6.0	0.0	**2.8**
(3,4)	5.3	5.3	5.1	4.0	9.3	4.0	6.0	1.0	0.0	1.0	2.0	0.0	**2.5**
(3,5)	7.7	6.3	4.0	8.0	9.3	5.8	10.0	1.0	6.0	1.0	2.0	0.0	**3.6**
Ideal Alternative	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	**10.0**

Figure 49 Fragment II of the Quantitative Model

We now conduct the preference value composition using the weight assignments relevant to the MANET operating in normal mode (Table 4). The last column of Figure 49 lists the "alternative values," or the strengths of each of the Node-Pair Links, which is the output of our VFT Decision analysis.

This ends our discussion of the second component of the MMM. The output of this component informs the third component, the Node Choice Optimization, where our selection is actually made. We discuss the optimization in detail in the next chapter.

VI. REINFORCING AVAILABILITY WITH A NETWORK FLOW MODEL

The third component of the MANET Distributed Functions Ontology (MDFO) Management Mechanism (MMM) is the Node Choice Optimization. We provide both background and related work on optimization. We then explain our specific network flow optimization problem both in general terms and in a formulaic representation. We touch on the complexity of the underlying algorithm as well as explain implementation details. Finally, we continue with the detailed example.

A. INTRODUCTION

Given the lack of network infrastructure, the devices that participate in a MANET act collectively to assist each other with communication functions (e.g., routing of message traffic). Because the individual resources of each device are finite, the overall MANET is also resource-constrained. MANET-level management must account for the impact of decisions on the individual device's resources to ensure that the device resource levels necessary for the MANET as a whole are not depleted. A device performing a function on behalf of the MANET may experience a significant depletion of resources (e.g., power) such that the device may no longer be able to participate in network communications. Additionally, reassignment of MANET functions exacts a toll on overall MANET resources so that they may be depleted unnecessarily if frequent reassignment of distributed functions occurs.

Optimization is concerned with finding the "best" solution from a set of *feasible solutions*, or acceptable solutions which meet the problem constraints. In our work, "best" is characterized by the composition of strong non-security functionality and security characteristics of a node-pair link as described in the VFT Decision Analysis. Additionally, we include the property of direct connectivity in our assessment of "best," which we introduce in this chapter.

The MANET Management Mechanism (MMM) Decision-Making Process described in Chapter IV, D includes the *Node Choice Optimization* function, as shown in Figure 16. This function implements a minimum cost flow decision model, where “units” flow from a considered device to the other devices in the MANET. The input into the model is twofold: a discrete network graph representing the connectivity of devices, and a set of strength assignments for all node-pair links in the MANET. The output of the model is a score representing the total cost of connecting a device assigned a MANET function to every other network node, as well as a determination of the extent to which each connection, or arc, is used. A final comparison of the output scores enables a management decision and provides an optimized connectivity map of the MANET. We describe the Node Choice Optimization in this chapter.

The use of a network flow model to optimize the MANET management decision process affords three major contributions. First, this approach allows us to reinforce the *availability* of MANET communications. Using this model emphasizes direct connectivity of nodes as well as central positioning of the node choice relative to the rest of the nodes in the network. Two important consequences result: energy efficiency and link reliability. By not having to route traffic in a multi-hop fashion (through many other devices), power consumption is lower and reliance on other devices less. Second, optimization of the node choice allows us to distribute the resource depletion among the devices in a fair manner, which yields a more *stable network* (i.e., the ability of a MANET to maintain its ad hoc virtual organizational structure as the underlying physical topology varies [52]. A node choice can support the required function (e.g., cluster-head) for a longer period, in turn reducing the frequency of re-elections. Fewer re-elections reduce the need for computation, update and announcement message traffic, and ultimately, battery consumption. By minimal turnover of node responsibilities, actual on-the-ground operations are less confusing and disruptive with fewer communications breakdowns between elements.

In Section B, we give additional background information about optimization, and Section C describes related work. Section D gives a general description of the model and Section E describes its mathematical formulation. The algorithm used to solve the optimization problem, an assessment of its complexity, and a high level description of the implementation are in Sections F through H. Finally, Section I contains the detailed example.

B. BACKGROUND ON OPTIMIZATION

In computer science, optimization refers to the process of making a device or a collection of devices run more efficiently in terms of time and resources (e.g., energy, memory). Optimization is a necessity for MANET management decisions due to the inherent individual and collective resource limitations within the network.

Mathematically, optimization entails minimizing or maximizing an objective function by choosing values for the input variables from within an allowed set. An objective function is a mathematical expression made up of one or more variables that are useful in evaluating solutions to a problem [40]. We give a mathematical explanation of optimization below.

- Set:

  $A =$ a set of feasible solutions to the objective function, f

- Variable:

  $x =$ an element (a vector of input variables) in the set of feasible solutions, A

- Objective Function:

  $f =$ a given function

If the optimization problem calls for minimizing the results of the function, then we find an element, x_0, of the set A such that:

$$f(x_0) \leq f(x) \quad \forall x \in A$$

If the problem calls for maximizing the results, then we find an element, x_0, of the set A such that:

$$f(x_0) \geq f(x) \quad \forall x \in A$$

The elements of the *allowed set*, *x*, are combinations of variable assignments that result in a *feasible solution* (a solution that satisfies all of the constraints in the optimization problem). A feasible solution that minimizes or maximizes the value of the objective function is called an *optimal solution*.

Linear programming (LP) is an optimization problem formulation in which the objective function is linear and the constraints that define the allowed set of variable input values are linear equalities and inequalities [28]. LP has an important property called *global optimality*. A resulting optimal solution is guaranteed to be the global, or overall "best" solution to the problem, and not a local optimal solution because of the linearity requirement. The graphical representation of a non-linear function in Figure 51 shows the difference between local and global optimum.

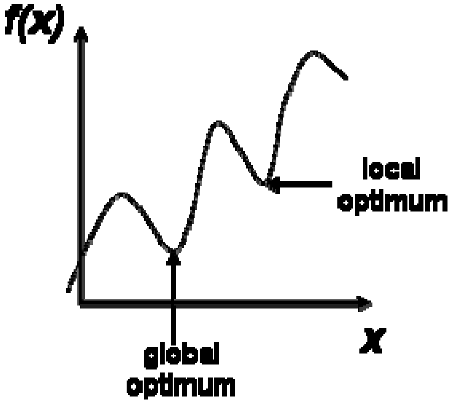


Figure 50 Graphical Depiction of a 2-Dimensional Non-Linear Programming Problem

Figure 51 graphically depicts an objective function with two variables (x_1, x_2) and linear constraints. The result is a polygon-shaped area that represents the feasible solutions of the problem. A *vertex* exists at each of the intersections of the linear constraints.

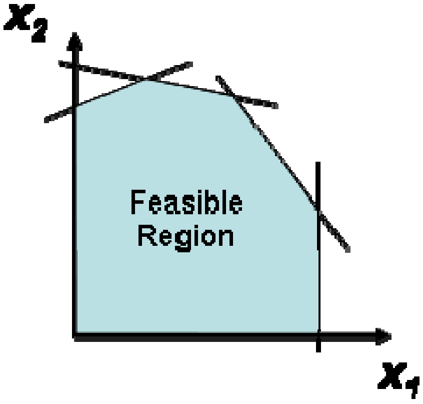


Figure 51 Graphical Depiction of a 2-Dimensional Linear Programming Problem

Solution methods to a linear programming problem (e.g., Simplex method) start at a vertex within the feasible region and iterate to the vertex yielding the optimal set of input variables. Section F provides additional detail on solution algorithms.

A *minimum cost flow problem* is a special case of linear programming in which the objective function minimizes the flow of units through a network of nodes and arcs [28][102]. The objective function and constraints are linear. There is a supply and a demand of units at network nodes, and the arcs have costs and bounds.

Linear programming allows for fractional flows, i.e., the variables may assume non-integer values. In the process of decision-making, we may require an integer result in order to arrive at a decision. By using LP, fractional solutions have to be rounded to the closest integer, which may produce a rounded solution that is infeasible or suboptimal. Instead of LP, practitioners often use integer programming, where the values of variables must be integers, in many practical cases of network optimization. An alternate approach to the generation of integer solutions is in the use of minimum cost flow optimization. If we restrict the supply and demand units to integers, the resulting solutions are in integer form.

C. RELATED WORK

Decision analysis practitioners that specialize in Value Focused Thinking often consider the weighted function that combines the attributes as an objective function [67]. However, the final comparison of the values of the weighted function across the possible alternatives is actually a rank-ordered choice.

There are numerous computer science algorithms that solve network problems similar to ours, including Dijkstra's Algorithm and Bellman-Ford Algorithm (single source to a single sink shortest path), Floyd-Warshall Algorithm (all pairs shortest path), and Ford-Fulkerson (maximum flow through a network) [24]. None of these algorithms solve our specific problem. In fact, a minimum cost flow model is a general model when compared with shortest path and maximum flow models. A maximum flow algorithm has bounds on the arcs but no costs, while a shortest path algorithm has costs but no bounds. Our minimum cost flow model, with both costs and bounds on the arcs, cannot be solved by any specialized algorithm designed to treat only one of these two aspects. Additionally, a maximum flow algorithm has a variable supply and demand at a source and sink node, and a shortest path algorithm has a supply and demand of one at the source and sink. Both of these aspects also differ from our problem [24].

There are many areas of active research where optimization is applied to real world problems. Problem areas include the designation of career fields for Army officers [105], mining of aggregate [84], and military capital planning [14].

The problem of optimizing MANET node selection is also well researched in terms of clustering and cluster-head selection. We explain the common approaches to optimization of this problem in Chapter II, Section B. The cluster-head selection continuum introduced in Figure 1 graphically depicts the shortcomings of the current optimization approaches.

We now give a general description of the optimization problem, to include details on how the problem was modeled.

D. GENERAL DESCRIPTION OF THE OPTIMIZATION PROBLEM

We model the MANET node-choice optimization problem as a minimum cost flow problem. Each node represents a device participating in a MANET with the potential of assuming the responsibilities of the required function (e.g., cluster-head). The arcs represent potential connections between the devices. An arc exists if two devices are able to communicate with each other. The use of each arc is subject to a cost, which is a function of the strength of the Node-Pair Link. We derive the strength values by combining both the non-security functionality factors and the security factors using VFT Decision Analysis (see Chapter V). To reinforce direct connectivity (where a device is an immediate neighbor of a second device), we apply a penalty for the reuse of an arc in the optimization model.

We solve a minimum cost flow problem for each node that possesses the potential to provide the required MANET function (e.g., cluster-head). Our initial assumption in the development of our model is that we have pre-selected a node to evaluate, called the *considered node*. We remove this assumption later, in order to consider all potential nodes.

We describe our linear objective function and linear constraints below. The system of constraint equations defines the set of candidate solutions, and the objective function evaluates the feasible solutions and finds the optimal objective function value. This value is integral to the MANET node choice decision once we relax the stated assumption. Additionally, we determine how the considered node is optimally connected to all of the other devices in the network, forming a connectivity map.

We now present the mathematical formulation of the optimization problem, with a final result of the objective function and the constraints.

E. MATHEMATICAL FORMULATION

We label nodes (devices) numerically (e.g., 1, 2, 3,…) within the complete graph that represents the MANET. A considered node is a device that we have selected for evaluation. We indicate arcs by specifying the two nodes that form the node-link-node entity (e.g., (1, 2), (2, 3),…). Capital letters represent sets of objects. We describe the formulation using indices, sets, parameters, variables, an objective function, and constraints. We reference the nodes of the network using the indices *i, j*. The graphical representation of the MANET, *G*, consists of the set of nodes (*N*) and the set of arcs (*A*).

The parameters include v_{ij}, the strength value of the node-pair link determined in VFT decision analysis. This value is a measure of how well the node-link-node entity [*i* : *(i,j)* : *j*] supports the required function (e.g., cluster-head). In order to convert an arc weight (the strength value) into an arc cost, we first determine the highest strength assessment, $v_{\max}$, that exists within the set of node-pair link entities in the entire MANET (*G*).

$$v_{\max} = \max_{(i,j)\in A} (v_{ij})$$

We then create the arc cost, V_{ij}, by subtracting the strength values from the maximum strength value. In effect, the strongest node-link pair has the lowest cost, consistent with the requirements of a minimum cost flow approach to our problem. The reason that we cast the problem in terms of costs instead of weights is to avoid the over-use of an arc merely because it contributes to overall utility during the optimization. We incorporate the penalty, p_{ij}, in order to reinforce direct connectivity in our optimization. We utilize the penalty to discourage the reuse of arcs in the collection of paths from the considered node to each of the other nodes. The supply and the demand parameters, s_i and d_i, respectively, ensure that every node is connected to the considered node, either directly or indirectly. At the considered node, we assign a supply of "units" equivalent to n-1, with n being the total number of nodes in the set of nodes, N. There is no demand at the considered node. The demand at each of the nodes not under consideration is 1 unit, while the supply is 0 units.

