Optimizing Military Tactical MANETs efficiently using PSO

by

Younchol Cho

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
December 18, 2009

Keywords: mobile ad-hoc network, hop-count, shortest path,
particle swarm optimization, network centric warfare

Approved by

Alice E. Smith, Co-chair, Professor of Industrial & Systems Engineering
Jeffrey S. Smith, Co-chair, Professor of Industrial & Systems Engineering
Abdullah Konak, Associate Professor of Information Science & Technology, Penn State Berks

Abstract

A mobile ad-hoc network (MANET) is a self-configuring network of autonomous agents designed to continuously support users who change the topology of the network dynamically and independently. The dynamic mobility of user nodes can cause communication links to disconnect if the network is not managed correctly. The autonomous agents are controlled to maximize the connectivity of user nodes considering military aspects. Military operations require the efficient use of limited resources and sometimes sacrifice network performance to accomplish given missions. Especially, military MANETs are exposed to a dangerous environment due to the enemy activities, so these hostile effects should be considered. Under these requirements and circumstances, the primary objective of the agents is to maximize the connection and quality of communication between user nodes and a control node. This is formulated as a shortest path problem using a hop-count metric. A population based heuristic algorithm, Particle Swarm Optimization (PSO), is developed to solve the military MANET problem. To best accommodate the aspects of military MANETs several crucial constructs are devised and tested. These are the Pre-deployed Agent Level (PAL), the Messenger Agent and the Priority node. Testing involves the common random waypoint model and two specific military scenarios - search and rescue and patrol. The proposed model in this thesis tries better represents military MANETs by considering enemy obstacles and military operation characteristics. It can be used to evaluate network performance before deploying an actual network in the battlefield and to properly size the

number of agent nodes. Also, the proposed approach could be used for commercial applications by slight modification of the objective function.

Acknowledgments

I want to thank God who allowed me to experience many valuable things through the difficulties I faced while studying for my doctoral degree at Auburn University. I will try to keep the teachings of the Lord in my heart forever. I would like to thank my country and Navy for giving me this great opportunity. I will dedicate my life to the Republic of Korea as a Korean navy officer to repay the benefits given by my country and Navy.

I would like to thank my wife Yokyung Kim, and my children, Eunju and Mansu for their love and support in the pursuit of this degree. This work would not have been possible without their understanding and support. I would also like to thank my parents, Younghwan Cho and Jonghwa Lim for their help and encouragement throughout my life.

Finally, I would like to thank Dr. Alice Smith and Jeffrey Smith, my thesis advisors and Dr. Abdullah Konak, a committee member for their great help in my research throughout my years at Auburn.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background

Today, most people carry at least one portable information device, such as laptops, mobile phones and PDAs, for use in their professional and private lives. The purpose of these devices is to exchange and acquire valuable information through well established communication technology. Let us imagine what would happen to the world if we could not use those devices for a day. It would seriously affect our normal life, and the world would immediately fall into disorder due to cessation of normal functioning of the technological infrastructure that supports many important parts of our world. The dependence of modern human life on information technology (IT) based on telecommunication networks is so prevalent that we cannot imagine a life without them [34].

The rapid development of information technology has integrated most parts of the world into one well organized system. Networking is a complex part of computing that makes up most of the IT industries. Without networks, almost all communication in the world would cease.

A telecommunications network is a network of links and nodes arranged in a way that messages may be passed from one part of the network to another through those links. These telecommunication networks can be split into two categories: wireline and wireless networks [105].

Wireline networks have provided users with very fast and reliable communications, and a large portion of the world economy now relies completely on these telecommunication networks.

Although a wireline network has the benefits of speed and security, it requires a great deal of time and cost for installation and maintenance. Moreover, it cannot respond to a dynamic situation or environment because of its requirement for infrastructure [26].

Therefore, wireless technologies are becoming quite popular and mobile internet service is a big trend. According to the survey conducted by the Pew Internet & American Life Project, 54% of those who have internet-ready phones have used their phone to go online. Also, 56% of PDA owners have used their portable device to connect to the internet [78]. Wireless networks include infrastructure-based networks and ad-hoc networks. Infrastructure-based wireless networks need some infrastructure, such as access points or base stations. So, they have a similar limitation to wireline networks, although not as severe. Most wireless infrastructure-based networks are established by a one hop radio connection, which is an intermediate connection within a string of connections linking two network devices in a network, to a wired network. On the other hand, mobile ad-hoc networks are decentralized networks that develop through self-organization, in which multi-hop communication is normal [76].

A wireless network is basically the same as a Local Area Network (LAN) or a Wide Area Network (WAN) of a wireline network, but there are no wires between hosts and servers. A Wireless LAN (WLAN) is a wireless local area network that links two or more computers or network devices without using wires. This gives users the mobility to move around within a broad coverage area and still be connected to the network. The most common WLAN, IEEE 802.11**,** covers ranges from hundreds of meters to a few kilometers, depending on antennas [86].

A Wireless Wide Area Network (WWAN) is different from a WLAN because it uses cellular network technologies. These cellular technologies are offered regionally,

nationwide, or even globally and are provided by many different wireless service companies. Cellular modems and mobile phones are good examples of this technology.

Wireless cellular systems have been in use since the 1980s. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system when they roam from one place to the other [6]. Mobile Ad-hoc Networks (MANET) have been developed from the wireless cellular system to overcome the limitation for use in an environment that does not have readily available infrastructure [18].

There are different types of agents which can be classified depending on the agent's abilities into static or mobile, reactionary or not; work alone or with other agents, autonomous or not,. A MANET is an autonomous collection of mobile nodes, users and agents forming a dynamic wireless network. Autonomous agents can independently respond to events, network state changes, and move to other locations and adjust their behavior accordingly to accomplish goals [8]. So, agents can work more intelligently when they are well informed about a network state and its users. Autonomous mobile agents in a military MANET placed in an unknown terrain is challenging under the following conditions of military applications [85]:

1) Dramatic change of geographical area (mission area) over time since dynamic nature of tasks,

2) Network nodes may be decreased by hostile attacks or malfunctions,

3) Isolation of network nodes, and

4) Intermittent communication due to a hostile environment

Mobile ad-hoc networks operate without any fixed infrastructure and offer quick and easy network deployment in situations where infrastructure is not possible [6]. In these networks, nodes typically cooperate with each other by forwarding packets for nodes which are not within the direct communication range of the source node. A MANET provides a practical way to rapidly build a decentralized communication network in an area where there is no existing infrastructure or where temporary connectivity is needed, e.g. emergency situations, disaster relief scenarios, and military applications. The distribution/routing technique used depends on multi-hop protocols in order to deliver messages between nodes connected to the network [65, 84, 96].

Nodes in a mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. The path between each pair of users may have multiple links and the radio between them can be heterogeneous if the network devices have different configurations. This allows an association of various links to be a part of the same network.

Mobile ad-hoc networks can operate in a standalone fashion or be connected to a larger network such as the Internet. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality [6]. Historically, mobile ad-hoc networks have primarily been used for tactical network related applications to improve battlefield communications/survivability and rescue operation in disaster sites.

In cases where group members have specific tasks to accomplish, group communication and synchronization are required. In military situations, for example, the members of a group of users have different targets. Thus, communication among group elements is an important issue and must be maintained for as long as possible [65]. MANET is a wireless network that continually re-organizes itself in response to environmental changes without using any

infrastructure. In order to accomplish assigned missions for a group like a military force or a rescue team, MANETs continuously communicate, collaborate, and interact among members in the network.

MANET is a key enabler for achieving the goals of Network-Centric Warfare (NCW) [69] that represent modern warfare trends. Advanced technology in combat can provide the right information at the right place and time, and shorten the "kill chain" (targeting cycle consisting of detecting a target, attacking it and assessing the result of the attack) by combining the several tactical levels of MANETs into a large strategic level of MANET. An example of this would be the U.S. armed forces' Global Information Grid (GIG) [27]. The ability to make more informed decisions faster is a central theme in the network centric warfare concept, since the key element for victory in modern warfare depends on the capability to deal with information related to the situation at hand [93]. The major challenges of MANET are to provide wireless, high-capability, secure, and networked connectivity. Compared with wired links and infrastructure based networks providing stable service, MANET capability is restrictive and has the potential for intermittent connectivity failure. So, participants must communicate using limited bandwidth through wireless links [82].

Military operations are usually performed in highly deteriorated and varied conditions due to natural and artificial obstacles. The effort for maintaining robust communication in a network or among networks in these military environments is an essential element. In fact, a network is the most important weapon for modern military operations. The information superiority based on a network will enable agile deployment of a lighter, leaner, more lethal combat enterprise that overwhelms any potential adversary before it responds [69]. In order to

meet the above practical needs, the performance of MANETs should be evaluated accurately under more realistic environments for before deployment.

We will focus on developing a more realistic and robust military MANET model in this study. The needs and problems encountered in developing a realistic military MANET model are related to simulating its operation environment as follows:

First, the representation of enemy effects in a military MANET operation is an indispensible factor for accurate evaluation before commissioning it into an actual tactical operation. However, hostile effects of enemies in the military MANET operation have not been fully studied in the literature, as far as we know. The enemies in the operation area attack the MANET nodes electrically or physically. Most research has focused only on electrical attack limiting the communication capability of MANET nodes [15, 50]. The transmission range of MANET nodes in a tactical battlefield fluctuate by an electrical attack (such as jamming), and transmission of radio signals by enemy forces to disrupt communications among MANET nodes, or the nodes could be destroyed by a physical attack. Also, the quality of wireless channels in the real world is variable due to a variety of propagation phenomenon based on the surrounding conditions, such as multipath resulting in radio signals reaching the destination node by two or more paths, atmospheric effects like fading and reflection, and obstacles [40]. As a result, the transmission range of network nodes cannot be constant, but varies depending on the surrounding conditions. So, implementing these characteristics to military MANET modeling is necessary to represent a realistic operational environment, which will help evaluate network performance more accurately.

Second, military MANETs have different operation objectives and functional characteristics from commercial ones. Maximizing connectivity between nodes in the mobile

wireless network is an important and common performance measure for MANETs. However, military MANETs, unlike commercial ones, may often pursue other objectives. The accomplishment of a given mission could be more important than other performance measures. Also, military MANET nodes need to be specified in terms of functions within the military unit structure. User (client node) and agent (service node) is a common classification for commercial networks. The military MANET may not be represented by this simple classification.

Third, the military MANET is required to be more efficient for longer operation since it tends to be operated with limited resources. Situation awareness established by robust networking is an effective weapon for the forces and commanders in waging war in a tactical operation area. This dramatically increases combat power [46]. However, because of the dynamic and unpredictable nature of military combat operations, it may be impossible to maintain full connection continuously. Especially, inefficient use of the network may shorten the operation time since battery capacity is limited. Sometimes, this situation forces military commanders to think about how to operate limited resources to maximize their networking capability.

Finally, MANET nodes' mobility in wireless networks should also be examined as a major consideration since it plays a key role in the performance evaluation of MANET [68]. The main role of a mobility model is to emulate the movement behavior of actual users in a network. There are many mobility models proposed in the literature such as random walk, random waypoint, group mobility, and reference point group mobility [5, 13, 58, 83, 87]. These models vary widely in their movement characteristics. Among those, the random waypoint model has generally been used as the default mobility model in many network simulations regardless of application since it describes the movement pattern of independent nodes by simple terms.

However, some military operations show different movement patterns from the random waypoint, in which the users' movement may be directed or coherent by operation purposes instead of moving randomly and independently. Zhou *et al.* (2004) suggest that users' mobility patterns in military scenarios may not be independent, but are related to one another. In other words, the mobility of nodes in a military network is much more coherent and directed than in civilian applications. One typical example is group mobility. In battlefields, nodes with the same mission usually move in groups such as swarms or tank battalions [109]. Consequently, the mobility pattern in military operation depends on the mission. Therefore, the mobility of a military MANET should represent the movement characteristics of a given mission.

The issues above are necessary for realistic representation of military MANET to test the effective operation of military MANETs under varied challenging conditions. In this thesis, a military MANET model which can deal with these issues is devised.

1.2 Research objectives

The primary objective of this dissertation is to develop a solvable realistic military MANET with autonomous agents under more realistic environments including employed enemy obstacles, and to develop a heuristic algorithm using Particle Swarm Optimization (PSO) to solve the model. The developed heuristic optimizer is expected to deploy the autonomous agents to the best locations at each time step based on given information such as MANET nodes' and obstacles' locations. MANET nodes have limited velocity and transmission ranges and user nodes are especially free to move around the tactical operation area. The decision variables which define the optimal solution are the agents' directions and magnitudes of motion. In order

to accomplish these objectives, the focus of the research has centered on the following detailed objectives:

To begin with**,** for a realistic military MANET model, we will implement three realistic considerations as follows:

First, the military network nodes are categorized to describe the different units under a command node in the military operation. Most MANET routing studies in the literature use two types of network node: user and agent. But in this study these are four types of network node: user, priority, agent, and control. Each node has a different responsibility and characteristic in the network. The control node is responsible for controlling the network nodes and also performs as an agent. An agent node is only responsible for supporting network connections. The priority node is basically the same type of node as the user. The difference between a user node and a priority node is the preference to be connected to the control node due to any urgent or crucial operation situation. That is, if a user node faces a situational event such as positioning in a dangerous location, fighting against enemies, and obtaining important operational information needed to be reported or broadcasted through the network immediately, it would be designated as a priority node. The priority node is converted to a user node when it gets out of the situational event.

Second, enemy obstacles constraining network nodes' capability electrically or physically are included. The network nodes' communication capabilities are degraded or destroyed by the enemy's hostile activities, such as electrical or physical attacks. These effects are modeled using the distance between a network node and enemies and the combat power of each node. The insertion of enemies to an operation environment will help increase the realism of the MANET model.

Third, a messenger option is implemented. The messenger is not a new resource, but an agent which has a temporary mission to search for disconnected users. During operation, users could be disconnected from the network. The agent node closest to the lost contact point is designated as a messenger searching for the disconnected user for an allowed time. This allowed time depends on the network state. That is, if there is extra capability of agents for the search, messenger operation time would be increased, otherwise it would be shorten by the capacity available. The main purpose of messenger implementation is to increase the performance of military MANETs. Sometimes, messenger agents are expected to improve network performance by reconnecting the disconnected users from the network.

Fourth, based on the realistic environment constructed above for a better military MANET evaluation, a heuristic algorithm is developed to find the efficient network paths in terms of military perspective by using proper network performance metrics such as hop-count, bandwidth, and a newly defined metric, Pre-deployed Agent Level (PAL). Routing by the minimum hop route has been used for a long time in wireless networks. The strong points of this method are simplicity and lower consumption of network resources than the shortest-distance path [80]. Minimum hop based routing is one of the popular methods in mobile ad-hoc networks and is suitable for the military MANETs. However, minimum hop routing does not take into account the link quality and stability [24]. So, it sometimes lacks response to network changes. We employ an important metric, PAL, to make up for this weakness. The hop-count based algorithm may not respond quickly to network changes as mentioned above since it uses the hop as its primary network performance metric. It does not consider the pre-deployment of agent nodes to the proper locations to prepare for abrupt needs. That is, a link between network nodes may be broken if it is not properly supported by agent nodes. The disconnection of the link

between users is more frequent quicker than other links due to users' free movement. Also, an agent node cannot immediately be deployed anywhere it is needed because of its velocity limitation. Consequently, hop-count alone may worsen network performance. So, PAL is developed and used in this study to deal with this problem.

Finally, in addition to the mechanisms proposed above to represent actual movement of specific military operation scenarios, two other mobility models are used. This expands our study beyond the random waypoint model which has been used as the default user mobility model in MANET research.

The experiments in this study are divided into two parts, the verification of proposed mechanisms effect and a cost benefit analysis. The three important mechanisms, PAL, messenger, and priority node, developed and for better network performance and representation of military MANETs are first assessed using different mobility models and scenarios without the physical destruction of network resources by combat. Then, a cost benefit analysis for computing the most efficient number of agents for a given operational scenario is performed, in which the physical destruction effect is included.

1.3 Dissertation overview

Chapter 2 reviews previous studies and knowledge related to military mobile ad-hoc networks and particle swarm optimization.

Chapter 3 discusses network-centric warfare (NCW) to increase understanding of new war paradigm. The key concept of modern warfare is NCW, and the mobile ad-hoc network as a tactical battlefield network is a basic component to enable NCW.

Chapters 4 and 5 present the military MANET developed for this study. Chapter 4

describes problems in a military operation environment and the mathematical models representing them and the detailed model description is shown in Chapter 5.

In Chapter 6, experiments are described and simulation results are provided with detailed analysis.

Chapter 7 presents a brief conclusion along with some suggestions for further study.

Chapter 2

Literature review

2.1 MANET performance

A wireless ad-hoc network allows network nodes to communicate with each other over a common wireless channel without support from a fixed infrastructure. The basic parameter for the MANET performance measure is the link, also called the arc, between nodes in a network. Regardless of what type of routing protocol is used, the first and most important requirement for communication between the nodes in a network is to have at least one path linking them.

Network nodes can directly talk to other network nodes if they are within their communication range, but in many cases in order to talk with a specific node they are required to communicate through other network nodes within transmission range.

The transmission range of network devices in a network is affected by factors such as transmission power of the devices and environmental conditions. In particular, military MANETs may operate under vulnerable environmental conditions, in which network nodes' capabilities may be limited. Especially, the enemy's hostile activities in a battlefield can seriously affect network communications. So, under these dynamic environments, the connectivity may not be guaranteed at all times for network nodes that are moving around the operation area continuously.

In order to maintain the connectivity between the nodes exceeding their communication capability we can add more relay nodes into the network. However, by simply doing this we may not improve the MANET performance as expected, since additional nodes may cause a traffic burden to the network. As an alternative, we can extend the transmission range by increasing the

signal strength but this may cause increased interference among the nodes. Consequently, the capacity of MANET may be decreased by the mutual interference of concurrent transmissions among network nodes.

Grossglauser and Tse [36] propose a communication model to improve the capacity of an ad-hoc network under various conditions affecting the MANET performance, with which a number of relay nodes are used to relay data and the data is relayed only when the relay node is closer to the destination, within a two-hop path. The drawback of this proposal is that the applications need to be delay tolerant because the communication is delayed until the mobile relay nodes are close to the destination nodes. This causes large delays when the size of the system is increased. Therefore, it is unsuitable for real time applications such as voice communications or remote control.

A fundamental characteristic of mobile wireless networks is the time variation of the channel strength of the underlying communication links. Such time variation is due to multipath fading, path loss via distance attenuation, shadowing by obstacles, and interference from other users. By considering such variations, a variety of properties have been proposed to evaluate a routing protocol. The metrics are usually divided into two groups: qualitative and quantitative. These property metrics used for evaluation of protocols should be independent from the routing protocols and represent the properties of given protocols [60]. Distributed operation, demand-based/proactive operation, security, bidirectional/unidirectional routing and sleep period operation are categorized into the qualitative property group. In particular, sleep period operation is required to avoid detection/jamming by an enemy. During the sleeping period, transmitting and/or receiving are stopped. On the other hand, for quantitative property, data throughput and delay, routing acquisition time and efficiency are considered. Data throughput and delay are

usually used for measuring network performance. Routing acquisition time indicates the time required to establish a route in a network.

MANET's performance should be measured using proper performance metrics based on properties due to the dynamic nature of mobile ad-hoc networks. In this research, the number of connected user nodes to the control node and the network bandwidth are the primary metrics are used to evaluate network performance. This research will focus on developing a method to model and optimize military MANETs under vulnerable situations, such as enemies in the operation area.

Some different routing algorithms which evaluate network performance based on the network connectivity have been described in the literature [1, 3, 28, 41, 47, 55, 75, 76, 79, 101]. The MANET performance of a military MANET in this study is evaluated in a vulnerable environment added by hostile forces' jamming and physical attacks. It is not well known how well MANET can perform in a vulnerable environment.

Jamming can be as simple as sending out a strong noise signal in order to prevent data packets in the network from being received. Hostile effects in military MANET operations are important considerations for planning and efficient use of limited resources since hostile action may seriously affect MANET performance. Providing efficient networking services in military MANETs is also very challenging in presence of mobility of users, unpredictable radio channel due to surrounding conditions and interference among network nodes.

Karhima *et al*. (1996) address the vulnerability of 802.11b (a set of IEEE standards that govern wireless networking transmission methods) based MANET to intentional jamming by Unattended Jammer (UAJ) and Unmanned Aerial Vehicle (UAV). These jammers use higher transmit powers than MANET nodes to obstruct the connectivity. In this research, the jammers

are fixed at locations through the simulation time span and have abilities to attack the MANET nodes based on the predefined combat power.

2.2 Network connection

A graph $G = G(V, E)$ consists of a set of nodes (vertices) and a set of edges (links, arcs). Graph theory is the study of graphs of mathematical structures that are used to model pair wise relations between objects from a certain collection in mathematics and computer science [34]. The set of nodes, denoted by $V = \{v_1, ..., v_n\}$, represents the ad-hoc network devices; and the set of edges, denoted by $E = \{e_1, ..., e_m\}$, represents the wireless communication links between nodes.

Wireless multi-hop networks are generally modeled as communication graphs. In a wireless multi-hop network, each node has a certain transmission range, and is able to send messages to other nodes within its own transmission range. A wireless network can be viewed as a communication graph, where the existence of each edge is decided by the transmission range of related nodes. Therefore, the connectivity of a network depends on the transmission ranges of all nodes. So, two nodes are able to communicate directly via a wireless link if they are within the range of each other. In terms of communication networks, all nodes of a connected network can communicate with each other over one hop or multiple hops, whereas in a disconnected network we may have several isolated sub networks which cannot communicate with one another.
Connectivity is a function of the number and locations of the nodes and wireless transmission range [6].

2.3 MANET performance metrics

Mobile networks have employed a variety of routing strategies to improve their performance under given environmental and operational conditions. The process of selecting a path among possible ones between two end users in a network depends on the variable link state over time. The link state can be expressed by costs or quality parameters that are computed based on many common types of network performance metrics such as hop-count, bandwidth, propagation delay and jitter [61, 72]. Furthermore, in many cases, the combined use of the metrics can improve the network performance as well as reduce the computation complexity. Various combinations of metrics are possible according to the application. The combination of hop-count and bandwidth is one of the most popular ones in the literature. However, the metrics should be able to represent the network properties of the system under consideration and be practical. Some metrics, such as delay and jitter, are not preferable due to their difficult computation. So, the metrics for a network must be combined together carefully by considering the complexity of computing paths based on them and the quality requirements of network flows [80].

In the long run, network routing can be chosen using either a single metric or a combination of metrics. To help the computation of combined metrics, the sequential filtering method has been utilized in many studies [80, 48, 49]. With the sequential filtering method, the metrics are divided into primary and secondary ones. Paths are computed first based on the primary metrics. Many routes are eliminated from the candidate set by the primary metrics. The candidate set of possible routes will be narrowed down using secondary metrics until a single path is found. The number of steps of the sequential filtering could be different with each application.

2.3.1 Hop-count

Mobile nodes in a wireless network are operating on a battery supply. So, mobile nodes naturally have strong power constraints and network life depends on the efficient use of this resource. In the real world, the number of relay nodes tends to be small. Therefore wireless communications share this limited number of relay nodes. Thus, each additional transmission causes the relay device to be busy for the length of the transmission and use beyond capacity prevents other nodes from transmitting. Therefore, unnecessary transmission should be minimized since additional hops or communications increase the delay of transporting the data packet due to the additional buffering, contention for resources, and transmission time required. Furthermore, efficient resource management can result in additional benefits other than reducing power consumption. For example, under a combat situation the least amount of transmission power minimizes the probability of detection or interception by enemy forces. As a result, a MANET routing protocol should be power efficient [39].

The hop-count is the number of hops separating a source node from its destination along the minimum path [97]. That is to say, it is the number of links passed by a packet between a source and a destination node. The hop-count based routing approach is one of the popular routing protocols for efficient use of the network. Most MANET protocols try to minimize the hop-count of the selected route. This is important in multi-hop wireless networks. For example, if a link between two nodes in a network requires at least 6 Mb/s bandwidth for delivering a data packet the more number of links on a selected shortest path, the more additional cost in terms of total amount of network resources consumed [37].

Under the situation of limited resources and battery efficiency issues, the hop-count based approach could be more effective than alternatives since it minimizes resource consumption.

However, the major drawback of this approach is potentially uneven network traffic. In addition, link quality may vary during the lifetime of a network because of the distance between the network nodes, transmitting power, antenna shape and orientation, radio interference, and environmental conditions. The links may be asymmetric by such variation. For instance, connectivity may change even under nodes at fixed locations and configured with the same transmission power. Connectivity could be affected by surrounding conditions other than location and transmission power factors. Due to these drawbacks, link quality based routing methods (e.g. QoS) have been considered and used [96].

The nodes in a MANET change location over time because of the dynamic nature. This mobility of MANET nodes may break the connection between nodes and lead to failure of the communication between them. Therefore, the consideration of link quality and stability in the context of link connection is as important as the selection of the shortest path. In the following section we will discuss this issue.

2.3.2 Link quality (Bandwidth)

As a network performance parameter, quality represents the state of a link by using metrics such as bandwidth, delay, etc. In this respect quality based routing is a method for traffic flow to meet quality requirements. The main purposes of this approach are to select routes satisfying a particular quality requirement and to provide efficient utilization of the network. There are three popular quality based routing algorithms based on the hop-count and bandwidth, which are Shortest-Widest Path (SWP), Widest-Shortest Path (WSP) and Shortest-Distance Path (SDP). WSP and SWP are relatively simple routing approaches [74].

WSP first considers the minimum hop-count as a primary metric, but if there is more than one such path it uses bandwidth to break the tie. That is, the shortest path which has maximum bandwidth will be chosen. Conversely, SWP chooses a path with maximum bandwidth as a primary metric, and then consider the minimum hop-count as a secondary metric. Preferring the shorter path (such as WSP) will minimize the consumption of network resources, while preferring the widest path (such as SWP) will balance network load as well as maximize the chance to meet the required bandwidth in case of inaccurate network state information [72].

Here, the bandwidth of a path indicates the minimum available bandwidth along the path. For example, if there is a path consisting of three links and each link's bandwidth is 10, 8 and 5 Mb/s, this path's bandwidth will be 5 Mb/s. SDP can dynamically balance the effect of hop-count and path load using a distance function. However, resource consumption and load distribution conflict with each other and both objectives in network operation cannot be accomplished at the same time. So, we should pick the one most suitable for a given situation, condition or operational objective [37].

2.3.3 Link stability

Link stability refers to the ability of a link to survive for a certain time period. In this respect link stability based routing is unique to wireless networks. The stability of a link has a direct relationship to the distance and signal strength between two nodes. That is, it depends on how long the two nodes remain within each other's communication range or signal strength is above a threshold.

Sridhar *et al*. (2005) propose an algorithm called Stability and Hop-count based algorithm for Route Computing (SHARC) that uses hop-count and residual lifetime of the link as

performance metrics. SHARC uses the shortest path algorithm by hop-count as the initial filter to narrow down route selections and then uses path stability by residual lifetime, a less robust indication, to choose the best route from among the available routes. Here, link stability is represented by the residual lifetime computed based on link age. The residual lifetime can be computed by the following equation [96]:

$$R_a = (\sum_{i>a}(l_i * i) / \sum_{i>a} l_i) - a \qquad (2\text{–}1)$$

Where:

R_a: the average residual link lifetime when the current link age is a

i: the link duration in seconds

l_i: the number of links with link duration in seconds

Link stability can be much more important in military MANETs in combat situations than in commercial networks since combat operations require a robust network connection to respond quickly and to maintain operational continuity. Because of these military aspects, some user nodes need to be supported with a higher priority than others even though it may sacrifice network performance. So, we designate priority nodes in this study. We will discuss this in more detail in Chapter 4.

In order to make a more efficient algorithm for maximizing network performance it is important to decide on proper metrics for network characteristics which are correspond to the surrounding conditions and operational properties. This will enable the routing algorithm to find the most available path efficiently and in a less expensive manner. Although a great variety of routing approaches have been employed, many previous studies have shown that algorithms with

a strong preference for minimum-hop routes almost always outperform algorithms that do not consider path length. The WSP is a good example. The shortest-path routing is particularly attractive in a large, distributed network, since path length is a relatively stable metric, compared with dynamic measurements of link delay or loss rate.

The completeness of the specified missions is usually the primary goal in military operations. So, network performance could be sacrificed under certain circumstances to accomplish a given mission. Successful mission performance under the modern warfare paradigm could be enhanced by maintaining a tight communication network for real time information exchange. That is, link connections in the networks should be able to be guaranteed. Hop-count, quality and stability are the most common considerations for network algorithms. For a better solution we have to combine those factors properly using the strong point of each factor [96].

2.4 MANET routing

Routing is the mechanism of directing data packet flow from the source to the destination [26] and is very crucial in the MANET, because changes in network topology and other states occur frequently and continuously.

One common and traditional way of achieving routes in mobile Ad-hoc routing is to consider each host as a router [12]. Ad-hoc mobile routing protocols can usually be categorized into three types: Table driven proactive, On-demand-driven reactive/Source initiated, and Hybrid protocols.

2.4.1 Table-driven routing (Proactive)

Table-driven routing is a proactive protocol. The most distinguishing characteristic of this routing is to continuously search for routing information within a network to keep routing tables available anytime they are needed, so it is called table-driven routing [28]. These routing protocols react to any change in the topology even if no traffic is affected by the change, and they require periodic control messages to maintain routes to every node in the network. The rate at which these control messages are sent must reflect the dynamics of the network in order to maintain valid routes. Thus, the maintenance of the routing tables requires significant bandwidth [17]. Representatives of this protocol category are briefly listed below.

- Destination-Sequenced Distance Vector Routing (DSDV): each node maintains a list of all destinations and number of hops to each destination [74].
- Clustered Gateway Switch Routing Protocol (CGSR): each node maintains a cluster member and a routing table [16].
- Wireless Routing Protocol (WRP): each node maintains four tables; distance, routing, link cost and message retransmission list [62].

2.4.2 On Demand-driven routing (Reactive)

As an alternative to proactive routing, On Demand-driven routing was introduced, which constructs paths when they are explicitly needed to route packets. This prevents the nodes from updating every possible route in the network, and instead allows them to focus either on routes that are being used, or on routes that are in the process of being set up.

The best routing can be found based on the available information about link state at the moment. In other words the routing decision depends much on the current information. Link

state information can be propagated by two ways, periodic and responding to a significant change in the link state metric. For example, the amount of change required for triggering an update could be decided by the user and any link advertises its available bandwidth metric whenever it changes by more than the set amount since the previous update message.

However, network performance could be affected by the frequency of propagating updated information. That is, frequent messaging of the information may cause too much network overhead, which may make an accurate routing decision not worth the expensive costs. So, a careful understanding of the trade-off between network overheads and an accurate routing decision should be required for adjusting the frequency of the link state update message [56, 90].

The proactive approach depletes too many resources by updating. If the update interval is too long, the network will simply contain a large amount of stale routes in the nodes, which results in a significant loss of packets. In every test case these reactive routing algorithms outperformed the proactive algorithms in terms of throughput and delay [17, 25]. Moreover, the reactive protocol is more realistic than the proactive way, considering limited resources available in the real world.

- Ad-hoc-On Demand Distance Vector (AODV): This routing protocol builds on the DSDV algorithm but improves it by minimizing the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes [76].
- Dynamic Source Routing (DSR): DSR is a routing protocol for wireless mesh networks and is similar to AODV. However, DSR uses source routing instead of relying on the routing table at each intermediate device [47].

- Signal Stability Routing (SSR): SSR selects the route based on signal strength and stability. A path that has stronger power and longer duration is chosen as the best route [1, 12].

2.4.3 Hybrid

Hybrid protocols try to combine proactive and reactive protocols. Zone Routing Protocol (ZRP) is a good example of a hybrid protocol, which divides the topology into zones and seeks to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. Any routing protocol can be used within and between zones since ZRP is modular [70, 71].

As discussed before, common classification of routing protocols is to divide them into proactive, reactive and hybrid routing. However, in [96] the authors classify routing protocols into hop-count based, QoS (e.g. bandwidth) based, and stability (or availability) based. Each of these classes of routing protocols can be either proactive or reactive [7].

2.5 Mobility

The introduction of relatively low-cost mobile computing devices is having a profound impact on everyday life. Commerce and family life are both affected by the ability to remain connected to other people and to exchange an ever increasing amount of information [88, 93]. The continuous improvement of mobile computing devices will extend the service range of mobile wireless networks and enable users' more dynamic movements. In a MANET we assume that nodes are free to move. The network topology and wireless link status are changed due to the mobility of nodes.

Many different measures of mobility for evaluating mobile ad-hoc network performance have been proposed, since a mobility model is imperative to evaluate a routing protocol of MANET using simulation [38, 93]. The most important characteristic of a mobility model is the degree of realism with respect to the movement of users, because more realistic models enable more accurate simulation and evaluation of network parameters. There are two broad categories of mobility models, trace-driven models and synthetic models. Trace-driven models use recorded histories of real users' traces. However, movement traces are unavailable in ad-hoc networks due to their decentralized nature. Therefore, we have to employ mobility models that determine the movement patterns of mobility nodes synthetically. These models supply the movement behaviors of mobile users using particular constraints or mathematical equations [68].

Other researchers [54] classify mobility models into stochastic and event-based group. They state that regardless of the selection of a mobility model, being able to measure the amount of mobility is as important as the realism of the model itself.

To achieve the greatest realism, mobility modeling must take into consideration three essential factors [97], which are spatial environments, user travel decisions and user movement dynamics. Moreover, a mobility model must address both regular and random components of a user's movement.

Signaling cost for maintenance of routes for a MANET is proportional to the rate of link changes and can be expressed as a function of the mobility of the nodes. Therefore, the performance of a MANET is closely related with the efficiency of the routing protocol in adapting to changes to the network topology and the link status. For assessing different routing protocols for MANETs, it is important to use mobility model with some index or quantitative measure that is relevant to the performance of the network [11, 76, 107].

Many authors have used different measures of mobility in their research. In [13, 93] the average speed of the nodes is used to represent their mobility, while the maximum speed is used in [39, 107]. The problem with using average or maximum speed as a measure of mobility is that the relative motion between the nodes is not reflected. Also, the same average or maximum speed in different mobility models or in networks with different physical dimensions often results from different rates of route changes [54].

Some researchers [39, 56] propose a remoteness function as a mobility measure for MANET. The remoteness is generally defined by the distance between two nodes, *i* and *j* simply.

$$R_{ij}(t) = F(d_{ij}(t)) \tag{2–2}$$

However, a more sophisticated definition is more useful for MANETs. For example, if a wireless node has R communication range and is located at a $3R$ distance, it can be considered as remote as a node located at a $10R$ distance. Similarly, if a node is well within communication range R, the node would not seem very remote even if the distance were doubled. The remoteness is changeable as the movement of the node may change the wireless link status with the node. Based on these observations, they present requirements that F satisfies:

$$\begin{aligned}
&(a) \quad F(0) = 0, \lim_{x\to\infty} F(x) = 1 \\
&(b) \quad \frac{dF(x)}{dx} \geq 0 \ \textit{for all } x \geq 0 \\
&(c) \quad \left.\frac{dF(x)}{dx}\right|_{x=0} = 0 \\
&(d) \quad \lim_{x\to\infty} \frac{dF(x)}{dx} = 0 \\
&(e) \quad \left.\frac{dF(x)}{dx}\right|_{x=R} \geq \frac{dF(x)}{dx} \ \textit{for all } x \geq 0.
\end{aligned} \tag{2–3}$$

Requirement (a) normalizes F to have unity maximum value and Requirement (b) guarantees that the remoteness is a monotonically increasing function of distance, and as a result $0 \leq F \leq 1$ from (a). Requirements (c) and (d) describe the boundary condition of F, which guarantee that the remoteness of a node at extreme locations does not change with the movement of the node. Finally, the remoteness is the most sensitive to the movement of the node by Requirement (e). The signal strength of a node in this study is described by the distance it can communicate with other node in the network. So, the remoteness of a node can be measured by its Euclidian distance to other nodes. Using this, our heuristic optimizer responds to links at the edge of a communication range.

Ishibashi and Boutaba [39] represent the relationship between mobility and MANET topology, where average link lifetimes exponentially decrease with increasing maximum velocity. Chu and Nikolaidis [19] analyze the relationship between mobility and connectivity, where the higher the velocities, the better the connectivity. Although it seems contradictory at first glance, basically it represents the same thing from a different perspective. The lifetime of a link has been described with three different definitions. First, the lifetime of a link is the time from when the nodes first move into each other's range so the link can be formed until the link is broken when they move out of communication range. However, it does not mean actual time that the link is available for use since it has to be detected by a node first to be used. This is true for breakage of the link. The second definition is the perceived link lifetime, which represents the elapsed time from the first detection to the link breakage detection. This usually extends beyond the end of the existence of a usable link. As a final definition they propose the time the link is first included in a path by the routing protocol. A failure not due to a network device but the nodes moving out of transmission range has the expected time to failure equal to half of the perceived link lifetime.

Military MANET is usually much more coherent and directed when it is compared with commercial ad-hoc networks and nodes will, in general, be more concentrated, rather than dispersed. Typical mobility models (e.g, random waypoint) used in most MANET analyses may not be sufficient for military MANETs [40]. The random waypoint model is an extension of a random walk, in which a user randomly selects a direction and a speed from a distribution within the problem space, and then randomly moves to the destination with the selected speed. When it reaches the destination, it pauses for some time and then this process is repeated again. The movement of one user node in this mobility model is modeled independently from all others [43].

The mobility of a military tactical battlefield network depends on the nature of the assigned mission. Perisa *et al*. (2007) analyze a military war game exercise and assert that many assumptions of random mobility models from the literature do not hold in military MANETs [73]. Although this is true, a recent survey of MANET simulation studies found that 65.8% of studies used the random waypoint model for mobility [68].

Chlamtac *et al.* (2005), in [18], present three essential factors for mobility modeling to achieve the greatest realism for military MANETs. There are spatial environments, user travel decisions and user movement dynamics. Moreover, a mobility model must address both the regular and the random components of a user's movement. For an accurate evaluation of the performance of a protocol, the mobility model must supply a stable movement pattern during the simulation time and attain its steady state for most of the simulation time [68].

In this thesis, two military operation based mobility models and the random waypoint model are used to represent military MANETs.

2.6 Particle Swarm Optimization (PSO)

Particle Swarm Optimization (PSO) is a population based stochastic optimization tool and this optimization technique is generally used for continuous nonlinear functions. PSO was first introduced by James Kennedy and Russ Eberhart in 1995 [28, 30, 53, 92].

PSO is based on social-psychological principles and includes two important concepts: experience and knowledge [29]. It has roots in artificial life in general, and particularly bird flocking, fish schooling, and swarming theory. It is also related to evolutionary computation, and has ties to both genetic algorithms and evolutionary programming [30, 52]. However, there is no survival of the fittest concept in PSO.

In [52] the authors state that "In theory at least, individual members of the school can profit from the discoveries and previous experience of all other members of the school during the search for food. This advantage can become decisive, outweighing the disadvantages of competition for food items, whenever the resource is unpredictably distributed in patches". This statement suggests that social sharing of information among conspeciates offers an evolutionary advantage: this hypothesis was fundamental to the development of particle swarm optimization.

2.6.1 Basic concept

PSO is initialized with a group of random particles which are candidate solutions chosen randomly within the problem space. Each particle in the swarm is represented by three component vectors: X, P and V and two fitness values. The vector X represents the current location of the particle in the search space, P records the particle's best location found so far by the particle and V is the gradient vector that defines the direction and magnitude the particle will travel if not disturbed. V is used to update X every iteration [26]. On the other hand, the two

fitness values are the x-fitness and p-fitness. The x-fitness records the fitness of the vector *X* and the p-fitness records the fitness of the vector *P*.

These particles interact with one another through the communication structure or defined social network. Each particle is evaluated by a fitness function and updated by the best fitness obtained by itself and by the swarm at each time step. Each particle keeps track of its coordinates in the problem space which are associated with its best solution so far. There are three aspects to evaluate solutions as follows:

- A global best that is known to all and immediately updated when a new best position is found by any particle in the swarm.
- A neighborhood best that the particle obtains by communicating with a subset of the swarm (in case of neighbor topology).
- The local best (or particle best), which is the best solution that the particle itself has been forced.

After each iteration, the particle updates its velocity and positions as shown in the following equations. As seen below the velocity of particles is updated by one of three different equations in equation (2-4) and then the position is updated based on the velocity. The desire to better control the scope of the problem space motivated researchers to implement an inertia weight (ω) or a constriction coefficient (*K*). The first equation among those represents the standard case that does not use either parameter, whereas the second and third equations are modified by using inertia weight (ω) or constriction coefficient (*K*), respectively. We will discuss these parameters in more detail in the next section.

$$V_t = V_{(t-1)} + \varphi_1 \cdot rand_1 \cdot (P - X_{(t-1)}) + \varphi_2 \cdot rand_2 \cdot (G - X_{(t-1)})$$

$$V_t = V_{(t-1)} \cdot \omega + \varphi_1 \cdot rand_1 \cdot (P - X_{(t-1)}) + \varphi_2 \cdot rand_2 \cdot (G - X_{(t-1)}) \quad (2\text{–}4)$$

$$V_t = K\left[V_{(t-1)} + \varphi_1 \cdot rand_1 \cdot (P - X_{(t-1)}) + \varphi_2 \cdot rand_2 \cdot (G - X_{(t-1)})\right]$$

$$X_t = X_{(t-1)} + V \quad (2\text{–}5)$$

Where,

- V_t: velocity of a agent at time t
- X_t: current location of a agent at time t
- ω: inertia weight
- K: constriction coefficient
- φ_1: control parameter representing experience information by itself
- φ_2: control parameter representing knowledge information about other agents
- P: local best of an particle
- G: global best of the swarm

Each particle modifies its position using its current position, current velocity (V_x, V_y), distance between the current position and particle personal best (P) and distance between the current position and global best (G). Two main steps in the PSO are initialization of swarm particles and fitness evaluation. The pseudo code in the Figure 2-1 shows the basic mechanism of PSO.

Initialize swarm particles

{

$X = \mathrm{U}\ (X_{min}, X_{max})$

$V = \mathrm{U}\ (V_{min}, V_{max})$

$P = X$

}

Do

{

$V = V + \varphi_1 \cdot rand_1 \cdot (P - X) + \varphi_2 \cdot rand_2 \cdot (G - X)$

$X = X + V$

If $(f(X) \geq f(P))$ then $P = X$

If $(f(X) \geq f(G))$ then $G = X$

} While (Stopping criteria not met)

Figure 2-1 PSO basic mechanism

Particles have two essential reasoning capabilities: memory of their own best position and knowledge of the global or their neighborhood's best. Members of a swarm communicate good positions to each other and adjust their own velocity and position based on these good positions [103]. As shown in the pseudo code the fitness evaluation of solutions is performed at every time step. The two best locations, P and G, are tracked by the particles while flying through the problem space.

Maintaining the G vector relies on a communication scheme within the swarm. As mentioned above, G is the best found in its neighborhood of particles or G is the global best if the swarm employs a global neighborhood. Although different neighborhood topologies have been studied in the literature, global neighborhoods seem to perform better in terms of computational costs [14]. For this reason, in this research, we use a global neighborhood.

There are two methods to determine the global best, synchronous and asynchronous. With the synchronous method, the global best location is updated after updating all particles. On the other hand, the asynchronous method determines the global best after each particle has been updated. In terms of number of iterations the asynchronous method finds solutions quicker because it uses a newly found global best location in subsequent particle updates immediately. This advantage usually makes asynchronous updates a better choice for a standard PSO. However, the synchronous method is easier to implement than the asynchronous method since it does not require evaluation of particles one by one. We use the synchronous method in this research.

PSO has been successfully applied in many research and application areas and often got better results more quickly than other methods. There are few parameters to adjust and it can be implemented easily and works well in a wide variety of applications with only slight parameter variation. The use of real numbers for decision variables leads it to be one of the most popular global optimizers [14, 52, 110]. Dengiz [26] develop a strategy optimizing the location of autonomous mobile agents in MANETs to maintain network connectivity using PSO. These mobile agents try to maximize network data flow, which is formulated as an all-pair maximum flow problem.

Baburaj and Vasudevan [4] propose a new PSO using the On Demand Multicast Routing Protocol (PSO-ODMRP) to improve the performance in routing messages in mobile ad-hoc networks. ODMRP is a mesh–based demand driven multicast protocol, where a mesh consists of a set of nodes, called forwarding nodes, responsible for forwarding data packets between a source and a receiver. PSO-ODMRP is well suited for MANETs that have a constrained power and frequently change topology.

Ji *et al*. (2004) describe how PSO algorithms can be applied to clustering techniques in MANETs. Here, the Weighted Clustering Algorithm (WCA), in which cluster heads are selected based on the weight of each node, is revised to be suitable for dense mobile nodes. A Divided Range PSO, in which particles are divided into groups and each group has four neighborhood nodes, is applied for the revised WCA above. It can assign different weights to and consider a combined effect of the transmission power, mobility and battery power of network nodes. This approach is efficient and effective when the distribution of mobile nodes is dense according to the simulation study [44].

2.6.2 PSO Parameters

As discussed above, particles update themselves with the internal velocity while going through problem space seeking best solutions. Thus, the velocity is the most important factor deciding the search process. Particles' velocities are limited by a maximum velocity. So in case where velocity exceeds the limit, it is reset to the specified maximum velocity [54]. Velocity changes in PSO are due to three parts, social, cognitive and momentum. The balance among these parts determines the balance of the global and local search ability. If all velocities are at the

maximum, particles will tend to search the periphery of the problem space. To control this problem PSO has introduced several parameters.

Shi and Eberhart [91] have shown that PSO searches wide areas effectively, but usually lacks precision for local search. Their suggestion for solving this issue is to implement an inertia weight (ω) in the standard equation that adjusts the velocity correction over time, gradually concentrating the algorithm into a local search, as shown in the following equation.

$$\omega = \omega_{\max} - \frac{\omega_{\max} - \omega_{\min}}{iter_{\max}} \times iter_{current} \tag{2–6}$$

Where,

- ω_{max} : initial weight
- ω_{min} : final weight
- $iter_{max}$: maximum iteration number
- $iter_{current}$: current iteration number

The inertia weight is used to balance global and local search abilities. A large inertia weight facilitates global searches while a small inertia weight facilitates local searches. The introduction of the inertia weight also eliminates the requirement of setting the maximum velocity each time the PSO algorithm is used.

There are other strategies to adjust the inertia weight. Eberhart and Shi (2000) describe that a fuzzy inertia weight improved PSO performance. Also, Eberhart and Shi (2001) suggest the adaptation of inertia weight with a random component, rather than time-decreasing [33]. In [77, 108], the authors assert that an increasing inertia weight obtained good PSO performance.

Another parameter, called the constriction coefficient, was introduced with the hope that it could ensure a PSO to converge to the optimal solution. Maurice Clerc [22] introduced the constriction factor (K) that improves the control of the velocities, as given by the following equation:

$$K = \frac{2}{\left|2 - \varphi - \sqrt{\varphi^2 - 4\varphi}\right|}, \text{ where } \varphi (=\varphi_1 + \varphi_2) > 4 \qquad (2\text{–}7)$$

The constriction factor approach controls system behavior, and results in convergence of the PSO over time. Unlike other methods, the constriction factor approach ensures the convergence of the search procedures based on mathematical theory. The amplitude of each particle's oscillation decreases as it focuses on a previous best point. The constriction factor approach can generate higher quality solutions than the conventional PSO approach [32, 67, 76, 91].

The PSO algorithm with a constriction factor can be considered as a special case of the PSO algorithm with inertia weight [22, 23, 31]. With use of an inertia weight or a constriction coefficient, V_{max} is no longer necessary for damping the swarm's dynamic. A PSO with a constriction coefficient is algebraically equivalent to a PSO with an inertia weight.

Eberhart and Shi (2000) describe the best approach to use with PSO as a "*rule of thumb*" is to implement the constriction factor (K) approach while limiting V_{max} (Maximum velocity) to X_{max} (Maximum distance), or implement the inertia factor approach while selecting ω, φ_1, and φ_2.

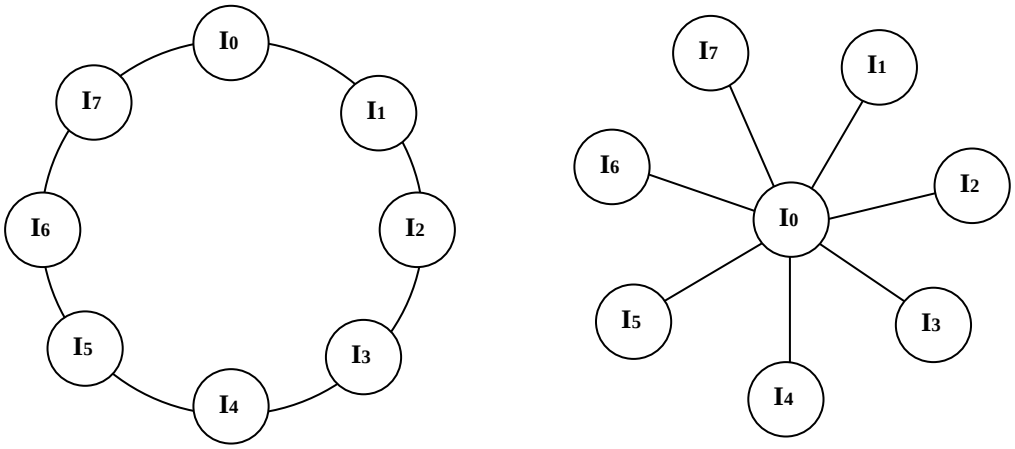
2.6.3 PSO Topology

There are static and dynamic versions of topology. The neighbors and neighborhood in a static topology are not changed during a run. However, the neighborhood changes in the dynamic version topology. The most common topologies applied in PSO are global (star) and local (ring) topology [81].

In star topology, each particle flies through the search space with a velocity that is dynamically adjusted according to the particle's personal best and by the global best by all particles achieved so far. In the ring topology, each particle's velocity is adjusted according to its personal best and the best performance achieved within its neighborhood.

The neighborhood of each particle in the local topology is generally defined as topologically near particles to the particle. The global topology also can be considered as a local topology with each particle's neighborhood the whole population. The number of particles in the neighborhood set can be expanded or contracted by adding particles that are two positions away, three positions away, etc. If the neighborhood set includes every single particle in the swarm, then the neighborhood is fully-connected, or global.

Local topology has the benefit of allowing parallel search, which results in a more thorough search strategy. Thus, it might have improved chances to find better solutions but converges more slowly than the global topology. Figure 2-2 shows an example of both topologies.



Local topology (Ring) Global Topology (Star)

Figure 2-2 Common topologies in PSO

2.7 Optimization in dynamic environments

The military mobile ad-hoc network is very dynamic due to its movement and variables concerning the natural or artificial factors existing in the operation space. Network performance is varied by changes in environment or condition, which should be managed by an optimizer. Change in environment requires re-optimizing the MANET system and a continuous tracking of the changing optimum [9]. Consequently, the optimal solutions are changed over time in the dynamic MANET environment.

Uncertainties in optimization are categorized into four classes by Jin and Branke [45].

1) Time-varying fitness functions: The evolutionary algorithm should be able to continuously track the changing optimum rather than requiring a repeated restart of the optimization process because the fitness function is deterministic at any time point but is dependent on time. The most difficult part here is to reuse information from previous environments to speed up the optimization process after a change.

2) Noise: Sensory measurement errors or randomized simulations in the fitness evaluation bring about noise.
3) Robustness: A common requirement in evolutionary optimization is that a solution should still work satisfactorily when the design variables change slightly since the design variables are subject to perturbations or changes after the optimal solution has been determined.
4) Fitness approximation: The fitness function can be approximated when the function is very expensive to evaluate, or an analytical fitness function is not available.

Military MANET problems are very dynamic. The optimal solution should be recomputed to respond to the dynamic changes. Therefore, our military MANET optimization problem falls into the first class of the category.

A MANET continues to face changes of the network topology and state over time due to dynamic factors in the environment such as mobility, various variables and obstacles, etc. The most distinctive and simplest way to respond to the changes is to consider each change as a new optimization problem that has to be solved from scratch. However, it may be inefficient under a limited time frame and not even applicable. So, using information transferred from previous time step helps increase the search speed after a change.

There are many different ways to transfer information from the previous search step. A common way is to keep the individual particles in the final population of the previous time step. However, in order to have populations respond properly and find the new optimum easily some special attention should be put on the changes in the environment at each time [10, 26, 45].

Similarly, in this study the best swarm particles' information at current time step is transferred to next time step.

The algorithm to solve the problem of optimizing the location for mobile agents should be flexible enough to react to network changes even though useful knowledge can be transferred from previous search step. Some meta-heuristics have been applied to dynamic optimization problems. PSO is one of those. Most meta-heuristics lose their adaptability to changes because of convergence during the run. Thus, a successful meta-heuristic should be able to maintain adaptability by introducing other metrics besides transferring knowledge [45]. If it is not supplemented, the hop-count based approach used in this research may lack adaptability when it is not required to maintain network connectivity at the moment. In other words, agent nodes may be placed at locations distant from the optimal ones near from future. That is, the mobile agents need to be within the proximity of the new optimal locations which need agents for network connection. If not, network cannot respond quickly to changes and network performance will degrade.

The maximum available velocity of the agents and other possible constraints limit the search in a MANET. Therefore, the mobile agent optimization problem is appropriate to dynamic environment solution methods because of these intrinsic characteristics.

In this research, a PSO with dynamic objective functions is developed to dynamically manage the motion of the mobile agents operated under various environments including some obstacles. This is expected to improve network performance. We will discuss this in more detail in Chapter 4

Chapter 3

Understanding Network-Centric Warfare (NCW)

Without distinction of field, information has played a key role as a means to improve current status or performance in each field throughout history. The 21st century is called the "Information Age" since its usage and importance in all fields, particularly military operations, has greatly increased. It is clear that that we must consider information as the most important means to survive in the competitive world and to assure victory in military combat. There are many limitations for military forces to combat effectively in the past when the communication and information systems were not developed sufficiently. All communications for information sharing or support were done by conventional methods such as express messenger or signal fire, etc. As a result, the geographically dispersed force was weak since it is almost impossible to respond to any operational changes immediately. In [15], the author states that "one purpose of network-centric warfare is to eliminate the geo-locational constraints by networking the forces using the most advanced technologies available." With the rapid development of information, communication and other associated technologies, these limitations are being reduced.

Today, we can easily see and experience many remarkable changes in our daily life due to technological innovations. Particularly, combat performed by U.S. forces in Iraq and Afghanistan demonstrated the changes in military operations and the trends in modern warfighting. It is time consuming work for a force to defeat an enemy using a poor network system providing only low level and delayed information. In this Chapter, we will figure out the importance of maintaining the individual network for real time information flow in modern military operation and combat.

3.1 What is NCW?

NCW is a new military theory of war pioneered by the U.S. DoD and is the term used by military personnel to define information-based warfighting. The Office of Force Transformation (OFT) was established in 2001 by the Office of Secretary of Defense to transform U.S. military capabilities. OFT describes that "NCW represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner"[64].

McKenna [99] addresses that network-centric warfare is a theory which proposes that the application of the "Information Age" concepts speed, communications and increased situational awareness through networking improves both the efficiency and effectiveness of military operations.

Alberts *et al*. (2000) describe that NCW is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, platforms, shooters and other military forces within a battle space. The increased combat power is obtained by shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and self synchronization [2].

In [66], authors describe the common picture of the combat situation enabled by NCW, which is available for all forces in a tactical network. This common picture can play the critical role of reducing uncertainty. In addition, military forces wherever they are, in air, ground and sea, once they are connected to the network can self-synchronize, or rapidly and effectively respond to combat situations.

The ultimate objective of NCW is to combine all forces in a network in order to obtain information superiority and increased combat power over enemy forces. This can be

accomplished by employing well developed information and related technologies. Most potential power comes from the proper combination of those available technologies. Walter (1997) describes three concurrent technical revolutions for the technological combination: information, sensor, and weapons technology [100]. The first, information technology, is the most basic one to multiply the military forces' power. Information can be produced using information technologies such as communication devices and various sensors to collect data from a battlefield. Under well developed and combined information technologies, information distribution to forces anywhere in the operation area is possible in real-time. The second technological revolution required for the network centric operations is in sensors. The technology of sensors pursues smaller, cheaper and numerous sensors for real-time surveillance over wide operation areas, so that much good quality data can be collected and provided. The third one is in weapons technology. The weapons revolution is a matter of increasing numbers of precise munitions by reducing costs. These technical revolutions will interact and multiply each other's impacts and maximize the effects that will change the character of war as we know it. These revolutions and changes in how we think about war have come to be embodied in the idea of network-centric operations.

Information was also used in traditional military operations in the past. The application level was comparatively lower than in modern military operations. In [95], the author addresses the difference between traditional military operations and network-centric operations. The traditional operation is performed by a set of steps: assign, plan, generate, and operation, whereas, network-centric operation is conducted based on the continuation concept. That is, between each step in a set of stepped cycle of traditional operations is a period of relative inaction for coordination. Thus, conventional operation cannot keep the continuation between steps. However,

the network-centric operation is not required to pause before deciding on further action thanks to the real-time situational awareness developed by networked forces in the tactical space.

NCW translates information advantages by a networking force in battle into combat power. It also enables more rapid, effective decision making and more precise power deployment at all levels of warfare and military operations. Consequently, new forms of organizational behavior may be expected under the NCW concept [59, 64].

The tactical environment of battlefields has been getting more complicated and requires fast reaction to environment changes. Under this circumstance, information superiority over an adversary can be achieved by NCW based on well developed information and communication technologies. Information through the network system can effectively be collected and distributed over large geographical areas in near real-time. As a result of effective use of information in military operations, the warfighting paradigm has shifted from mass and platform centricity to information and effective network-centricity. Platform-centric forces lack the ability to leverage the synergies created through a network, while network-centric forces are more adaptive and ready to respond to uncertainty in a very dynamic environment at all levels of warfare and across the range of military operations [15, 64]. In short, the collaboration among networked forces by enabling the free flow of information and quickly providing it to combat units in the battle space increases the forces' power in waging war.

NCW is also commonly called network-centric operations (NCO). However, we can specify the relation between them as NCW is the theory, while NCO is the theory put into action. In other words, NCO represents the implementation of NCW.

The goal of NCO is to maximize the effectiveness of an operation by effective use of power, which is called Effective Based Operation (EBO). The meaning of effective use of power

includes faster, fewer, and lighter weapons, fewer losses, higher accuracy, etc. Commanders can decide faster and provide optimal power in a timely manner and control the deployed forces better with accurate situational information. Consequently, they can go one step ahead of enemy forces and perform combat under more advantageous conditions [64].

EBO is a trend in military operations and is possible only by network-centric operation. In [94], Smith presents that effective-based operations are "sets of actions directed at shaping the behavior of friends, neutrals, and foes in peace, crisis, and war." OFT also describes that "EBO is a methodology for planning, executing, and assessing military operations designed to attain specific effects that achieve desired national security outcomes." As a result, network-centric operations are really about optimizing combat power for effective use [95]. The real payoff in network-centric operations is minimizing combat by causing the enemy to yield, or forestalling the foes by effective and accurate attacks on the enemy's critical targets. This efficiency revolves around the ability of network centric forces to perform precise EBO which focus on enemy behavior. Therefore, these operations are psychological rather than physical. That is why the enemy's decision-making process and ability to take action should be primary targets for attack.

U.S. forces experienced and proved the importance of effective-based operations based on information superiority through two recent combats, Operation Enduring Freedom (OEF) in Afghanistan and Operation Iraq Freedom (OIF) in Iraq, as mentioned before. U.S. armed forces were networked better based on the relatively advanced technologies than enemy forces in those conflicts. A well established network provided U.S. forces with shared awareness, supporting forces to be effective and protecting forces from external risks. It eventually enhances their lethality and survivability in those operations. That is, a commander of a well networked force

can quickly develop an operational picture, distributing critical information to his own forces, and use power to the maximum effectiveness [64].

The most important change with NCW is precision and real time data distribution through the network. Many advantages for forces operating on the basis of this concept were created. Therefore, military forces waging modern war should be able to adapt to new environments enabled by the network-centric warfare concept.

3.2 Tenets and governing principles for NCW

The Office of Force Transformation under the U.S. DoD presents four tenets for NCW [64]: Information sharing based on robust networking, Situational awareness, increased collaboration and self-synchronization, and Mission effectiveness. In addition to these four tenets, the following principles are also proposed in order to guide the application of NCW:

1) Fight first for information superiority: All combat starts from information warfare. Therefore, regardless of conflict or peace time, information superiority should be maintained over the enemy or potential adversary. By using all sources, our information capability should be maximized to reduce our own information needs. Conversely, increasing the enemy's information needs, reduce his ability to access information and raises his uncertainty.
2) Shared Awareness: All forces within a network should be able to obtain a common understanding and situational awareness. To do so, all information users are responsible for posting correct information without delay as suppliers.
3) Rapid decision, command, and effective operation: Make faster decisions and commands, and enhance the capabilities for effective operation on the basis of information superiority. Information superiority assured by shared awareness eliminates procedural boundaries

between services and within processes. It eventually enables the lowest organizational levels to be able to conduct joint operations and to achieve rapid and decisive effects.

4) Self-Synchronization: Adapt rapidly to changes in the battlefield without performing the slow functional steps from the traditional military operations. It eventually increases the operational tempo by improving the subordinate level of the commander's common understanding about the operational situation.
5) Dispersed forces and demassification: Move combat power from the linear battles pace to non-contiguous operations, and also move from mass centricity to information centricity for effectiveness. That is to say, modern combat is conducted simultaneously in many locations and maximize the effect with minimum power use.
6) Deep sensor reach: Detect high quality and valuable information on items or enemy forces of interest to achieve decisive effects.
7) Alter initial conditions at higher rates of change: Change operation conditions at a high rate by using information advantage. It confuses the enemy and forces it to redo all operation decisions and plans. As a result, the operation speed of enemy forces is delayed.

3.3 Domains of conflict in NCW

The office of Force Transformation developed a construct for NCW in which four domains are recognized, as follows:

1) Physical domain

   As a traditional domain of warfare, there are four different environments in the physical domain, which are the land, sea, air and space. That is, the physical platforms and

communication networks that connect military forces reside in one of the environments of physical domain.

2) Information

   Information collected, manipulated and shared by networked forces, the commander's intent and command and control of military forces belong to this domain.

3) Cognitive

   There are many abstract, invisible and intangible components in a military operation such as: leadership, training and experience level, fighting spirit, cohesion, and the commander's intent, doctrine, tactics, techniques and procedures. Although these are spiritual components, they directly affect combat. That is, the victory or defeat is decided by the cognitive level of a military force. The cognitive domain consists of the mind of warfighters.

4) Social

   The necessary human elements for NCW belong to this domain. In this social domain, humans interact to exchange information, get situational understanding, and make collaborative decisions. A commander's intent and will is conveyed to the subordinate forces.

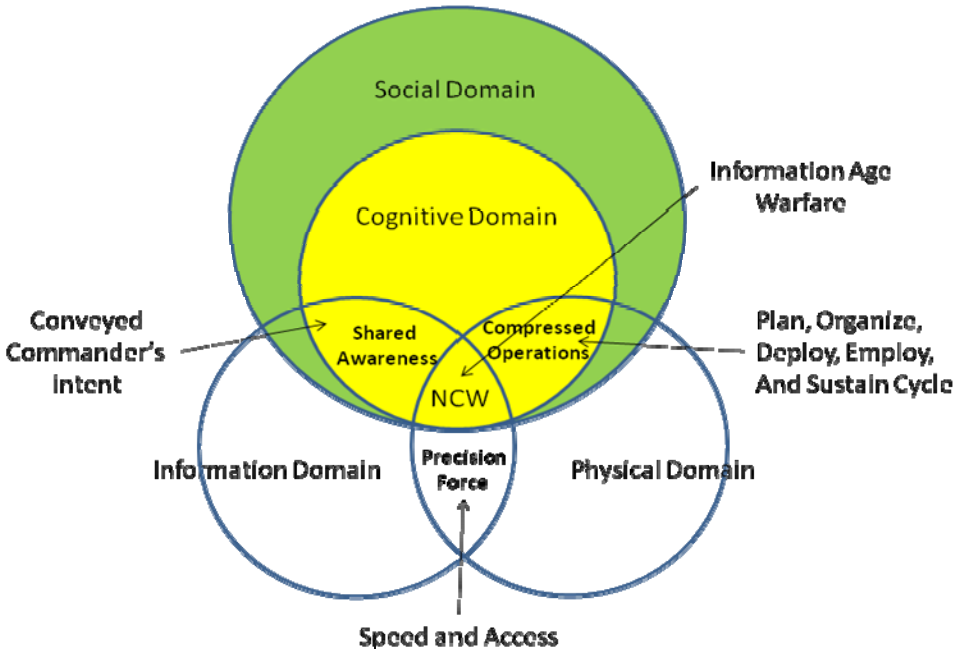


Figure 3-1 Domain of conflict [65]

The information and cognitive domains intersect to form shared awareness and the commander's intent is conveyed at this intersection. Speed and access at the intersection between the physical domain and the information domain enable a precision force which is very important to the conduct of successful joint operations. The intersection between the physical and the cognitive domain enables compressed operations. As shown in the figure all four domains intersect to form NCW at the very center.

In the past most innovations that created significant warfighting advantages were concentrated on the physical domain, and were translated into the tactical level of advantages. Even though those ideas were considered as platform-centric warfare, there were also many innovations focusing on information advantages. Today, with the development of communication and information technologies, the military warfighting paradigm is shifting from platform-centric

to network-centric warfare. The implementation of NCW brings about information advantages in military warfighting. The common tactical picture created by the combination of advanced technologies and networking reduces the uncertainty about the operational situation. As a result, successful employment of information under the new war paradigm increases combat power. We will discuss more about this in the next section.

3.4 Information warfare

The physical strength and skills of the players in a sports team decide the game. For example a quarterback's fast and precise passing skill in a football team and a boxer's agility and punch power may directly affect the result of the match. Similarly, the advanced weapon system of a military force which has long range and strong power is one of the most important components to assure victory in combat. However, this physical level of power strength cannot guarantee that they will always defeat their adversary. Actually, we have known some historical warfare in which powerful force is defeated by a weaker force. The primary reason of its defeat is that it neglected collecting information about its adversary and implementing it, on the other hand, the other force used information effectively to overcome its physical weakness.

Using information in warfare is not new. Sun Tzu [98] and Clausewitz [20] both were very emphatic about using it in warfare. Sun Tzu states that if you know your enemy and you know yourself, you will win a hundred battles. Also, Clausewitz describes warfare by using the term "fog and friction". Fog refers to the commander's lack of clear information and friction means physical difficulties to military action. That is, uncertainty and impediments to the effective use of military force due to unforeseeable incidents in combat tend to lower the level of performance. The traditional role of information in military combat was to identify the enemy's

location and power strength. That is, it was just knowledge at the level of intelligence. However, thanks to the development of information and communication technology, its role has changed. Information itself has become a target or weapon. The identification of the change has given rise to the term of information warfare.

Information warfare is not about technology but about using information. The purpose of using information in a conflict is to influence the adversary's decision making and operational capability, and public opinion, in order to achieve specific objectives.

During the conflict, each side tries to take actions to affect adversary information and information systems while protecting its own information and information systems. Today, many different types of attack on information systems are available. The most common attack, as an external attack, is to spread viruses through the enemy's network in order to deny his information processing. There exist many solutions such as firewalls, intrusion detection and prevention systems, anti-virus software, anti-spyware software, cryptographic protocols, and access control mechanisms to protect the information systems from these kinds of attacks. However, internal attacks by compromised users are always difficult to handle because they bypass traditional security solutions. The Libicki model that is referred to most commonly presents seven information types of warfare: Command and control warfare (C2W), Intelligence based warfare, Electronic warfare, Psychological warfare, Hacker warfare, Economic information warfare, and Cyber warfare [57].

3.5 Decision making and security in NCW environment

Schechtmann (2002) analyzed information warfare according to the OODA loop. U.S. Air Force Colonel John Boyd developed the OODA loop based on his previous work on a fast-transient brief which suggests keeping a faster operation tempo than the enemy to assure a

victory from conflict. OODA is an abbreviation of Observe, Orient, Decide, and Act. The brief description of each component is as follows [89]:

1) Observation: It is the behavior of becoming aware of the operational situation and environment by careful and directed attention.
2) Orientation: It is the process of converting the collected raw data to valuable information supporting the forces by using analysis and synthesis. The human brain forms a mental image of the environment.
3) Decision: The information from the orientation phase is analyzed and various options of action are formed. The options are considered to the extent allowed by time, and a choice is made.
4) Act: The decision is implemented. It leads to unfolding interaction within the environment.

The OODA is a model to address human decision making. As the first step of the OODA loop, the operational environment is scanned for data. This is possible by robust networking of forces in the area. All forces within the network share what they know at the current time and location. This collected data, or intelligence, is processed further for creating information and a mental image of the situation. Then, a decision is made among alternatives identified through the orientation, and it is carried out.

In short, it is possible to perform compressed operations by OODA. The force can cause the enemy, to be confused and disoriented by changing the environment rapidly. This confusion and disorientation causes the enemy to pause frequently for reprocessing. Consequently, the enemy is more delayed in making accurate decisions and is eventually defeated.

Each party in a conflict tries to confuse the opposite party as much as it can by using all possible means. Fog and friction increased by frequent environment change affects the operation tempo of the enemy. One of the most practical ways is to destroy the enemy's communication and information system so that its network cannot function properly any more. At the same time, our decision making process should be protected from this kind of attack.

Needless to say, the decision making process is very important, so it always becomes a primary target of the enemy. To secure the decision process and its accuracy, it is crucial that the network is not vulnerable to friction and fog by the enemy. For example, data collection in the observation phase can be obstructed by offensive actions such as physical attack or deceptive actions. And the input from observation will have direct effects on the orientation phase and the decision phase. Especially, action could be impaired by disrupting communications using various negative actions such as jamming the network, delaying and modifying packets, and injecting erroneous packets into the network. These security problems have been an issue in both commercial and military networks since the internet was commercialized for network communications [89].

Network security is divided into three categories: Content, Communication, and Network security. Content security is to protect the content between the two communicating peers, and communication security is about protecting the data between each source and destination over the network. The difference between content and communication security is that the end user in communication security can be more than two users while there is only one in content security. Network security is to protect the network itself so that it can perform properly. The main purpose of the network is to function as a tool for command, control, and communication.

Therefore, the network must be secured to protect the decision making process from enemy attacks in a network-centric environment.

In the past, military technologies in most fields have led commercial ones. However, this has been reversed and no barrier between the two fields exists. Many IT equipment and weapon systems for military use are also used in civilian organizations. Due to this fact, military networks are vulnerable to attack since they use open standards and commercially off the shelf (COTS) products. Furthermore, the distinctive characteristics of military operation environments such as terrain, weather condition, wireless, and enemy forces increase the burden of security.

Failure in securing the network from various negative activities by the enemy can lead to defeat in warfighting. The enemy can easily access the network when security measures fail. As a result, the decision making process, information sharing and situational awareness are more vulnerable.

Future military systems under the new paradigm of NCW will be based on a network of heterogeneous networks wired and wireless access networks, sensor networks, ad-hoc networks, and fixed and temporary backbone networks. Among these, military networks have a close connection with wireless networks. We will discuss wireless networks in the following section.