The variables include x_{ij}, the numerical value representing the flow on an arc. In our minimum cost flow problem, an arc may be used only once for a path from the considered node to one of the other n-1 nodes, but an arc may be traversed multiple times for a collection of paths. We associate the arc cost parameter (V_{ij}) with x_{ij}. z_{ij} represents the flow on an arc that is in excess of one, signifying that we have reused a connection. We associate the penalty parameter (p_{ij}) with z_{ij}.

For the objective function, we minimize the sum of the arc costs times the number of times that an arc is traversed and the penalty incurred should excess flow occur on a link. The function is linear (e.g., there are no terms raised to powers, squared, etc.).

The constraints are linear equalities and inequalities. The first is the flow balance constraint. For a given node, the summation of the number of units supplied at and flowing into the node must equal the summation demanded at and flowing out of the node. In terms of units, flow in must be equal to flow out. The second constraint is on the upper bound of x_{ij}. In potential solutions, an arc may not be used ($x_{ij}=0$). However, the flow has an upper bound of $1+z_{ij}$, the penalized flow in excess of 1. If $x_{ij}>1$, then z_{ij} is positive.

- Indices:

  $i, j =$ MANET nodes or devices

- Sets:

  $N =$ set of nodes $(1,2,...i,j,...n)$
  $A =$ set of arcs $((1,2),(1,3)...(2,3)...(i,j)...(n-1,n))$

- Parameters:

  V_{ij} $=$ cost of directly connecting $i, j = (v_{\max} - v_{ij})$
  p_{ij} $=$ penalty of using an arc (i, j) to connect i and k where $j \neq k$
  s_i $=$ supply at node i

  $$= \begin{cases} n-1, \text{ where } i \text{ is the considered node} \\ 0, \text{ otherwise} \end{cases}$$

  d_i $=$ demand at node i

  $$= \begin{cases} 0, \text{ where } i \text{ is the considered node} \\ 1, \text{ otherwise} \end{cases}$$

- Variables:

  $x_{ij} =$ flow on arc (i, j)
  $z_{ij} =$ flow in excess of 1 on arc (i, j); associated with a penalty for >1 hop

- Objective Function (note: for a given considered node, find the subgraph of *G* that has the least cost. The flows on an arc, x_{ij}, are determined with respect to a given subgraph):

$$\min \sum_{(i,j)\in A} V_{ij} x_{ij} + \sum_{(i,j)\in A} p_{ij} z_{ij}$$

- Constraints:

$$s_j + \sum_i x_{ij} = d_j + \sum_k x_{jk} \qquad \forall j \in N$$

$$0 \le x_{ij} \le 1 + z_{ij} \qquad \forall (i,j) \in A$$

A discussion of the algorithms available to solve this objective function follows in the next section.

F. ALGORITHM

In general, a minimum cost flow problem is a special case of linear programming (LP) [28][102]. As such, we have expressed the node-choice optimization problem as a linear objective function constrained by linear equalities and inequalities. Any linear programming algorithm solves the minimum cost flow problem, including the simplex algorithm and the interior point (barrier) method [38].

In practice, there are two common algorithms for solving LP problems: the interior point method [66] and the Simplex method [102]. The interior point method is sometimes more efficient than the simplex algorithm for highly constrained optimization problems. Neither algorithm evaluates every possible solution to the set of constraint equations. The Simplex method exploits the fact that an optimal solution for a LP problem occurs at a *vertex* of its feasible region [28]. When we plot the constraints of a 2-dimensional or 3-dimensional problem, the result is the multi-dimensional space of feasible solutions. Because the constraints are linear, a vertex forms whenever two lines intersect for the 2-dimensional problem. The Simplex algorithm uses a feasible solution located at such a vertex as a starting point, which may or may not be the optimal solution. The algorithm iterates through other feasible solutions by moving through adjacent vertices until the value of the objective function no longer decreases (or increases) and the algorithm identifies the optimal solution Table 1 [27][88]. Figure 52 depicts the iterative nature of the Simplex algorithm. The problem is 2-dimensional, with variables x_1, x_2. The lines represent linear equalities or inequalities.

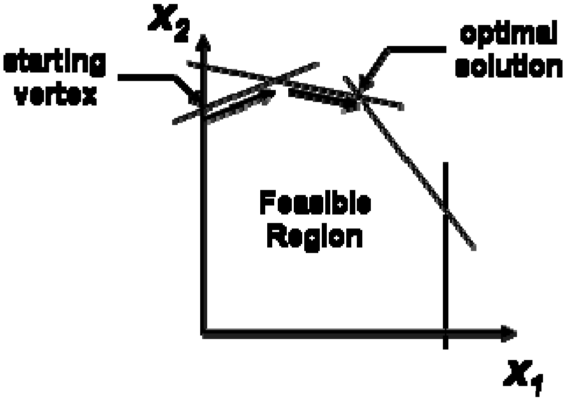


Figure 52 Simplex Algorithm

We now comment on the complexity of the solution algorithms.

G. THEORETICAL COMPLEXITY

Complexity theory characterizes an algorithm's run time performance as a function of problem size using the number of steps taken or the amount of memory used to solve a given problem. The Simplex algorithm varies significantly in both its practical and its theoretical run time performance [27]. This algorithm is the most commonly used method for solving the minimum cost flow problem due to its superior average performance [15]. The Simplex method, however, does not provide theoretical assurance that the algorithm runs in polynomial time [2]. The simplex algorithm's worst-case theoretical complexity is exponential, in that the solution time grows very quickly as a function of problem size [88].

If the problem size is extremely large, it may be beneficial to ensure polynomial running time by using an underlying algorithm that differs from Simplex. Researchers have developed many other algorithms that improve the theoretical run time of solving the minimum cost flow problem [2][87]. We discuss a strongly polynomial-time algorithm as a representative algorithm with improved worst-case performance. The running time of strongly polynomial-time algorithms still depends on the dimensions of the problem (n, the number of nodes, and m, the number of arcs) [87]. The number of nodes in a MANET is typically less than 100, while the number of arcs may approach 1,000. Algorithms in this class differ from the Simplex algorithm in that they utilize scaling, or the creation of an initial approximate solution by relaxing a problem constraint by an amount, Δ, followed by iteration to the optimal solution by successively decreasing the amount of violation (Δ) [2]. The enhanced capacity scaling algorithm has a theoretical (worst-case) run time performance shown in Figure 53 [2].

$$\begin{aligned}&O((m\log n)(m+n\log n))\\&n\ = \text{the number of nodes}\\&m = \text{the number of arcs}\end{aligned}$$

Figure 53 Theoretical Complexity of the Enhanced Capacity Scaling Algorithm

Details on the specific implementation of this algorithm are in [2].

When using the Simplex algorithm, practitioners rarely experience the case of worst-case run time. The practical performance of this algorithm is bounded in polynomial time, with results that exceed strictly polynomial-time algorithms such as the enhanced capacity scaling algorithm. As a result, the algorithm of choice for practitioners is the simplex algorithm [88][15]. Because of this fact, we use the Simplex method to solve our formulated minimum cost flow problem.

A number of optimization tools may be used to implement the Node Choice Optimization component of the MMM. We next describe our implementation.

H. IMPLEMENTATION

To model the node choice optimization problem, we use a modeling tool known as AMPL (“A Mathematical Programming Language”) [40]. Developed at Bell Laboratories, AMPL is a high level, algebraic modeling language for linear and nonlinear optimization problems. Besides its ability to model optimization problems, AMPL also aids in comprehension and completeness of the model logic, due to the similarity of its syntax to algebraic notation [40]. AMPL provides for an easy way to express common linear programming structures (e.g., flow constraints).

Although AMPL allows us to mathematically model the optimization problem, the application does not solve the problem itself. In our implementation, AMPL calls upon an external solver called CPLEX to solve the objective function. CPLEX implements the Simplex algorithm. Input into AMPL includes a model file (.mod extension), a data file (.dat), and an execution program (.run). The AMPL execution program calls the model file which feeds the mathematical description of the model into AMPL. The penalty (p_{ij}) is set within the model file. The program then calls the data file in order to make assignments of values to the set of nodes (N) and the set of arcs (A) as well as the arc weights (v_{ij}) imported from the VFT analysis. Finally, the execution program calls the Simplex solver. AMPL invokes CPLEX (version 10.2) as the solver in our work. The problem parameters, variables, objectives, constraints, and the general network "flow" that we describe in the formulaic representation transfer easily into the clear syntax used in AMPL coding.

The output file shows the result of the optimization procedure, which includes: a score of the total cost of connecting the considered node to every node in the MANET and a list of the extent to which each network arc is being used in the optimal path.

Finally, we now relax the initial assumption used in the development of our model. Instead of focusing on a single pre-selected node, or the *considered node*, we evaluate multiple potential nodes in the MANET. One approach is to include every MANET device in the set of evaluated nodes and run the optimization procedure on every member of the set. A second approach is to evaluate a restricted set of nodes. The advantages of a reduced set include fewer minimum cost flow optimization problems and a smaller number of final comparisons. Both advantages directly result in reduced time and complexity for the solution process. We provide the option of choosing to base the restricted set on highest node out-degree (i.e., the number of direct connections) as a way to focus on network stability [53], or on other means such as excluding recently-joined nodes.

We run the optimization problem on all of the potential nodes in the restricted set. Each potential node is assigned a score representing the optimal cost of connecting the considered node to every other node in the MANET. A final comparison of the scores across the nodes in the restricted set allows for an optimal node choice. The node choice is the one with the lowest resultant score, proving that it is the global optimal choice to conduct the MANET function.

In Section I, we elaborate on our implementation through a comprehensive detailed example.

I. DETAILED EXAMPLE

We complete the detailed example with the application of the Node-choice Optimization Function to the first Concept of the Operation (CONOP #1): the five-device MANET. The network topology is shown in Figure 4. The input into this component is the set of strength assignments for the Node-Pair Links.

Within a data file, we assign the nodes and links to their respective sets as well as enter the strengths as elements of the parameter "value." See the data file for CONOP #1 in Appendix C. The model file is a translation from the formulaic representation of the linear program to AMPL code. The model file for this CONOP is located in Appendix B. The execution program, or run file, calls the model file and the data file, as well as the underlying solver (e.g., CPLEX 10.2). The code is located in Appendix A.

The execution program writes the results of the minimum cost flow optimization to an output file. The output file for CONOP #1 in Normal Mode is located in Appendix D, with a fragment shown in Figure 54. The output includes: a score of the total cost of connecting the considered node to every node in the MANET ("Total_Cost") and a list of the extent to which each network arc is being used in the optimal path. The first two columns of numbers in Figure 54 list the connected network nodes (e.g., "1 2" represents Device 1 connecting to Device 2). The third column is the number of times that the connection, or arc, is used between the two network nodes. It is necessary for a device to reuse a connection in order to reach a device that is not directly connected. Finally, the penalty "z" is exacted when a connection is reused.

```
 Total_Cost = 20.1005

:  Connect   z    :=
1 2    1    0
1 3    2    1
1 4    1    0
3 5    1    0;
```

Figure 54 Fragment of Optimization Output

This ends our discussion of the final component of the MMM. The output of this component, the selection of the most optimal node choice, is the output of our overall decision framework. We now deviate from the detailed example and apply the framework to a different scenario, CONOP #2. Next, we validate the framework by using three different validation techniques.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. DECISION FRAMEWORK APPLICATION AND VALIDATION

In this chapter, we apply the framework to CONOP #2, a MANET with 30 devices, in order to evaluate the framework's effectiveness in a more complex setting. Then, we validate the framework by using three different validation techniques. The techniques are based upon behavioral validation, where we assess the quality of the framework's output. Finally, we present a security-related scenario.

A. APPLYING THE DECISION FRAMEWORK TO A COMPLEX MANET

Although a very realistic scenario, CONOP #1 consists of only five devices. CONOP #1 is very useful in demonstrating the intricacies behind our decision framework and validating the underlying informal model (see Section B). In this section, we apply the decision framework to CONOP #2, the Corps in the Attack. There are 30 devices with varying security attributes and non-security functionality. We show the topology in Figure 55. It is very difficult to identify a suitable choice for cluster-head given the complexity of the topology, notwithstanding the extremely large number of inputs in the decision data set.