3.6 Wireless networks

Today, military and commercial networks are increasingly mobile and wireless. Furthermore, in the military operation, ad-hoc networks are relied on to ensure communication in difficult environments such as a battlefield. Both the military and civilian environments depend on the same technology. However, many military requirements are different due to its nature. Wireless networks introduced by innovated communication and information technology have

changed our living pattern and method of waging. Now military forces can operate in a distributed manner while maintaining communication. The shared awareness system based on the wireless networking brings many remarkable benefits to forces operating under a high level of uncertain battle situations. Candolin [15] defines wireless networks in five categories based on the communication coverage. The wireless network spectrum is specified as seen in Figure 3-2 below.

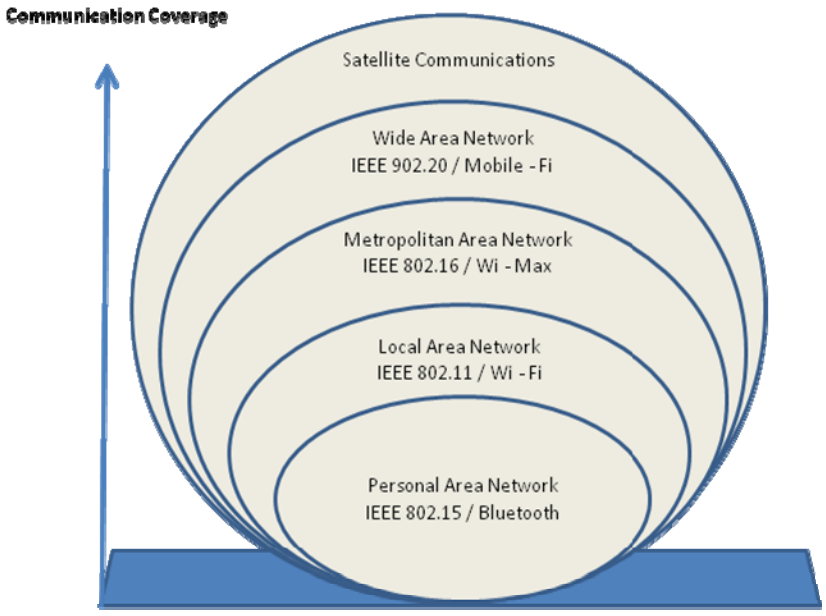


Figure 3-2 Wireless networks and their coverage [15].

Satellite communication at the highest level is considered as the most important communication network in modern warfare. The dream of getting connected "anywhere and at any time" is able to come true by the full implementation of satellite communication. Especially, the direct connection between satellites and networks can maximize the flexibility of military operations by information flow in real time. Among those in the lower levels of networks,

Wireless LAN is useful for a small military force operation and practical for fighting with terrorists currently.

Wireless LAN is a network linking two or more computers without cables in a limited local area such as a company or home. WLAN gives users the mobility to move around within a broad coverage area when connecting to the network. The transmission range of WLAN is about 100m, and the rate is specified between 1 Mbps and 108Mbps. WLAN is defined in the IEEE 802.11 standard and specified into infrastructure and ad-hoc modes. Network nodes in the infrastructure mode are connected to a wireless access point which typically is connected to a wired network, while in the ad-hoc mode they communicate in a peer-to-peer fashion.

Wi-Fi, which stands for Wireless Fidelity, is a WLAN technology defined in the IEEE 802.11 standards and promoted by the Wi-Fi forum, an online community dedicating to the exchange of technical or non-technical ideas related to Wi-Fi. One of the benefits of Wi-Fi is that it is able to provide high speed internet access with low requirements for transmission power. Thus, it is a feasible technology even for small, battery driven devices. It also adds flexibility to local area networking, as it supports user mobility. Wi-Fi is the most cost-efficient wireless technology today [15, 106]. The disadvantage is the lack of support for QoS, and the lack of privacy protection for users.

Satellites are important communication assets for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, missile warning capability, etc. A communication satellite is stationed in space for the purposes of telecommunications. Modern communications satellites use a variety of orbits including geostationary orbits, Molniya orbits, other elliptical orbits and low (polar and non-polar) earth orbits. As we know, the coverage by satellite communication is huge and even the

whole earth can be covered. At first satellite communications could not be available to all users because of high usage fees and the limitation of two-way high-speed communication requiring only short time delay, but the decrease in cost and developed technology has made it possible even for individuals to take advantage of satellite communications. Therefore, it is no longer limited to governments, military, and large corporations. INMASAT is one of examples which have been used for military operations and provides communications over geostationary satellites.

The U.S. Armed forces have used 28 satellites for global positioning support and six orbital constellations for Intelligence, Surveillance, and Reconnaissance (ISR): one for early warning, two for imagery, and three for signals intelligence [102]. Despite the growing number of military satellites, 84 percent of satellite communications bandwidth in the Operation Iraqi Freedom (OIF) Theater was provided by commercial satellites. Communication services by commercial satellites may face problems related to interoperability and security. The U.S. DoD has made efforts to build a satellite-based military internet in the future to reduce or remove currently identified network problems. As a part of this plan, the Transformational Satellite Communications (TSAT) program is being run by the Air Force. With this program, five geosynchronous orbit satellites will be launched and provide warfighters worldwide with high-speed, high-capacity communications [21, 42, 102].

3.7 Tactical battlefield network

Speed and precision are vital factors in the modern warfighting paradigm as discussed previously. A scout from a remote place, which is very close to an enemy's camp, is observing the camp and flies a small unmanned aerial vehicle (UAV) to collect more detailed information.

The small UAV flies in the sky over the enemy's camp and scans targets of interest without being detected by the enemy. This data from the critical area is directly sent to a control center in real time, through satellite communications, where a decision maker and his staff are located. They analyze the data to get exact information on the target and discuss what to do. They are looking for the leader of a terrorist organization at the moment. At last, they find the target, terrorist leader, and decide to kill him. The mission is assigned to a responsible force in that area. A predator UAV charged with a precision guided missile takes off and launches a missile to the target area.

This is a scene from a recent movie. This simply summarizes the important characteristics of modern combat. As we identified from the movie scene, the place where the scout was operating is a deep location close to the enemy camp but far away from his camp. Naturally, no predefined infrastructures are available there. Only satellite communications or another wireless network can connect the scout with the control center. This is an ad-hoc network which is a collection of nodes that do not need to rely on a predefined infrastructure to establish and maintain communications [14]. Therefore, the coverage of an ad-hoc network depends on the locations of the network participants. An ad-hoc network is also referred to as a tactical battlefield network in the military. Although nodes in the ad-hoc network may be connected to a wired infrastructure, ad-hoc network nodes are most likely wireless.

Military forces in many different operations have experienced the fact that networking is always constrained by time. That is, the speed of establishing a network in a tactical space cannot catch up with the operational movement of forces in the area. Military forces have already moved ahead when network infrastructures are ready for use. This had motivated the military to innovate the networking technology for their forces so they can be networked robustly where and

when needed. The DARPA Packet Radio Networks and the Survivable Adaptive Networks (SURAN) programs sponsored by the U.S. government in 1970s and 1980s were the predecessors of today's mobile ad-hoc networks.

The forces of a network and given mission usually determine the required network technology and size. Members of a tactical battlefield network are diverse in the capability of moving speed and transmission range. Human soldiers, trucks, air fighters, and battle ships as network nodes have different capabilities. This heterogeneousness is a trend in military mobile ad-hoc network.

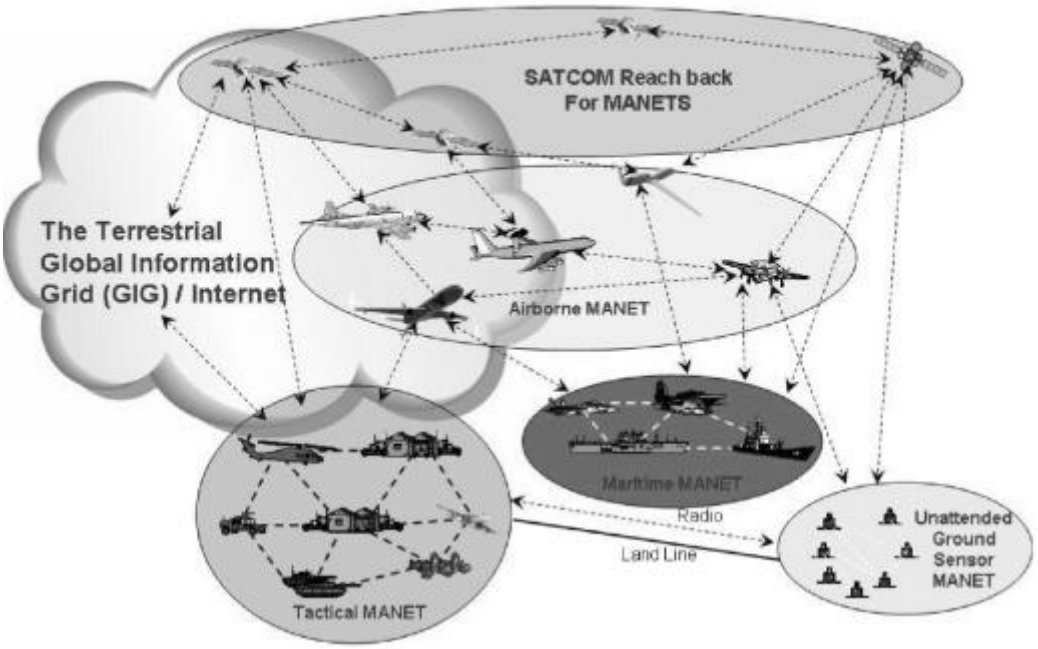


Figure 3-3 MANET interoperability [82]

In summary, there exist networks of various size and technology in military battle fields. The real-time free flow of information vertically and horizontally among networked forces in a theater are the first priority to assure victory in waging modern war. NCW focuses on the combat

power that can be generated from the effective networking of the combat forces. Shared awareness and collaboration in a battlefield, which are given by robust communications and rapid exchange of data via one or more networks, provide the forces in battle with potential power. Well networked forces show the NCW characteristics of speed of command, high tempo and responsiveness, massing of effects, cooperative engagement, and self-synchronization to a degree that cannot be matched by any non-NCW capable opponent.

All of the individual warfighting entities such as satellite, aircrafts, UAVs, ships and unattended sensors, and all tactical warfighting nodes in Figure 3-3 must be integrated into the grid to achieve the goals of NCW. So, all forces and networks are able to maintain the connectivity with each other and minimize the uncertainty. Consequently, this NCW-compliant integration can provide a common picture of the battlefield to all network nodes, even to the tactical edge nodes. Interconnecting these edge nodes will rely upon mobile ad-hoc networking (MANET) technologies [69]. Achieving this tactical edge connectivity will depend on the development of significantly improved MANET technologies.

The tactical battle field is the basic level in an entire network. A top command network is made up of several tactical battlefield networks. Therefore, as a basic network, each tactical battlefield network is required to maintain robust communication with other networks under varied military operation environments.

Chapter 4

Military MANET Description and mathematical model

There are many different types of obstacles in military combat and operation areas which limit network performance naturally or artificially. Unlike obstacles due to natural causes such as weather conditions or terrain shape some obstacles are intentionally produced by enemy forces. We call those kinds of obstacles “Enemy” in this research.

A military MANET model representing military operation scenarios including enemies’ hostile activities in the operation area is developed in this chapter. The optimizer under combat conditions should be able to effectively deploy the agent nodes to the best locations so that network performance can be maximized every time step. Two decision variables are the agent’s direction and velocity. The network performance is evaluated at each time step during the operation. The network objective function can be evaluated when the node coordinates of agents are known.

4.1 Proposed military MANET operation system

The mobile agents play key roles in maintaining network connectivity in a network, particularly when the client nodes are positioned beyond their communication range with the control node. The network performance in this research is mainly evaluated by the number of connected user nodes to the control node and the network bandwidth among connected users at each time step. Therefore, the proper positioning of the mobile agents to maximize those

performance parameters is crucial in the optimizing process of military MANETs, since it determines the links among nodes in a network.

The basic operation method for deploying agents is to control their directions and magnitudes of velocities. This is possible when the location information of the MANET nodes is given. A global positioning system (GPS), which is implemented by many mobile phones or mobile network devices, provides all network nodes with valuable location information. The mobile network nodes change their locations to perform the given mission in the tactical theater over time. However, we assume that paths of users are not known in advance. The military MANET should be able to respond to these changes of location of the network nodes. That is, the required system should be able to use the location information from previous environments and continuously adapt to the change of network environment conditions as well. This is a non-linear problem which requires a heuristic algorithm with a continuously changing objective function. As a result, the PSO algorithm, which is a population based heuristic with a time varying fitness function, is applied to solve the military operation problem.

We assume that the location information is always available if the network nodes are connected with the control node since a GPS can be mounted on the network nodes. And this could technically be possible by broadcasting the location information provided by the GPS. Also an ESM sensor to detect the direction of jamming coming from an unknown location of enemy is available for each network node.

As we addressed before, four different types of nodes are used in the study to represent real military operation scenarios, which are different from commercial ones. Especially, the control and agent nodes are considered as service nodes which should be controlled by the

MANET control system throughout the operation period to maintain network connectivity. These MANET nodes are discussed in the following section.

4.2 Military MANET nodes

For military MANETs, we functionally divide military operation units into three groups: command/control, execution, and support. The command/control unit, which is represented by a control node, manages all of its assigned subordinate units. Before performing the command/control function, it is important to collect data by using available information acquisition assets, analyze the data within a given time frame, and distribute information through a network for proper and quick decision making. Consequently, effective command/control would be possible over subordinate units only through a robust networking of forces in the network.

Execution units, which are represented by user nodes, perform the commands received from the control center or the higher unit in the command/control hierarchy. They also report operation situations at their current locations to the control center to support drawing a common picture of the tactical space, which will be provided for all networked forces. Of course, the execution units could exchange valuable information with each other over the network, but the decision making of important actions directly related to a given mission is performed through communication with the control center.

Finally, support or service units, which are represented by agent nodes, seek to provide all units in an operation network with a tight communication relay service for enabling military operation functions such as command/control, information acquisition and exchange, and execution required for mission accomplishment.

The nodes representing network devices in the mobile ad-hoc network are generally divided into user (client) and agent (server) nodes in the literature reference. But considering the nature of military operation discussed above, those nodes need to be further specified to represent realistic scenarios. So, we have extended the general classification with four different types of node: control, agent, user and priority node. The classification and brief descriptions of each category are given as follows:

1) Agent node

   The support unit described above is represented by an agent node. The agent node is responsible for connecting network nodes positioned beyond their communication ranges in a network to maintain the network at the best condition possible. For this purpose, agent nodes are repositioned based on the information about the location of the network nodes and the communication capabilities using the distances between nodes.

2) Control node

   The command/control center is represented by the control node. The command/control center in military operations plays a key role of controlling agents in the network to perform a given mission. Particularly, the control node in this research performs two additional tasks. It is responsible for supporting user nodes like other agent nodes and it designates any user node required for a tighter connection with the control node as a priority node, which has priority for network service.

Unlike traditional MANET models, user nodes are divided into two types, user and priority in this military MANET. The user and priority nodes represent a variety of combat or forward military units from individual soldier to battalion military unit level or greater. These

user nodes are free to move according to their mobility characteristics within a tactical theater.

3) User node

   User nodes represent an individual soldier or a military combat unit at a variety of organizational levels. The user nodes require network service while moving around the tactical space.

4) Priority node

Because of the dynamic and unpredictable nature of military operations, it is impossible to guarantee full connectivity among nodes all of the time. So, this unavoidable limitation forces the operation planner or manager (military commander) to classify users into priority based on the tactical situation. Any user node which is considered as an important node related to the tactical situation can be designated as a priority node by the control center. Priority nodes should have preference over user nodes to be connected to the control node since MANET has a limited number of agent nodes.

4.3 Network states

The connections between network nodes are decided by their signal strengths and the network connection for a network node in this research means that the network node is able to communicate with the control. Therefore, any network node which is disconnected from the control node is referred to as an isolated node. However, in order to represent effectively the network states corresponding to an environment change, more distinctive definitions for possible cases are required. First, the exact definitions regarding isolation are as follows:

- Isolated user: Disconnected with the control and all agents
- Isolated agent: Disconnected with the control and all users

- Isolated user-agent cluster: One or more agents and/or one or more users connected together, but disconnected from the control node

Based on these definitions of isolated nodes, two network states, State 1 and 2, are defined in this research. If there is no isolated user in the network, the network is State 1. Otherwise, it is categorized into State 2.

There are two different ways to evaluate the network performance in this research, and these depend on the network state. According to the network state, the objective function required for the fitness evaluation is decided. That is, objective function 1 in equation (4-7) is used to evaluate the network under the network state 1 and the objective function 2 is used in equation (4-8) under the state 2. We will discuss more about the objective functions in Section 4.4.

4.4 Military MANET optimizer

The movements of the mobile agents are under the control of the location optimizer that is responsible for maximizing the performance objectives as a function of the current coordinates of the nodes and enemy's hostile activities in a MANET operation space. The objective function gauges the network performance based on predefined parameters such as number of connected user nodes, number of connected agent nodes and network bandwidth. These performance parameters can be computed using detailed performance measures such as hop-count or bandwidth.

The network performance measures typically show flat behavior over large portions of the search space. However, the measures may also show sudden changes in certain regions of the search space depending on the network states. In order to overcome this issue, the objective

function on which network performance is evaluated, should be able to respond to any small changes in the network environment. In this research, this is accomplished by using a hop-count based algorithm with additional performance metrics which can help improve network performance.

4.4.1 Performance metrics

As we discussed above, the objective function for the evaluation of a network should be made up of proper performance metrics which represent the network characteristics and respond well to the network changes. In order to do that, some different parameters are employed to evaluate the military MANETs in this research and also two different objective functions are used for evaluating the networks under different network conditions. The evaluation of network performance is conducted by sequential filtering based on the metrics, which are divided into two categories, primary and secondary.

The primary metrics category evaluates the networked level (NWL) of a network. NWL includes four metrics, the Number of Connected Users (NCU), the Number of Connected Agents (NCA), the Pre-deployed Agent Level (PAL), and the Number of Agent-User Links (NAUL). These primary metrics are common in both objective functions.

On the other hand, the network evaluation by secondary metrics is divided into two and depends on the network states mentioned previously. There are two different network states as discussed before previously, State 1 and State 2, in this study. The network state at every step is decided by whether there is any isolated user node in the network. If any user node is isolated, it is State 2, otherwise, State 1. Under the desired network state (State 1) the network is evaluated for network quality (NQ) using bandwidth (BW) and control centered (CC) metrics, while the

network evaluation for State 2 is performed by the Search Range (SR). The definitions of these metrics used here are given as follows:

1) NWL: Networked Level which is computed by sum of NCU, NCA, PAL, and NAUL. The priority among these metrics is represented by the assigned weight to each metric. The highest weighted parameter is NCU, the lowest one is NAUL. NCU is used as a primary performance measure in this study due to its importance in the military. PAL is also an important parameter, but it is weighted by a relatively smaller number than NCU and NCA since it is just to maximize network connection. As a result, the optimizer can maximize network performance using these weighted differentiated metrics.
2) NCU: Number of Connected Users. The number of connected user nodes which maintain connection with the control node at the moment. NCU includes both connected user nodes and connected priority nodes (NCP).
3) NCA: Number of Connected Agents. The number of connected agent nodes which maintain connection with the control node at the moment.
4) PAL: Pre-deployed Agent Level. PAL is the indication of the agent nodes' performance. Under PAL, each agent is required to support at least two user nodes and the user nodes being supported by that agent are different from those being supported by other agents. Similarly, a user node is required to have at least one agent support and the agent node supporting a user node should be different from those supporting other user nodes. PAL enables the agents to be distributed through the network to support more user nodes over time. Each network node meeting above

conditions represents one unit of PAL. The mathematical formula of PAL is given in Section 4.5.

5) NAUL: Number of Agent-User Links. NAUL is a direct link between agent and user. This parameter is used for maintaining a high quality connection within a cluster which might be isolated from the main network.
6) BW: Total bandwidth of a network. Bandwidth represents the signal strength between a network node and the control node. It is computed based on the distance between the two nodes. We will discuss this in more detail in the next section.
7) CC: Control Centered. The sum of the distances between the agents and the control node. By this metric all agents can be controlled to stay close to the control node as much as possible under a given network condition. The purpose of this metric is to respond quickly to network needs. For example, an extra agent is needed to be deployed to other location to improve network connections when the user has been supported by the agent is killed or disconnected for long time. Under this kind of situation, CC metric help deploy the agent to any proper location.
8) SR: Search Range. The distance between a messenger and the estimated destination of an isolated user. The messenger is an agent that is designated for isolated user node search by the control node. We will discuss this later in this chapter.

The optimizer continues to evaluate the network based on the above performance metrics and optimize the location of agent nodes to keep maximizing the network connection during the operation. In the following section, we will discuss a hop-count based algorithm and how to compute the network bandwidth. Bandwidth is used to check the connectivity and quality of the path between two nodes in a network.

4.4.2 Hop-count based algorithm

Finding the shortest path from a source to a destination in a network is a common problem and there are many ways to do it. Here, the meaning of “shortest path" may be the least number of hops (links or arcs) or the least total weight [58, 96]. In [68] the shortest path problem is simply defined as the problem of finding a path between two nodes such that the sum of the weights of its constituent edges is minimized.

For finding the shortest path between two designated nodes in a network, the minimum hop-count is used in this research. The hop-count approach considers only the minimum number of hops, or links, required to establish a path between two nodes regardless of the link quality or stability or distance. As described before, it can minimize the waste of limited resources in the longer term. However, it may select an inferior route when there are more than two paths available, since it considers only the minimum hop. In order to improve this measure we introduce other metrics representing network quality and stability as subsidiary ones. The shortest path is evaluated by the primary metric, hop-count. If there are two or more shortest paths which have same number of hops, the tie among the paths is broken using the second metric based on the bandwidth. Each link’s bandwidth for fitness evaluation is different from the one measured by the distance alone. In order to measure the level of the quality and stability of a link, the jamming Effect Level is also used. The description of these metrics will be given in the following section.

Bandwidth (not including Jamming Effect Level) is the most common metric to measure the network performance and is measured as a bit rate expressed in bits/s or multiples of it (kb/s, Mb/s etc.). We use bandwidth to measure the quality of a path. Connections among nodes in a network depend on the transmission ranges based on each other’s signal strength. That is to say,

the transmission range of a link between two nodes is decided by the one having the smaller transmission strength.

The basic goal of the links in a network is to deliver sufficient signal strength from a source node to a destination node to achieve some performance requirements. However, signal strength could be varied by environmental conditions. The estimation of the signal power under a great variety of existing conditions is not easy work and it may be impossible to predict exactly. Also, this is beyond our research scope. Therefore, we assume that the estimation of the path loss in this research follows the propagation model for free space scenario. However, this propagation model could be replaced by another propagation model corresponding to the application.

To represent the tactical battlefield network in the lower level of military mobile network, the wireless local area network is considered in this research. The wireless IEEE 802.11 is a set of standards for wireless local area network computer communication. It is technically possible to create a multi-hop network that covers several square kilometers and operates in the 5GHz and 2.4GHz radio band [26]. The free space path loss equations are given in two ways as seen in following equations depending on the distance measure unit, km or mile.

$$L_p = 32.4 + 20\log f + 20\log d_{ij} \quad (f \text{ in MHz}, d_{ij} \text{ in km}) \tag{4–1}$$

or $$L_p = 36.6 + 20\log f + 20\log d_{ij} \quad (f \text{ in MHz}, d_{ij} \text{ in miles}) \tag{4–2}$$

Where L_p is the path loss in decibels (dB), d_{ij} represents the distance between two nodes and f is the signal frequency.

For the path loss model, Dengiz (2007) applies equation (4-1) to an industry company's product specification sheet to compute the data transfer rate versus distance [26]. The relationship between path loss and data rate is shown in Table 4-1.

Table 4-1 Path loss vs. data rate

Data rate (Mbps)	Receive Sensitivity (dBm)
54	-75
48	-76
36	-80
24	-84
18	-88
12	-90
9	-90
6	-93
2	-93

For a normalized wireless transmission range, he uses equation (4-3) to estimate the normalized data rate from the Euclidean distance (d_{ij}) between two nodes, i and j. To calculate the normalized bandwidth of each link the following equation is used in this research as well.

$$DataRate(i,j) = \left(1 + e^{10\cdot(d_{ij}-0.5)}\right)^{-1} \tag{4–3}$$

So, once we get the Euclidean distance between nodes, the available data rate can be easily computed using equation (4-3).

There is another factor affecting network bandwidth in military MANET scenarios, and this is an electrical attack (jamming) by enemy forces existing in the operation area. The communication capability of the network nodes are constrained by this jamming effect. In addition, nodes which are located near jammers could be attacked and killed by their attack. This

is referred to as the Kill Effect Zone (KEZ). We will discuss enemy effects in more detail in Section 5.4.1.

4.5 Mathematical formulation

In order to construct the network graph $G = (N, E)$ at each step, the Euclidean distances among network nodes are measured.

$$d_{ijt} = \sqrt{(x_{it} - x_{jt})^2 + (y_{it} - y_{jt})^2} \tag{4–4}$$

If the Euclidean distance between two nodes in a free space environment is less than the minimum possible communication range of those, the nodes are connected to each other as shown in the following equation.

$$e_{ijt} = \begin{cases} 1 & if\ min(TR_{it}, TR_{jt}) \geq d_{ijt} \\ 0 & otherwise \end{cases} \tag{4–5}$$

In the real world, the transmission capabilities of network nodes can be limited by environmental conditions as discussed. Although there are many possible factors causing this limitation such as terrain shape, weather condition, and electrical attacks by enemy forces. All of these are not studied in this research. We consider only the jamming effect by enemy forces. The possible bandwidth for a link is computed based on the Euclidean distance and jamming effective level. And then if the possible bandwidth for the link is larger than the minimum bandwidth required under current environmental condition, they can be connected with each

other. However, the minimum bandwidth is assumed as one distance unit here since we do not consider reduction of bandwidth by environmental conditions in this research.

Notation

r_{it}	Rotation angle from x-axis of the i^{th} agent node at time t
v_{it}	Speed of the i^{th} agent node at time t
v_{max}	Maximum speed of the agent node
(x_{it}, y_{it})	x and y coordinates of the i^{th} agent node at time t
(X_{min}, X_{max})	x-axis boundaries
(Y_{min}, Y_{max})	y-axis boundaries
M	Weight for the swarm having at least one of its particles within the kill effect range. If all particles are out of the kill effect range, M is 0
NN	User and agent node set
AN	Agent node set
UN	User node set
CN	Control node
IU_t	Isolated user node set at time t
PN_t	Priority node set at time t
MA_t	Messenger agent set at time t
TN_t	Total number of alive user or agent nodes at time t
TU_t	Total number of alive user nodes at time t
TA_t	Total number of alive agent nodes at time t
TP_t	Total number of priority nodes at time t

d_{ijt}	Euclidean distance between node *i* and *j* at time *t*
TR_{it}	Transmission range of node *i* at time *t*
Pn	Weight for priority node
e_{ijt}	e_{ijt} is 1 if there is a link (single hop) between node *i* and *j* at time *t*, otherwise is 0
$P_t(i, j)$	$P_t(i, j)$ is 1 if there is a path between nodes *i* and *j* at time *t*, otherwise is 0
SU_{it}	The set of user nodes supported by agent node *i* at time *t*
SA_{it}	The set of agent nodes supporting user node *i* at time *t*
BW_{ijt}	Bandwidth of a link between node *i* and *j* at time *t*, $i \neq j$
JL_{ijt}	Jamming effect Level for the link between node *i* and *j* at time *t*, $i \neq j$
$ShortestPathBW_t(i,j)$	Shortest path bandwidth between node *i* and *j* at time *t*
$PathBW_t^k(i, j)$	k^{th} path bandwidth between node *i* and *j* at time *t*
$N_t^k(i, j)$	A set of nodes on the k^{th} path between nodes *i* and *j* at time *t*

The purpose of the optimizer is to deploy the agents into the best locations in order to provide MANETs with maximum communication quality. To meet this goal, different metrics representing military MANET characteristics are employed to evaluate network performance; these are hop-count, bandwidth, and jamming effect level.

For instance, let's say we want to find a path between nodes *i* and *j*. First, the link matrix is constructed based on the location information. Two different matrices are required to compute the cost for a link or path in the network, which are one hop-count matrix and bandwidth matrix.

The hop-count matrix is used to search for the shortest hop path, while the bandwidth matrix is used to find the highest quality or cheapest cost path among the shortest paths which have the same number of hops. The link between two nodes is represented by the binary value (1

or -1) in the hop-count matrix. On the other hand, the cost of each link in the bandwidth matrix is represented by the computed bandwidth based on Euclidean distance and jamming effect level. As a result, each cost in the bandwidth matrix is real number representing the possible bandwidth of the link for fitness evaluation.

The hop-count based algorithm first finds the possible paths between nodes *i* and *j* using minimum hop-count. The path which has the smallest number of hops is selected as the shortest path. If there is only one path, it will be the best route without requiring further consideration. However, in many cases, there exist two or more shortest paths which have same number of hops. So, the tie among the possible paths should be broken by the bandwidth of each path. That is, the path with the fewest hops and which has the largest bandwidth is selected as the best path.

Each link's bandwidth is calculated by equation (4-3). Euclidean distance between the nodes is first measured. Then, for the actual possible bandwidth calculation for fitness evaluation, jamming effective level, which is changed over time, is added to the computation. A path between any two end nodes could be composed of several different links. Among those, the link which has the smallest bandwidth is chosen for the path's possible bandwidth. Finally, the path that has the smallest hop count and the largest actual bandwidth will be the best route for the connection between two end nodes, source and destination.

Network performance depends on the location of the agent nodes, so the optimizer continually relocates the agent nodes to the locations which best improve the network performance. Consequently, the agent nodes' coordinates are decided by the direction and velocity randomly generated by PSO. So, these direction and velocity of agent are decision variables. Particularly, in the measurement of network performance, a priority node path is

weighted by a positive value (*Pn*) to represent its priority to the military operation, as described earlier.

As we discussed, several network parameters are used to evaluate network performance and these parameters need to be differentiated by their importance in a network. So, different weights are introduced to represent these priorities for network connection as seen in equation 4-6. Network parameters are NCU, NCA, PAL and NAUL in order of importance and weighted by λ_1, λ_2, λ_3 and λ_4, respectively. Also, while optimizing a network if any particle in a swarm enters the kill effect range of an enemy, network performance at that moment will be penalized a big positive number (*M*). As a result, agent nodes would not be deployed into the kill effect range. The mathematical model based on the above concept is given as follow:

$$O1: max\left\{\left(NCU\cdot\lambda_1+NCA\cdot\lambda_2+PAL\cdot\lambda_3+NAUL\cdot\lambda_4\right)-M\right\} \tag{4–6}$$

$$O2-S1: max\left(\frac{BW}{CC}\right) \text{ (if } IU_t=\phi) \tag{4–7}$$

$$O2-S2: min\left(SR\right) \quad \text{(if } IU_t\neq\phi) \tag{4–8}$$

$$NCU=\sum_{i\in UN}P_t(i,CN)+\sum_{i\in PN_t}P_t(i,CN)\cdot Pn$$

$$NCA=\sum_{i\in AN}P_t(i,CN) \tag{4-9}$$

$$PAL=\left(\sum_{i=1}^{TU_t}uPAL_i+\sum_{i=1}^{TA_t}aPAL_i\right) \tag{4-10}$$

$$NAUL=\sum_{i\in UN,\,j\notin UN}e_{ijt} \tag{4-11}$$

$$BW=\sum_{i\in NN}ShortestPathBW_t(i,CN) \tag{4-12}$$

$$ShortestPathBW_t(i,CN) = \max_k \left\{ PathBW_t^k(i,CN) \right\}$$

$$PathBW_t^k(i,CN) = \min_{m,n \in N_t^k(i,CN)} \left\{ BW_{mnt} \cdot JL_{mnt} \right\}$$

$$CC = \sum_{i \in AN,\, j=CN} d_{ijt} \tag{4-13}$$

$$SR = \sum_{i \in IU_t,\, j \in MA_t} d_{ijt} \tag{4-14}$$

Subject to

$$\begin{aligned} &0 \le v_{it} \le v_{max} \quad \forall_i \in AN \\ &0 \le r_{it} \le 2\pi \quad \forall_i \in AN \end{aligned} \tag{4-15}$$

$$\begin{aligned} x_{i(t+1)} &= \begin{cases} X_{min}, & \text{if} \quad x_{it} + cos(r_{it}) \cdot v_{it} < X_{min}, \quad \forall_i \in AN \\ X_{max}, & \text{if} \quad x_{it} + cos(r_{it}) \cdot v_{it} > X_{max}, \quad \forall_i \in AN \\ x_{it} + cos(r_{it}) \cdot v_{it}, & \text{otherwise} \qquad\qquad\quad \forall_i \in AN \end{cases} \\ y_{i(t+1)} &= \begin{cases} Y_{min}, & \text{if} \quad y_{it} + sin(r_{it}) \cdot v_{it} < Y_{min}, \quad \forall_i \in AN \\ Y_{max}, & \text{if} \quad y_{it} + sin(r_{it}) \cdot v_{it} > Y_{max}, \quad \forall_i \in AN \\ y_{it} + sin(r_{it}) \cdot v_{it}, & \text{otherwise} \qquad\qquad\quad \forall_i \in AN \end{cases} \end{aligned} \tag{4-16}$$

$$\begin{aligned} aPAL_i &= \begin{cases} 0 & \text{if } SU_{it} \text{ is identical to } SU_{jt} \text{ for any agent node}, i \ne j \\ 1 & \text{otherwise} \end{cases} \\ uPAL_i &= \begin{cases} 0 & \text{if } SA_{it} \text{ is identical to } SA_{jt} \text{ for any user node}, i \ne j \\ 1 & \text{otherwise} \end{cases} \end{aligned} \tag{4-17}$$

The performance evaluation of a network is conducted by two different objective function sets based on the network states, as discussed before. The objective function set 1

consists of O1 and O2-S1 and set 2 is made up of O1 and O2-S2. The objective function set for the evaluation is determined by the network state at the moment. That is, network performance is evaluated by set 1 if no isolated user node is in the network. Otherwise, it is evaluated by set 2.

The sequential filtering method is used for the network evaluation in this study. First, network is evaluated by O1 and is compared with the previous fitness evaluation. If it is improved by O1, then O2-S1 or O2-S2 does not matter. However, if the current fitness evaluation by O1 is the same as previous one, the tie should be broken by O2-S1 or O2-S2 based on network state. O2-S1 in Equation (4-7) can be maximized by minimizing the distance between agents and the control node (computed by Equation (4-13)) and maximizing the network bandwidth (computed by Equation (4-12)). By this objective function, the idle agents can be deployed to other location to support other network connections.

If any user node is isolated from network, the messenger is operated to reconnect the disconnected user. This is represented by Equation (4-8). The *NCU*, *NCA*, *PAL* and *NAUL* metrics are computed using the equations, (4-9) through (4-11). Especially, to compute the PAL, first $aPAL_i$ or $uPAL_i$ should be computed by Equation (4-17). Equation (4-11) is used for the isolated cluster, by which agents in the cluster support the users in that cluster instead of moving toward the control node to be deployed other locations.

Finally, the location of each agent every time is decided by the decision variables, their velocity and direction, and constrained by the boundaries of operational area as described in Equation (4-16).

Chapter 5

Military MANET System and simulation environment

The optimization process for routing agents to the best locations is divided into three main phases. The first phase is to read location information. The control center collects information about the tactical operation in the assigned area such as the network nodes' locations and enemies. The connection matrix is constructed based on this information. Second, the optimizer performs the network performance evaluation using the predefined objective functions. Finally, the agent nodes will be deployed by either the PSO or a self deploy rule. If the agent node is connected to the control node, it will be deployed by the PSO. Otherwise, it will self deploy toward the center of future estimated locations of the last connected users or to support the users in a cluster.

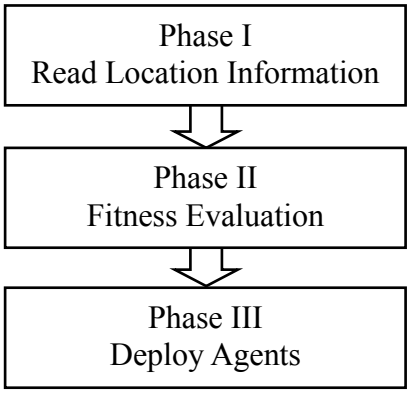


Figure 5-1 Main optimization framework

The main decision making processes for deploying agents are shown in Figure 5-1. The loop of these three phases of optimization process will be repeated during the simulation run. The detailed control logic is executed based on this main framework.

5.1 Routing by network state

There are two different network states in this study and the optimization process is differently applied by network state. As we discussed before, network performance is evaluated differently when there is an isolated user. This is the search effort to reconnect an isolated user in a real operation and thus to improve network performance.

First, it is checked if there is any isolated user node in the network. If all user nodes are connected with the control node, the network is evaluated by the objective function O2-S1, otherwise it is evaluated by objective function O2-S2 again. Then, all candidate locations for the agent nodes are evaluated and agents are deployed to the best location of those candidates. Different deployment rules are applied according to the agent status at the moment. That is, if an agent maintains connection with the control node, it will be deployed by the PSO logic. If the agent does not meet above condition, it will be deployed by the isolated agent deployment rule. We will discuss this in more detail in Section 5-3. The optimization framework by the network state is given in the following Figure 5-2.

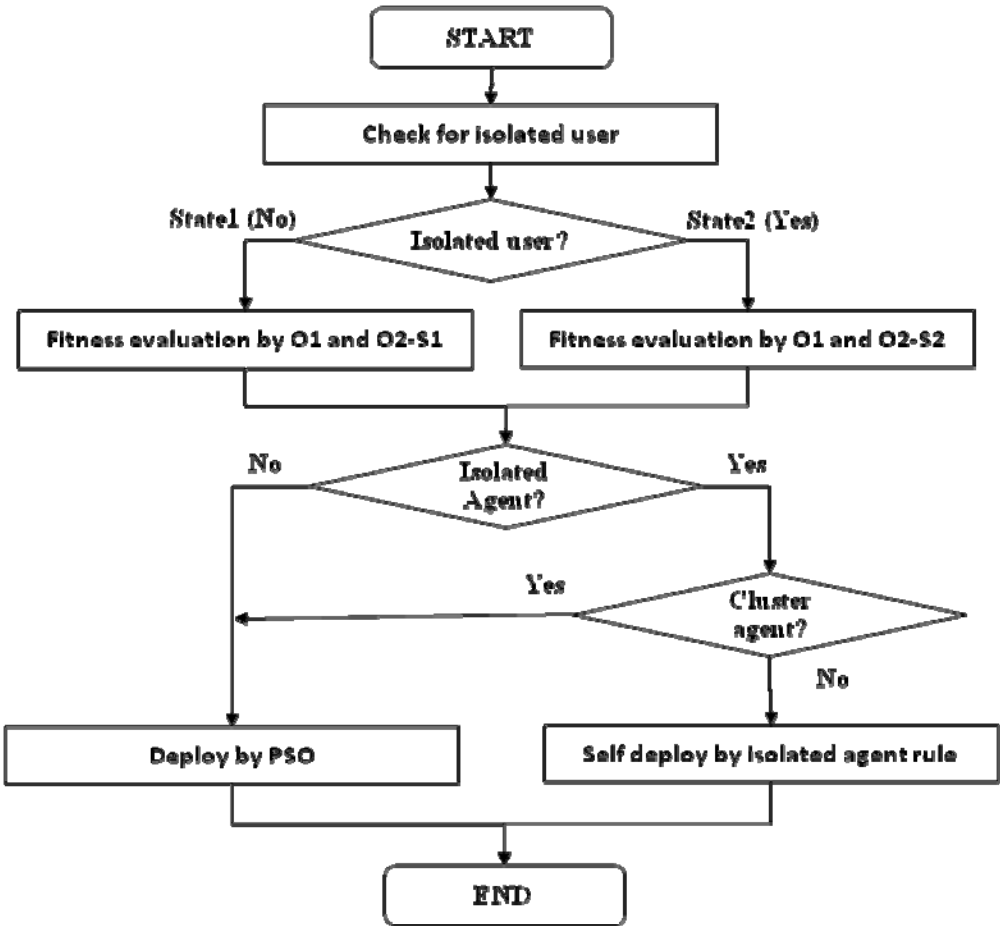


Figure 5-2 Optimization by network states

5.2 User node mobility model

The movement pattern of user nodes in a network depends on the given mission. The random waypoint model is very suitable for representing mobile phone users who move freely around the service area. It has also been implemented for military applications. However, some military operations, such as search & rescue and convoy, require more suitable to these environments.

All user nodes move toward their assigned destinations from the initial locations with a random velocity. In a real military operation, combat units cannot directly move to their

destinations due to the dynamic surrounding conditions which may limit its movement. To represent this two parameters, the perturbation level (τ) and the rotation angle (θ) for a user node, are employed so that the movement of users in the network can simulate a real world operation.

The user direction is calculated by the direction to current destination and the perturbation direction. First, the direction to the assigned destination from the current location ($\vec{TarDir}_{it}$) is calculated by equation (5-1).

$$\vec{TarDir}_{it} = \frac{(Destination.x_{it}, Destination._{yit}) - (x_{it} - y_{it})}{\left|(Destination.x_{it}, Destination._{yit}) - (x_{it} - y_{it})\right|} \tag{5-1}$$

All user nodes under dynamic environmental conditions cannot directly move to their destinations, but take random paths every step. That is, a user's direction is perturbed by a uniformly distributed random number between (-π/2, π/2) (Rotation angle (θ) = *U(–π/2, π/2)* and the perturbation level weight τ. These parameters can be adjusted for a given application. The perturbation direction for a user is created by following processes.

$$RotMatrix = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{5-2}$$

$$\vec{PerDir}_{it} = \vec{TarDir}_{it} \cdot RotMatrix \tag{5-3}$$

As shown in equation (5-3), the perturbation direction is computed by the direction to the assigned destination and the rotation matrix. After randomly generating a rotation angle θ, the perturbation direction is computed using the destination direction already computed and the

rotation matrix. Finally, the user node direction at each time step is calculated by following equation:

$$\vec{Userdir}_{it} = \vec{TarDir}_{it} \cdot (1-\tau) + \vec{PerDir}_{it} \cdot \tau \tag{5-4}$$

Where, τ is probability weight for the perturbation direction and 1- τ is the weight for the real destination direction. Although τ is set by 0.1 in this study, it can be changed by user's application. The location of a user from the previous time step is updated by the new user direction and the user speed as randomly generated by equation (5-5). The user node's velocity is also generated by a randomly distributed number between a preset minimum and maximum.

$$\begin{aligned} &UserSpeed = U(min,max) \\ &Userloc.x_{it} = Userloc.x_{i(t-1)} + UserSpeed \cdot \cos(\vec{UserDir}.x_{it}) \\ &Userloc.y_{it} = Userloc.y_{i(t-1)} + UserSpeed \cdot \sin(\vec{UserDir}.y_{it}) \end{aligned} \tag{5-5}$$

Where,

$\vec{TarDir}_{it}$: Destination direction for user *i* at time *t*

$\vec{PerDir}_{it}$: Perturbed direction by Rotation Matrix for user *i* at time *t*

$\vec{UserDir}_{it}$: Direction for user *i* at time *t*

After updating the user's location at each time step, a check is made to see if the user node has arrived at the assigned destination. If so, another new destination will be generated for the user node. There exist only two cases that require reassigning a user's destination. One is arrival to the destination and the other is arrival to the boundary of the problem space. The user

node mobility in this study is represented by either random waypoint or directed movement pattern which is constrained by predefined destinations or by movement within a responsibility.

5.3 Isolated agent behavior

During MANET operation, an agent node could become disconnected with the control node and if it is not a member of an isolated user-agent cluster, this node is referred to an "Isolated agent". These isolated agents cannot be controlled by the control node. Therefore, an instruction for reconnecting the isolated agents to the network as soon as possible is required for better network operation. Under this rule, an agent node can think and behave intelligently to find the right location to contact the network again by itself when it is isolated from the network. This kind of agent behavior is called "semi-intelligent agent behavior" [26].

An agent keeps track of the location of users which are connected with it by a single hop and this accumulated data is used to estimate the users' locations at four time steps later. The center of the predicted location of the last connected users will be the most attractive direction for the isolated agent in this research.

The isolated agent moves toward the center of the last connected users' location at four times in advance with maximum velocity by this self deploy rule until it connects with any user node in the network.

5.4 Enemy behavior

There may be many obstacles limiting MANET performance in a military operation area. Because of obstacles, the transmission ranges and movements of network nodes may be constrained. However, it is very difficult to measure the impact of these obstacles accurately and

it may be impossible since it is the result of mixed effects of weather condition, terrain shape, jamming by hostile forces and other surrounding conditions. There are also many different obstacles in a military combat operation area which limit the network performance naturally or artificially. Unlike obstacles due to natural causes such as weather condition or terrain shape, some obstacles are intentionally installed or deployed to those areas by enemy forces. The obstacles in the artificial obstacle category are employed in this study and termed Enemy.

5.4.1Enemy effective zones

Enemies are fixed at the initially assigned locations without moving throughout the simulation time and its mission is to degrade the communication capability of the network nodes and destroy those positioned within the kill zone. These effects are shown in Figure 5-3. Two different enemy's effective zones based on the distance between a MANET nodes and an enemy are introduced to represent enemy's effects in this study: the Jamming zone and the Kill zone, and the distances, d_1 and d_2, are uniform widths. The effective zones are defined with a radius circle from an enemy and jamming zone includes the kill zone. That is, any network node entering the effective zone first receives the jamming effect and then it may get physical attacks within the kill zone by the enemy as it nears to the enemy. The jamming effect level is determined by the Euclidean distance between the network node and the enemy, while the kill of a network node in the kill zone occurs randomly using a predefined probability based on a potential combat power.

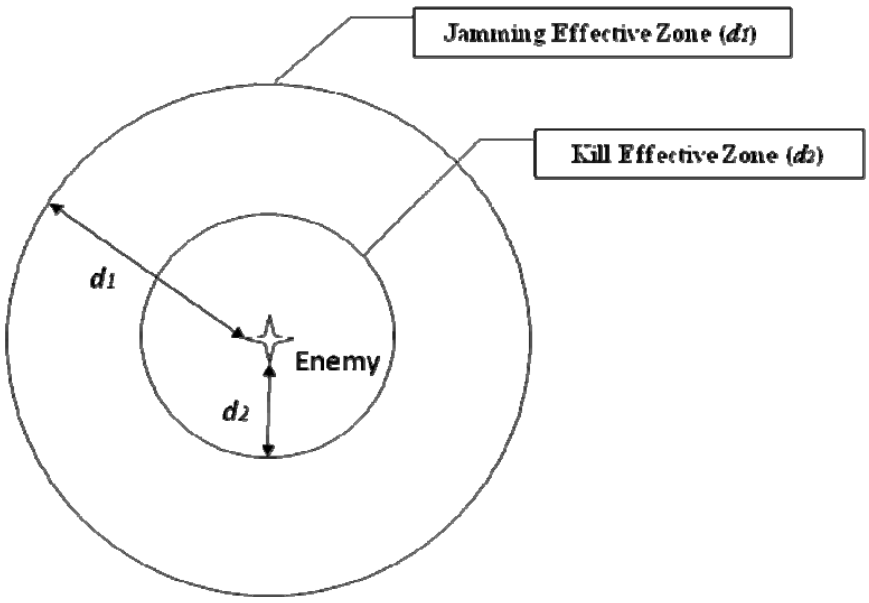


Figure 5-3 Enemy effect zones

As combat units, users can also attack and kill the enemies. The combat powers of the user and the enemy are represented by probabilities. We will discuss this more in detail in Section 5.7. The effective range and relative combat power of a resource (network node or enemy) could be adjusted accordingly to the military application.

5.4.2 Jamming effect

The signal strength represents the communication capability that a MANET node can communicate with other in a network and it is reduced by the jamming effect of enemy. The communication capability over a link between two nodes in a network decreases as the distance between them increases. In order to measure the jamming effect level for a link we use the relationship between signal strength and the distance between nodes constructing the link. The equation (5-6) shows the relationship between the signal strength and the distance under a free

space environment. This is not exact method but it is simple and a good approximation for appropriate the jamming level over a link [35].

$$P_{loss} = (4\pi d / \lambda)^2 \tag{5-6}$$

As seen in above equation, the loss of signal power (P_{loss}) is decreased as the distance (d) between two objects increases. This relationship is applied for estimating the jamming effect level in the research.

In order to limit a network device's capability, the jamming strength should be greater than its signal strength and this is common in a real military operation. For example, let's say the ratio of signal strength of jammer to network device is 3:2. That is, if the communication range of a network device is 1, the jamming effect range is 1.5. The jamming effect range is usually much longer than the network devices transmission range. Accordingly, if any node of a network link is within the jamming effect range, the performance of the node and link is degraded as much according to the distance to the jamming obstacle. The closer network device approaches the jammer, the stronger the jamming effect.

As a result, a node's communication capability is decreased and a poor quality of service by the reduced bandwidth. The jamming effect is normalized by the distance between the jammer and the network device as shown in Table 5-1. The table is developed under the assumption that the signal strength ratio between the jammer and the network device is 3:2. This ratio is applied to the scenarios in the study.

Table 5–1 Distance vs. Jamming effect level

d	d^2	*normalized jamming effect*
0.1	0.01	1.00
0.2	0.04	0.98
0.3	0.09	0.96
0.4	0.16	0.93
0.5	0.25	0.89
0.6	0.36	0.84
0.7	0.49	0.78
0.8	0.64	0.72
0.9	0.81	0.64
1.0	1.00	0.56
1.1	1.21	0.46
1.2	1.44	0.36
1.3	1.69	0.25
1.4	1.96	0.13
1.5	2.25	0.00

5.5 Prediction of user future location

MANET users are free to move within the given operation space. This causes some users to disconnect from the network during operation due to the limited number of agents. In order to maximize the chance for reconnecting an isolated user, we need information about the likely location of the isolated user.

Dengiz (2007) used the laws of kinematics to predict the future location of users in his research. Kinematics has commonly been used to estimate the future location of an object in the literature [26]. The location of a network node is described by its x and y coordinates. The change of location can be described by velocity and acceleration. That is, velocity is described by the magnitude of the position change and acceleration is represented by the rate of change of

velocity. These two kinematic factors are used to predict the future location of an isolated user in this research as well.

In this method, the only data required for the estimation of an isolated user's future location is its position history for three previous time steps. The basic mechanism of future location prediction based on the kinematics is as follows [26]:

$$\begin{aligned} v_{t-2} &= (x, y)_{t-2} - (x, y)_{t-3} \\ v_{t-1} &= (x, y)_{t-1} - (x, y)_{t-2} \\ v_t &= (x, y)_t - (x, y)_{t-1} \end{aligned} \tag{5-7}$$

Velocity, the magnitude of the position change for three time steps, is first computed by equation (5-7). v_t indicates the velocity at time t and similarly $(x, y)_t$ means the location of a user at time t.

$$a_{t-2} = \frac{v_{t-1} - v_{t-2}}{\Delta t} \tag{5-8}$$

$$a_{t-1} = \frac{v_t - v_{t-1}}{\Delta t}$$

$$\Delta a_{t-1} = \frac{a_{t-1} - a_{t-2}}{\Delta t} \tag{5-9}$$

Based on the computed velocities, the acceleration of a user is calculated as shown in equation (5-10) and (5-11).

$$\hat{a}_t = a_{t-1} + \Delta a_{t-1} \cdot \Delta t \tag{5-10}$$

$$\hat{v}_{t+1} = v_t + \hat{a}_t \cdot \Delta t \tag{5-11}$$

$$\Delta xy_t = v_t + \frac{1}{2} \cdot \hat{a}_t \cdot \Delta t \tag{5-12}$$

Equation (5-10) shows the computation of predicted acceleration ($\hat{a}_t$) at the next time step. Then, the estimated velocity ($\hat{v}_{t+1}$) and the magnitude of the position change (Δxy_t) can be computed by Equation (5-11) and (5-12), respectively.

$$XY_{t+1}^{P} = XY_t + \Delta xy_t \tag{5-13}$$

$$XY_{t+H}^{P} = XY_t + \Delta xy_t \cdot H \tag{5-14}$$

Finally, the predicted location of a user at the next time step (XY_{t+1}^{P}) is calculated by equation (5-13). If we want to predict a user node's location at the *t*+10 time step, it can be computed by multiplying Δxy_t by the prediction horizon (*H*) 10 as seen in equation (5-14).

5.6 Messenger behavior

During MANET operation, user nodes may be isolated from the network as we discussed before. When a user node is isolated, the control center tries to reconnect the isolated user if the network has any remaining capability, with which agents can perform other missions without degrading current network performance, for supporting the isolated user.

The control center designates an agent to search for the isolated user by choosing the closest agent from the last contact point and multiple messenger agents could be possible depending on the number of disconnected users. The pseudo code for a messenger agent is shown in Figure 5-4. This designated agent is referred to as a messenger. The messenger searches for the isolated user by using its predicted location. However, this search activity is permitted only for given time by the control center. Therefore, after the allowed time for search, the messenger is deployed to other location to support other network nodes if the isolated user is still missing.

```
Start {
        // for any disconnected user node j
        Set  SearchTime = st
        Set  NetState = 2
        Set MinD  = Big Value // Initial minimum distance
        for (AN_t=1 to AN_t=n) {
                Dist_n = distance (UN_j, AN_n)
                if (Dist_n < MinD) {
                        MinD = Dist_n
                        Messenger = n
                }
        }
        while  (Search Time Steps < st) {
                Fitness Evaluation by O1 and O2-S2
        }
} End
```

Figure 5-4 Pseudo code for a messenger

We expect that the messenger helps improve network performance by reconnecting the isolated user. However, it may worse the network performance since it requires operate some messengers among the limited number of agents under the circumstance that cannot even guarantee the reconnection of the isolated users. As a result, the search time for a isolated user should properly be determined by considering the mission and network performance.

5.7 Network node behavior in an enemy effect zones

In order to represent the different behavior of network nodes depending on the node type, we divided network nodes into four categories as discussed in Chapter 4.2.

All network nodes receive a jamming effect once they get into the jamming zone. Even though each network node can recognize its reduction of communication capability as it approaches an enemy, it is difficult to identify the location of enemy. However, the enemy location can be estimated using tactical information about the enemy and the jamming effect level. In this research, it is assumed that MANET node has an ESM sensor to detect the bearing of a jammer and two networked nodes within the jamming effect zone of an enemy are at least required to identify the location of an enemy. Also, any network node entering the kill effect zone of an enemy without knowing it can automatically detect the enemy.

User node's movement in the kill zone is not stopped by the enemy, that is, user node tries to fight against the enemy on the way its destination. On the other hand, agent nodes try to escape from the zone because of their weak combat power even though they have a combat capability. The combat power of each resource in this study is assumed as shown in Table 5-2. The kill probability of resources is determined by the distance between them, a user and an enemy or an agent and an enemy. That is, the kill probability of a user within a kill effect zone

increased as the user approaches an enemy. This kill probability is a function of index probability and distance to an enemy. The index probability for both user and agent node is differently defined here, which would determine the combat level in a battlefield.

Table 5-2 Combat power of resources and Index probability

Resources	User	Agent	Enemy
Combat power	1	0.1	1
Index probability	0.05	0.2	-

By using the index probability and the distance between resources, the kill probability can be computed by the equation below.

$$\text{Kill probability } (p) = min\left(1, \frac{Kill\ Effect\ Range}{distance\ between\ resources\ (d_{ij})} * Index\ probability\right) \quad (5\text{-}15)$$

Figure 5-5 shows the kill probability between a user and an enemy resource when they are within a kill effect range together. Particularly, within 0.05 distance, one of resources must be killed by the other one.

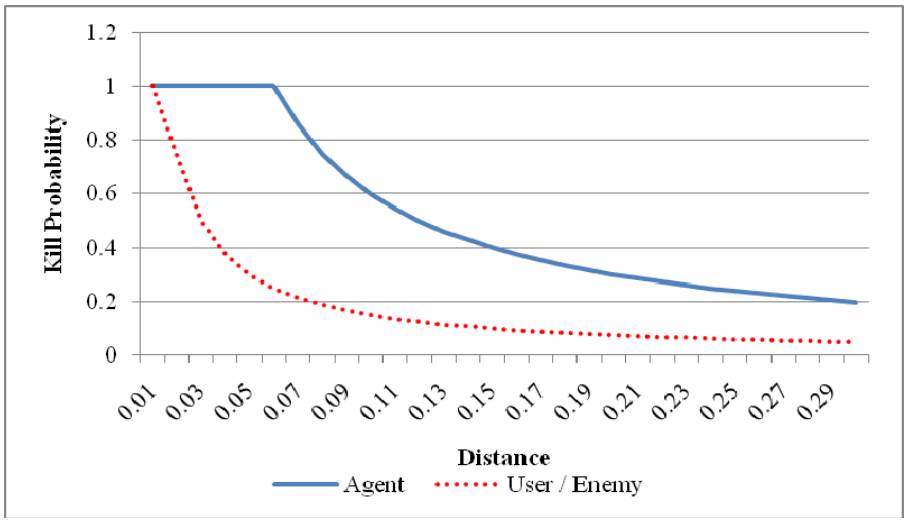


Figure 5-5 Kill probability of resources in a kill effect zone

Although the chance that agents enter the kill zone is very low since the location of enemies can be detected by ESM sensors in advance, the possibility still exists. The movement of agent nodes in the kill zone is shown in Figure 5-6:

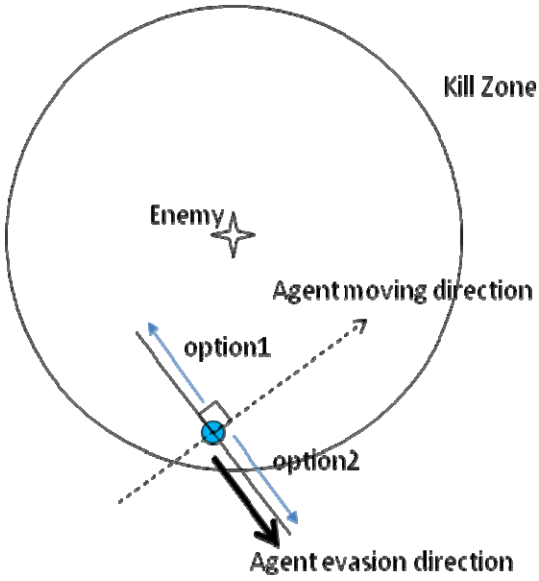


Figure 5-6 Agent behavior in the kill zone

Although many ways are available in real operation, to simplify there are only two possible options for agents to escape from the enemy in the kill zone. Both options are perpendicular to the user's original moving direction as shown in Figure 5-6. The user node will take the option which enables it to get out of the dangerous zone most quickly. That is, agent node in the kill zone compute the distance to the enemy from both possible locations it can reach from its current location with a maximum velocity. The option which enables the agent to be further distant from the enemy is the evasion direction. The agent in Figure 5-6 will take the option 2 to get out of the risk area quickly.

5.8 PSO parameters

The PSO performance can be improved by inertia weight and cognitive coefficients [34]. The inertia weight gets important effect on balancing the global search and the local search in PSO. The selected inertia weight in this study decreases linearly from 0.9 to 0.4 during a simulation running and computed using Equation 2-6. This selection has provided improved performance in many applications. Also, the cognition parameters are set by the common practice, 2.05 each. From the preliminary experiments the population size and the maximum number of iterations are set by 20 and 100, respectively.

Chapter 6

Simulation experiments and analysis

For the representation of a realistic military MANET operation, an enemy force's hostile activities are employed, with assumptions in this study. Several important performance metrics are created and used to improve network performance under the vulnerable conditions caused by the enemy obstacles in a tactical military operation area. Computerized simulations are performed to analyze network performance under the different scenarios considering the number of enemy obstacles, number of MANET nodes, and user mobility.

The simulation experiments are first performed to verify the effect of metrics used in this thesis. This verification is conducted based on three different user mobility models using a small or medium sized problem: random waypoint (RW), search and rescue (SR), and convoy and defense (CD). Those user movements are created for testing a more realistic military MANET environment, which are briefly discussed in the following section and shown with initial and operation formation figures. Then, the metrics effects are tested with medium and large sized problems for only RW again. The three different sizes of problem are represented in Table 6-1. The problem size is determined by the number of network nodes and the number of enemies involved.

Table 6-1 Test problems

	Small	Medium	Large
Users	5	10	20
Agents	4	8	16
Enemies	3	4	4

Also, the efficiency of the developed heuristic algorithm in terms of the number of hops required for a user node connection is tested by comparing it with the shortest distance based algorithm. To properly gauge the effect of metrics, destruction of network nodes or enemies is not included into the metric verification experiments, but it will be simulated for the cost benefit analysis later.

The cost benefit analysis is also conducted based on different sized problems, but the problem size differs by the mobility model. That is, the experiment with RW is conducted on the three sized problems as in the experiment for verification of metrics effect, however, the tests with SR and CD are performed only for the small and medium sized problems because of computation time with large sized problems.

The heuristic algorithm is coded and run in a C++ environment and the simulation results can be animated using a MANET simulation test bed especially developed. It can show the dynamic movement of MANET nodes including the enemy effects in the problem space.

6.1 Simulation environment

At the initial time step each MANET node is generated at its assigned location. The network is in the connected state. The user nodes start to move toward their destinations which are randomly given or predefined depending on the assigned mission or mobility model. User

nodes' velocities and directions are also randomly assigned at each time step. However, to evaluate network performance under the same test conditions, the target destination, velocity and direction of a user node are generated using the same random number seeds for the different cases. As a result, the user nodes in different scenarios take the same paths.

The simulation area is a two dimensional 6×6 distance square unit. The communication range of all MANET nodes is 1.0 distance unit. The velocity of MANET nodes is described by Euclidean distance unit traveled per unit time step, which is constrained by a minimum and a maximum velocity. The velocity range of a user node is between 0.02 and 0.05, whereas for an agent node, including the control node, it is between 0 and 0.07. However, enemy locations are not changed through the simulation time. This is true for all user movement patterns employed in this study.

6.2 Test mobility models

The metrics verification experiment is conducted based on three different mobility models in order to compare network performance under different operation environments. Each mobility model represents a different movement pattern of military operation. The random waypoint is very common in MANET research as a default mobility model. User nodes with the random waypoint randomly move around the operation area without being directed by a control unit or an operational plan. User nodes' movements are directed in the SR and CD mobility models by a predefined operational plan. These movement patterns are described below.

6.2.1 Random Waypoint (RW)

This movement pattern is used to represent military operations with a high random movement of users within a given operation area. All target directions for users are randomly generated without any predefined movement schedule. All MANET nodes are connected with each other at the initial time step and they start to spread out according to their random assigned destinations, velocities and directions. Figure 6-1 and Figure 6-2 show the initial formation and movement of network nodes and enemies.

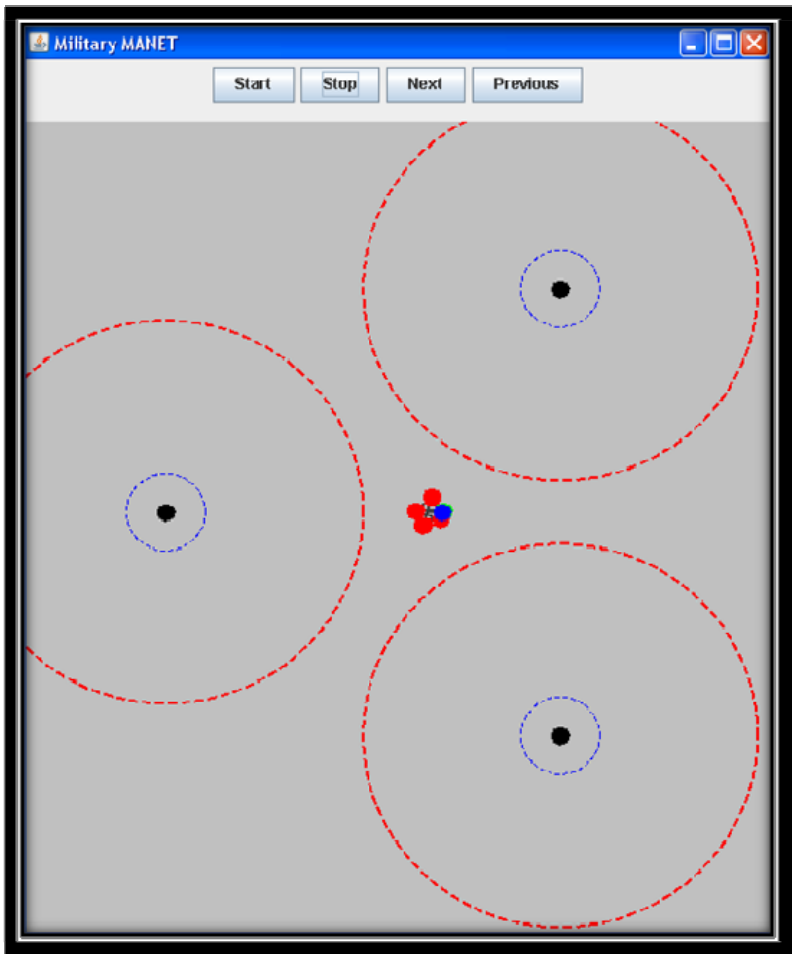


Figure 6-1 Initial formation with RW

Black balls surrounded by a blue and a red circle are enemies and the group of nodes in the center in Figure 6-1 includes the MANET nodes. User nodes (red balls) start to move toward their destination and are followed by agent nodes (green) and the control node (blue).

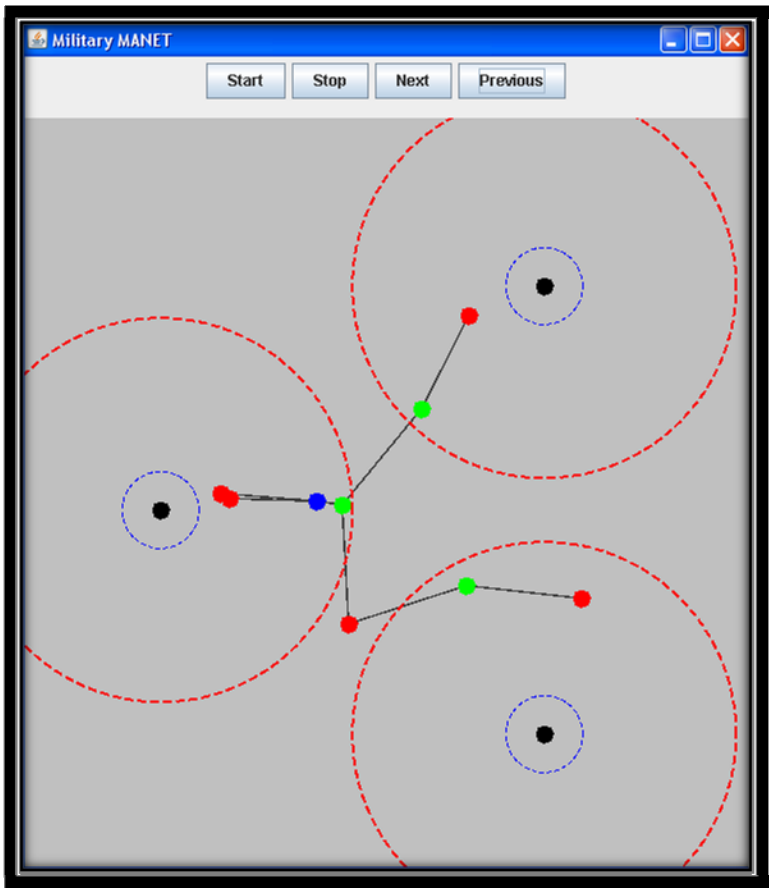


Figure 6-2 Operation formation with RW

6.2.2 Convoy and Defense (CD)

This movement pattern represents a military operation convoying a core body to a destination. A core body, such as a command unit, a VIP or war supplies, is located at the center of the formation and users surround it while maintaining a predefined distance. The purpose of this operation is to protect the important resources from enemy forces and convoy it safely to a

target point. Each user is assigned a responsible area, each rectangular box in Figure 6-3, to perform this mission and the user's movement is constrained by the assigned area. There are four pre-assigned patrol boxes in which two user nodes operate and stay inside during the simulation.

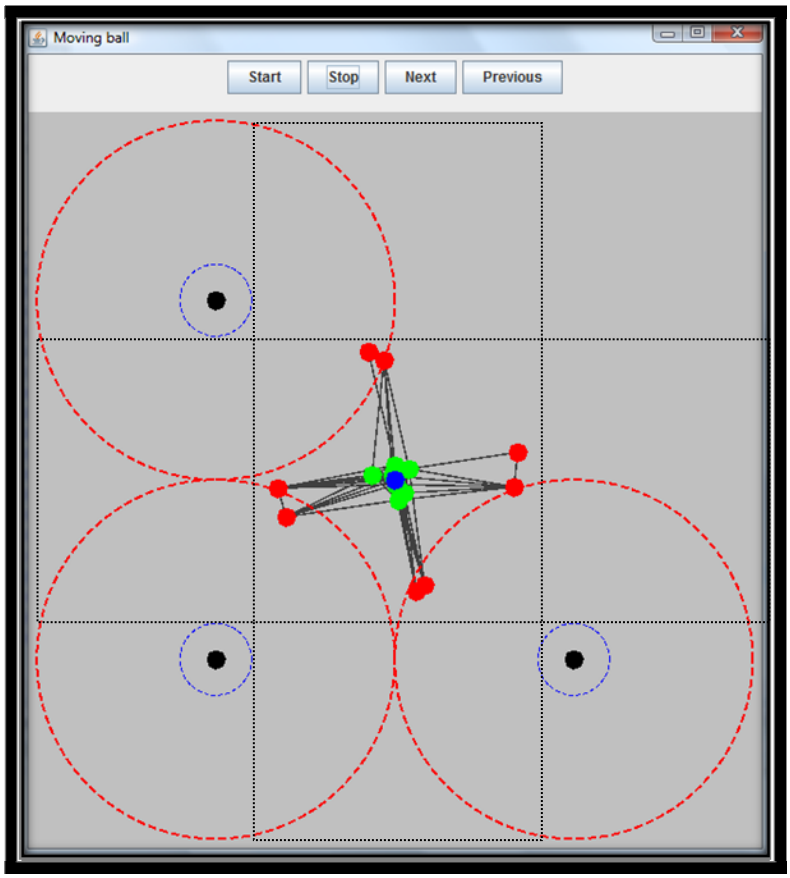


Figure 6-3 Initial formation with CD

Once a simulation is run, user nodes move into their responsible box. However, the control node is fixed at the initial location through the simulation span. Figure 6-4 shows the movements during the operation simulation.