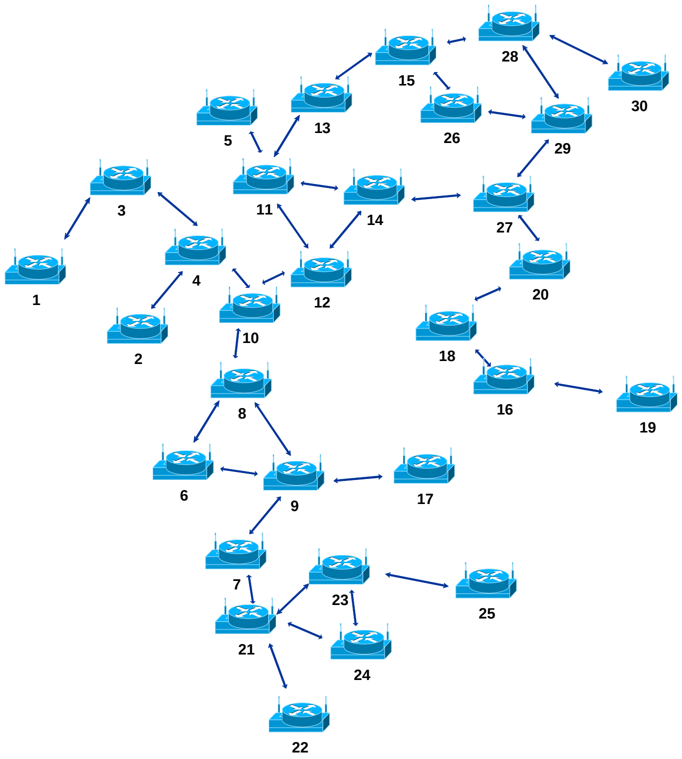


Figure 55 CONOP #2: MANET Topology

We follow the procedure described in the detailed example on the MANET in CONOP #2. The resulting optimized node choice is Device 12, with a total cost of 1,790.4. Some of the considered nodes had total costs three times that of Device 12. This makes sense, since Device 12 is centrally located and has three direct connections. The resulting connectivity map is shown in Figure 56. We do not depict the total number of connections between devices in the figure due to the higher number of arc reuses. For example, link (12, 10) is used 15 times, with 14 arc reuses. For an idea of the number of arcs reused, refer to Figure 57.

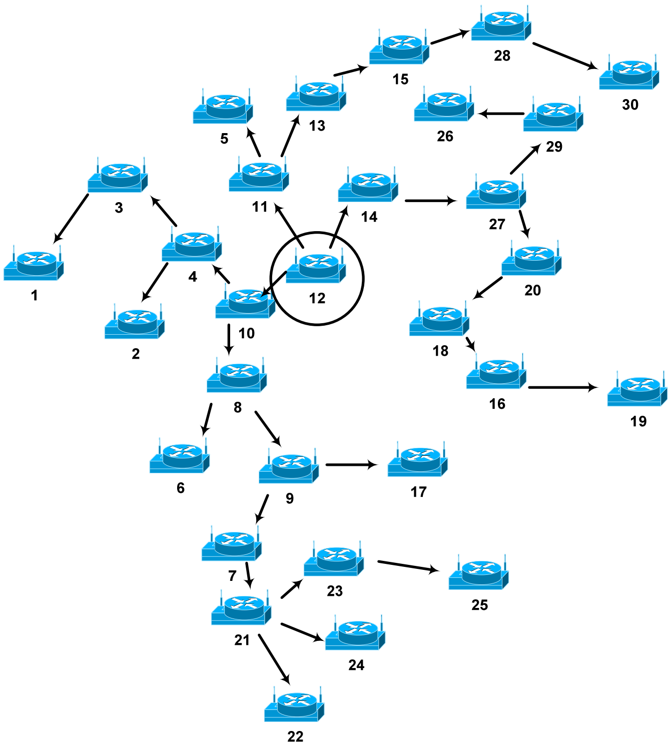


Figure 56 CONOP #2: Optimized Connectivity Map

```
Node From To    Connect z
        3  1          1   0
        4  2          1   0
        4  3          2   1
        7  21         5   4
        8  6          1   0
        8  9          8   7
        9  7          6   5
        9  17         1   0
       10 4           4   3
       10 8          10   9
       11 5           1   0
       11 13          4   3
        12 10        15  14
       12 11          6   5
       12 14          8   7
       13 15          3   2
       14 27          7   6
       15 28          2   1
       16 19          1   0
       18 16          2   1
       20 18          3   2
       21 22          1   0
       21 23          2   1
       21 24          1   0
       23 25          1   0
       27 20          4   3
       27 29          2   1
       28 30          1   0
       29 26          1   0
```

Figure 57 CONOP #2: AMPL Output Showing Connections

As demonstrated by CONOP #2, our decision framework is scalable up to a MANET with a large number of devices (30). Literature suggests that MANET efficiency decreases considerably when a device is required to transmit messages traffic more than two hops [53]. Large-sized networks are prevalent in sensor networks, where the primary purpose of the network is not persistent communication.

Now that we have shown that the framework is useful in a complex MANET, we validate the framework by assessing its behavior.

B. VALIDATION OF THE DECISION FRAMEWORK

The logic of validation allows us to move between the two limits of dogmatism and skepticism.

Paul Ricoeur, philosopher

The goal of this section is to provide *validation* of our decision framework and its underlying conceptual modeling of a MANET. There are many differing viewpoints on the definition and the establishment of validation [90]. A generally accepted definition of validation is: "the process of establishing confidence in the soundness and the usefulness of a model with respect to its purpose" [39]. Since both conceptual and formal models are partial representations of reality, we require confidence that the models represent the organizational and decision-making details of the actual system. The framework's parameters and structure should be consistent with those of the real system [90]. In effect, validation is an argument of the correctness of the framework's translation from reality. The conceptual model underlying the framework represents the reality of a MANET.

Because the concept of establishing "client confidence" is difficult to interpret, validation techniques vary widely [79]. We focus on our conceptual model's *behavioral validity*, or the confidence in the framework's capability of producing an acceptable behavior, or output [90]. The output of our conceptual model is the selection of a device to perform a distributed function (in this case, cluster-head). We employ three widely used techniques to validate our framework: face validity, content validity, and discriminant validity [114].

Face validity, also referred to as expert opinion, is a superficial assessment of the degree to which we accurately translate the conceptual model from the reality of the MANET. This technique of validity requires intuitive judgment [5]. The criterion, or, "standard for judgment," is the model itself [114].

Content validity also assesses the accuracy of the translation, or the ability of the conceptual model to reflect the properties of the content domain (e.g., MANET). This technique depends on a theoretical, non-statistical, basis for assessment [114].

Discriminant validity is a type of criterion-related validity, where the performance of the conceptual model is checked against some criterion other than itself. Discriminant validity is the degree to which the decision framework is not similar to other selection methods that attempt to produce the same output in the same reality [114]. We will contrast our conceptual model's cluster-head selection to the results of other selection methods. The criteria are other translations of the reality of the MANET.

We validate our conceptual model using the first Concept of the Operation (CONOP #1): the five-device MANET. The network topology and the device and link characteristics of the components of the network are repeated in Figure 58 and Table 5, respectively.

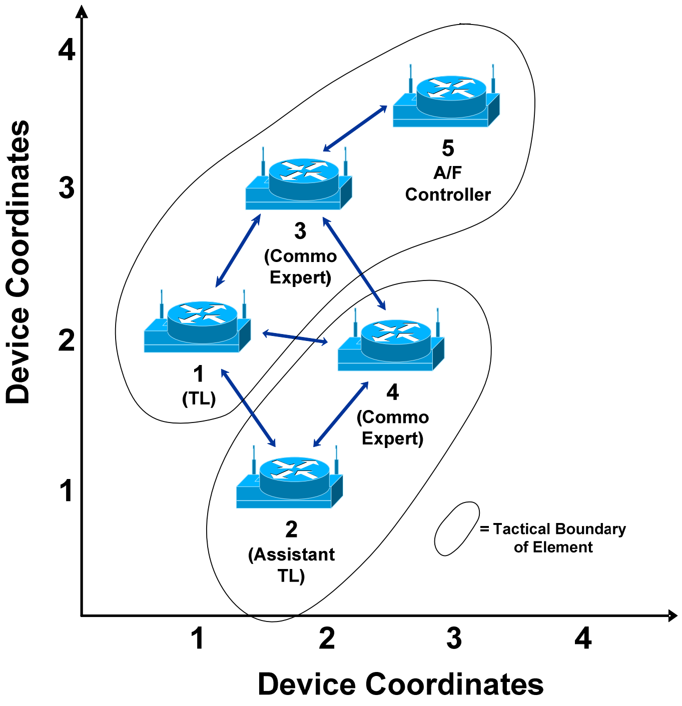


Figure 58 CONOP #1: MANET Topology

	Device 1	Device 2	Device 3	Device 4	Device 5
Process. Capability	500 MIPS	500 MIPS	800 MIPS	600 MIPS	1200 MIPS
Trust Zone					
MTM	w/ secure coprocessor	w/ secure coprocessor		enabled	w/ PKI smartcard
Total Memory	128 MB	256 MB	2048 MB	512 MB	2048 MB
Available Memory	64 MB	64 MB	1250 MB	128 MB	1250 MB
Power and battery (internet usage)	5.0 hours battery	5.0 hours battery	9.0 hours battery	7.5 hours battery	15.0 hours battery
Location	(1, 2)	(2,1)	unknown	(3, 2)	(3, 4)
Mobility rate	23 mph	2 mph	15 mph	2 mph	10 mph
Controls		lightweight PKI server			
Activated Capability	Firewall	Camera			Camera
Inactive Capability			Long-range communications	Printer	Long-range communications
Throughput	1 2 (2 Mbps) 1 3 (4 Mbps) 1 4 (2 Mbps)	2 1 (2 Mbps) 2 4 (3 Mbps)	3 1 (4 Mbps) 3 4 (7 Mbps) 3 5 (25 Mbps)	4 1 (2 Mbps) 4 2 (3 Mbps) 4 3 (7 Mbps)	5 3 (25 Mbps)
Latency	1 2 (100 ms) 1 3 (50 ms) 1 4 (100 ms)	2 1 (100 ms) 2 4 (100 ms)	3 1 (50 ms) 3 4 (50 ms) 3 5 (35 ms)	4 1 (100 ms) 4 2 (100 ms) 4 3 (50 ms)	5 3 (35 ms)
Physical Distance of Links	1 2 (350 m) 1 3 (350 m) 1 4 (500 m)	2 1 (350 m) 2 4 (350 m)	3 1 (350 m) 3 4 (350 m) 3 5 (350 m)	4 1 (500 m) 4 2 (350 m) 4 3 (350 m)	5 3 (350 m)
MLS Capability	Dedicated Mode	Dedicated Mode	Multilevel Mode	System High Mode	Multilevel Mode
Authentication	2-factor w/ biometric reader	2-factor w/ biometric reader	Password	Password	2-factor w/out biometric reader
Encryption	NSA Type 1	NSA Type 1	NSA Type 4	NSA Type 4	NSA Type 1
Current session level	SECRET	SECRET	SECRET	SECRET	SECRET
EAL	6	6	1	1	3
User Qualification	Commander	Commander	Senior Operator	Senior Operator	Junior Operator
Site	Secure operations center	Field	Open terminal (café)	Field	Field

Table 5 CONOP #1 Device and Link Characteristics

1. Face Validity

The conceptual model is an accurate translation of the reality of a MANET.

Proof

Let $G = (N, A)$ be a weighted, directed graph that represents the MANET. N is the set of nodes representing the devices in the MANET. A is the set of links representing the communications channels between devices. This representation allows the conceptual model to consider network flow within *G* in the optimization of the node choice.

Suppose *i* and *j* are elements of the set *N*, and (*i*, *j*) is an element of the set *A*. Let [*i* : (*i*, *j*) : *j*] represent the node : link : node entity. The use of an entity representing a node-pair link offers a way to assess device characteristics relative to neighboring devices.

The entity [*i* : (*i*, *j*) : *j*] is characterized as a function of both device-specific non-security functionality and security attributes, which provides a holistic assessment of a MANET device. The security policies of confidentiality, integrity, and availability of network information are considered in the characterization of [*i* : (*i*, *j*) : *j*].

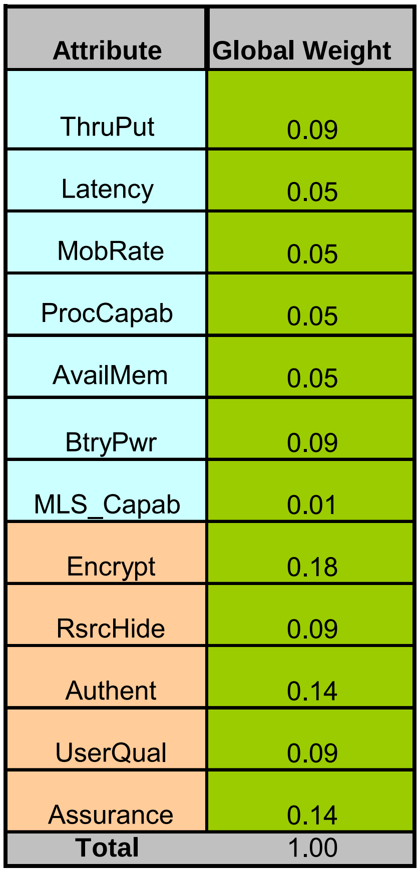
The network flow within *G* in the optimization component reinforces the availability of network information by rewarding direct connectivity between devices (e.g., if there exists a link (*i*, *j*) between *i* and *j*, then *i* and *j* are directly connected).

Suppose that we require a method to compare the elements in the set *N* in order to determine the best suited node to perform a distributed function. The output of running the conceptual model on *G* is a score representing the total cost of connecting a device assigned a MANET function to every other network node, as well as a determination of the extent to which each connection, or link, is used. The score of node *i* may be compared to the score of node *j*, thus producing a method for determining the best suited device.

2. Content Validity

To further assess the accuracy of our conceptual model's translation of an actual MANET, we use a content validity approach. We base our assessment on the results of our framework when applied to three contexts related to CONOP #1: (1) a MANET operating in normal mode, (2) a MANET operating in emergency mode, and (3) a test case based strictly on connectivity. The results of the three applications are qualitatively compared against reality (the content domain of the MANET).

A MANET in Normal Mode operates with a balance of both non-security and security functionality, as determined by the decision-maker. For CONOP #1, Normal Mode, the suggested weight assignments shown in Table 6 are global weights, in that the numbers are relative to the weights of all of the attributes that are involved in the system measurement. For example, the attribute listed first (throughput) has a weight of 9%, when compared to all of the other attributes. The first seven attributes are non-security functionality related, and the last five are security attributes.



Attribute	**Global Weight**
ThruPut	0.09
Latency	0.05
MobRate	0.05
ProcCapab	0.05
AvailMem	0.05
BtryPwr	0.09
MLS_Capab	0.01
Encrypt	0.18
RsrcHide	0.09
Authent	0.14
UserQual	0.09
Assurance	0.14
Total	1.00

Table 6 Weight Assignments in Normal Mode

We show the results of running the model on the 5-node MANET in Normal Mode in Figure 59. The first column lists the context. The second, third and fourth columns show the output. In the second column, the *Node ID* lists the device being evaluated as possible cluster-head, the *Score* represents the total cost of connecting the device to every other network node, and the *# of Arcs Reused* is an indicator of the extent to which the node is centrally located within the MANET. If an arc is reused, then a MANET node is not directly connected to the evaluated node, and a penalty is assessed. The third column shows the Node Choice, based on a final comparison of the output scores. The fourth column provides an optimized connectivity map of the MANET.

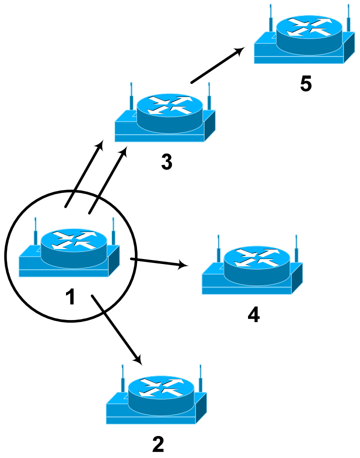
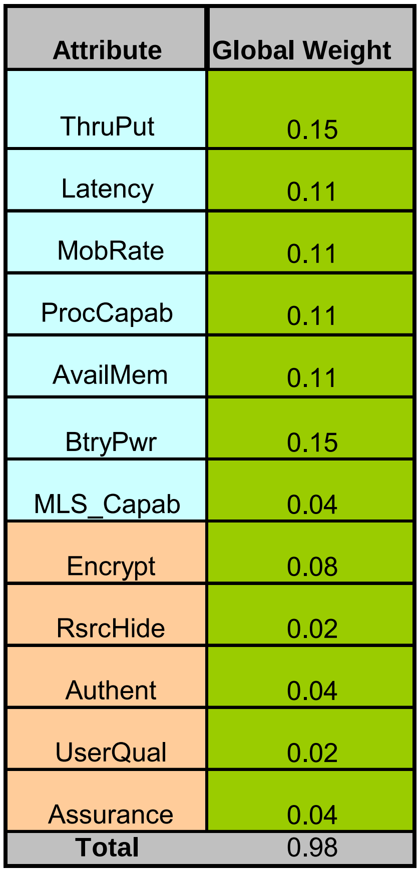
Context	Node ID | Score | # of Arcs Reused	Node Choice	Connectivity Map
Normal Mode	1 20.1 1 2 30.3 2 3 20.2 1 4 24.7 1 5 47.8 4	1	

Figure 59 5-Node MANET in Normal Mode

Qualitatively, the results in Figure 59 agree with the actual MANET from CONOP #1. The devices with the closest three scores (1, 3, and 4) all have three direct connections; each with only one arc re-use that incurs a penalty. Device 1, the node choice, has stronger security features than 3 and 4, to include better encryption, authentication, and resource-hiding mechanisms. Additionally, Device 1 has a user qualification of "commander." Device 3 has better non-security functionality than the other devices, including better link quality of service and higher levels of available memory and battery power. Device 3 and 4 are senior operators. Because we value both security and non-security functionality while in Normal Mode, Device 1 is the reasonable node choice.

In the second context, a MANET operating in Emergency Mode, time may be critical. A decision-maker may turn off some security in order to maximize non-security functionality. The decision-maker may decide that the risk of unintended information disclosure or modification is acceptable in order to attend to an emergency. The re-prioritization is reflected in the change in weights. For CONOP #1, Emergency Mode, the suggested weight assignments are shown in Table 7. Note that the global weights of the first seven attributes (the non-security functionality) have increased, while those of the five security attributes have decreased.



Attribute	**Global Weight**
ThruPut	0.15
Latency	0.11
MobRate	0.11
ProcCapab	0.11
AvailMem	0.11
BtryPwr	0.15
MLS_Capab	0.04
Encrypt	0.08
RsrcHide	0.02
Authent	0.04
UserQual	0.02
Assurance	0.04
Total	0.98

Table 7 Weight Assignments in Emergency Mode

We show the results of running the model on the 5-node MANET in Emergency Mode in Figure 60.

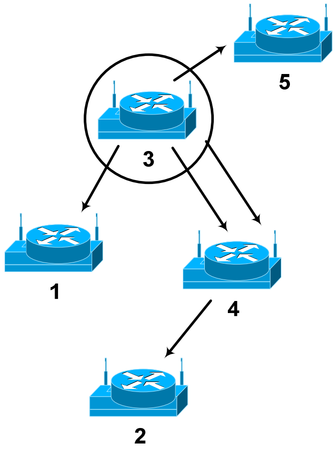
Context	Node ID | Score | # of Arcs Reused			Node Choice	Connectivity Map
Emergency Mode	1 2 3 4 5	16.4 25.8 13.9 14.9 31.6	1 2 1 1 4	3	

Figure 60 5-Node MANET in Emergency Mode

Qualitatively, the results in Figure 60 agree with the actual MANET from CONOP #1. Devices 1, 3 and 4 are, once again, close in score. These devices have three direct connections; each with only one arc re-use that incurs a penalty. Device 3, the node choice, has better non-security functionality than the other devices, including better link quality of service and higher levels of available memory and battery power. Device 4 is second in terms of non-security functionality. Because we weight non-security functionality heavier than security while in Emergency Mode, Device 3 is the reasonable node choice.

In the final context, we look at the performance of our model strictly based on connectivity. We fix every value in the set of strength assignments to "1". The set of strength assignments is the output of the Value Focused Thinking decision analysis. Thus, all the MANET devices and links have identical security and non-security functionality and are evaluated under an identical weight assignment (e.g., the weight assignments in Table 6 or Table 7). This context tests the output of the model based on connectivity alone.

We show the results of running the model on the 5-node MANET in Connectivity Test Mode in Figure 61.

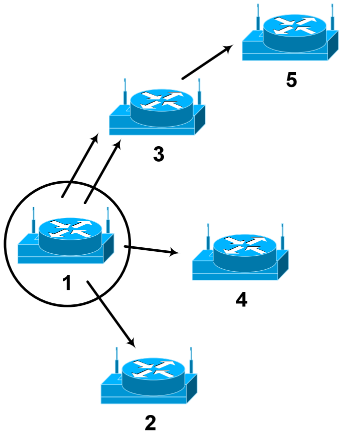
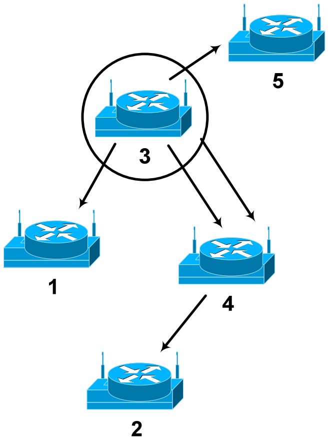
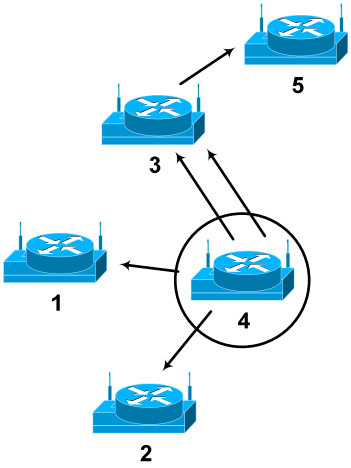
Context	Node ID	Score	# of Arcs Reused	Node Choice	Connectivity Map
Connectivity Test Mode	1 2 3 4 5	1.0005 2.0007 1.0005 1.0005 4.0008	1 2 1 1 4	1, 3, 4	
	1 2 3 4 5	1.0005 2.0007 1.0005 1.0005 4.0008	1 2 1 1 4		
	1 2 3 4 5	1.0005 2.0007 1.0005 1.0005 4.0008	1 2 1 1 4		

Figure 61 5-Node MANET in Connectivity Test Mode

Based on the direct connectivity of the devices in CONOP #1 alone, the results in Figure 61 are accurate. Devices 1, 3 and 4 are all suitable choices for cluster-head. These devices all have three direct connections; each with only one arc re-use that incurs a penalty. The model is accurate in the selection of a node based on connectivity alone.

3. Discriminant Validity

In this section, we take a criterion-related approach to further validating our informal model. The discriminant approach assesses the degree to which the output diverges from similar models that attempt to solve the same problem. We compare our selection technique to three other selection methods: (1) operationally-driven choice, (2) single metric (battery power), and (3) multiple metric (Weighted Clustering Algorithm, WCA) [17]. We discuss the three other selection methods in detail in Chapter II. We continue to use CONOP #1 as the overarching scenario. The results of the three comparisons are qualitatively compared with respect to the content domain (e.g., MANET).

In the first comparison, we use our selection technique with a MANET operating in Normal Mode and an operationally-driven choice selection method. This latter method is the selection technique currently in use by both Harris Corporation and Thales Communicates in their MANET-capable radios (see Chapter I). Before a team goes on an operation, their radios are configured with a master/slave relationship. Typically, the ad hoc hierarchy matches the organizational or the command hierarchy. For CONOP #1, operationally-driven choice, the selection of “master” is Device #1 (the team leader) and “alternate master” is Device 2 (the assistant team leader). The connectivity map is based upon team integrity, in that all of the devices within a tactical boundary (e.g., team) directly communicate with each other. Device #1 (the team leader) conducts cross-team communicates with Device #2 (the assistant team leader). We show the results of the comparison in Figure 62.

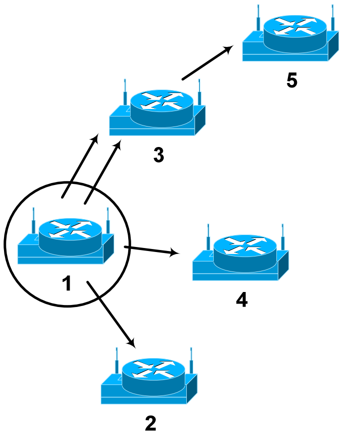
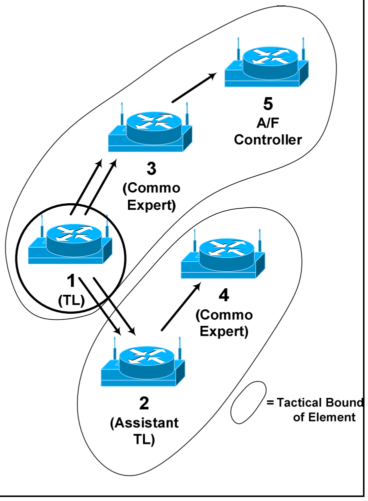
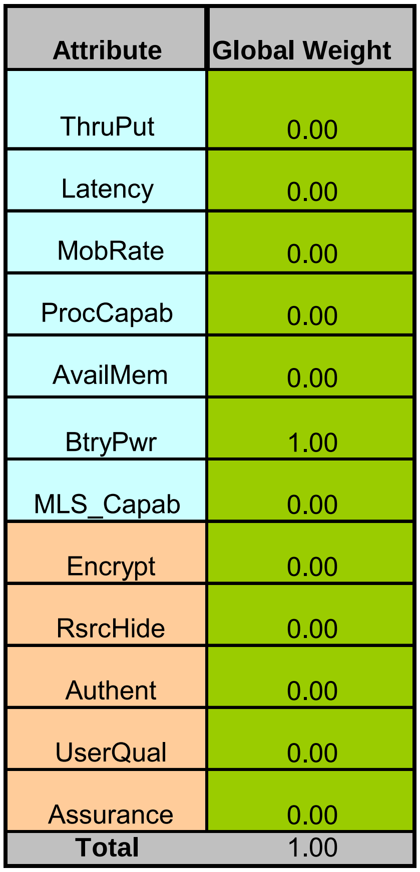
Context	Node ID | Score | # of Arcs Reused	Node Choice	Connectivity Map
Normal Mode	1 20.1 1 2 30.3 2 3 20.2 1 4 24.7 1 5 47.8 4	1	
Operationally-Driven Choice	N/A	1	 5 A/F Controller 3 (Commo Expert) 1 (TL) 4 (Commo Expert) 2 (Assistant TL) = Tactical Bound of Element

Figure 62 5-Node MANET Comparison Between Normal Mode and Operationally-Driven Choice

In CONOP #1, both techniques chose the same device, Device 1, to act as cluster-head. Device 1 has strong security characteristics and is centrally located within the MANET, with three direct connections. However, in reality, the team leader is not always coupled with the device having the best non-security functionality and security properties. Our method chooses the device that is best suited to perform the MANET function (e.g., cluster-head), while the operationally-driven choice method always chooses the organizational leader. A second difference arises in the connectivity map.