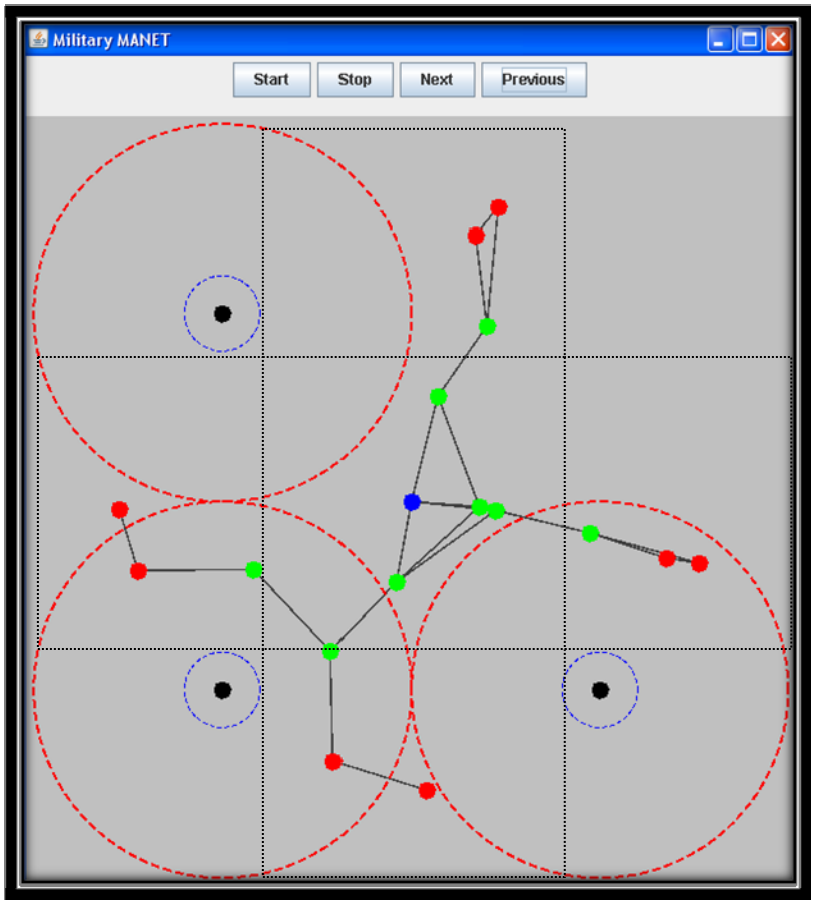


Figure 6-4 Operation formation with CD

6.2.3 Search and Rescue (SR)

One of the most important considerations in a search operation is that a given responsibility area can be covered as much as possible to accomplish an assigned mission efficiently. To meet this requirement, the responsibility area is uniformly divided into several sub-sectors. The number of sub-sectors is generally equal to the number of available users. Each user assigned to an individual sub-sector to search and rescue targets. As shown in Figure 6-5, user nodes start to search from initial points where the network is fully connected, and follow paths which are predefined to cover the given search area in Figure 6-6.

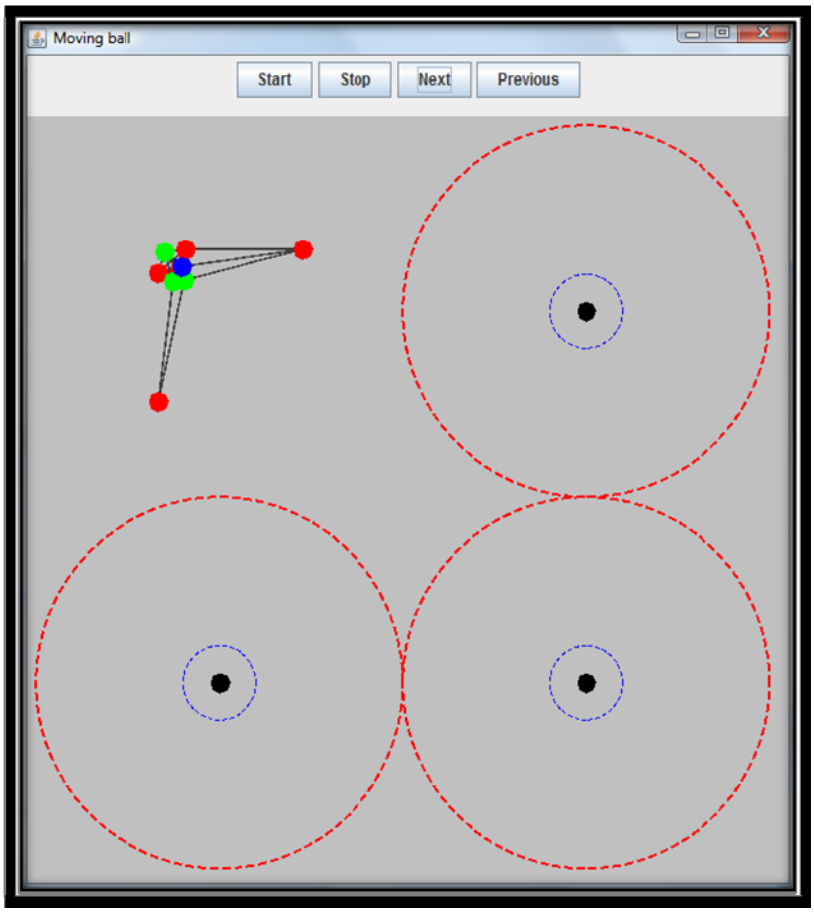


Figure 6-5 Initial formation with SR

The purpose of this operation is to search or rescue some targets such as mines, lost friendly forces, etc. The performance of a search and rescue operation depends on the effective use of limited resources. For effective deployment of users in this operation, users need to be directed by an operational plan. First, each user node travels through predefined target points. This enables users to uniformly cover the responsibility area without wasting limited resources by duplicated deployment of users. Figure 6-6 shows the characteristics of this movement. This is the least random movement among those mobility models used in this study.

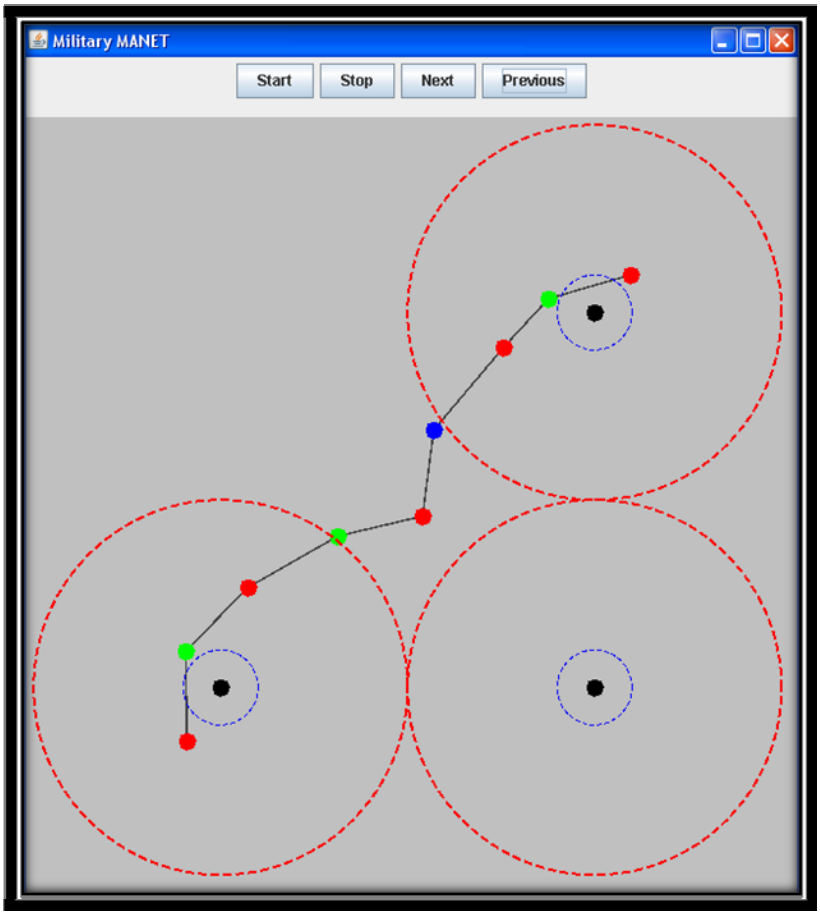


Figure 6-6 operation formation with SR

6.3 Performance measures

The primary goal of a military MANET in this study is to maximize the connection of user nodes, with the control node and to provide users in an operation space with a common view of the battle space. Military MANETs are usually operated under vulnerable conditions like enemy's hostile activities and the available resources for MANET operation are limited. So, the efficient operation of given service resources becomes an important consideration for military operations. Network performance is compared based on the following metrics:

1) The average number of connected user nodes with the control node is computed by Equation (6-1).

$$PM_1 = \frac{\sum_{t=1}^{ts}\left(\sum_{i \in UN} P_t(i, CN)\right)}{ts} \tag{6-1}$$

Where, *ts* is the simulation time span in the given problem scenario. The indication of a path connection, $P_t(i, j)$ is 1 if there is a path connection between a user nodes *i* and the control node *j*, otherwise it is 0. Network performance is evaluated by PM_1 as the primary performance measure.

2) The average number of hops per user node connection with the control node, PM_2, given in equation (6-2). In particular, this metric is used to evaluate the efficiency of a MANET optimizer.

$$PM_2 = \frac{\sum_{t=1}^{ts}\left(\frac{\sum_{i \in UN, j=CN} Hop_{ijt}}{\sum_{i \in UN} P_t(i, CN)}\right)}{ts} \tag{6-2}$$

Here, Hop_{ijt} represents the number of hops between user node *i* and the control node *j*.

3) The average total propagation loss by jamming, PM_3, can be computed by subtracting actual bandwidth (aBW_{ij}) from the possible bandwidth (pBW_{ij}) which is calculated by the distance between node *i* and *j* as given in equation (6-3). By this metric, the average of jamming by enemies in the operation area can be measured. This metric is used only for the enemy case scenarios.

$$PM_3 = \frac{\sum_{t=1}^{ts}\left(\sum_{i\in UN, j=CN}\left(pBW_{ijt} - aBW_{ijt}\right)\right)}{ts} \quad (6\text{-}3)$$

4) The last performance measure of this study is the Mission Completeness Rate (MCR). This is computed by dividing total number of connected priority nodes by total number of priority nodes as shown in Equation (6-4).

$$PM_4 = \frac{\sum_{t=1}^{ts}\left(\frac{\sum_{i\in PN} P_t(i, CN)}{TP_t}\right)}{ts} \quad (6\text{-}4)$$

Any user node entering the priority node assigning zone is defined as a priority node. TP_t represents the total number of priority nodes at time t.

By using these performance measures listed above, we will evaluate a MANET performance.

6.4 Effect of metrics under different mobility

The implemented metrics in this study, PAL, messenger, and Priority node are expected to improve MANET performance from considering military aspects. These effects are verified under different test environments by the mobility models and number of network nodes and enemies. As we mentioned before, the kill scenario is not included in the experiments for metric verification. The test problems for RW and SR include 9 network nodes (5 users, 3 agents, 1 control) and 3 enemies, while that for CD includes 17 nodes (8 users, 8 agents, 1 control) and 3 enemies. Each problem is tested with 100 replications and each replication is simulated for 200 time steps for RW and CD and for 180 time steps for SR mobility.

6.4.1 PAL effect

PAL, which is newly developed to support the weakness of the hop-count based algorithm for military MANET, is the most important metric in this study. The main function of this metric is to properly distribute agent nodes within a given tactical area to support the user nodes moving toward their randomly assigned or predefined destinations in a timely manner.

The simulation results in Table 6-2 show the effect of the PAL metric. The PAL effect is compared with the result of the No PAL case. The difference between No PAL and PAL is verified by a paired-T test with the primary performance measure (PM_1).

Network performance by PAL is much improved in all cases. For each mobility pattern, network connectivity is improved by 2.63%, 10.5% and 12.6%. For all mobility models by increasing the number of enemies, the network performance is degraded by small successive decrements. The PAL metric is the most effective for SR mobility.

Table 6-2 PAL effect with the hop-count based algorithm

Mobility	Num Enemy	No PAL		PAL		p-value
		Avg NCU	*Avg Jamming*	*Avg NCU*	*Avg Jamming*	
RW	0	3.850	-	3.970	-	0.006
	1	3.792	0.313	3.944	0.248	0.000
	2	3.672	0.653	3.819	0.534	0.000
	3	3.540	0.981	3.647	0.801	0.019
	Avg	3.714	0.649	3.845	0.527	
CD	0	6.456	-	7.400	-	0.000
	1	6.453	0.308	7.314	0.242	0.000
	2	6.420	0.719	7.213	0.561	0.000
	3	6.449	1.109	7.226	0.793	0.000
	Avg	6.445	0.712	7.288	0.532	
SR	0	3.702	-	4.401	-	0.000
	1	3.547	0.075	4.223	0.167	0.000
	2	3.379	1.591	3.999	1.281	0.000
	3	3.314	1.773	3.830	1.522	0.000
	Avg	3.486	1.14633	4.113	0.99	

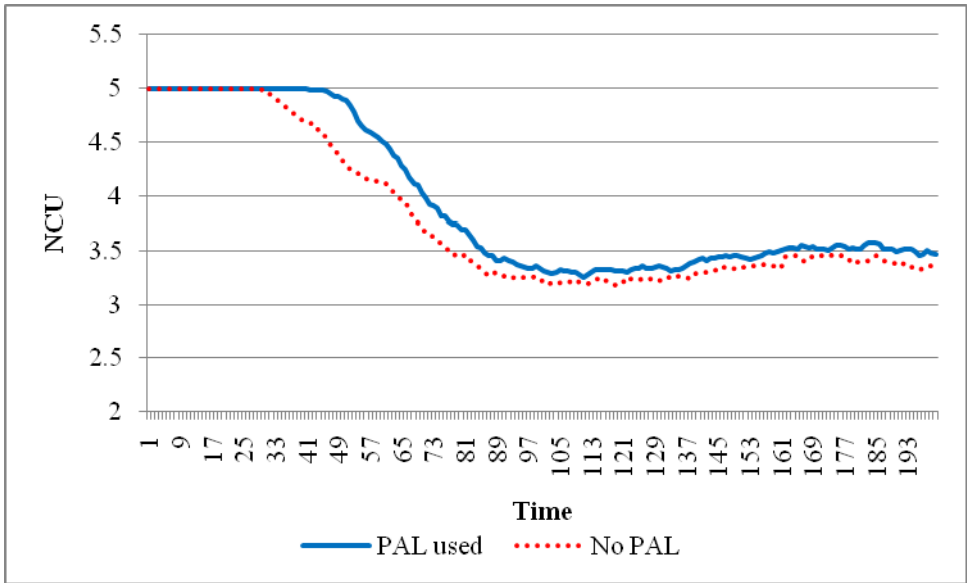


Figure 6-7 Comparison of PAL and No PAL (RW, 1E)

The PAL effect with RW is a little smaller than in the other two mobility models. However, the average plot line of the PAL case is always positioned above the No PAL case as shown in Figure 6-7. Also, the performance difference by the paired-T test is statistically significant. The p-values in the far right column in Table 6-2 are the paired-T test results between the two cases.

On the other hand, this performance improvement by PAL is much clearer with CD and SR than with RW as shown in Figure 6-8 and Figure 6-9. The 95% confidence interval plot for the two cases shows this difference more clearly. There are two groups of line in the figures. From the top, each line indicates the mean, upper and lower confidence limits of a 95% confidence interval on the mean.

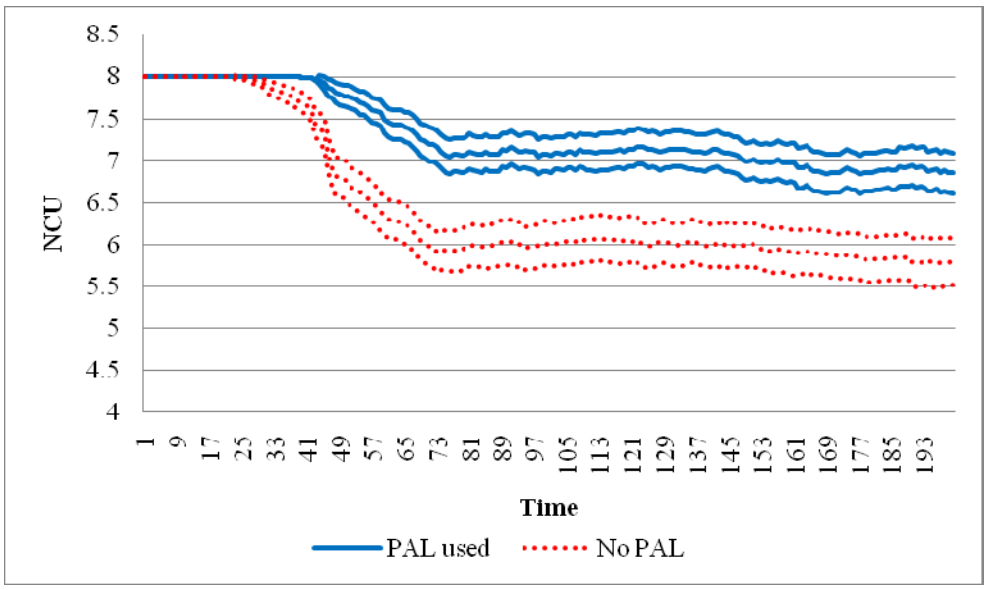


Figure 6-8 Comparison of PAL and No PAL (CD, 1E)

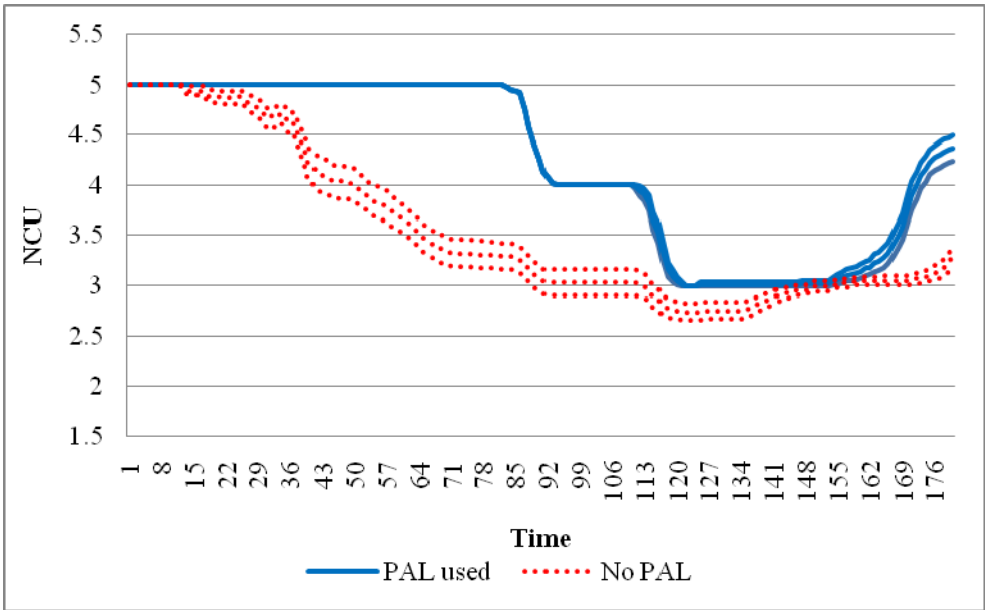


Figure 6-9 Comparison of PAL and No PAL (SR, 1E)

The step–shaped plot of the PAL case in Figure 6-9 is related to the characteristics of SR movement. Around the time range between 95 and 110, one of user nodes at the end of both sides

of search space is disconnected from the network due to the shortage of agents. So, NCU is decreased to 4 from 5. At about 110 time, NCU is again decreased to 3 when the user node in the other side of search space is disconnected. It takes about 40 time steps for the disconnected users to start to recover the connection with the control node again. Messenger is not employed in either scenario in Figure 6-9. If messenger agents were employed, the plot would change since NCU can be improved by their use.

Table 6-3 PAL effect with the shortest distance based algorithm

Mobility	Num Enemy	No PAL		PAL		p-value
		Avg NCU	*Avg Jamming*	*Avg NCU*	*Avg Jamming*	
RW	0	3.890	-	3.997	-	0.003
	1	3.827	0.418	4.003	0.348	0.000
	2	3.753	0.789	3.878	0.711	0.001
	3	3.566	1.239	3.748	1.015	0.000
CD	0	6.575	-	7.438	-	0.000
	1	6.877	0.346	7.429	0.288	0.000
	2	6.777	0.693	7.493	0.555	0.000
	3	6.777	1.210	7.422	0.873	0.000
SR	0	3.854	-	4.3999	-	0.000
	1	3.546	0.116	4.233	0.146	0.000
	2	3.377	1.858	4.039	1.158	0.000
	3	3.322	1.856	3.886	1.285	0.000

This PAL effect is also effective for the shortest distance based routing algorithm. Network performance is improved for all cases and mobility models as shown in Table 6-3. Based on these results, we can postulate that PAL effect depends on the randomness of user mobility. Among user mobility models used in this study for experiment, RW is the mobility model with the most randomness, whereas SR has the least randomness user node directions are predefined.

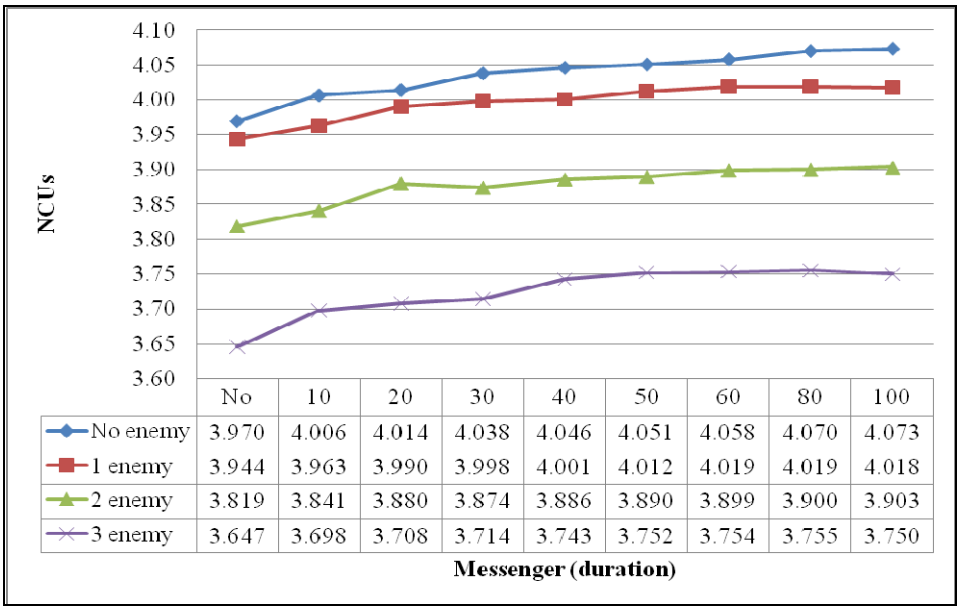
6.4.2 Messenger effect

The purpose of operating messengers is to reconnect isolated users from the network. Messengers employed in this study are expected to improve network performance by reconnecting disconnected users. To accomplish that, the proper duration for operating messengers is crucial to manage the limited number of agents effectively in a military MANET operation. So, the operation time of messenger for each mobility model needs to be considered first.

6.4.2.1 Random waypoint (RW)

For all cases in Figure 6-10, both no enemy and enemy cases, the user node connectivity by messenger is approximately increasing in messenger time. The operation time of a messenger with RW mobility is not limited if user nodes are not killed by enemy attack or any other reasons. That is, the better network performance can be accomplished by operating messengers for longer time. The 95% CI plot in Figure 6-11 represents the advantage of using messenger visually. The messenger case is always better than the no messenger case in the plot. Disconnected user nodes

might be reconnected by either messenger agents or other network nodes (users or agents). The average percentage of reconnected users reconnected by only messenger nodes is about 20.05%.



	No	10	20	30	40	50	60	80	100
No enemy	3.970	4.006	4.014	4.038	4.046	4.051	4.058	4.070	4.073
1 enemy	3.944	3.963	3.990	3.998	4.001	4.012	4.019	4.019	4.018
2 enemy	3.819	3.841	3.880	3.874	3.886	3.890	3.899	3.900	3.903
3 enemy	3.647	3.698	3.708	3.714	3.743	3.752	3.754	3.755	3.750

Figure 6-10 Messenger effect (RW)

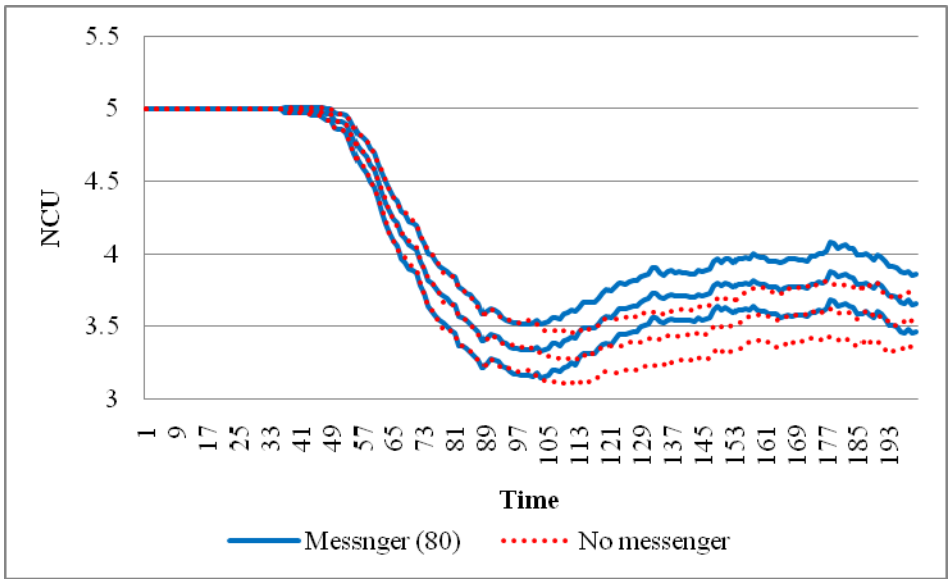
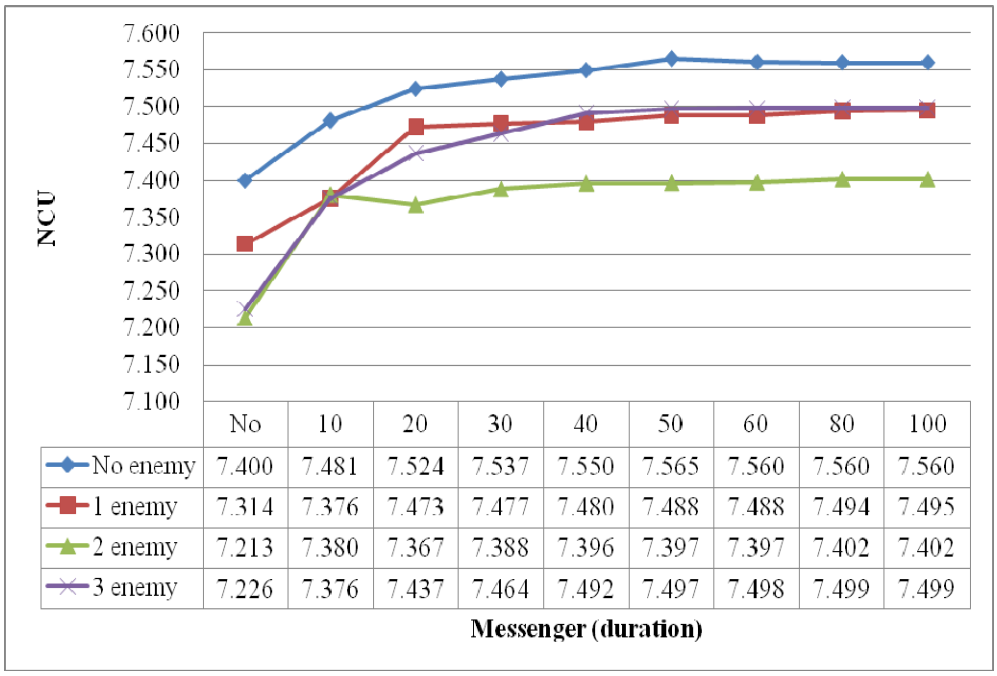


Figure 6-11 Comparison of the Messenger and No messenger (RW)

6.4.2.2 Convoy and defense (CD)

Figure 6-12 and Figure 6-13 summarize the effect of the messenger with CD mobility. CD mobility does not show full random mobility like the random waypoint. However, users are free to move within their responsibility area. That is, each user's mission area has been shifted from the entire operational space to a small patrol box in CD mobility. The messenger effect in CD is a little greater than in RW. The average improvement for RW is about 1.82%, but is 2.5% for CD.



	No	10	20	30	40	50	60	80	100
No enemy	7.400	7.481	7.524	7.537	7.550	7.565	7.560	7.560	7.560
1 enemy	7.314	7.376	7.473	7.477	7.480	7.488	7.488	7.494	7.495
2 enemy	7.213	7.380	7.367	7.388	7.396	7.397	7.397	7.402	7.402
3 enemy	7.226	7.376	7.437	7.464	7.492	7.497	7.498	7.499	7.499

Figure 6-12 Messenger effect (CD)

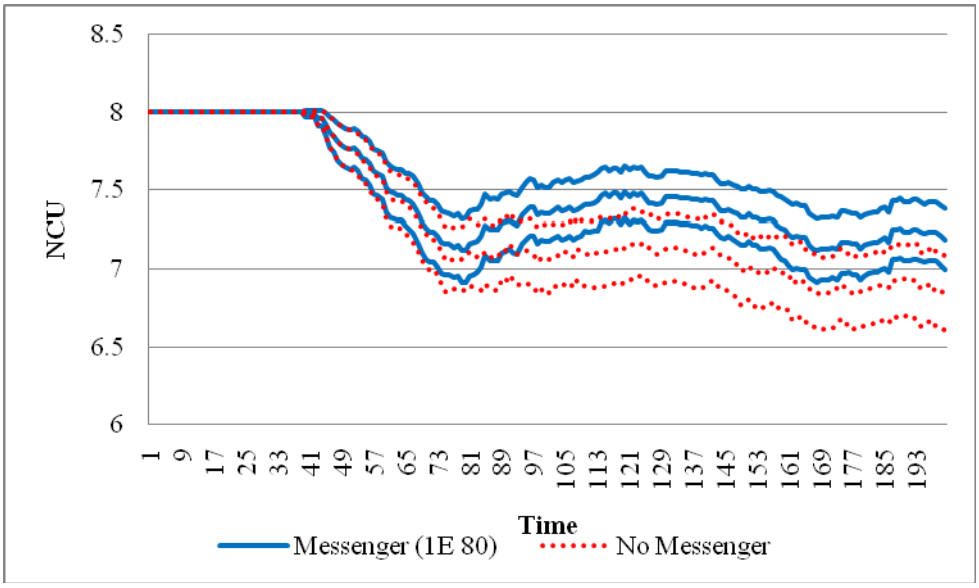
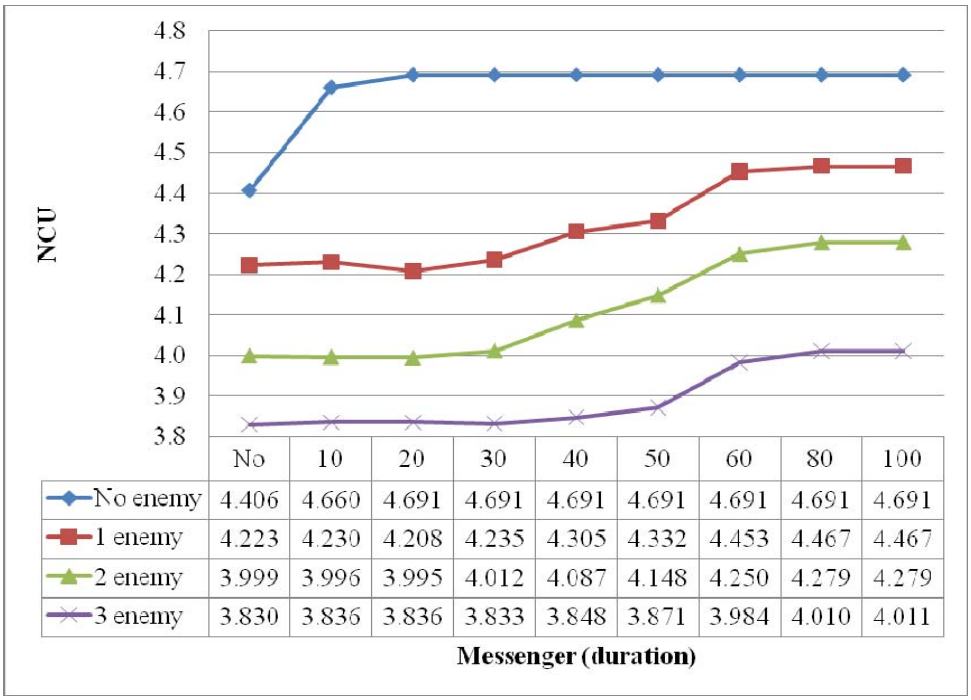


Figure 6-13 Comparison of the Messenger and No messenger (CD, 1E)

6.4.2.3 Search and Rescue (SR)

SR mobility is the most directed movement among the mobility models used in this study because of its predefined operational plan. User nodes in SR go through their predefined paths or destinations. It has relatively low randomness. However, the effect of the messenger is the largest in this lowest random mobility model as shown in Figure 6-14 and Figure 6-15. The average improvement with SR is about 4.94%, almost twice of that in CD and triple of that in RW. The movements of disconnected users in SR operation are limited to their assigned search areas, so using a messenger can improve the connectivity significantly.



	No	10	20	30	40	50	60	80	100
No enemy	4.406	4.660	4.691	4.691	4.691	4.691	4.691	4.691	4.691
1 enemy	4.223	4.230	4.208	4.235	4.305	4.332	4.453	4.467	4.467
2 enemy	3.999	3.996	3.995	4.012	4.087	4.148	4.250	4.279	4.279
3 enemy	3.830	3.836	3.836	3.833	3.848	3.871	3.984	4.010	4.011

Figure 6-14 Messenger effect (SR)

The difference between the messenger and no messenger cases is very clear in SR as shown in the 95% confidence interval plot in Figure 6-15. For first 90 time steps, a messenger is not required since all user nodes are connected with the control node. But, after this time range, messengers play a key role for network connections. The confidence interval plot in Figure 6-15 shows the definite advantage of using messengers.

The no messenger case maintains the three user nodes connected state between time 120 and 150 without reconnecting the disconnected users. This is because the agents move back to the control node when they lose connection with the users. However, in the messenger case, agents are converted to messengers when they lose connection with the users which they have served. The messengers try to reconnect the disconnected users for a given time by moving close to the estimated location of disconnected user as much as possible. As shown in Figure 6-15, the disconnected users start to be reconnected right after disconnecting from the network.