Our model in Normal Mode results in the reuse of just a single arc. The operationally-driven choice, which is confined by the tactical boundaries of the elements, reuses two arcs in the connectivity among devices in the MANET.

In the second comparison, we use our selection technique with the battery power attribute weighted at 100% and a single metric rank-ordered choice method. For our selection technique in Battery Power Mode, the weight assignments are shown in Table 8. Note that the only weight in the table is in the battery power row (100%). For our comparison, we use battery power as the single metric in a rank-ordered choice method. In a rank-ordered choice method, the battery power of each MANET device is enumerated and put in order from highest to lowest. The device with the highest battery power is selected.



Attribute	Global Weight
ThruPut	0.00
Latency	0.00
MobRate	0.00
ProcCapab	0.00
AvailMem	0.00
BtryPwr	1.00
MLS_Capab	0.00
Encrypt	0.00
RsrcHide	0.00
Authent	0.00
UserQual	0.00
Assurance	0.00
Total	1.00

Table 8 Weight Assignments for Battery Power Mode

We show the results of the comparison in Figure 63.

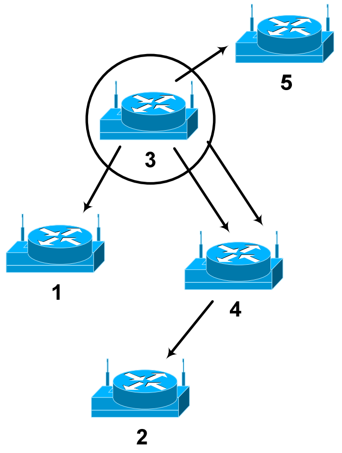
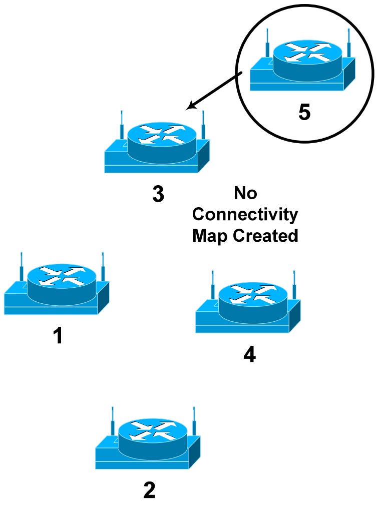
Context	Node ID | Score | # of Arcs Reused	Node Choice	Connectivity Map
Battery Power Mode	1 21 1 2 32.4 2 3 17 1 4 17 1 5 34.4 4	3	
Context	**Node ID | Score**	**Node Choice**	**Connectivity Map**
Single Metric (Battery) Rank-Ordered Choice	1 5 hours 2 5 hours 3 9 hours 4 7.5 hours 5 15 hours	5	

Figure 63 5-Node MANET Comparison Between Battery Power Mode and Single Metric (Battery) Rank-Ordered Choice

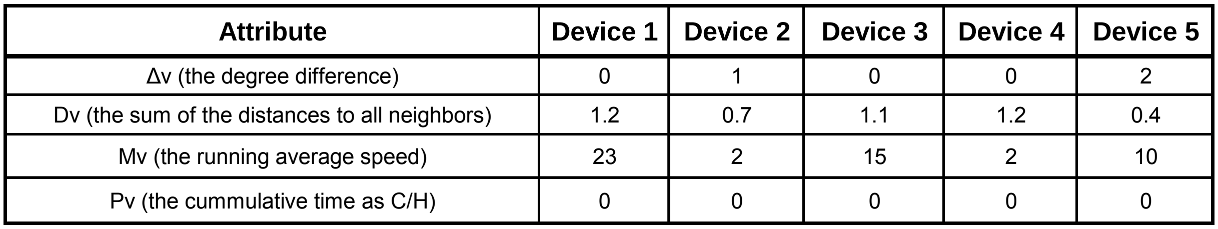
Both battery power approaches select different devices as cluster-head. Our model in Battery Power Mode selects Device #3, which has weaker security features and a battery level of 9 hours. This device has three direct connections, with the reuse of one arc. The rank-ordered choice method selected Device #5 based on its strong battery (15 hours). The method does not have high fidelity input, in that the selection is based upon only one criterion. Device #5 has the least direct connections (one) and is the device least centrally located. Additionally, the method does not create a connectivity map.

In the third comparison, we evaluate our selection technique without any security considerations and a common multiple metric rank-ordered choice method (WCA). For our selection technique in No Security Mode, the security attributes are assigned a weight of zero, with only non-security functionality attributes contributing to the decision process. The weight assignments are shown in Table 9.

Attribute	**Global Weight**
ThruPut	0.19
Latency	0.14
MobRate	0.14
ProcCapab	0.14
AvailMem	0.14
BtryPwr	0.19
MLS_Capab	0.05
Encrypt	0.00
RsrcHide	0.00
Authent	0.00
UserQual	0.00
Assurance	0.00
Total	1.00

Table 9 Weight Assignments for No Security Mode

The Weighted Clustering Algorithm [17] includes four metrics for selection: a node's degree difference (a proxy measure of throughput), the sum of the distance to all neighbors (a proxy measure of signal attenuation), the running average speed (a measure of mobility), and the cumulative time that the node has acted as cluster-head (a proxy measure for battery power). We use a value of three for the ideal degree, or the number of nodes that a cluster-head can handle. A summary of the variables used to calculate the cluster-head for CONOP #1 using WCA is shown in Figure 64. We assume that this is the initial cluster-head selection; $P_v = 0$ for all devices. Additionally, we had to match a device attribute from our model to WCA's three proxy values.



Attribute	Device 1	Device 2	Device 3	Device 4	Device 5
Δv (the degree difference)	0	1	0	0	2
Dv (the sum of the distances to all neighbors)	1.2	0.7	1.1	1.2	0.4
Mv (the running average speed)	23	2	15	2	10
Pv (the cummulative time as C/H)	0	0	0	0	0

Figure 64 WCA Attribute Values using CONOP #1 Data

The WCA weighted linear sum equation is:

$$\begin{aligned} w_v &= \text{combined weight} \\ &= w_1\Delta_v + w_2D_v + w_3M_v + w_4P_v \\ &= (0.19)\Delta_v + (0.14)D_v + (0.14)M_v + (0.19)P_v \end{aligned}$$

The weight vector applied to the WCA selection method above parallels the weight assignments in the No Security Mode, Table 9. Note that WCA does not require the weight factors to sum to one. The devices are rank ordered by combined weight, and the device with the lowest combined weight is the node choice for cluster-head. The selected device's neighbors form the cluster, and the algorithm is run again until all of the devices are assigned to a cluster.

We show the results of the comparison in Figure 65.

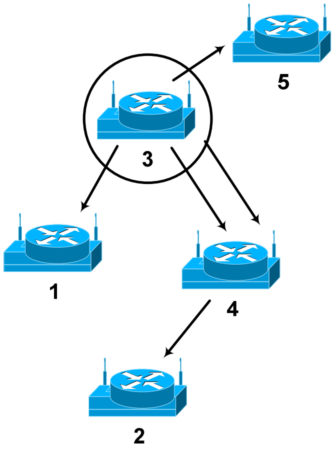
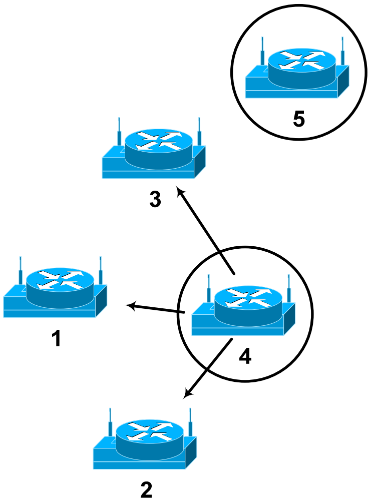
Context	Node ID	Score	# of Arcs Reused	Node Choice	Connectivity Map
No Security Mode	1 2 3 4 5	21 32.4 17 18.2 38	1 2 1 1 4	3	
Context	**Node ID**	**Score**		**Node Choice**	**Connectivity Map**
Multiple Metric (WCA) Rank-Ordered Choice	1 2 3 4 5	3.4 0.6 2.3 0.4 1.8		4	

Figure 65 5-Node MANET Comparison Between No Security Mode and Multiple Metric (WCA) Rank-Ordered Choice

The No Security Mode choice is Device 3, which has strong non-security functionality and three direct connections. WCA selects two cluster-heads, Device 4 and Device 5, due to the requirement that all members of a cluster must be directly connected to a cluster-head. Device 4 has lower mobility and a smaller degree difference (i.e., higher throughput) than the other devices, making it the best choice. Device 5 has strong security and non-security functionality, but has only one direct connection. The resulting connectivity map has two clusters with two different cluster-heads requiring inter-cluster communication capabilities.

4. Security Scenario

In this section, we conduct a thought experiment based upon a realistic security scenario. We utilize the MANET in CONOP #2, with a requirement for a lightweight certificate authority (LCA). The LCA node is responsible for managing the security certificates on behalf of the network.

Assume that the LCA is selected without consideration of device security properties. Device 27 is designated the LCA as shown in Figure 66. However, Device 27 is not a high-assurance node and does not have resource-hiding hardware such as a Mobile Trusted Module. Device 27 stores the network's security certificates in a way such that they are not hidden.

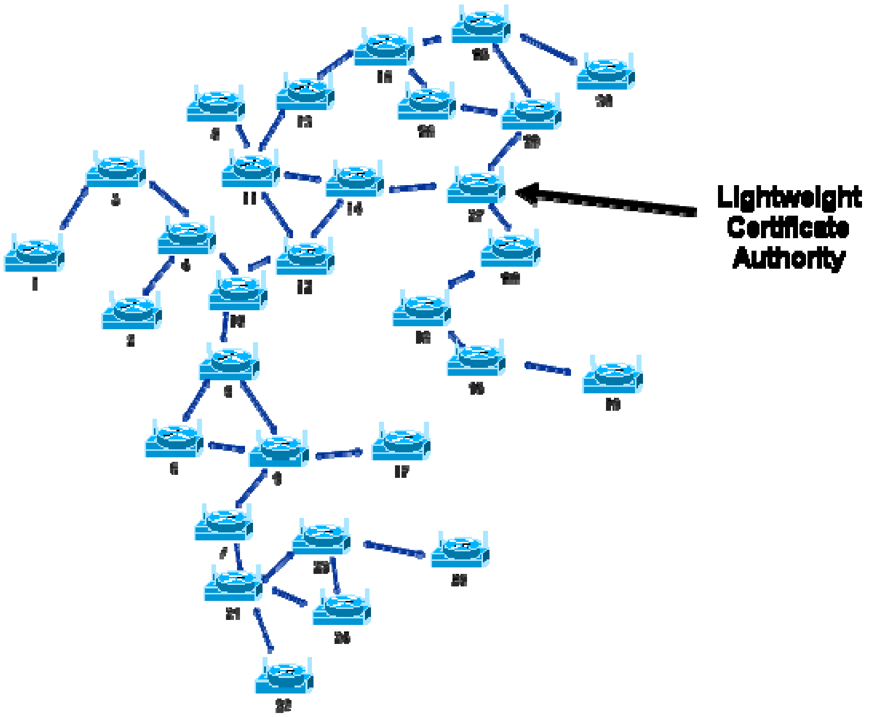


Figure 66 Trust Authority (TA) Selection

Suppose an adversary acts to compromise the certificates by running an exploit against the device. The adversary may break Device 27's security and compromise the network's security certificates. The adversary could then corrupt or steal information that is flowing between MANET devices and cause the organization's mission to fail.

Thus, the inclusion of security characteristics is an important aspect of a MANET resource decision.

This concludes the validation of our decision framework. In order to summarize the research and to describe the contributions of our work, we now present our conclusions and an assessment of future work that may extend the usefulness of the decision framework.

VIII. CONCLUSIONS AND FUTURE WORK

In this chapter, we provide the conclusions of our research. We highlight the important contributions of our work, as well as describe future work that may extend the usefulness of our decision framework.

A. CONCLUSIONS

We have successfully developed a conceptual framework that offers the ability to include multiple, qualitative security factors into decision processes. The use of Value Focused Thinking (VFT) in the decision framework allows for the combination of quantitative and categorical (e.g., qualitative) attributes in a meaningful way. This research addresses the IRC's hard problem of security measurement and is generally applicable to any situation requiring a decision based upon subjective or qualitative input data.

The decision framework, as applied to a Mobile Ad Hoc Network, improves the ability to manage the resources of the MANET and directly results in efficient, effective connectivity and security of inter-device communications. Our work provides an optimized MANET management decision framework that is robust in its ability to combine the functional characteristics of the MANET with security factors. This framework has enhanced the capability to understand the operational configuration of nodes in a MANET, allowing for a more accurate, security grounded decision-making process for dynamic MANET management. We have introduced the *MANET Distributed Functions Ontology*, which organizes the commonly used decision parameters and incorporates security parameters that are often neglected. We expect that the ontology's structural relationships, between the parameters and the dynamics of the MANET, may lead to reduced complexity in the decision-making algorithm and improve the ability to make decisions in a more timely fashion. We expect the incorporation of security attributes and relations will enhance the ability to service the network as well as provide more robust security.

The use of VFT allows for the combination of quantitative and qualitative attributes in a meaningful way, something that proposed cluster-selection algorithms cannot accomplish. We have demonstrated the ability to include multiple, qualitative security factors into MANET decisions. Our specialized minimum cost flow model serves to optimize our decision and reinforce connectivity, which is a big factor in the efficient use of energy in the network. Our work leverages these two node-choice components to enhance the confidentiality, integrity, and availability of MANET communications. In addition, our framework provides the ability to tune security attributes as the context of the MANET changes. Our work is a first step towards a near-objective, automated decision capability for MANETs. Qualitatively, we find that our decision framework produces sensible choices for node selection, with the added benefit of the inclusion of security factors.

Because our work allows for a more holistic device characterization to include security considerations, the MANET management process can optimize the node choice and increase the overall stability of the virtual topology in the face of continual physical mobility. A suitable choice maximizes the functionality, efficiency, and security of the intra-device MANET communications, leading to minimal disruption in the actual operations of tactical military units, first responders, and disaster response teams.

B. FUTURE WORK

To increase the overall confidence in our framework, it is possible to expand our existing behavioral validation approach to include a higher degree of expert input and additional scenarios (e.g., more CONOPs). In Artificial Intelligence terms, we use *human annotation*, or the judgment of a domain expert, as “ground truth” against which we assess our framework’s behavior (e.g., node choice). Evaluation of the scenarios by an increased number of experts will instill greater confidence in the ground truth of acceptable output behavior. Further, measuring additional scenarios against the ground truth could lead to an increased identification of the tradeoffs between the measureable attributes.

Additional future work includes developing extensions to our framework by applying it to other security scenarios where decisions have to be made that impact the security of both communicated data and the information system itself (e.g., which network printer should a print job be sent to). The extensions will serve to further demonstrate the relevance of the framework to the security community.

The framework may also be extended to network science problems. Based on organizational objectives and human interaction factors, our approach may identify the hierarchy of members in the social network to include the identification of the "cluster-head." In the case of a terrorist organization, quantifying the interaction between members may allow us to make an improved decision on how to best interdict the organization's operations.

An interesting study may be the use of the optimized connectivity map as a basis for routing decisions within the MANET. Currently, selection algorithms and routing algorithms run independently of each other. In a resource constrained environment such as a MANET, the redundancies in computation and message passing between the two algorithms may cause unnecessary depletion of battery power. Although our framework focuses on improving the selection methodology, it has the potential of eliminating the need for a separate routing algorithm via the use of the near optimal connectivity map.

Finally, our framework may become the centerpiece of a lightweight version of the Department of Defense's Risk Adaptive Access Control (RAdAC). Currently, the RAdAC architectures that exist for wired networks include a single device with large databases and unlimited resources [21]. For a mobile network such as a MANET, the access policy decision point (PDP) and the enforcement point (PEP) responsibilities will have to be shared by the participating devices.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. (EXECUTION PROGRAM)

The following AMPL program is the ***execution program***. Notice that it calls both the model file (detailed1.mod) and the data file (dSec.dat), as well as utilizes the CPLEX external solver.

```
# BEGIN FILE

model detailed1.mod;
data dSec.dat;
option solver cplexamp;


param V;          # highest utility value from the set of arcs

        let V := max{(i,j) in LINKS} value[i,j];
        let {(i,j) in LINKS} cost[i,j] := V - value[i,j] + 0.0001;
display cost, value, V > out;

let {(i,j) in LINKS} penalty[i,j] := V; # penalty equal to highest link
                                                cost
param count;

let count := 1;

param best_soln;

let best_soln := sum{(i,j) in LINKS} value[i,j];

repeat {

for {i in NODES: ord(i) = count} {
      let supply[i] := card(NODES)-1;
      let demand[i] := 0;

display supply, demand > out;
expand Balance > out;

      solve;

if Total_Cost < best_soln then {
      let best_soln := Total_Cost;
}

display best_soln;
      option omit_zero_rows 1;
      option display 1_col;
      display Total_Cost, Connect, z > out;
      display best_soln > out;
      let count := count + 1;
      let supply[i] := 0;
      let demand[i] := 1;
}
}

until count = card(NODES) + 1;
      display best_soln > out;

# END FILE
```

APPENDIX B. (MODEL FILE)

The following AMPL file is the ***model file*** (detailed1.mod).

```
# BEGIN FILE


set NODES ordered;
set LINKS within (NODES cross NODES);

param supply {NODES} >=0 default 0; # total connections to superdude
param demand {NODES} >=0 default 1; # connection from superdude

check: sum {i in NODES} supply[i] = sum {j in NODES} demand[j];

param cost {LINKS} >= 0;            # cost per unit
param value {LINKS} >= 0;           # utility per unit
param capacity {LINKS} >= 0 default 1;    #   max   connections   on   arc
without penalty
param penalty {LINKS} default 0.50;

var Connect {(i,j) in LINKS} >= 0;  # connections that use arc (i,j)
var z {(i,j) in LINKS} >= 0;

minimize Total_Cost:
      sum{(i,j)  in  LINKS}  cost[i,j]  *  Connect[i,j]  +  sum{(i,j)  in
LINKS}
penalty[i,j] * z[i,j];

subject to Balance {k in NODES}:
      supply[k] + sum{(i,k) in LINKS} Connect[i,k]
            = demand[k] + sum {(k,j) in LINKS} Connect[k,j];

subject to penalty_for_reuse {(i,j) in LINKS}:
      Connect[i,j] <= 1 + z[i,j];



# END FILE
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. (DATA FILE)

The following AMPL file is the ***data file*** (dSec.dat).

```
# BEGIN FILE
      set NODES := 1 2 3 4 5;
      set LINKS :=      (1,2) (1,3) (1,4) (2,4)
                        (3,4) (3,5)
                        (2,1) (3,1) (4,1) (4,2)
                        (4,3) (5,3);
      param value :=
                      1 2         6.4
                      1 3         2.9
                      1 4         2.5
                      2 4         2.8
                      3 4         2.4
                      3 5         3.6

                      2 1         6.4
                      3 1         2.9
                      4 1         2.5
                      4 2         2.8
                      4 3         2.4
                      5 3         3.6;