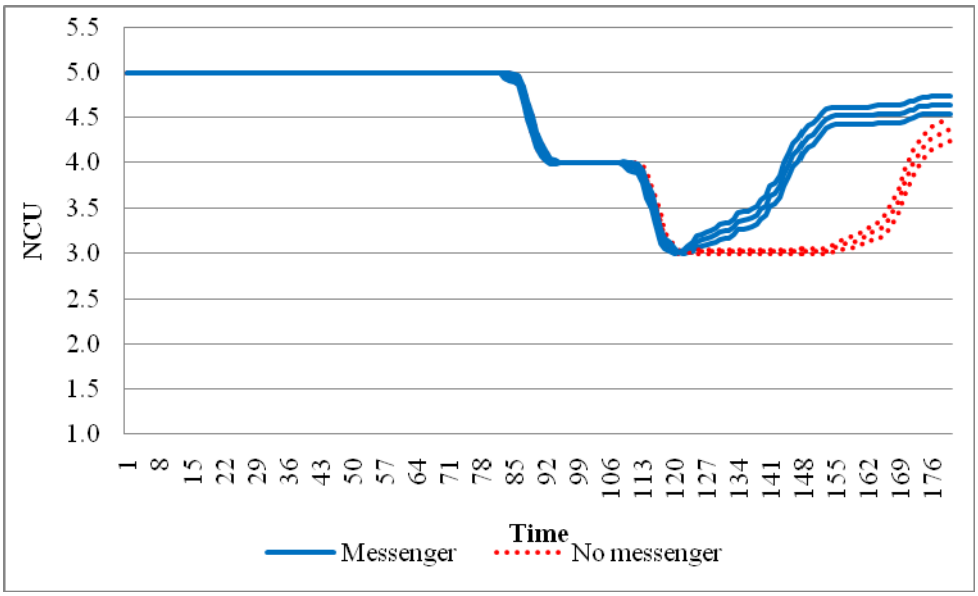


Figure 6-15 Comparison of the Messenger and No messenger (SR, 1E)

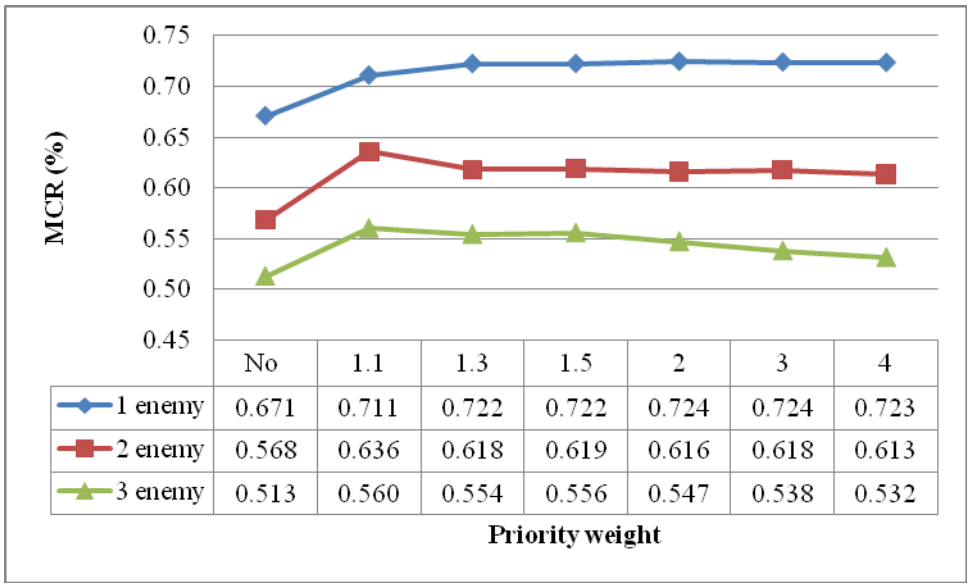
6.4.3 Priority node effect

Unlike the other metrics, a priority node does not guarantee improved network performance. The purpose of the priority node in this study is to represent a more realistic military MANET operation scenario. A user node that requires the priority service of agents because of the operational situation (such as combat, positioning close to interested target) is defined as a priority node, as addressed in Section 4.2. In this study, the connectivity of priority nodes is needed for mission success and a priority node is weighted by a higher positive value to increase its connectivity. Another parameter, Mission Complete Rate (MCR), is employed to measure the effectiveness of the priority node concept. The distance to an enemy is used in this study to assign a priority node.

A radius circle from an enemy is set as a priority assigning zone (PAZ), similar to the jamming zone and the kill zone. Any user node entering this circle is assigned a priority node

which requires service before other user nodes outside the PAZ. This zone is set to 0.7 unit distance for this experiment.

6.4.3.1 Random waypoint



	No	1.1	1.3	1.5	2	3	4
1 enemy	0.671	0.711	0.722	0.722	0.724	0.724	0.723
2 enemy	0.568	0.636	0.618	0.619	0.616	0.618	0.613
3 enemy	0.513	0.560	0.554	0.556	0.547	0.538	0.532

Figure 6-16 MCR changes by priority node weights (RW)

As shown in Figure 6-16, MCR (%) is improved for all enemy cases by assigning priority nodes, but this improvement of MCR may require some tradeoff of NCU as shown in Figure 6-17. Network performance is decreased as the priority weight increases.

For one enemy case with RW, the best weight looks seems to be 4 from Figure 6-17 considering both NCU and MCR. However, as the number of enemies is increased the best weight for a priority node is changed to 1.1 as shown in Figure 6-18 and Figure 6-19.

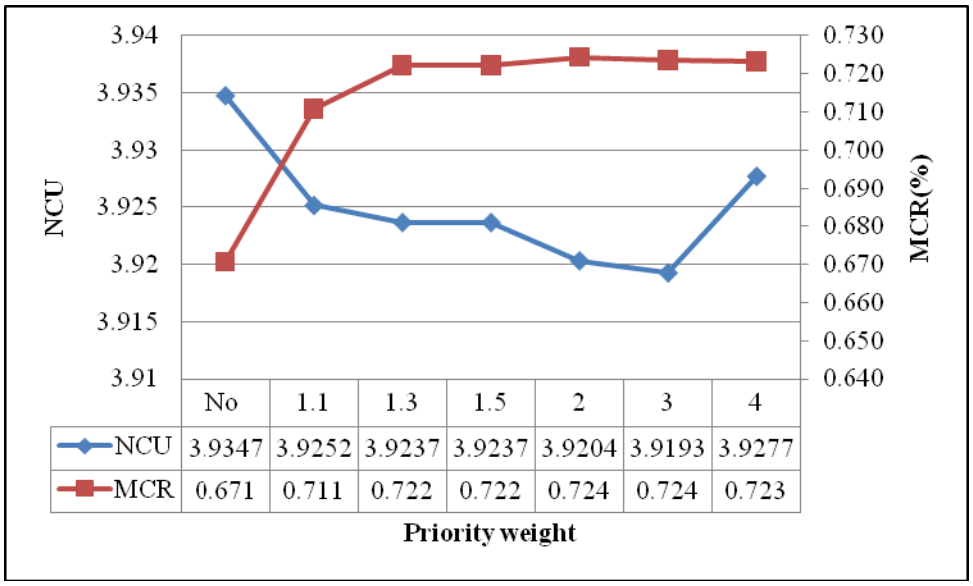


Figure 6-17 Priority node effect (RW, 1E)

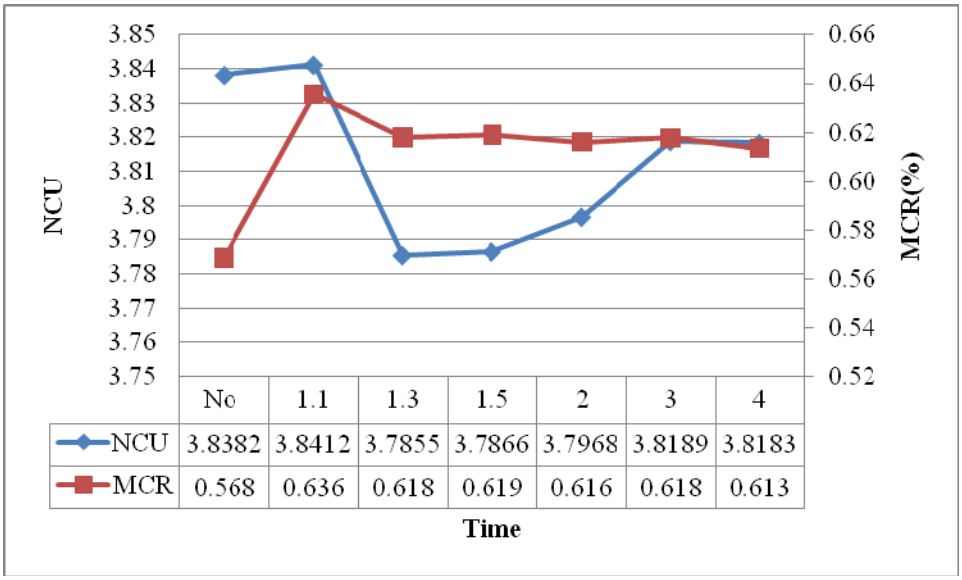


Figure 6-18 Priority node effect (RW, 2E)

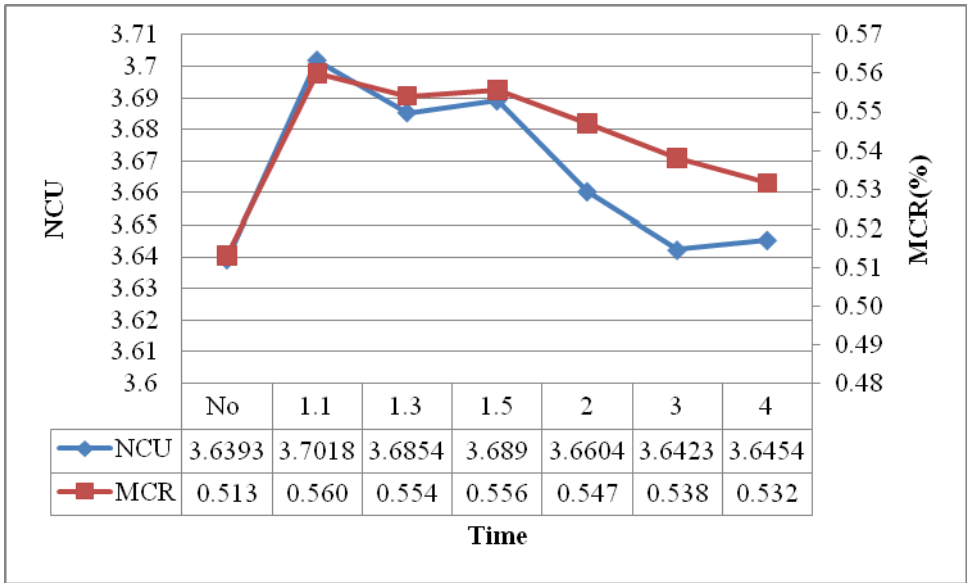
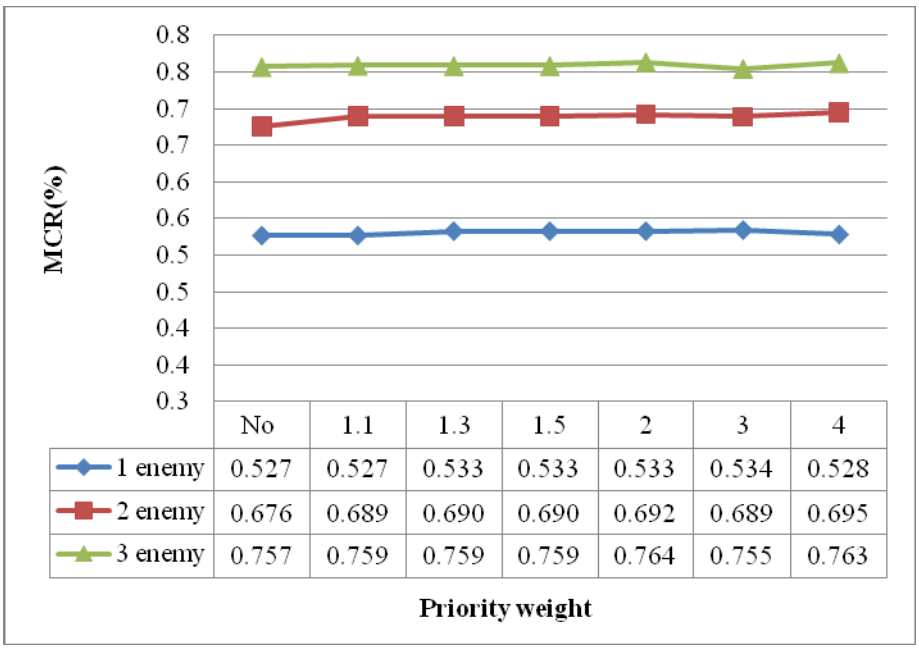


Figure 6-19 Priority node effect (RW, 3E)

Especially, in the three enemy case (3E), both NCU and MCR are increased when the priority is weighted by 1.1 as shown in Figure 6-19. As a result, the best priority weight which can maximize MCR and minimize the reduction of NCU at the same time is 1.1. However, the number of agents in the small sized problem are not enough to cover the users through the given operation area. So, assigning an agent to support a priority node degrades the network performance since other users may not be served.

6.4.3.2 Convoy and Defense (CD) and Search and Rescue (SR)

The priority node metric is not as effective in CD and SR as in RW. Figure 6-20 through Figure 6-23 do not show any critical difference from the no priority node case. MCRs in Figure 6-20 maintain almost steady state for the three enemy cases even though the priority weight is increased.

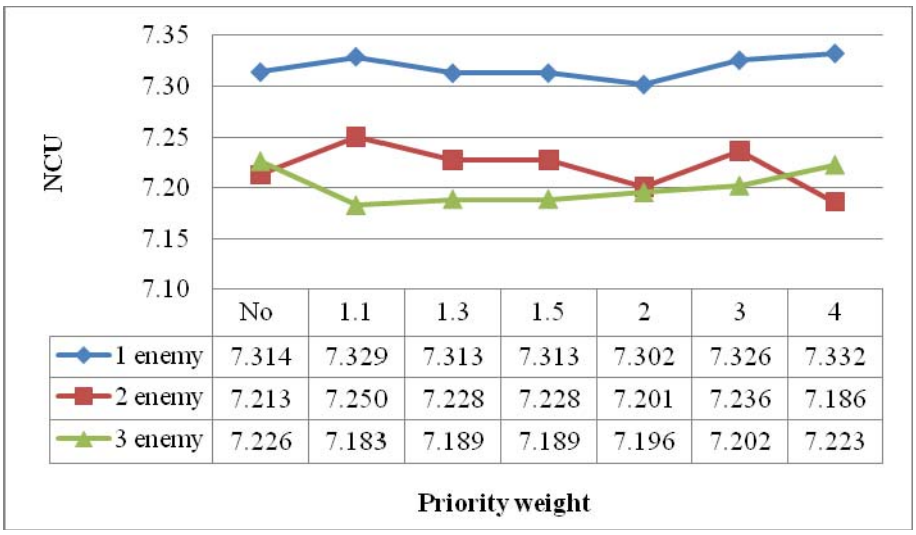


	No	1.1	1.3	1.5	2	3	4
1 enemy	0.527	0.527	0.533	0.533	0.533	0.534	0.528
2 enemy	0.676	0.689	0.690	0.690	0.692	0.689	0.695
3 enemy	0.757	0.759	0.759	0.759	0.764	0.755	0.763

Figure 6-20 MCR changes by priority node weight (CD)

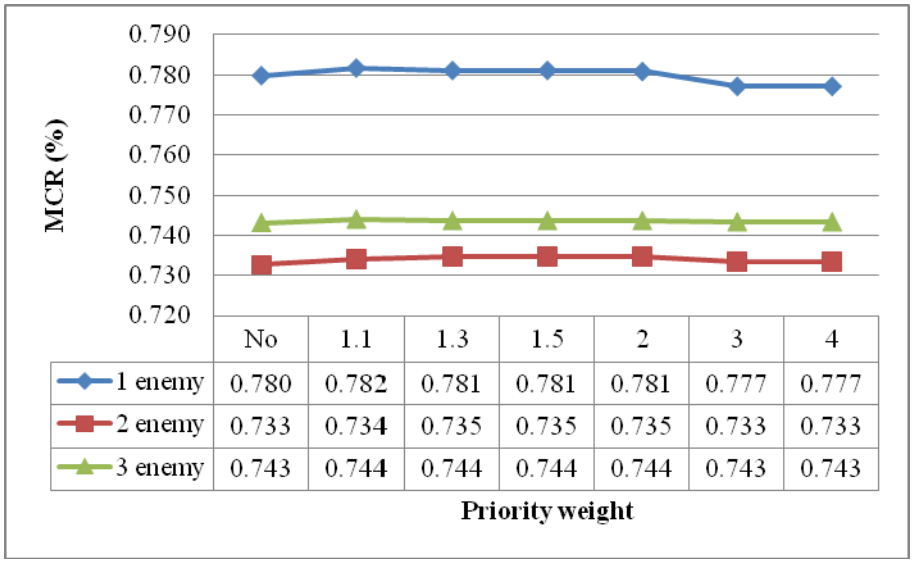
Although network performance fluctuate a little compared with MCR chart, it is almost constant too. This is related to the randomness of user mobility. As discussed before, CD and SR have lower randomness than RW.

The network nodes in CD and SR move and spread out by their predefined movement plans. Agent nodes are matched with their responsible user when users reach their mission area or are distributed enough from other users. Consequently, there are only a few cases where agent nodes should give up supporting user nodes to connect priority nodes because of the distribution of network nodes through the operation area by a predefined plan. As a result, the use of the priority node in CD and SR does not make any critical change with network performance.



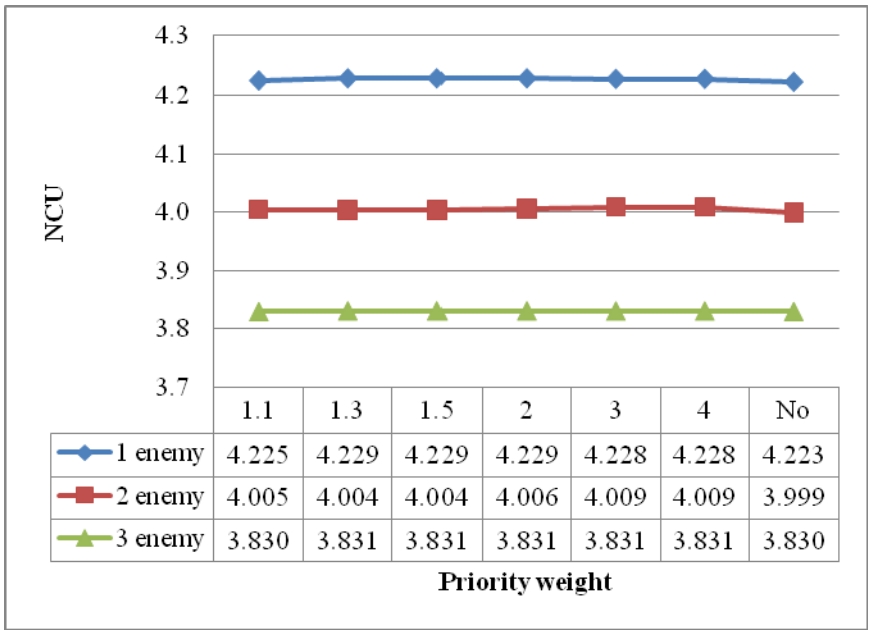
	No	1.1	1.3	1.5	2	3	4
1 enemy	7.314	7.329	7.313	7.313	7.302	7.326	7.332
2 enemy	7.213	7.250	7.228	7.228	7.201	7.236	7.186
3 enemy	7.226	7.183	7.189	7.189	7.196	7.202	7.223

Figure 6-21 NCU changes by priority node weights (CD)



	No	1.1	1.3	1.5	2	3	4
1 enemy	0.780	0.782	0.781	0.781	0.781	0.777	0.777
2 enemy	0.733	0.734	0.735	0.735	0.735	0.733	0.733
3 enemy	0.743	0.744	0.744	0.744	0.744	0.743	0.743

Figure 6-22 MCR changes by priority node weights (SR)



	1.1	1.3	1.5	2	3	4	No
1 enemy	4.225	4.229	4.229	4.229	4.228	4.228	4.223
2 enemy	4.005	4.004	4.004	4.006	4.009	4.009	3.999
3 enemy	3.830	3.831	3.831	3.831	3.831	3.831	3.830

Figure 6-23 NCU changes by priority node weights (SR)

Until now, we have tested the effects of metrics employed in this study based on different mobility models. In summary, PAL and messenger have improved network performance for all mobility patterns even though there exist some differences in effect according to the randomess level. The effect of PAL and messenger is greater with a low random mobility model. On the other hand, the priority node metric is effective with a high random mobility model like the random waypoint model

6.4.3.3 Efficiency of employed algorithm

As discussed before, in this section we compare the efficiency of hop-count based routing with the shortest distance based routing approach in terms of the number of required hops for a user node connection.

Table 6-4 shows the results. Considering the number of hops used for a user connection, the hop-count based algorithm is better than the shortest distance based algorithm for the

experiments with all mobility models used. The efficiency difference between hop-count and shortest distance based routing is about 10.4% with RW, 24.4% with CD and 4.01% with SR. The efficiency is the largest in the CD and the smallest in the SR. As we know, the small effect with SR is related to the randomness of mobility as mentioned earlier.

Table 6-4 Efficiency of algorithms as measured by number of hops per connected user

Mobility	Enemy	Hop-count	Shortest distance	Difference	p-value
RW	0	2.698	2.871	0.173	0.000
	1	2.692	3.018	0.326	0.000
	2	2.718	3.103	0.385	0.000
	3	2.785	3.163	0.378	0.000
	Average	2.723	3.039	0.316 (10.4%)	
CD	0	4.692	5.110	0.418	0.000
	1	4.664	6.648	1.984	0.000
	2	4.665	6.490	1.825	0.000
	3	4.554	6.261	1.707	0.000
	Average	4.644	6.127	1.484 (24.2%)	
SR	0	3.117	3.133	0.016	0.000
	1	3.093	3.175	0.082	0.000
	2	3.113	3.313	0.2	0.000
	3	3.093	3.315	0.222	0.000
	Average	3.104	3.234	0.13 (4.01%)	

The 95% CI plots in Figure 6-24 show this result visually and suggest that the hop-count based routing is much more efficient than the shortest distance based routing.

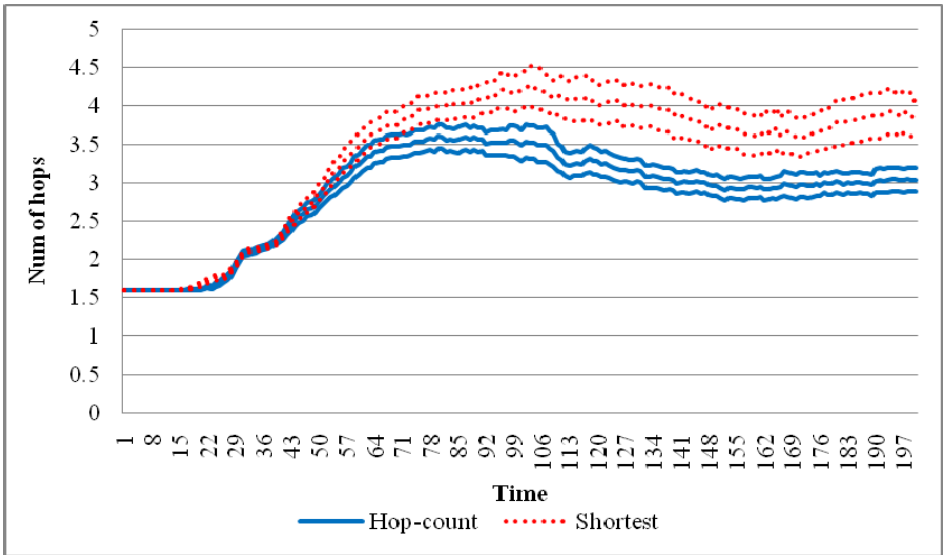


Figure 6-24 Comparison of number of hops used for a user connection (RW, 2E)

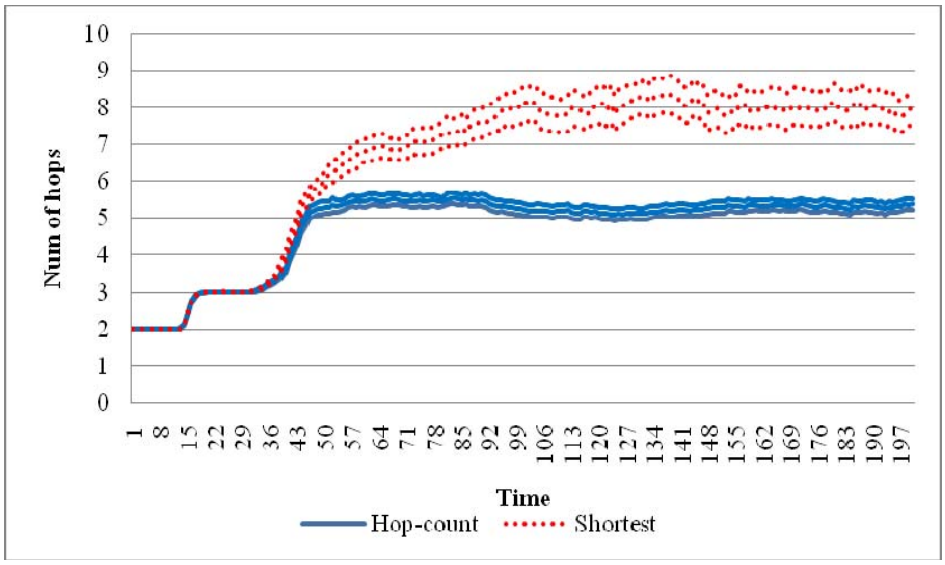


Figure 6-25 Comparison of number of hops used for a user connection (CD, 2E)

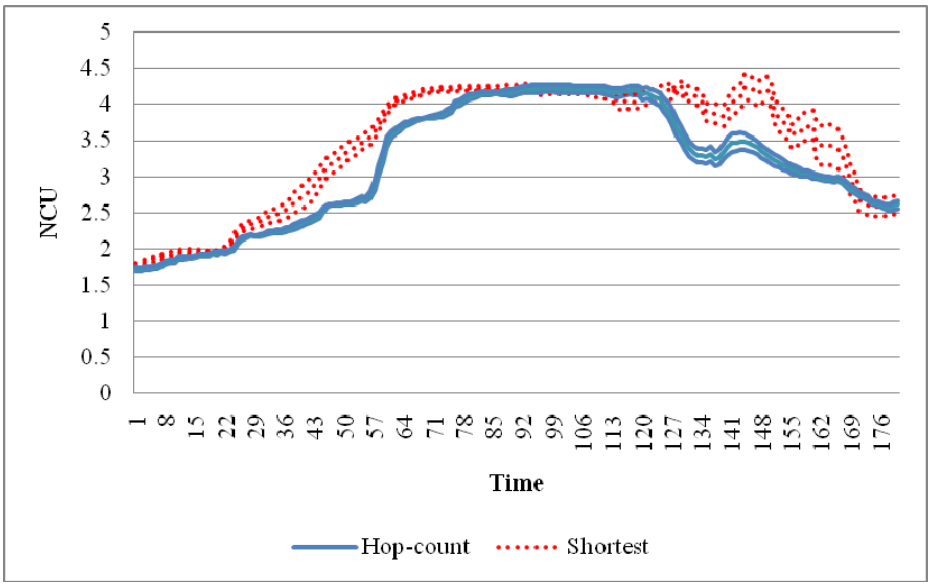


Figure 6-26 Comparison of number of hops used for a user connection (SR, 2E)

As shown in Figure 6-26, the efficiency gap between the two routing approaches is a little smaller in SR than in other mobility models. This is also related to the movement characteristics and randomness of the mobility model. For a few time ranges, the shortest distance based routing looks more efficient. This is because network performance by the hop-count based routing is higher than the shortest distance based routing and the connection at the moment requires many hops.

We have tested the effect of metrics using the small sized problems. These will be further tested with medium and large sized problems using random waypoint in the next section. By this extended test, the effects of metrics can be verified.

6.5 Effect of metrics for medium and large sized problem with RW

The networks for the experiments in this study are tested over the same size of operational area. The difference among those is the number of network nodes or enemies. So,

network density is increased by the network size. SR and CD are not considered in this section because of computations involved.

6.5.1 PAL effect

PAL is also very effective for both medium and large size problems as shown in Table 6-5. Paired-T test p-values in the right column verify the effect of PAL. For test scenarios, about 8~10% improvement is obtained by PAL.

Table 6-5 PAL effect with medium and large problem

Mobility	Num Enemy	No PAL		PAL		p-value
		Avg NCU	*Avg Jamming*	*Avg NCU*	*Avg Jamming*	
Medium	0	8.279	-	9.156	-	0.000
	2	8.041	1.613	8.863	1.363	0.000
	4	7.875	3.053	8.756	1.994	0.00
	Avg	8.065	2.333	8.925	1.679	
Large	0	17.876	-	19.309	-	0.000
	2	17.536	5.147	18.873	4.422	0.000
	4	17.116	8.457	18.699	6.710	0.000
	Avg	17.509	6.802	18.960	5.566	

The 95% CI plots of the PAL effect in Figure 6-27 and Figure 6-28 indicate the definite difference between the PAL used and No PAL cases. We replicated only 20 times for each scenario because of the computational effort involved. So, if the number of replications is

increased, the confidence interval of each group would be narrowed, and the difference between two cases in Figure 6-27 would be clearer.

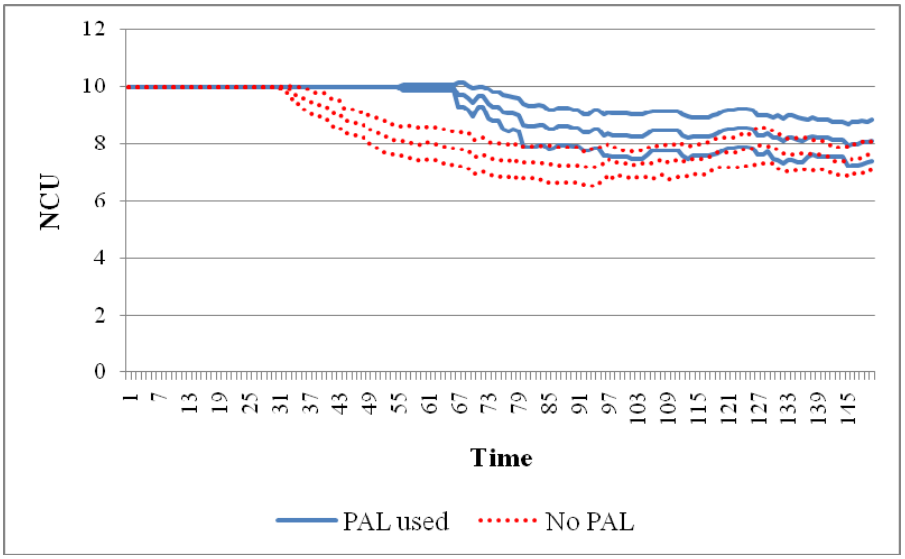


Figure 6-27 Comparison of PAL and No PAL (Medium, no enemy)

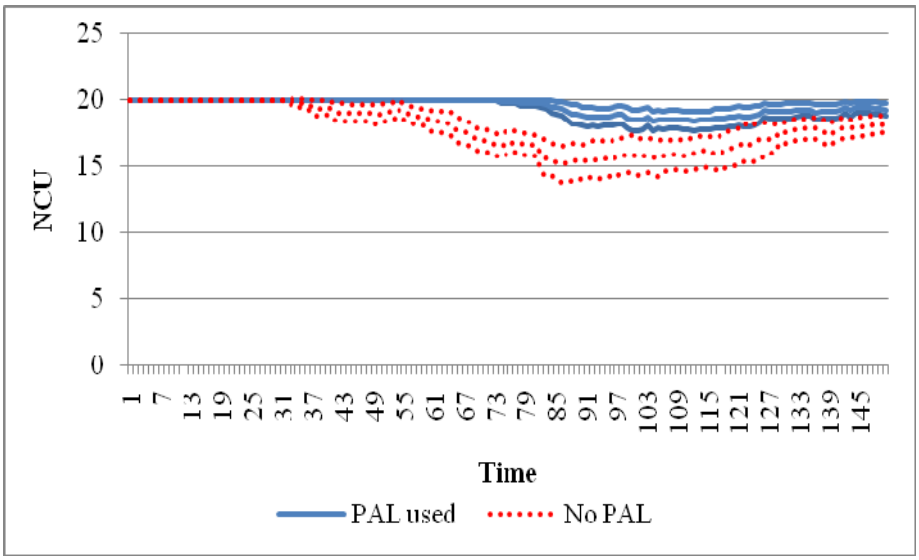


Figure 6-28 Comparison of PAL and No PAL (Large, no enemy)

6.5.2 Efficiency of employed algorithm

By looking at the results shown in the table and figures below, the hop-count based routing algorithm requires a smaller number of hops to connect a user node with the control node. For most of simulation time span, it is better than the shortest distance based algorithm. But, this is reversed for a few time ranges as shown in Figure 6-29 and Figure 6-30. The reason is the same as discussed in Section 6.4.3.3.

Table 6-6 Efficiency (# hops/connected user) of algorithms with medium and large problems

Mobility	Hop-count	Shortest distance	Difference	p-value
Medium	3.738	4.057	0.319 (7.9%)	0.000
Large	4.217	4.407	0.19 (4.3%)	0.000

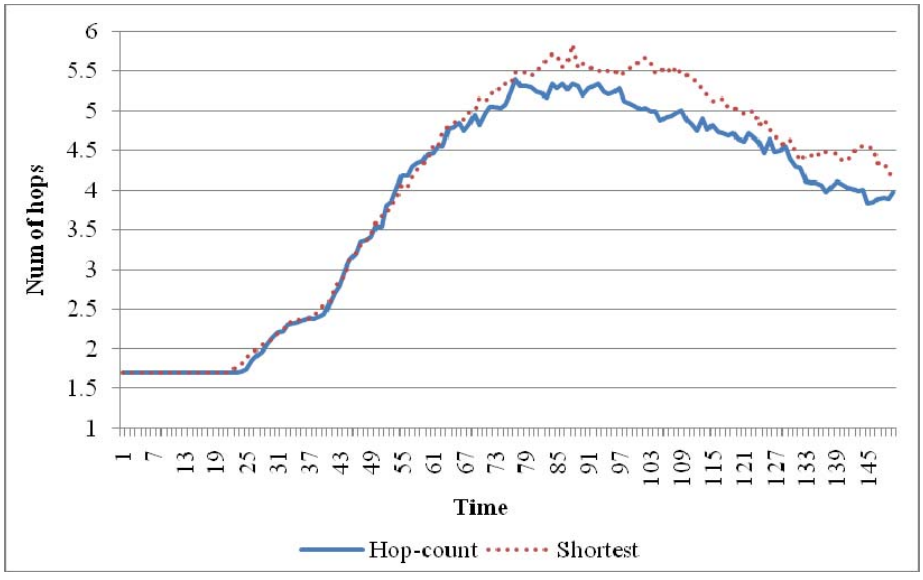


Figure 6-29 Comparison of number of hops used for a user connection (Medium)

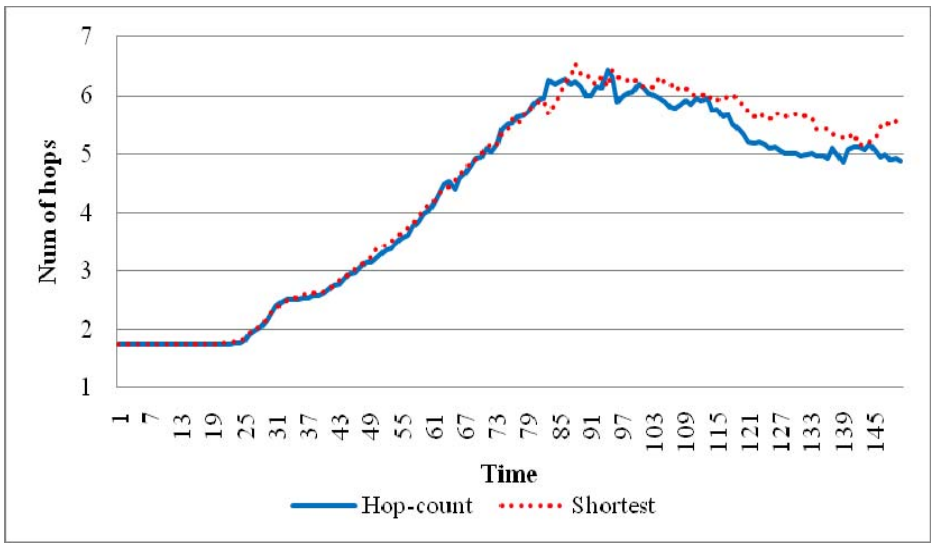


Figure 6-30 Comparison of number of hops used for a user connection (Large)

6.5.3 Messenger effect

The messenger effect shows almost the same pattern by problem size and number of enemies. Network performance in medium sized problems is improved by messenger, but its improvements are limited by the operation time of messengers. The best messenger is 80 time step for the two enemy case and 40 time step for the four enemy case. After these operation times of messenger, network performance is not improved further. Messenger operation time is shorter in the four enemy case than in the two enemy case. This is related to the number of enemies in the operation area. That is, the randomness of network is increased by more enemy numbers and it increases the time required for reconnecting the disconnected users from the network. Consequently, network performance is degraded by wasting agents. Also, reconnecting a disconnected user under a combat situation may be impossible because of its destruction by enemy. So, the messenger operation time is shortened by increasing the number of enemies.

However, if the number of agents in the network is enough to cover the effect of increased enemies, the operation time would not be affected. As shown in Figure 6-31 and Figure

6-32, the messenger operation time for the four enemy case is almost same as the two enemy case. The average percentage of users reconnected by messengers is about 29.1%. It is higher than in the small sized problem since it has more extra agent capability.

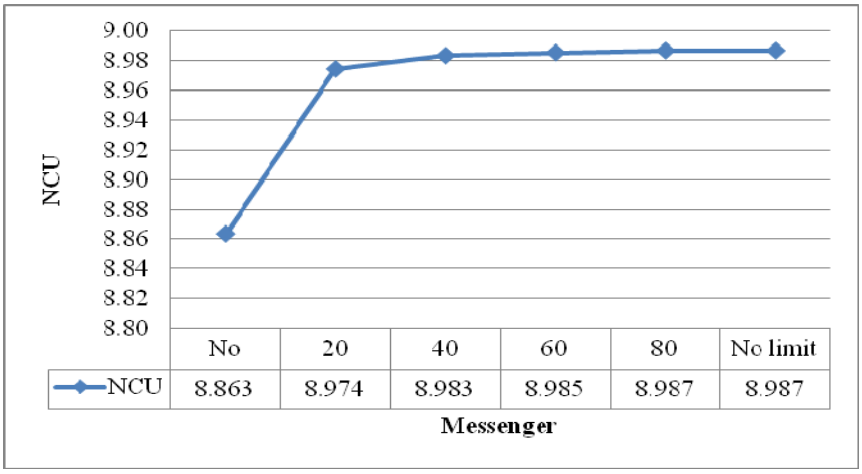


Figure 6-31Messenger effect (Medium, 2E)

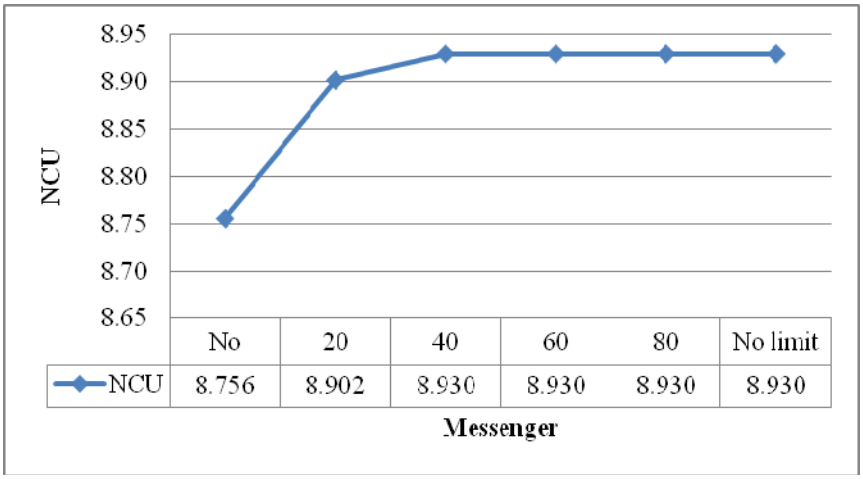


Figure 6-32 Messenger effect (Medium, 4E)

On the other hand, the number of network nodes in the large sized problem is twice that of the medium sized problem, but both problems use the same number of enemies and size of the

problem space. As a result, the only difference between them is network density. That is, the density of the large sized problem is much more than that of the medium sized problem.

As shown in Figures 6-33 and 6-34, the network performance improvement by 20 messenger duration is small but notably different from other time values in the figure. So, 20 is definitely the best messenger operation time for both scenarios. This improvement is also very small compared with the one made in the medium sized problems. The shorter messenger and small improvement of network performance are related to the high density in large sized problem.

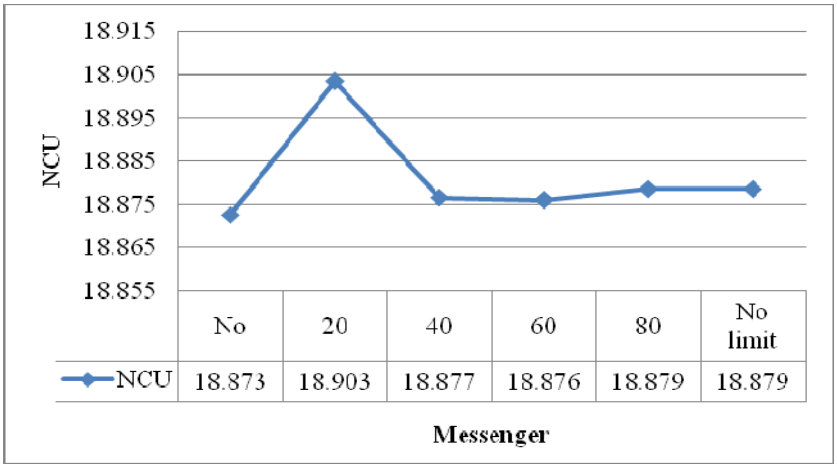


Figure 6-33 Messenger effect (Large, 2E)

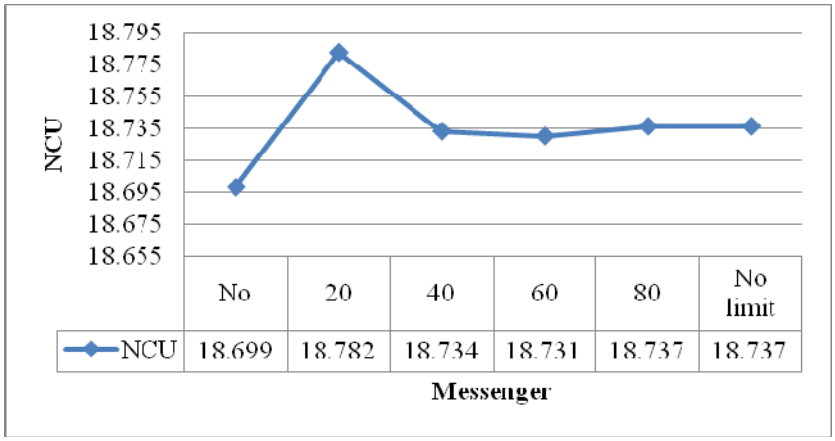


Figure 6-34 Messenger effect (Large, 4E)

6.5.4 Priority node effect

In the small sized problem the best priority weight was 1.1 considering the tradeoff with network performance. MCR in the small sized problem could be improved by a small weight, but it requires higher weights for both medium and large problems as shown in Figures 6-35 through 6-38.

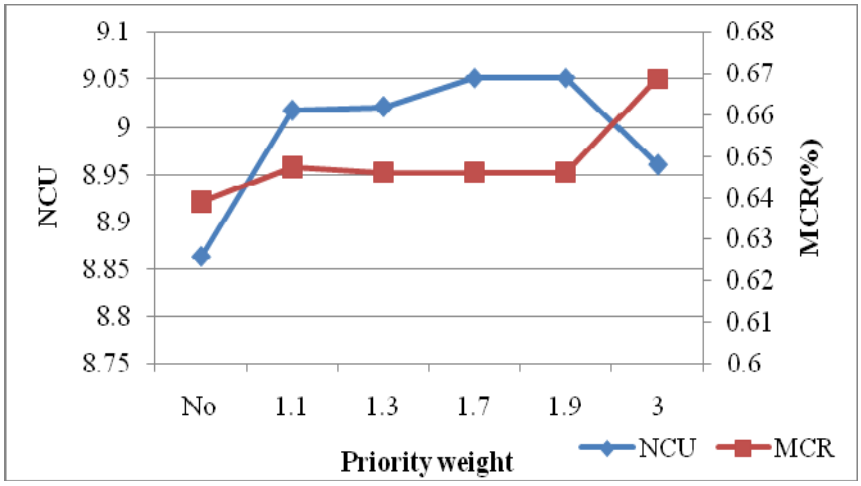


Figure 6-35 Priority node effect (Medium, 2E)

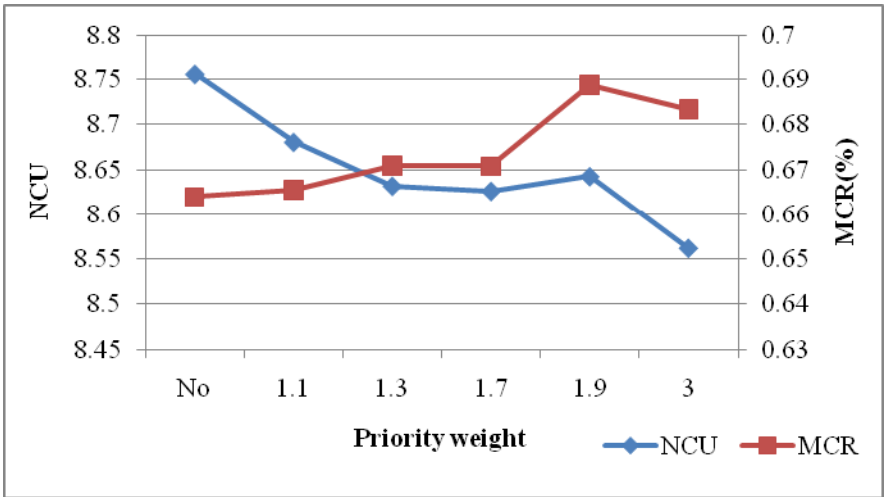


Figure 6-36 Priority node effect (Medium, 4E)

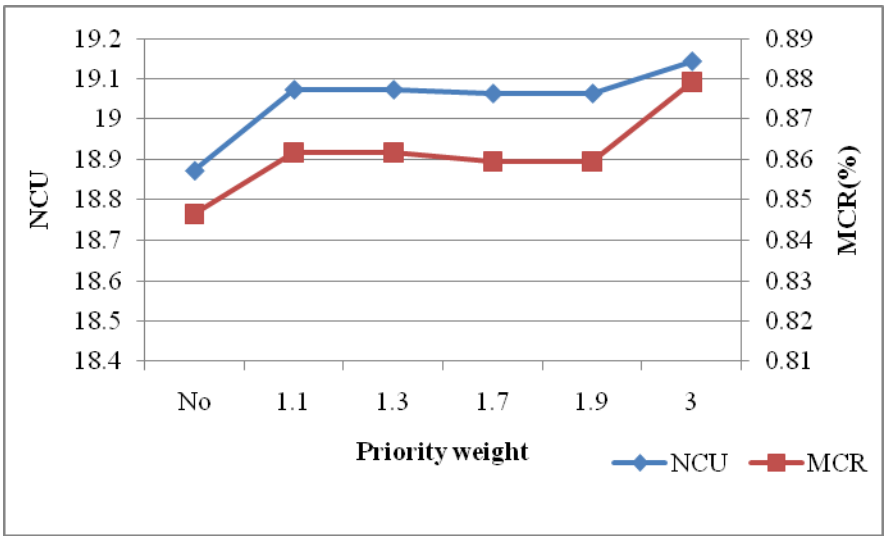


Figure 6-37 Priority node effect (Large, 2E)

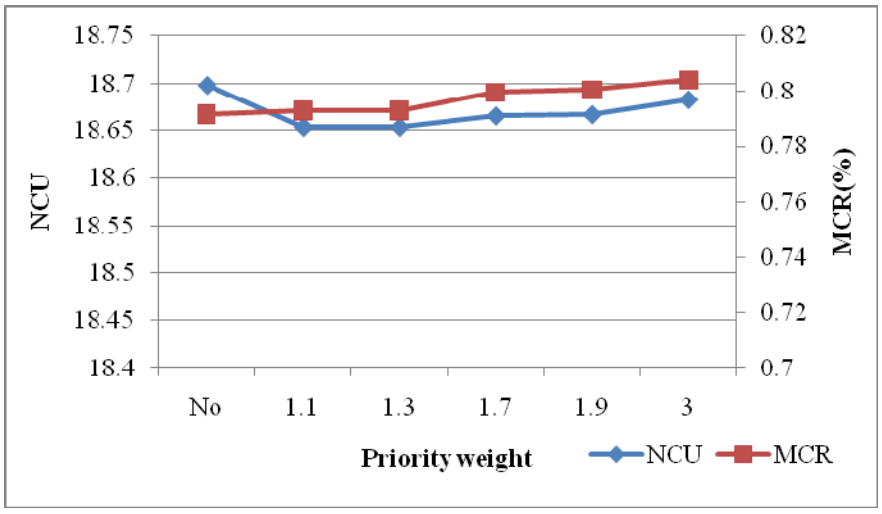


Figure 6-38 Priority node effect (Large, 4E)

The above figures represent the effect of priority node in enemy scenarios. First, MCR is improved by increasing the priority weight regardless of the problem size and the number of enemies. However, NCU under increased number of enemy cases for both problem sizes is

decreased by the higher priority weights as shown in the above figures. That is, although the agents in the two enemy case have to support the priority nodes first, NCU is not worsened since it still has some extra capability to serve other user nodes. On the other hand, NCU is degraded in the four enemy case because of the shortage of agents to serve other user nodes.

However, the effect of priority node is very small with the large problem with four enemies as shown in Figure 6-38. Both NCU and MCR are not significantly changed by weighing the priority nodes. From this fact, we guess that the effect of priority node in enemy scenarios is related to the density and the number of enemy of a network.

Based on the metrics verification results with different sized problems and user mobility models we conclude the effect of agent behaviors as followings:

- PAL is effective for all sizes of problem and all user node mobility models. It is most effective with low randomness mobility models.
- Messenger is sensitive to the network density. The effect of messenger becomes smaller and the operation time is shortened as network density increases.
- Priority node is sensitive to both the number of enemies and network density. NCU is degraded by increasing the weights and the number of enemies. MCR with few enemies continues to increase by increasing the weights. However, Priority node is not effective with high density networks.

6.6 Cost benefit analysis

In previous sections we have verified the effectiveness of devised approaches for military MANETs. From the military operation aspect, the most efficient number of agents is an important consideration to establish a sucessful operation plan since it is impossible to operate

enough agents every time. Therefore we have conducted experiments to choose the best number of agents under various scenarios. The results obtained from this analysis can be used by commanding officers or operation planners for decision making during the operation planning step.

We generated three different sizes of problem for this experiment. RW is used for the three different sized scenarios. This was chosen because it enable us to use all approaches devised in this study and is suitable for combat scenarios. However, CD is used only for the medium size and SR only for the small size because of computation time. In addtion, for SR mobility, the physical destruction of network resources by combat is not considered since we assume that no combat sitaution is expected during a search and rescue operation.

First, for all combat scenarios (small, medium, large) an appropriate messenger operation time will be found. Then, the most efficient number of agents is assumed by the number of agents to a 95% actual user node connectivity goal is identified. This efficient number is determined for both the no enemy and the enemy scenarios and compared.

6.6.1 Cost benefit analysis with RW

The three different sized scenarios are tested using RW in this section and eight enemies are used for the large size scenario to represent an acute combat situation as mentioned above.

6.6.1.1 Combat scenario 1 (Small size)

There is almost no limitation for messenger time in the small size of networks. However, it is different for real militray combat operations since some network nodes could be killed by the enemy. That is, our expectation is that the messenger effect would be smaller or the operation

time be shorter under the kill environment. The messenger time for combat scenario 1 is about 60 as shown in Figure 6-39. Network performance is improved by 3.6% and it is not changed by any other longer messenger time.

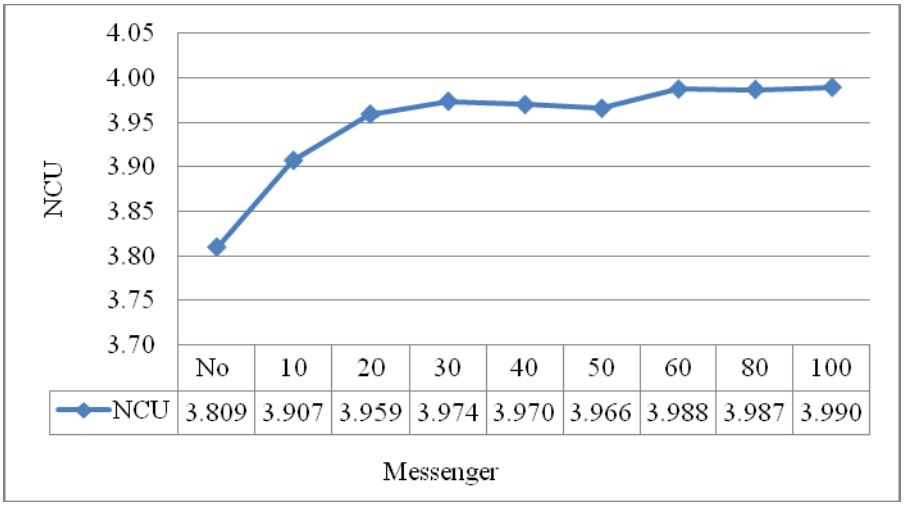


Figure 6-39 Messenger effect (S1)

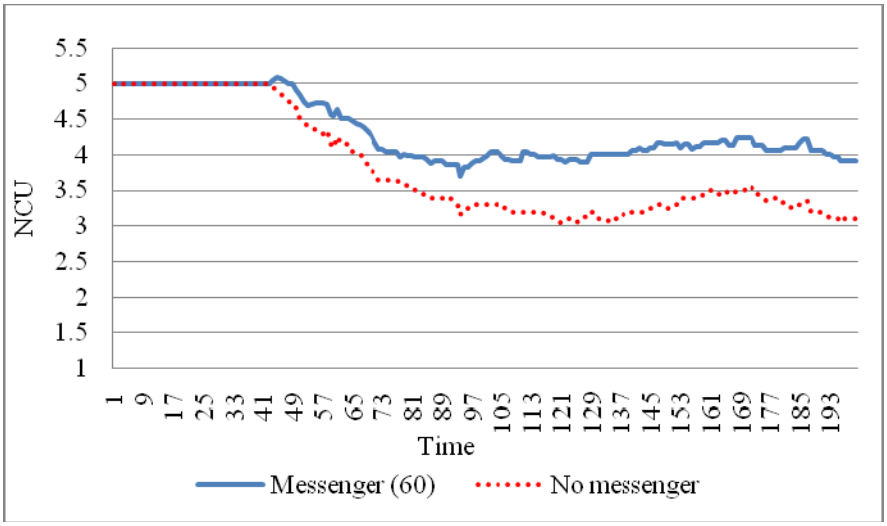


Figure 6-40 Comparison of network performance by messenger (S1)

Figure 6-40 clearly shows the effect of messenger in combat scenario 1. Network performance with messenger is always better than with no messenger case. So, we will use messenger for 60 time steps for the experiments to find the most efficient number of agents. Each priority node is weighted by 1.1 according to the experiments shown earlier.

95% network connectivity in scenario 1 indicates 4.75 network node connections with the control node if no users are killed. However, some of network nodes could be killed by combat with enemies during the operation. So, the 4.75 target connection may be impossible to accomplish under a combat environment. As a result, actual connectivity (%) is required to measure network performance. If no enemy were in the combat area, fewer agents would be required to reach the target connctivity level since network connectivy is not reduced by jamming. However, it is true only compared with the enemy scenarios without the kill environment. That is, the number of agents required in the enemy case may be smaller than the no enemy case by the actual connectivity. Figure 6-41 represents the result under the no enemy condition. 11 agents (96.4%) are required to meet the target connectivity in this case and network connectivity continues to be improved as more agent nodes are employed.

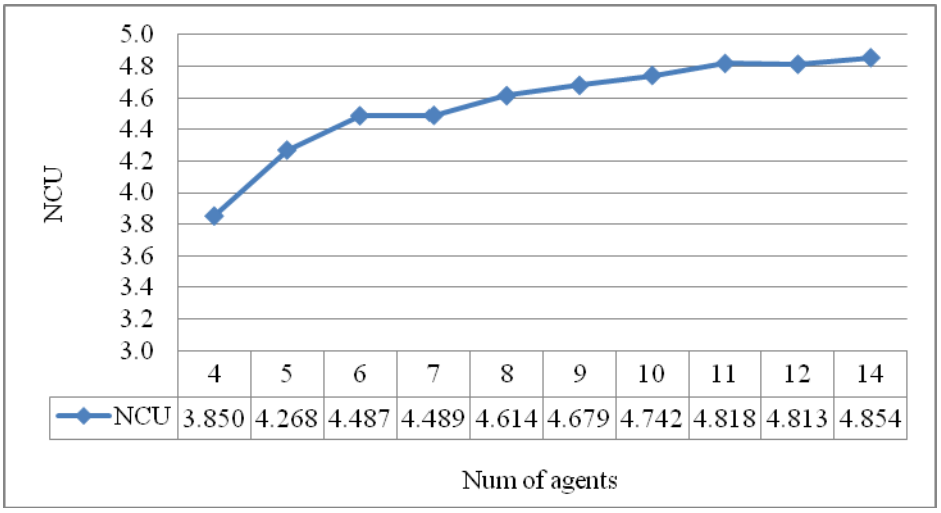


Figure 6-41 Efficient number of agents in the no enemy case (S1)

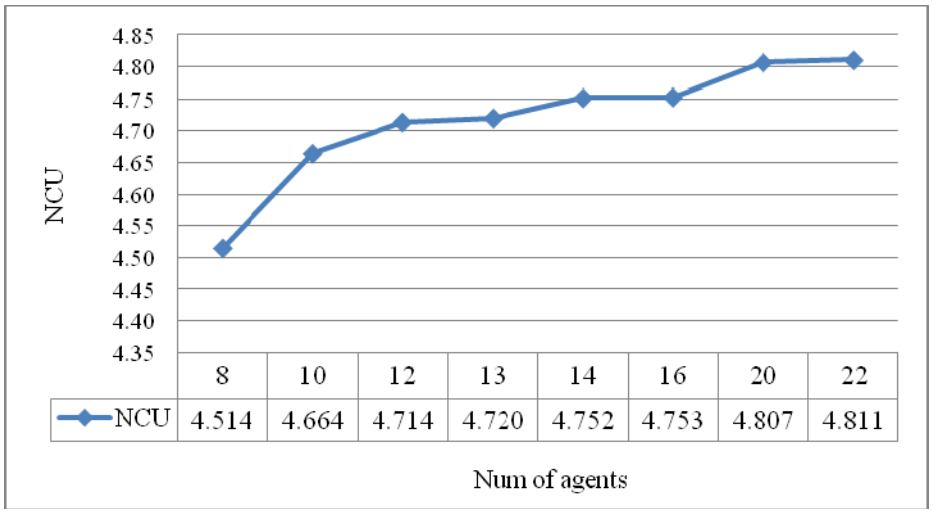


Figure 6-42 Efficient number of agents in the enemy case (S1)

As shown in Figure 6-42, 14 agents are required under the enemy case. However, the actual connectivity with 10 agents is about 95.6%, 96.8% with 12 agents this and 99.3% with 13 agents. So, under the enemy condition, the target connectivity can be accomplished using only 10 agents.

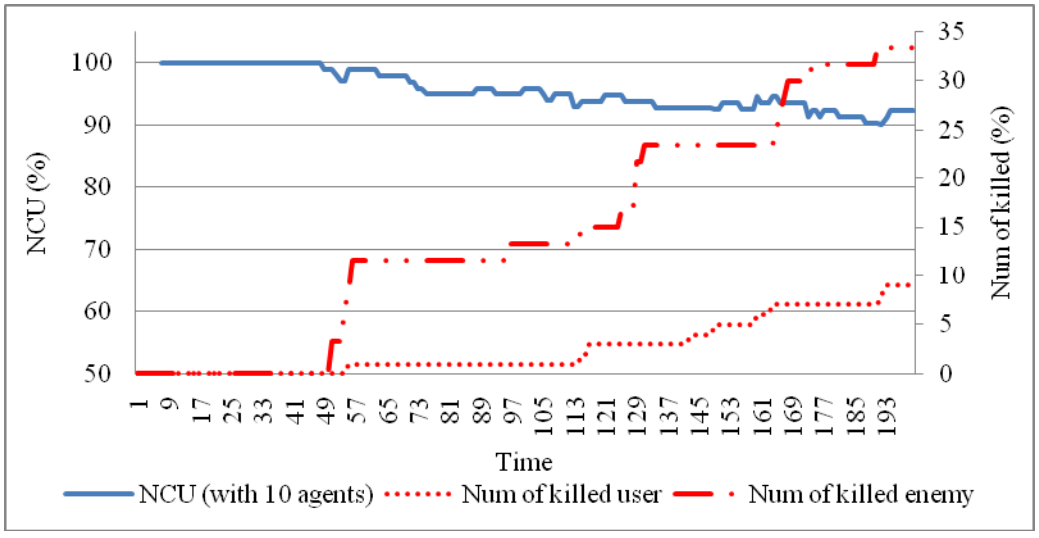


Figure 6-43 Network performance and number of killed resources (S1)

In Figure 6-43, the average number of killed users and enmies are 0.45 and 1, respectively. But no agent node is killed because the agent nodes follow the users and the locations of enemies are usually identified before agents enter the kill zone. So, the possibility of an agent being killed is relatively low in this scenario.

6.6.1.2 Combat scenario 2 (Medium size)

In the combat scenario 2, more network nodes and enemies are included, thus it is more complicated than scenario 1. As we do in combat scenario 1, the messenger time for this scenario will be found first before performing further experiments.

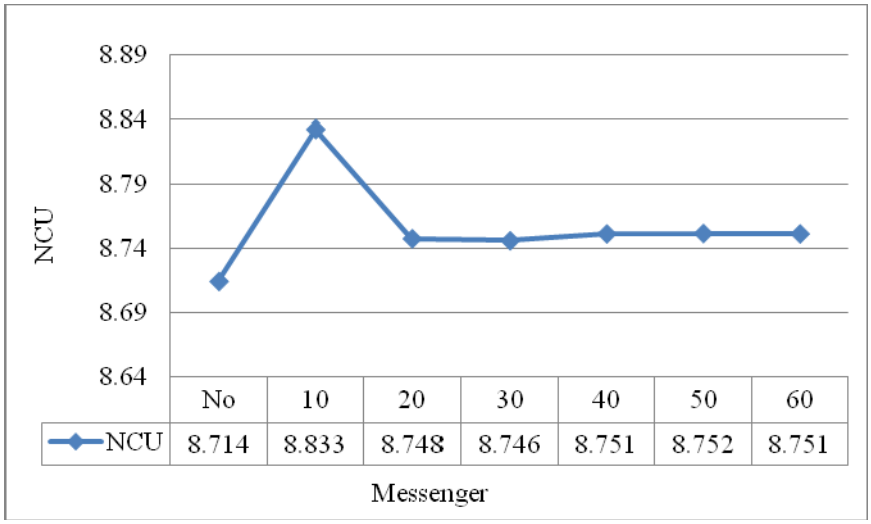


Figure 6-44 Messenger effect (S2)

For combat scenario 2, the best messenger time is 10 as shown in Figure 6-44. This is much shorter than in scenario 1. The improvement by messenger is also smaller than scenario 1. The difference between the no messenger and the messenger (10) scenarios is only 1.19%. From

Figure 6-45, network performance with messenger (10) is equal to or better than the no messenger scenario through the simulation time span, but the gap is not big.

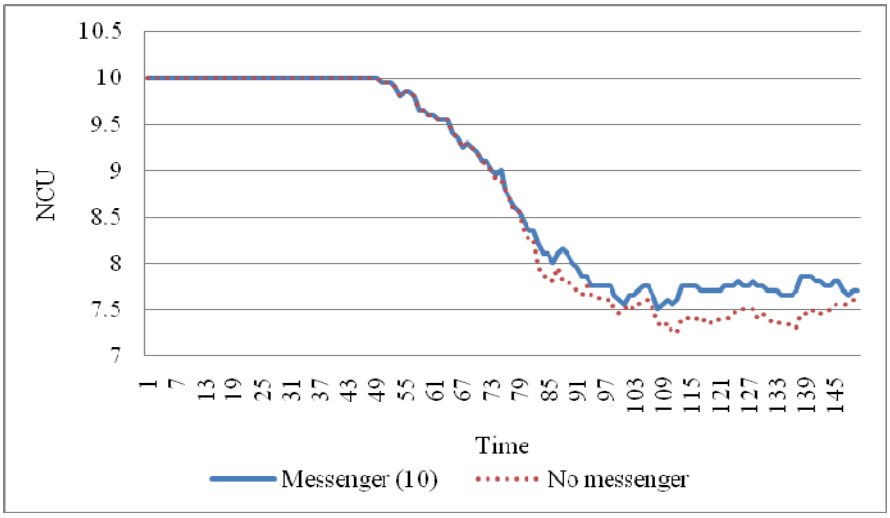


Figure 6-45 Comparison of network performance by messenger (S2)

The minimum required number of agents meeting the target connectivity under the no enemy condition is 10 and network performance can be improved more by adding more agents as in scenario 1 as shown Figure 6-46.

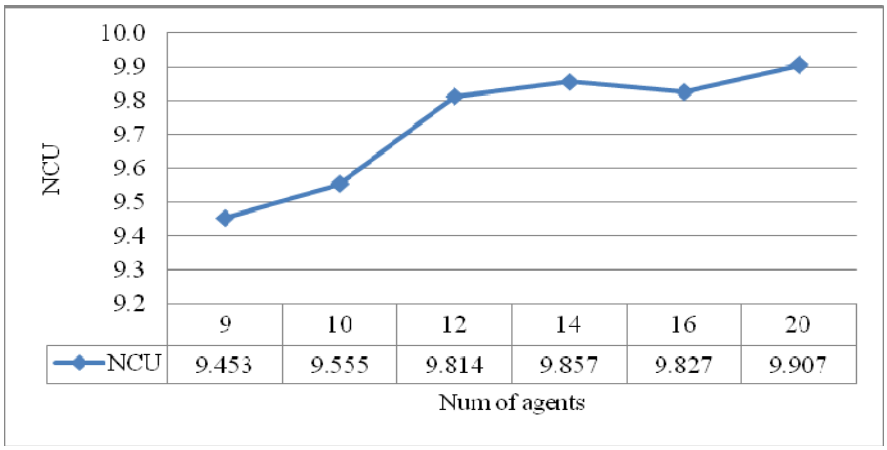


Figure 6-46 Efficient number of agents in the no enemy case (S2)

For the enemy case, the efficient number of agents is 14 and the actual connectivity is 95.1%. The difference between the no enemy and enemy scenarios is a little larger than in scenario 1 and we think that it is related to the interaction with the enemies such as jamming and combat since the numbers of enemies and network nodes for scenario 2 are twice that of scenario 1.

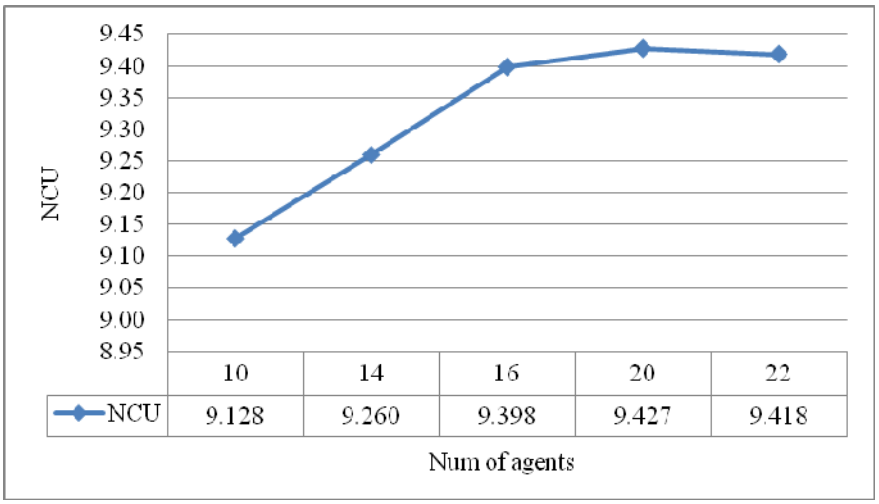


Figure 6-47 Efficient number of agents in the enemy case (S2)

By adding more agents, network connectivity continues to be improved to certain limit, possible network connectivy considered by current network state, as shown in Figure 6-47.

Figure 6-48 shows the relation between NCU and the number of killed users over time. Under the combat 2 condition, about 0.75 user nodes and 1.15 enemies are killed. NCU is reduced as the number of killed users is inceased since some of users are killed by enemies.

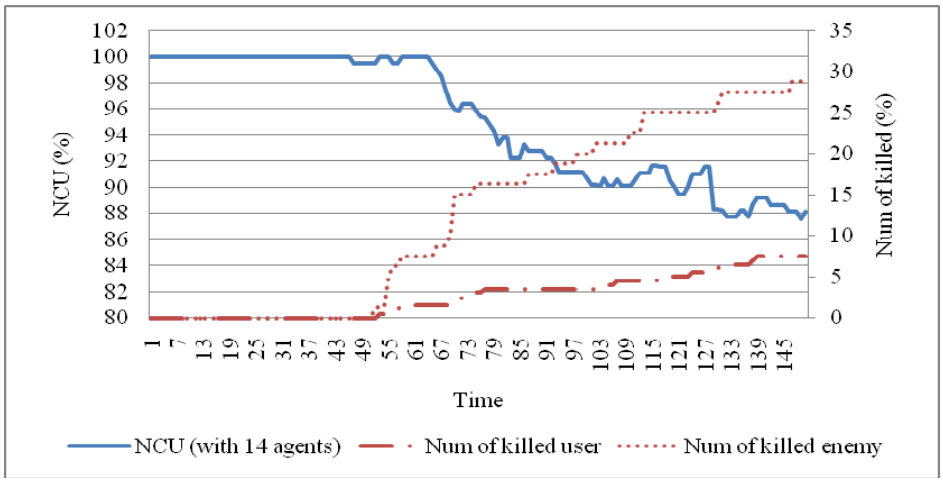


Figure 6-48 Network performance and number of killed resources (S2)

The movements of network nodes in combat scenario 2 are represented in Figure 6-49. Currently, no network nodes and enemies are killed. There are 4 enemies which have jamming (red circle) and kill effect zones (blue circle). If network nodes enter the jamming zone, they start to lose their communication capability because of the jamming effect. Most MANET nodes are inside a jamming zone at the moment. If any node enters a kill zone, it fights with the enemy; the combat is simulated by the kill probability and the combat power of network nodes and enemies.

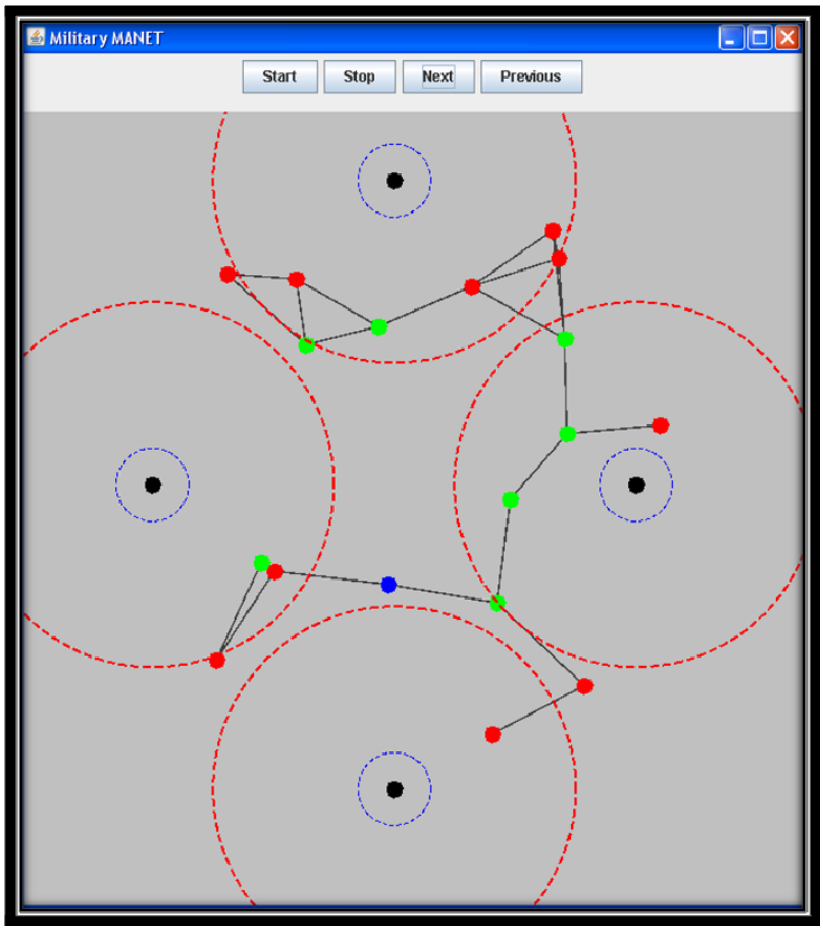


Figure 6-49 Animation picture of combat scenario 2
(Red: user, Green: agent, Blue: control, Black: enemy)

6.6.1.3 Combat scenario 3 (Large size)

In this scenario, 36 network nodes are used and the operation area size is the same as in scenarios 1 and 2. So, network density is relatively higher than previous scenarios and user nodes in this network are expected to help improve the network connection. So, 16 agents in the default network size of scenario 3 may be enough to serve 20 user nodes without adding more agent nodes. The experiment results in Figure 6-50 confirm this expectation.