# END FILE
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. (OUTPUT FILE)

The following data file shows the resulting ***output*** when the previous AMPL program is run on the five node network.

```
# BEGIN FILE

:     cost  value    :=
1 2   0.0001   6.4
1 3   3.5001   2.9
1 4   3.9001   2.5
2 1   0.0001   6.4
2 4   3.6001   2.8
3 1   3.5001   2.9
3 4   4.0001   2.4
3 5   2.8001   3.6
4 1   3.9001   2.5
4 2   3.6001   2.8
4 3   4.0001   2.4
5 3   2.8001   3.6
;

V = 6.4

: supply demand    :=
1    4      0
;

subject to Balance[1]:
        -Connect[1,2] - Connect[1,3] - Connect[1,4] + Connect[2,1] +
        Connect[3,1] + Connect[4,1] = -4;

subject to Balance[2]:
        Connect[1,2] - Connect[2,4] - Connect[2,1] + Connect[4,2] = 1;

subject to Balance[3]:
        Connect[1,3] - Connect[3,4] - Connect[3,5] - Connect[3,1] +
        Connect[4,3] + Connect[5,3] = 1;

subject to Balance[4]:
        Connect[1,4] + Connect[2,4] + Connect[3,4] - Connect[4,1] -
        Connect[4,2] - Connect[4,3] = 1;
```

```
subject to Balance[5]:
        Connect[3,5] - Connect[5,3] = 1;

Total_Cost = 20.1005

:  Connect   z    :=
1 2    1     0
1 3    2     1
1 4    1     0
3 5    1     0
;

best_soln = 20.1005

: supply demand    :=
1    0     1
2    4     0
3    0     1
4    0     1
5    0     1
;

subject to Balance[1]:
        -Connect[1,2] - Connect[1,3] - Connect[1,4] + Connect[2,1] +
        Connect[3,1] + Connect[4,1] = 1;

subject to Balance[2]:
        Connect[1,2] - Connect[2,4] - Connect[2,1] + Connect[4,2] = -4;

subject to Balance[3]:
        Connect[1,3] - Connect[3,4] - Connect[3,5] - Connect[3,1] +
        Connect[4,3] + Connect[5,3] = 1;

subject to Balance[4]:
        Connect[1,4] + Connect[2,4] + Connect[3,4] - Connect[4,1] -
        Connect[4,2] - Connect[4,3] = 1;

subject to Balance[5]:
        Connect[3,5] - Connect[5,3] = 1;

Total_Cost = 30.3007

:  Connect   z    :=
1 3    1     0
2 1    2     1
```

```
2 4     2     1
3 5     1     0
4 3     1     0
;

best_soln = 20.1005

: supply demand    :=
1    0      1
2    0      1
3    4      0
4    0      1
5    0      1
;

subject to Balance[1]:
          -Connect[1,2] - Connect[1,3] - Connect[1,4] + Connect[2,1] +
          Connect[3,1] + Connect[4,1] = 1;

subject to Balance[2]:
          Connect[1,2] - Connect[2,4] - Connect[2,1] + Connect[4,2] = 1;

subject to Balance[3]:
          Connect[1,3] - Connect[3,4] - Connect[3,5] - Connect[3,1] +
          Connect[4,3] + Connect[5,3] = -4;

subject to Balance[4]:
          Connect[1,4] + Connect[2,4] + Connect[3,4] - Connect[4,1] -
          Connect[4,2] - Connect[4,3] = 1;

subject to Balance[5]:
          Connect[3,5] - Connect[5,3] = 1;

Total_Cost = 20.2005

:   Connect   z    :=
1 2     1     0
3 1     2     1
3 4     1     0
3 5     1     0
;

best_soln = 20.1005

: supply demand    :=
1    0      1
2    0      1
3    0      1
4    4      0
5    0      1
;

subject to Balance[1]:
        -Connect[1,2] - Connect[1,3] - Connect[1,4] + Connect[2,1] +
        Connect[3,1] + Connect[4,1] = 1;

subject to Balance[2]:
        Connect[1,2] - Connect[2,4] - Connect[2,1] + Connect[4,2] = 1;

subject to Balance[3]:
        Connect[1,3] - Connect[3,4] - Connect[3,5] - Connect[3,1] +
        Connect[4,3] + Connect[5,3] = 1;

subject to Balance[4]:
        Connect[1,4] + Connect[2,4] + Connect[3,4] - Connect[4,1] -
        Connect[4,2] - Connect[4,3] = -4;

subject to Balance[5]:
        Connect[3,5] - Connect[5,3] = 1;

Total_Cost = 24.7005

:   Connect   z    :=
3 5     1     0
4 1     1     0
4 2     1     0
4 3     2     1
;

best_soln = 20.1005

: supply demand    :=
1    0      1
2    0      1
3    0      1
4    0      1
5    4      0
;

subject to Balance[1]:
        -Connect[1,2] - Connect[1,3] - Connect[1,4] + Connect[2,1] +
        Connect[3,1] + Connect[4,1] = 1;

subject to Balance[2]:
        Connect[1,2] - Connect[2,4] - Connect[2,1] + Connect[4,2] = 1;

subject to Balance[3]:
        Connect[1,3] - Connect[3,4] - Connect[3,5] - Connect[3,1] +
        Connect[4,3] + Connect[5,3] = 1;

subject to Balance[4]:
        Connect[1,4] + Connect[2,4] + Connect[3,4] - Connect[4,1] -
        Connect[4,2] - Connect[4,3] = 1;

subject to Balance[5]:
        Connect[3,5] - Connect[5,3] = -4;

Total_Cost = 47.8008

:  Connect   z    :=
1 2    1    0
3 1    2    1
3 4    1    0
5 3    4    3
;

best_soln = 20.1005

best_soln = 20.1005

# END FILE
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., and D. Raffo, "Securing the OLSR protocol," in *Med-Hoc-Net*, pp. 1-10, June 2003.

[2] Ahuja, R., Magnanti, T., and J. Orlin, *Network Flows: Theory, Algorithms, and Applications*, Prentice Hall, New Jersey, 1993.

[3] Akella, J. and D. Siewiorek, "Modeling and Measurement of the Impact of Input/Output on system Performance," in *Proc. of the International Symposium on Computer Architecture*, pp.390-399, September 1991.

[4] Amis, D. and R. Prakash, "Load-Balancing Clusters in Wireless Ad Hoc Networks," in *Proc. of the 3rd IEEE ASSET'00*, pp. 25-32, March 2000.

[5] Ananthanarayanan, R., Mohania, M., and A. Gupta, "Management of Conflicting Obligations in Self-Protecting Policy-Based Systems," in *Proc. of the 2nd International Conference on Autonomic Computing*, pp. 1-12, September 2005.

[6] Apple Technical Specifications (2008), "Technical Specifications," [Online]. Available: http://www.apple.com/iphone/specs.html, accessed: February 2008.

[7] Baker, D.J., and A. Ephremides, "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm," in *Proc. of IEEE Transactions on Communications*, Vol. COM-29, No. 11, pp. 1694-1701, November 1981.

[8] Basu, P., Khan, N., and T. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks," in *Proc. of IEEE ICDC-SW 2001*, pp. 413-418, April 2001.

[9] Bell, D., "Looking Back: Addendum," Nov. 2006, [Online]. Available: http://www.selfless-security.org/papers/addendum.php#ivt, accessed: March 2008.

[10] Berners-Lee, T., Hendler, J., and O. Lassila, "The Semantic Web," in *Scientific America*, pp. 34-43, May 2001.

[11] Beuran, R., Ivanovici, M., Dobinson, B., Davies, N., and P. Thompson, "Network Quality of Service Measurement System for Application Requirements Evaluation," in *Proc. of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS '03)*, pp. 380-387, July 2003.

[12] Blackberry Press Release (2007), "Blackberry Enterprise Solution is the First Mobile Platform to Achieve Common Criteria Certification," [Online]. Available: http://www.blackberry.com/news/press/2007/pr-25_09_2007-02.shtml, accessed: February 2008.

[13] Borenstein, D., "Towards a Practical Method to Validate Decision Support Systems," in *Decision Support Systems*, Vol. 23, No. 3, pp. 227-239, July 1998.

[14] Brown, G., Dell, R., and A. Newman, "Optimizing Military Capital Planning," *Interfaces*, Vol. 34, No. 6, pp. 415-425, 2004.

[15] Carlyle, M., "Overview of Operations Research - Prescriptive vs. Descriptive Modeling & Robust Decision Support," lecture to SE4935, Ph.D. Seminar and Training, March 2008.

[16] Chan, I., Chung, A., Hassan, M., Lan, K. and L. Libman, "Understanding the Effect of Environmental Factors on Link Quality for On-Board Communications," in *Proc. of Vehicular Technology Conference*, Vol. 3, pp. 1877-1881, September 2005.

[17] Chatterjee, M., Das, S., and D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks," *Journal of Cluster Computing*, Vol. 5, No. 2, pp. 193-204, April 2002.

[18] Chen, H. and S. Megerian, "Cluster Sizing and Head Selection for Efficient Data Aggregation and Routing in Sensor Networks," in *Proc. of the Wireless Communications and Networking Conference, 2006,* Vol. 4, pp. 2318-2323, April 2006.

[19] Chen, Y., and A. Liestman, "Approximating Minimum Size Weakly-Connected Dominating Sets for Clustering Mobile Ad Hoc Networks," in *Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networks and Computers*, pp. 165-172, June 2002.

[20] Cheshire, S., "Latency and the Quest for Interactivity," November 1996, [Online]. Available: http://www.stuartcheshire.org/papers/LatencyQuest.html, accessed: April 2008.

[21] Choudhary, R., "A Policy Based Architecture for NSA RAdAC Model, " in *Proc. of the 2005 IEEE Workshop on Information Assurance and Security*, pp. 294-301, June 2005.

[22] CISCO Systems, Inc., "IP over RF: Optimized Routing Over Wireless Radio Links in Mobile Ad Hoc Networks," Internal Whitepaper, Received: March 2008.

[23] Cleary, D., Danev, B., and D. O'Donoghue, "Using Ontologies to Simplify Wireless Network Configuration," in *Proc. Of Formal Ontologies Meet Industry Workshop*, pp. 1-16, June 2005.

[24] Cormen, T., Leiserson, C., Rivest, R., and C. Stein, *Introduction to Algorithms*, MIT Press, Cambridge, MA, 2004.

[25] Corson, S. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," *RFC 2501*, p.1, January 1999.

[26] Crosby, G., Pissinou, N., and J. Gadze, "A Framework for Trust-Based Cluster-head Election in Wireless Sensor Networks," in *Proc. of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pp. 13-22, June 2006.

[27] Cunningham, W., "A Network Simplex Method," in *Mathematical Programming*, Vol. 1, pp. 105-116, 1976.

[28] Dantzig, G., *Linear Programming and Extensions*, Princeton University Press, Princeton NJ, 1963.

[29] Davis, R., *The Fundamentals of Top Management*, Harper Publishing Co., New York, 1951.

[30] De Keyser, W., and P. Peeters, "ARGUS: A New Multiple Criteria Method Based on the General Idea of Outranking," in *Applying Multiple Criteria Aid for Decisions in Environmental Management*, pp. 263-278, 1994.

[31] Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, December 1985.

[32] Dinerman, A., "What Does a Modular Brigade Utilize? An Investigation into Traffic Patterns for a Deployed Modular Brigade in Iraq," White Paper, June 2006.

[33] Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 1999.

[34] Donnelly, H., "Tactical Networker: Creating a Dynamic, Self-forming Network for Formations on the Move," *Military Information Technology*, Vol. 10, No. 9, October 2006.

[35] Dzija, J., Foster, J., Hernandez, S., Nardi, S., Theriault, P., and C. Wynne, "How to Conduct Effective Focus Groups and Surveys," *Maine Adult Education Strategic Plan Booklet*, January 2005, [Online]. Available: http://maine.gov/education/aded/dev/strategic_plan/focusgr.rtf, accessed: April 2008.

[36] Ehrlich, N., "The Advanced Mobile Phone Service," *Communication Magazine*, Vol. 17, pp. 9-15, March 1979.

[37] Ewing, P., Tarantino, W., and G. Parnell, "Use of Decision Analysis in the Army Base Realignment and Closure (BRAC) 2005 Military Value Analysis," *Decision Analysis, Informs*, Vol. 3, No. 1, pp.33-49, March 2006.

[38] Forrest, J., and J. Tomlin, "Implementing Interior Point Linear Programming Methods in the Optimization Subroutine Library," in *IBM Systems Journal*, Vol. 31, No. 1, pp. 26-38, March 1992.

[39] Forrester, J. and P. Senge, "Tests for Building Confidence in System Dynamics Models," in *TIMS Studies in the Management Sciences*, Vol. 14, pp. 209-228, 1980.

[40] Fourer, R., Gay, D. and B. Kernighan, *AMPL: A Modeling Language for Mathematical Programming*, Duxbury Press, Boston, MA, 2002.

[41] Gerla, M. and J. Tsai, "Multicluster, Mobile, Multimedia Radio Network," in *Wireless Networks*, Vol. 1, No. 3, pp. 255-265, 1995.

[42] Ghosh, R., Das, A., Som, P., Bhattacharya, R., Venkateswaran, P., and S. Sanyal, "A Novel Optimized Clustering Scheme for Mobile Ad hoc Networks," in *Proc. XXVIIIth URSI General Assembly*, pp. 1-4, October 2005.

[43] Gonzalez, O., Leon, C., Miranda, G., Rodriguez, C., and C. Segura, "A Parallel Skeleton for the Strength Pareto Evolutionary Algorithm 2," in *Proc. of 15th EuroMicro International Conference on Parallel, Distributed, and Network-Based Processing*, pp. 434-441, 2007.

[44] Gruber, T., "Ontology," *Encyclopedia of Database Systems*, Springer-Verlag, Berlin, September 2007.

[45] Hamill, J., Deckro, R., and J. Kloeber, "Evaluating Information Assurance Strategies," *Decision Support Systems*, Vol. 39, No. 3, pp. 463-484, May 2005.

[46] Harris Product Specification (2008), "AN/PRC-152 Type-1 Multiband Multi-mission Handheld Radio," [Online]. Available: http://www.rfcomm.harris.com/products/tactical-radio-communications/an-prc-152.pdf, accessed: March 2008.

[47] Heinzelman, W., Chandrakasan, A., and H. Balakrishnan, "Energy-Efficient Communications Protocol for Wireless Microsensor Networks," in *Proc. of the Hawaii International Conference on System Sciences*, Vol. 2, pp. 8020-8030, January 2000.

[48] Ho, C., Singh, Y., and H. Ewe, "An Ant Colony Optimization Approach to Building Clusters in Ad Hoc Networks," in *Proc. of the Multimedia University International Symposium on Information and Communication Technologies*, pp. TS1B 1-4, October 2004.

[49] Hockenberry, C. (2007), "What the iPhone specs don't tell you…," [Online]. Available: http://furbo.org/2007/08/21/what-the-iphone-specs-dont-tell-you/, accessed: March 2008.

[50] Holger, K., and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, John Wiley and Sons, London, 2005.

[51] Howard, C., "Systems Maintenance Programs - The Forgotten Foundation and Support of the CIA Triad," in *SANS Institute GSEC*, Vol. 1, No. 3, January 2002, [Online]. Available: http://www.sans.org/reading_room/whitepapers/policyissues/498.php, accessed: December 2007.

[52] Huda, M., Yasmeen, F., Kamioka, E., and S. Yamada, "Optimal Path Selection in MANET Considering Network Stability and Power Cost," *Information Technology Journal*, Vol. 6, No. 7, pp. 1021-1028, 2007.

[53] Hui Cheng, J., Wang, X., and S. Das, "Stability-based Multi-objective Clustering in Mobile Ad Hoc Networks," in *Proc. of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks*, Vol. 191, pp. 27-35, August 2006.

[54] IETF Document (2008). "IEEE 802.11."

[55] INFOSEC Research Council, "National Scale INFOSEC Research Hard Problems List," November 2005, [Online]. Available: http://www.infosec-research.org/documents.html, accessed: April 2008.

[56] Intel Corp., "Introducing the 45 nm Next-Generation Intel Core Microarchitecture," Intel White Paper, 2007, [Online]. Available: http://www3.intel.com/technology/architecture-silicon/intel64/45nm-core2_whitepaper.pdf, accessed: March 2008.

[57] Intel Product Brief, "The classmate PC powered by Intel for emerging markets worldwide," [Online]. Available: http://www.intel.com/intel/worldahead/classmatepc/, accessed: March 2008.

[58] Irvine, C. and T. Levin, "Toward Quality of Security Service in a Resource Management System Benefit Function," in *Proc. of the Heterogeneous Computing Workshop*, pp. 133-140, May 2000.

[59] ITU Recommendation I.380, "Internet Protocol (IP) Data Communication Service - IP Packet Transfer and Availability Performance Parameters," ITU, February 1999.

[60] Jensen, P., "Linear/Integer Programming - Jensen Solver," 2004, [Online]. Available: http://www.me.utexas.edu/~jensen/ORMM/computation/unit/mp_add/subunits/lp_add/jensen.html, accessed: November 2007.

[61] Johnson, D., "Routing in Ad Hoc Networks of Mobile Hosts," in *Proc. of the Workshop on Mobile Computing Systems and Applications*, Vol. 5, No. 1, pp. 158-163, December 1994.

[62] Joint Tactical Radio System (JTRS) Operational Requirements Document (ORD), ver. 3.2, JROCM 087-03, April 2003.

[63] Jonsson, E., "An Integrated Framework for Security and Dependability," in *Proc. of NSPW*, pp. 22-29, September 1998.

[64] Kahn, R, Gronemeyer, S, Burchfiel, J. and R. Kunzelman, "Advances in Radio Packet Technology," in *Proc. IEEE*, Vol. 66, pp. 1468-1496, November 1978.

[65] Kaplan, A., "Applications for Real-Time Access," in *Oracle Magazine*, p. 1, May/June 2006.

[66] Karmarkar, N., "A New Polynomial-Time Algorithm for Linear Programming," in *Combinatorica*, Vol. 4, pp. 373-395, 1984.

[67] Keeney, R., and H. Raiffa, *Decision-making with Multiple Objectives*, Wiley, New York, 1976.

[68] Kim, J., Hensgen, D., Kidd, T., Siegel, H., St. John, D., Irvine, C., Levin, T., Porter, N., Prasanna, V., and R. Freund, "A QoS Performance Measure Framework for Distributed Heterogeneous Networks," in *Proc. of the 8th Euromicro Workshop on Parallel and Distributed Processing*, pp. 18-28, January 2000.

[69] Kirkwood, C., *Strategic Decision-making: Multiobjective Decision Analysis with Spreadsheets*, Duxbury Press, Belmont, CA, 1997.

[70] Kopelson, C., "Flash Off Road," [Online]. Available: http://www.flashoffroad.com/, accessed: March 2008.

[71] Lee, R., Kwan, P., McGregor, J., Dwoskin, J., and Z. Wang, "Architecture for Protecting Critical Secrets in Microprocessors," in *Proc. of the 32nd Annual International Symposium on Computer Architecture*, pp. 2-13, 2005.

[72] Lemos, R., "US Army Requires Trusted Computing," *Security Focus*, July 2006, [Online]. Available: http://www.securityfocus.com/brief/265, accessed: April 2008.

[73] Levin, T., Irvine, C., and E. Spyropoulou, "Quality of Security Service: Adaptive Security," in *The Handbook of Information Security*, Vol. 3, pp. 1016-1025, December 2005.

[74] Lewis, T., *Critical Infrastructure Protection in Homeland Security*, John Wiley & Sons, New York, 2006.

[75] Lexikon's History of Computing, Microprocessor Chips: Intel, 2003, [Online]. Available: http://www.computermuseum.li/Testpage/MicroprocessorChipsTable.htm, accessed: February 2008.

[76] Li, X., "Genetic Algorithm Simulated Annealing Based Clustering Strategy in MANET," in *Proc. of ICNC 2005*, pp. 1121-1131, July 2005.

[77] Liang, L., Sun, Z., and D. He, "New Parameters and Metrics for Multiparty Communications," in *Next Generation Internet Networks*, pp. 396-403, April 2005.

[78] Lin, C. and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks," in *IEEE JSAC*, Vol. 15, pp. 1265-75, September 1997.

[79] Markham, J., "Elements of Client Confidence in System Dynamics Interventions: A Case-Based Ethnographic Study," in *Proc. Of the 13th ANZSYS Conference*, pp. 1-11, December 2007.

[80] Moody, J., and D. White, "Structural Cohesion and Embeddedness: A Hierarchical Concept of Social Groups," in *American Sociological Review*, Vol. 68, No. 1, pp. 103-127, 2003.

[81] National Information Assurance Partnership (NIAP), "Defining the Common Criteria Evaluation and Validation Scheme," [Online]. Available: http://www.niap-ccevs.org/cc-scheme/defining-ccevs.cfm, accessed: September 2007.

[82] Neiger, D. and L. Churilov, "Goal-Oriented Business Process Modeling with EPCs and Value-Focused Thinking," in *Proc. of the International Conference on Business Process Management*, Vol. 3080, pp. 98-115, 2004.

[83] Netfast News Release, "Trusted Network Connect' Puts Hardware Security Agent In Every PC," February 2005, [Online]. Available: http://www.netfastusa.com/xq/asp/id.1509/p.5-6-1/qx/PressRelease_view.htm, accessed: March 2008.

[84] Newman, A. and M. Kuchta, "Using Aggregation to Optimize Long-Term Production Planning at an Underground Mine," *European Journal of Operational Research*, Vol. 176, No. 2, pp. 1205-1218, 2007.

[85] Nilsson, A., Chon, W., and C. Graff, "A Packet Radio Communication System Architecture in a Mixed Traffic and Dynamic Environment," in *Proc. Computer Networking Symposium*, IEEE CH1586, pp.51-66, July 1980.

[86] Noy, N., and M. Musen, "Ontology Versioning in an Ontology Management Framework," in *IEEE Intelligent Systems*, Vol. 19, No. 4, pp. 6-13, July 2004.

[87] Orlin, J., "A Faster Strongly Polynomial Minimum Cost Flow Algorithm," in *Proc. of the Twentieth Annual ACM Symposium on Theory of Computing*, pp. 377-378, May 1988.

[88] Orlin, J., "A Polynomial Time Primal Network Simplex Algorithm for Minimum Cost Flows," in *Proc. of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 474-481, January 1996.

[89] Orwat, M., Levin, T. and C. Irvine, "An Ontological Approach to Secure MANET Management, " in *Proc. of the Third International Conference on Availability, Reliability, and Security*, pp. 787-794, May 2008.

[90] Pala, O., Vennix, J., and J. Kleijnen, "Validation in Soft OR, Hard OR and System Dynamics: A Critical Comparison and Contribution to the Debate," in *Proc. of the 17th International Conference of the System Dynamics Society*, pp. 1-17, 1999.

[91] Perkins, C., and E. Royer, "Ad hoc On-Demand Distance Vector Routing," in *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, February 1999.

[92] Perkins, C., and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in *Proc. of SIGCOM 94*, pp. 234-244, August 1994.

[93] Pfleeger, C. and S. Pfleeger, *Security in Computing*, Prentice Hall, Upper Saddle River, NJ, 2003.

[94] Protégé Home Page. (2007). [Online]. Available: http://protege.stanford.edu/, accessed: December 2007.

[95] Rainey, B., "RE: Technical Question on the JTRS Enhanced MBITR [JEM]," E-mail, April 2008.

[96] Rainey, R., "Additional Technical Questions on the JTRS Enhanced MBITR [JEM]," E-mail Correspondence from Thales Communications, Inc., May 2008.

[97] Raskin, V., and S. Nirenburg, "Ontology in Information Security: a Useful Theoretical Foundation and Methodological Tool," in *Proc. of New Security Paradigms 2001*, Session 3, pp. 53-59, September 2002.

[98] Reidt, S. and S. Wolthusen, "An Evaluation of Cluster-head TA Distribution Mechanisms in Tactical MANET Environments," in *Proc. of International Technical Alliance in Network and Informational Science*, pp. 1-7, September 2007.

[99] Ricci, L., and L. McGinnes, "Embedded System Security Designing Secure Systems with Windows CE", Applied Data Systems Whitepaper, 2003-2004.

[100] Saltzer, J., Reed, D. and D. Clark, "End-to-End Arguments in System Design," in *ACM Transactions on Computer Systems (TOCS)*, Vol. 2, No. 4, pp. 277-288, November 1984.

[101] Sanzgiri, K., Levine, B., Shields, C., Dahill, B., and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proc. of the 10th IEEE International Conference on Network Protocols (ICNP'02)*, pp. 1-10, August 2002.

[102] Shamir, R., "Efficiency of the Simplex Method: a Survey," in *Management Science*, Vol. 33, No. 3, pp.301-334, March 1987.

[103] Sheng, H., Nah, F., and K. Siau. "Strategic implications of mobile technology: A Case Study Using Value-Focused Thinking," *Journal of Strategic Information Systems*, pp. 1-22, 2005.

[104] Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley and Sons, New York, 1993.

[105] Shrimpton, D. and A. Newman, "The US Army Uses a Network Optimization Model to Designate Career Fields for Officers," *Interfaces*, Vol. 35, No. 3, pp. 230-237, 2005.

[106] Smith, R., "Introduction to Multilevel Security," University of St. Thomas Course Material, part 1, 2007, [Online]. Available: http://www.cs.stthomas.edu/faculty/resmith/r/mls/m1intro.html, accessed: February 2008.

[107] Smith, S., "Magic Boxes and Boots: Security in Hardware," *Computer*, Vol. 37, No. 10, pp. 106-109, October 2004.

[108] Suranovic, S., "Economies of Scale and Returns to Scale," *International Trade Theory and Policy*, Chapter 80-1, February 2007, [Online]. Available: http://internationalecon.com/Trade/Tch80/T80-1.php, accessed: May 2008.

[109] Thales Product Specification (2008), "Multiband Inter/Intra Team Radio (MBITR)," [Online]. Available: https://secure.thalescomminc.com/cart2/tcDesc.asp, accessed: May 2008.

[110] The Boy Genius Report (2007), "Blackberry 9000 specs revealed, our early Christmas present to you," [Online]. Available: http://www.boygeniusreport.com/2007/11/30/blackberry-9000-specs-revealed-our-early-christmas-present-to-you/, accessed: February 2008.

[111] The gadgeteer (2006), "the OQO Model 01+ Ultra Personal Computer," [Online]. Available: http://the-gadgeteer.com/review/oqo_model_01_ultra_personal_computer, accessed: February 2008.

[112] ThomasNet, "Software Provides Smartphone Security Functionality," August 2007, [Online]. Available: http://news.thomasnet.com/fullstory/526426, accessed: March 2008.

[113] Tran, L., Phone Conversation from Harris RF Communications, May 2008.

[114] Trochim, W., "Measurement Validity Types," in *Research Methods Knowledge Base*, October 2006, [Online]. Available: http://www.socialresearchmethods.net/kb/measval.php, accessed: May 2008.

[115] Trusted Computing Group, Mobile Phone Working Group, "Use Case Scenarios - v 2.7", September 2005, [Online]. Available: https://www.trustedcomputinggroup.org/groups/mobile/Final_use_cases_sept_22_2005.pdf, accessed: January 2008.

[116] Turgut, D., Das, S., Elmasri, R., and B. Turgut, "Optimizing Clustering Algorithm in Mobile Ad Hoc Networks Using Genetic Algorithm Approach," in *Proc. of IEEE GlobeCom*, pp. 62-66, March 2002.

[117] Uusilehto, J., "Establishing Mobile Security," in *TMC Internet Telephony*, Vol. 10, No. 6, June 2007.

[118] Uusilehto, J., "Start: How to Establish Mobile Security," December 2006, [Online]. Available: http://www.mobilehandsetdesignline.com/196701831;jsessionid=BT4B5T15OGMLGQSNDLQCKH0CJUNN2JVN?printableArticle=true, accessed: February 2008.

[119] Wallace, LTG W., Testimony Before the House Armed Services Committee on C4I Interoperability, October 2003.

[120] Wang, C. and W. Wulf, "A Framework for Security Measurement," in *Proc. of the National Information Systems Security Conference*, pp. 522-533, October 1997.

[121] Winjum, E., Spilling, P. and O. Kure, "Trust Metric Routing to Regulate Routing Cooperation in Mobile Wireless Ad hoc Networks," in *Proc. of 2005 European Wireless (EW 2005)*, pp. 399-406, April 2005.

[122] WordReference.com. (2008). [Online]. Available: http://www.wordreference.com/definition/decision, accessed: November 2007.

[123] Yu, J., and P. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks," in *IEEE Communications Surveys & Tutorials*, Vol. 7, No. 1, pp. 32-48, March 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Susan Alexander
   OASD/NII DOD/CIO
   Washington, DC

4. Dr. Lee Badger
   Defense Advanced Research Projects Agency (DARPA)
   Arlington, VA

5. Hugo A. Badillo
   National Security Agency (NSA)
   Fort Meade, MD

6. Terry Benzel
   USC/ISI
   Marina del Rey, CA

7. George Bieber
   OSD
   Washington, DC

8. John Campbell
   National Security Agency (NSA)
   Fort Meade, MD

9. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

10. Dr. Grace Crowder
    National Security Agency (NSA)
    Fort Meade, MD

11. Louise Davidson
    National Geospatial Agency
    Bethesda, MD

12. Steve Davis
NRO
Chantilly, VA

13. Vincent J. DiMaria
National Security Agency (NSA)
Fort Meade, MD

14. Dr. Tim Fossum
National Science Foundation (NSF)
Arlington, VA

15. Jennifer Guild
SPAWAR
Charleston, SC

16. Dr. Ted Huffmire
Naval Postgraduate School
Monterey, CA

17. Dr. Cynthia Irvine
Naval Postgraduate School
Monterey, CA

18. Dr. Steven King
OSD-ATL
Rosslyn, VA

19. Steve LaFountain
National Security Agency (NSA)
Fort Meade, MD

20. Dr. Greg Larson
IDA
Alexandria, VA

21. Tim Levin
Naval Postgraduate School
Monterey, CA

22. Dr. Karl Levitt
National Science Foundation (NSF)
Arlington, VA

23. Dr. Kyle Lin
Naval Postgraduate School
Monterey, CA

24. John Mildner
SPAWAR
Charleston, SC

25. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

26. Dr. Alexandra Newman
Colorado School of Mines
Golden, CO

27. Thuy Nguyen
Naval Postgraduate School
Monterey, CA

28. Dr. Mark Orwat
Naval Postgraduate School
Monterey, CA

29. Jim Roberts
Central Intelligence Agency
Reston, VA

30. Ed Schneider
IDA
Alexandria, VA

31. Mark Schneider
National Security Agency (NSA)
Fort Meade, MD

32. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

33. Ken Shotting
National Security Agency (NSA)
Fort Meade, MD

34. Dr. Gurminder Singh
Naval Postgraduate School
Monterey, CA

35. CDR Wayne Slocum
SPAWAR
San Diego, CA

36. Dr. Ralph Wachter
ONR
Arlington, VA

37. Matt Warnock
Booze-Allen-Hamilton