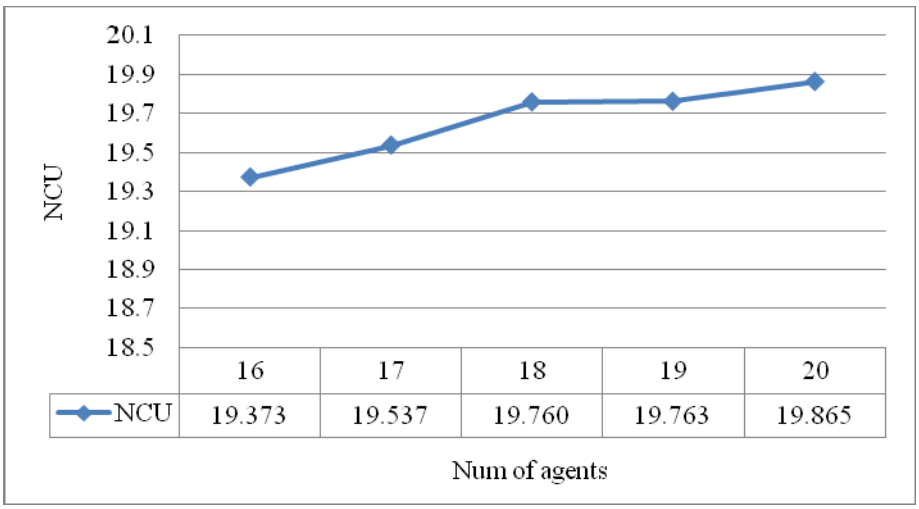


Figure 6-50 Efficient number of agents in the no enemy case (S3)

Network connectivity of this default scenario 3 (no enemy) is already beyond the target performance by 16 agents as seen in Figure 6-50. To simulate an acute combat situation, 8 enemies are used in scenario 3, so more network nodes and enemies would be destroyed by the increased chance of combat.

First, we will go over the effect of messenger time in this high density, combat operation condition. As shown in Figure 6-51 network performance is not improved after it reaches the best at messenger time 50.

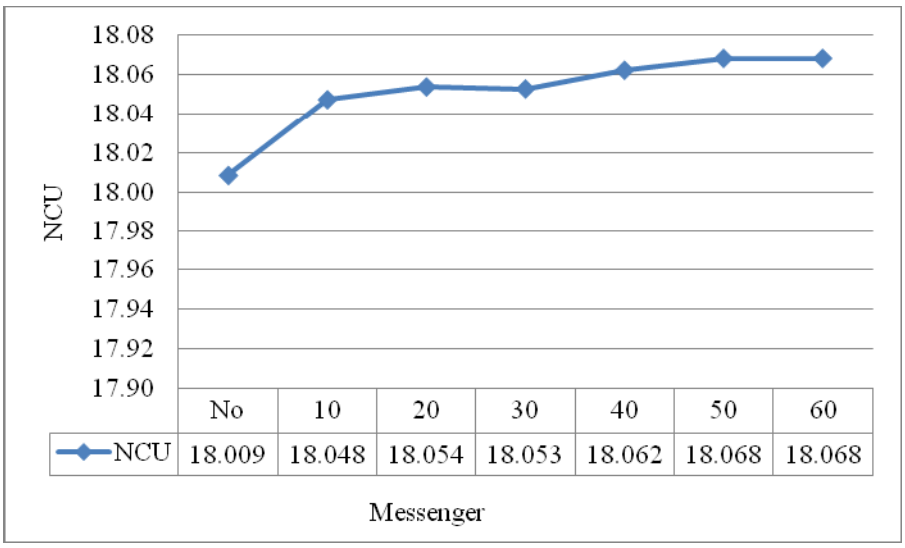


Figure 6-51 Messenger effect (S3)

Network performance by messenger is improved by 3.6% with scenario 1 and 1.19% with scenario 2 as discussed previously. But only 0.3% of network connection is increased by messengers in scenario 3. As we already discussed the messenger effect with a high density network in Section 6.5.3, the messenger effect is also very small in this large sized problem including the kill event by combat.

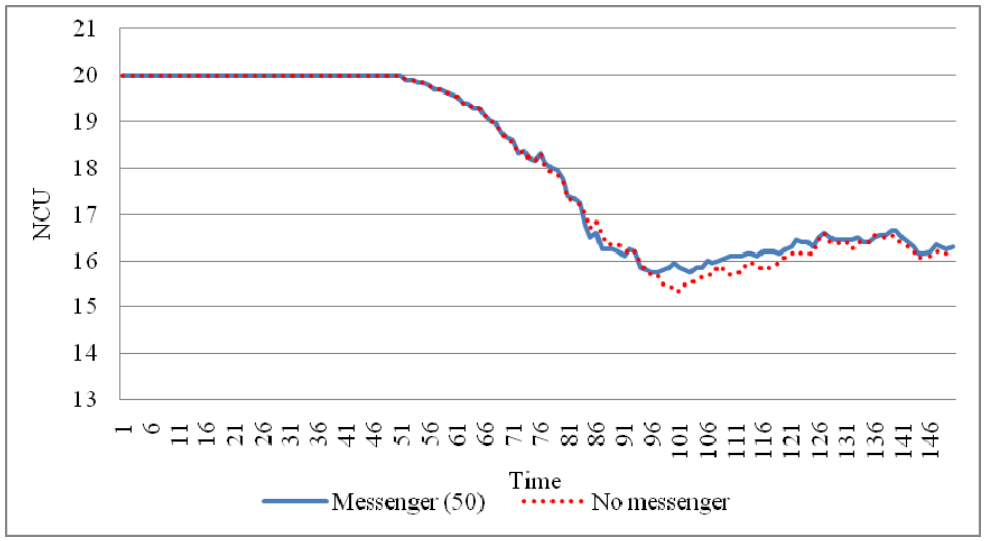


Figure 6-52 Comparison of network performance by messenger (S3)

The average NCU plot in above Figure 6-52 shows a small effect of messenger in scenario 3.

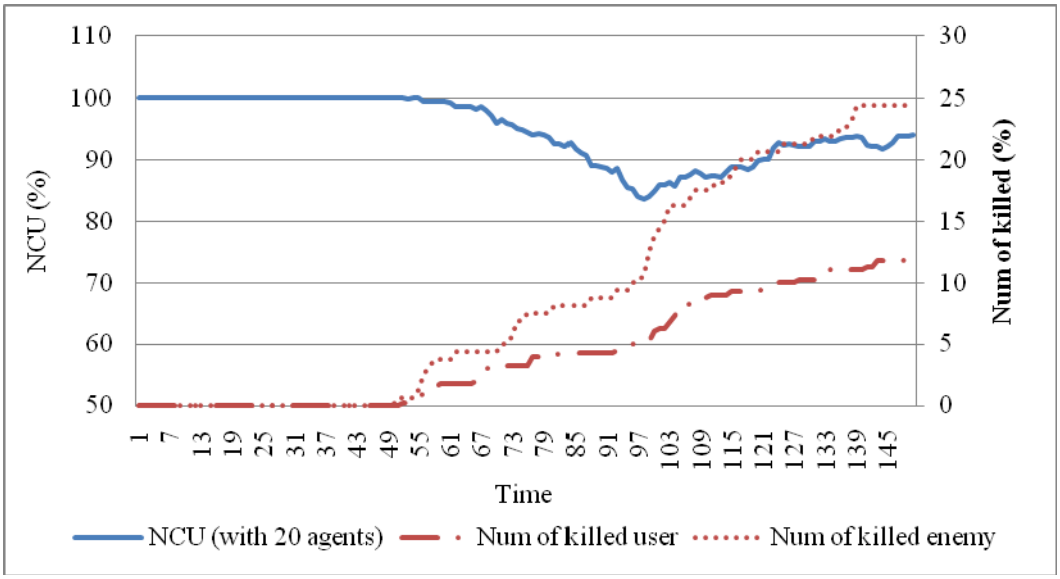


Figure 6-53 Network performance and number of killed resources (S3)

The combat between users and enemies is much more severe than in scenario 1 and scenario 2. The average number of killed users and enemies is 2.4 and 1.95, respectively, and the highest number of killed users is 5 during the simulation. Figure 6-53 shows network performance, percentage of killed users and percentage of killed enemies over time. Network performance starts to go down along with users' destruction but after time step 100 experiences no further deterioration. Under this circumstance, as shown in Figure 6-54 below, deploying more agents does not help improve network performance. The actual user node connectivity is between 94.3% and 94.9% by the number of agents more than 16 as shown in Figure 6-54. This actual connectivity level could be accomplished by 14 agents. As a result, the number of agents in the scenario 3 does not matter.

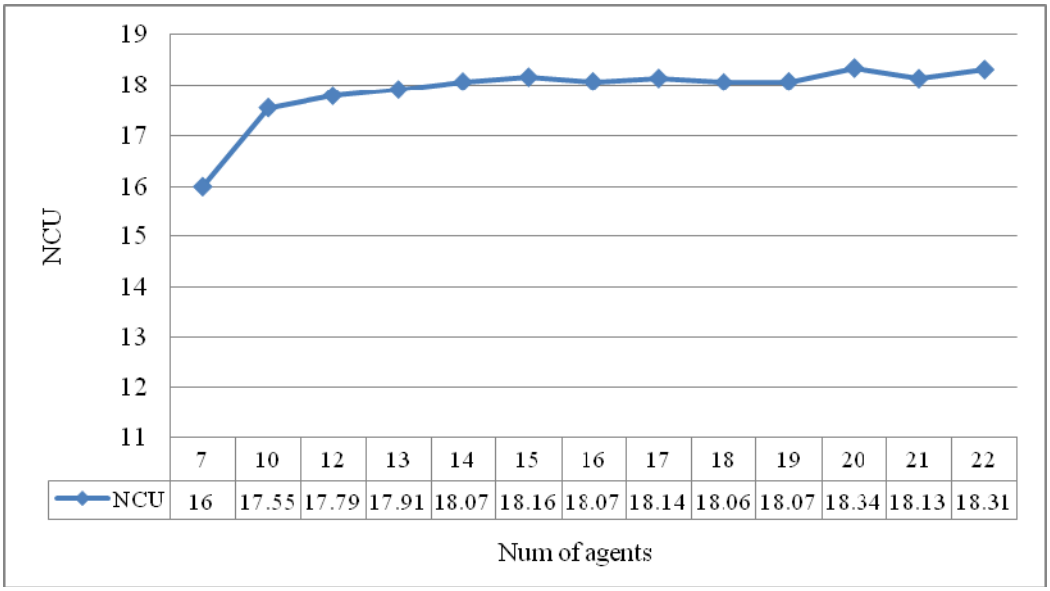


Figure 6-54 Efficient number of agents in the enemy case (S3)

6.6.2 Cost benefit analysis with CD

The cost benefit analysis with CD is performed only for medium size problems. There are four patrol boxes in this test scenario and an enemy is assigned to each patrol box. As shown in Figure 6-55, network performance using messenger agents improves regardless of messenger duration. The best messenger operation time among those tested is 10. The number of connected user nodes using the best operation time increases by 2.64%.

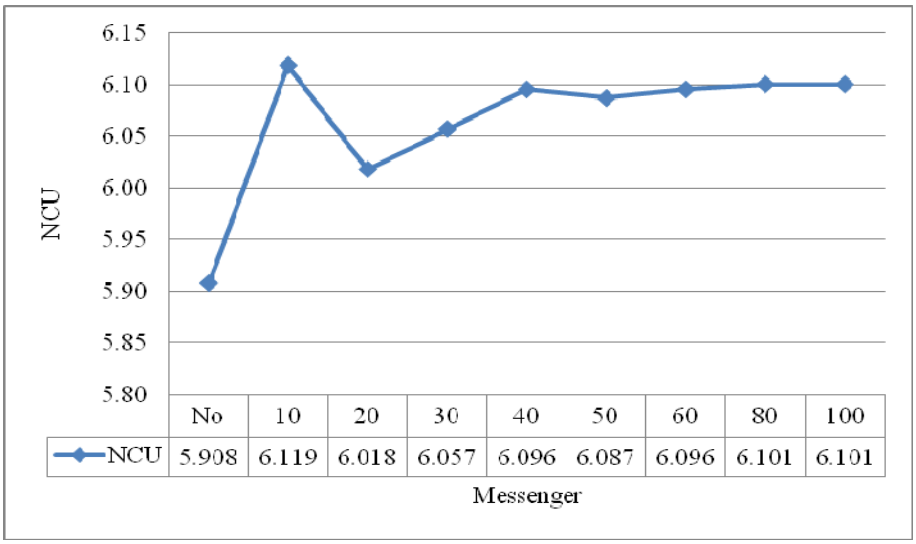


Figure 6-55 Messenger effect in the combat scenario with CD

The performance of messenger case maintains dominates the no messenger case throughout the simulation time span as shown in Figure 6-56.

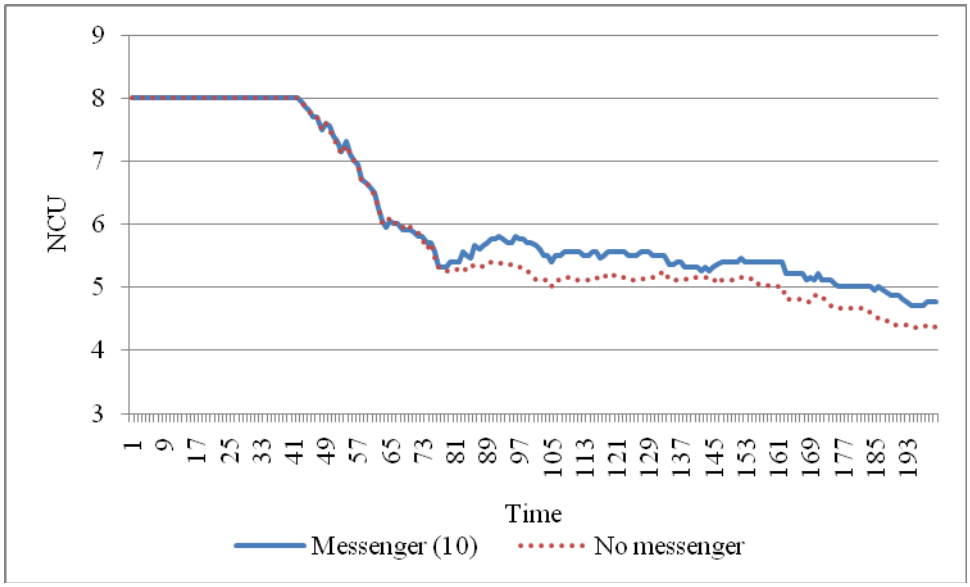


Figure 6-56 Comparison of network performance by messenger in the combat scenario with CD

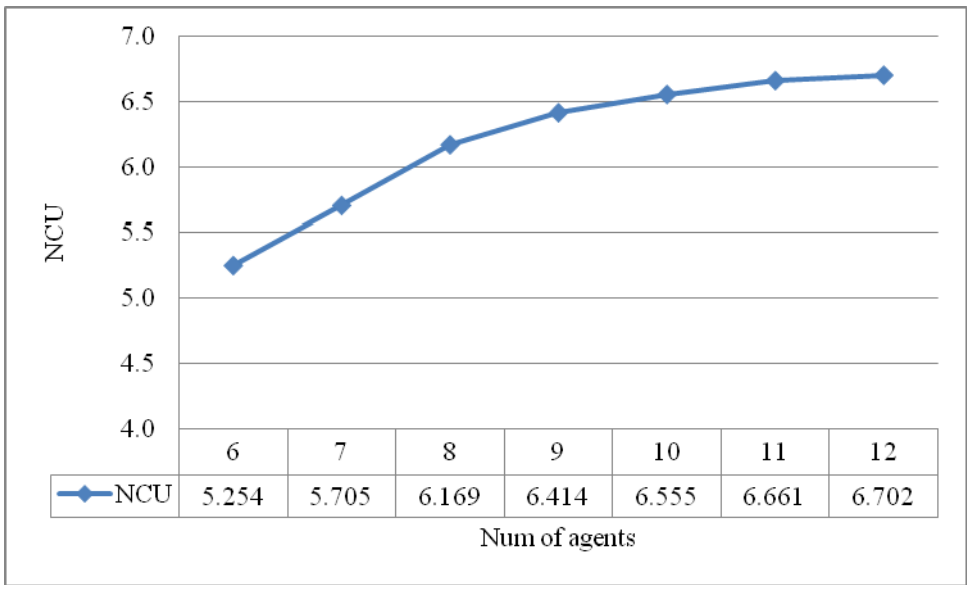


Figure 6-57 Efficient number of agents in the combat scenario with CD

Figure 6-57 shows the simulation result to find the efficient number of agents meeting the operational goal. The actual network connectivity which can be accomplished using eight assigned agents for this scenario is about 89.3%, which does not meet the target connectivity, so more agents are required to reach the target connectivity. The actual network connectivity using nine agents is about 93.6% and about 95.7% using ten agents. So, at least two more agents need to be assigned for this operation in order to reach the target.

Figure 6-58 shows the percentage of actual network connectivity, the percentage of killed users and enemies over time. During operation, about 53% of enemies and 30% of users are killed by combat.

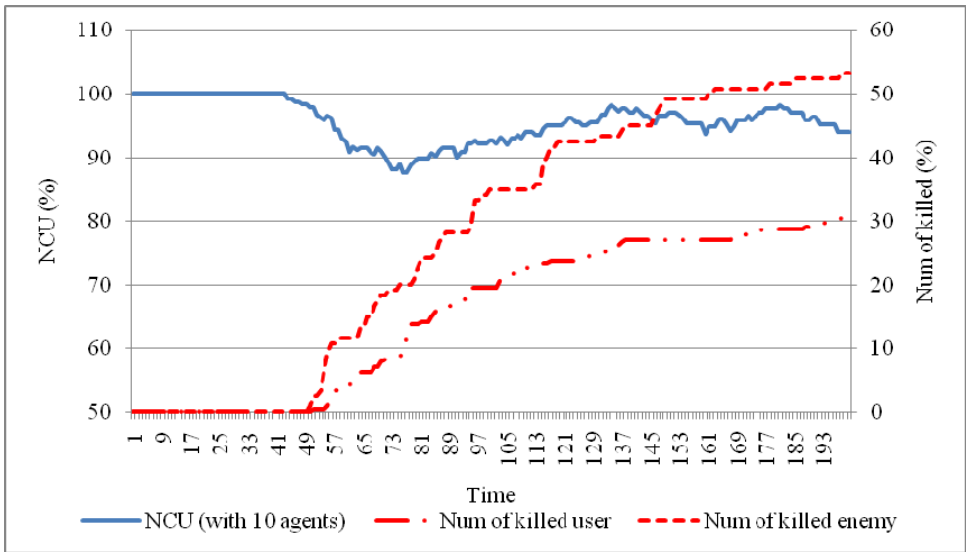


Figure 6-58 Network performance and number of killed resources in the combat scenario with CD

6.6.3 Cost benefit analysis with SR

A combat situation at the initial planning phase of a search and rescue operation is rarely considered since search and rescue is commonly conducted in safe area. There many types of search formations for the SR operation; these are determined by the operational situation of the assigned tactical space and the given mission. The line formation search implemented in this study is the most common type of search operation since it enables the forces to cover the entire search space uniformly and quickly for a given time.

It is assumed that neither network nodes nor enemies are killed in this scenario and the movement paths of users are predefined by the network devices' capability. Thus, the number of agents required to support the users assigned to the operation may roughly be estimated by considering these predefined paths and the number of users. Consequently, the randomness level of this operation is relatively low compared with other mobility models. In this section, a planned search operation executed by five users is considered using simulation.

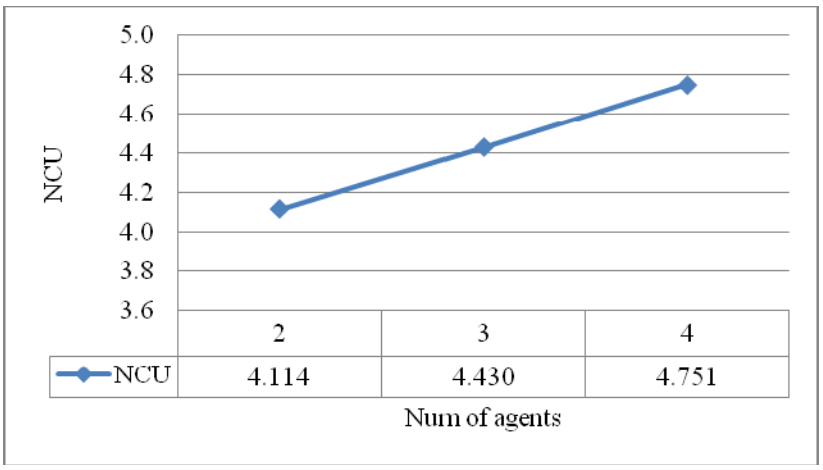


Figure 6-59 Efficient number of agents in the combat scenario with SR

Four agents are assigned to this SR operation by considering the radius of action of the users. As expected from the initial operation plan, four agents are enough to support the users. Network performance by four agents is about 95.02% which satisfies the target connectivity. However, the target connectivity cannot be accomplished with fewer agents than four as shown in Figure 6-59.

In summary, the most efficient number of agents needed to accomplish the target connectivity of a military MANET depends on the operational situation such as combat level, obstacles, and network density. The target network performance could be met by a relatively smaller number of agents in a high density network because of the many operating users. Some operations are vulnerable or obstructed by obstacles. In this kind of situation, it may be very difficult to accomplish target performance because of highly random operations. In particular, under a severe combat situation, the operation of agents could be disturbed by the uncertainty about whether the disconnected users are alive or killed. That is, agents could be deployed to support killed users. This relates to choosing messenger duration for disconnected users. So, the messenger approach may not effective in the severe operations.

Chapter 7

Conclusions

The efficient use of networks for acquisition and sharing of valuable information among friendly forces in a tactical battlefield is a crucial factor for an force awareness and it contributes to the outcomes of combat in the information age. Especially, under an environment where rapid reaction and dynamic mobility are required, the importance of mobile ad-hoc networks has been increased.

In this thesis, a military MANET model that represents vulnerable combat environments realistically is proposed and a heuristic algorithm to optimize mobile agents is developed using PSO.

The communication connectivity for military MANETs in this thesis is measured by the connection between users and the control node, and the optimization of this communication network is done by the hop-count based routing approach to manage limited resources efficiently. However, the hop-count based approach shows a lack of response to network changes even though it can reduce resource requirements by minimizing use of hops. To compensate, a new approach, termed PAL, is developed in this thesis. PAL enables mobile agents to self-configure towards the best location in advance, responding to the change of user nodes' topology. This pre-deployment of mobile agents makes it possible to support users at the needed time and be placed effectively without wasting resources.

The representation of a real network system is very important in order to evaluate the performance of a network. The evaluation of network performance is also necessary to plan an

efficient military MANET operation plan under varied military combat operation environments. To accomplish these requirements, we conceptualize a realistic military MANET under combat environments by introducing enemy obstacles, by specifying network nodes in more detail, and by designing and using new performance metrics representing the characteristics of military MANETs. Through hostile activities of enemy obstacles such as jamming and killing, the capability of MANET nodes is reduced and MANET nodes may even be killed in combat with enemies. In addition, MANET nodes are split into four different types by the function in the military unit structure. This classification of network nodes represents the characteristics of military MANET which differ from commercial networks. With PAL, two additional approaches (messenger and priority node) are employed to support the reality of the proposed military MANET model. Messengers cannot only enhance model reality but also improve network performance by emulation of a real military operation searching for the disconnected users.

To test the effect of the new approaches, we use three different user mobility models: random waypoint (RW), search and rescue (SR), and convoy and defense (CD). These mobility models are used to verify the effect of the approaches over different military movement patterns. User nodes' movement in SR and CD is directed and controlled by an operation plan, so the randomness level of these is relatively lower than with the random waypoint. The effects of PAL, messenger and priority nodes have a close relationship with randomness of the user mobility. Also, network density and the combat level (number of enemies) in the network are significant factors to the effectiveness of PAL, messenger and priority nodes.

The proposed heuristic algorithm based on the hop-count routing approach is expected to be useful for military operations that require efficient use of limited resources under various operational conditions. By adjusting the simulation parameters employed in the proposed model

such as combat level by the number of enemies, minimum bandwidth required for a connection between nodes, enemy effect ranges and the perturbation level (τ) in the employed user mobility model, it is possible to simulate a great variety of military operational environments and to evaluate networks under those varied military operation conditions. The simulation based on this proposed model can be useful to estimate the optimal number of agents before deploying an actual network in a battlefield.

For future research, the following can be studied further by extensional or modification to the proposed model:

The proposed military MANET is focused on a tactical battlefield network consisting of identical types of network devices. However, this could be extended by introducing different types of network devices in terms of velocity, transmission range, etc. For example, network devices designed for individual soldier, tank, UAVs, or combat aircraft have different capabilities. All these devices can be combined for a strategic level of military network.

Also, the obstacle behavior can be modified. The obstacles used in this thesis are fixed throughout the simulation. A better simulation of military combat could be possible by giving mobility to these enemy obstacles.

Finally, users are free to move independently in any direction within a fixed range of space, but this could be modified to have users coordinate their movements with the control node. That is, the control node directs the movement of users considering the network capability at the moment.

References

[1] Abolhasan, M., Wysocki, T., and Dutkiewicz, E., "A review of routing protocols for mobile Ad-hoc Networks," *Ad-hoc Networks* 2 (1) (2004) 1–22.

[2] Alberts, D., Garstka, J., Stein, F., Netwrok centric warfare – developing and leveraging information superiority, 2nd edition, CCRP2000, 2000.

[3] Ammari, H. and El-Rewini, H., "A location information-based route discovery protocol for mobile ad-hoc netoworks," in: *Proceedings of the IEEE International Conference on Performance, Computing, and Communications*, 2004, 625-630.

[4] Baburaj, E. and Vasudevan, V., "An intelligent mesh based multicast routing algorithm for MANETs using Particle Swarm Optimization," *IJCSNS International Journal of Computer Science and Network Security* 8(5) (2008) 214-218.

[5] Bai, F., Sadagopan, N. and Helmy, A., "The important framework for analyzing the impact of mobility on performance of routing for Ad-hoc Networks," *Ad-hoc Networks Journal - Elsevier Science* 1(4) (2003) 383-403.

[6] Bakht, Humayun**,** Wireless Infrastructure: Understanding mobile Ad-hoc Networks, 2008, Accessed on July 17, 2008; Available at: http://www.computingunplugged.com/issues/issue200406/00001301002.html

[7] Belding-Royer E.M. and Toh, C. K., "A review of current routing protocols for Ad-hoc mobile wireless networks," *IEEE Personal Communications Magazine* (1999) 46–55.

[8] Bluetronix. Autonomous agents, Accessed on July 6, 2009; Available at: http://www.bluetronix.net/autonomous_agents.htm

[9] Branke, J., E. Salihoğlu, S. Uyar, "Towards an analysis of dynamic environments," in: *Proceedings of the 2005 Conference on Genetic and Evolutionary Computation,* 2005, 1433-1440.

[10] Branke, J., "Evolutionary approaches to dynamic optimization problems – updated survey," in: *Proceedings of the GECCO Workshop on Evolutionary Algorithms for Dynamic Optimization Problems*, 2001, 27-30.

[11] Broch J., Maltz, D. A., Johnson, D. B., Hu, Y. –C. and Jetcheva, J., "A performance comparison of multi-hop wireless ad-hoc network routing protocols," in: *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile computing and networking*, 1998.

[12] Buruhanudeen S., M., Othman, B. and Ali, M., "Existing MANET routing protocols and metrics used towards the efficiency and reliability- An overview," in: *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 2007, 14-17.

[13] Camp, T., Boleng, J. and Davies, V., "A survey of mobility models for ad-hoc network research" *Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad-hoc Networking: Research, Trends and Applications*, 2(5) (2002) 483-502.

[14] Carlisle, A. and Dozier, G., "An off-the-shelf PSO." In: *Proceedings of the 2001Workshop on Particle Swarm Optimization*, 2001, 1-6.

[15] Catharina, C., Securing military decision making in a network-centric environment, PhD thesis, Helsinki University of Technology, 2005.

[16] Chiang, C.-C., "Routing in clustered multi-hop, mobile wireless networks with fading channel," in: *Proceedings of IEEE SICON_97*, 1997, 197–211.

[17] Chin, K., "The behavior of MANET routing protocols in realistic environments," in: *Proceedings of the Asia-Pacific Conference on Communications*, Perth, Australia, 2005, 906-910.

[18] Chlamtac, I., Conti, M and Liu, J., "Mobile ad-hoc networking: imperatives and challenge," *Ad-hoc Networks* 1(1) (2003) 13-64.

[19] Chu, T. and Nikolaidis, I., "Node density and connectivity properties of the random waypoint model," *Computer Communications* **27** (10) (2004) 914–922.

[20] Clausewitz, C.; Vom Kriege. Auflage mit historischkritischer Wurdigung von W. Hahlweg, Bonn: Dummler. 1980.

[21] Clay Wilson, Network centric operations: background and oversight issues for congress, CRS Reports for Congress, 2007.

[22] Clerc, M., "The swarm and the queen: towards a deterministic and adaptive particle swarm optimization," in: *Proceedings of 1999 Congress on Evolutionary Computation*, 1999, 1951-1957.

[23] Clerc, M., and Kennedy, J., "The particle swarm: explosion, stability, and convergence in a multi-dimensional complex space," *IEEE Trans. Evol. Comput*. 6 (2002) 58-73.

[24] Couto, D. D., Aguayo, D., Chambers, B and Morris, R., "Performance of multi-hop wireless: Shortest path is not enough," in: *Proceedings of the First Workshop on Hot Topics in Networks (HotNets-I)*, 2002.

[25] David Oliver Jörg, Performance comparison of MANET routing protocols in different network sizes, Computer Science Project, University of Berne, Swizerland, 2003.

[26] Dengiz Orhan, Maximizaing connectivity and performance in mobile ad-hoc networks using mobile agents, PhD thesis, Auburn University, AL., 2007.

[27] DoD CIO, Department of defense global information grid architectural vision, 2007, Accessed on April 2 2009; Available at: http://defenselink.mil/cio-nii/docs/GIGArchVision.pdf.

[28] Dow C. R., Lin, P. J., Chen, S. C., Lin, J. H. and Hwang, S. F., "A study of recent research trends and experimental guidelines in mobile ad-hoc networks," in: *Proceedings of 19th International Conference on Advanced Information Networking and Applications*, 2005, 72-77.

[29] Eberhart, R. C. and Kennedy, J., "A new optimizer using particle swarm theory," in: *Proceedings of the sixth International Symposium on Micro Machine and Human Science*, IEEE service center, 1995, 39-43.

[30] Eberhart, R. C. and Shi, Y., "Evolving artificial neural networks," in: *Proceedings of Int'l Conference on Neural Networks and Brain*, 1998. Beijing, P. R. China.

[31] Eberhart, R. C. and Shi, Y., "Particle swarm optimization: developments, applications and resources," in: *Proceedings of Congress on Evolutionary Computation,* 2001, Seoul, Korea.

[32] Eberhart, R. C., & Shi, Y., "Comparing inertia weights and constriction factors in particle swarm optimization," in: *Proceedings of the IEEE Congress on Evolutionary Computation,* 2000, 84–88, San Diego, CA.

[33] Eberhart, R. C., & Shi, Y., "Tracking and optimizing dynamic systems with particle swarms," in: *Proceedings of the IEEE Congress on Evolutionary Computation*, 2001, 94–100, Seoul, Korea.

[34] Frodigh, M., Johansson, P., Larsson, P., "Wireless ad-hoc networking: The art of networking without a network," *Ericsson Review* 4 (2000) 248-263.

[35] Green, D. B. and Obaidat, M. S., "An accurate line of sight propagation performance model for ad-Hoc 802.11 Wireless LAN (WLAN) devices," in: *Proceedings of IEEE ICC 2002*, New York, 2002.

[36] Grossglauser M. and Tse, D.N.C., "Mobility increases the capacity of ad-hoc wireless networks," *IEEE/ACM Transactions on Networking*, 10(4) (2002) 477-486.

[37] Guerin, R., A. Orda, A., "Computing shortest paths for any number of hops," *IEEE/ACM Transactions on Networking*, 10 (5) (2002) 613–620.

[38] He L., Wei, Y., "A measure of mobility for evaluating mobile ad-hoc network performance," in: *Proceedings of ICMMT2008*, 3 (2008) 1528-1531.

[39] Ishibashi B., Boutaba, R., "Topology and mobility considerations in mobile ad-hoc networks," *Ad-hoc Networks*, 3 (2005) 762-776.

[40] Jack. L. B., Chimento, P. F., Haberman, B. K. and Kasch, W. T., "Key challenges of military tactical networking and the elusive promise of MANET technology," *Communications Magazine*, 44(11) (2006) 39-45.

[41] Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A. and Viennot, L., "Optimized link state routing protocol for ad-hoc networks," in: *Proceedings of the IEEE International Multi Topic Conference (INMIC 2001), Technology for the 21st Century*, 2001, 62-68.

[42] James Canan, (2006). Timing in battle: The T-Sat edge, American Institute of Aeronautics and Astronautics, Inc., Aerospace America.

[43] Jardosh, A., Belding-Royer, E. M., Almeroth, K. C. and Suri, S., "Towards realistic mobility models for mobile ad-hoc networks," in: *Proceedings of ACM MobiCom*, 2003, 217-229.

[44] Ji, C., Zhang, Y., Gao, S., Yuan, P. and Z. Li., "Particle swarm optimization for mobile ad-hoc networks clustering," in: *Proceedings of IEEE International Conference on*, vol.1, 2004, 372-375.

[45] Jin, Y., Branke, J., "Evolutionary optimization in uncertain environments – a survey," *IEEE Transactions on Evolutionary Computation* 9 (3) (2005) 303-317.

[46] John J. Garstka, Network centric warfare: an overview of emerging theory, 2000, Accessed on September 17, 2008; Available at: http://www.mors.org/publications/phalanx/dec00/feature.htm.

[47] Johnson, D.B., Maltz, D. A., Dynamic source routing in ad-hoc wireless networks, in: H.K. T. Imielinski (Ed.), Mobile Computing, Kluwer, Boston, 1996, 153–181.

[48] Kalaba, R. and Tesfatsion, L., "Exact sequential, smoothing and prediction for non linear systems," *Non-Linear Analysis* 12 (6) (1998) 599-615.

[49] Kalaba, R. and Tesfatsion, L., "An organization principle for dynamic estimation," *Journal of Optimization Theory and Applications*, 64 (3) (1990) 445-470.

[50] Karhima, T. Lindroos, P. Hall, M. Haggman, S.-G., "A link level study of 802.11b mobile ad-hoc network in military environment," in: *Proceedings of Military Communications Conference (MILCOM 2005),* vol.3, 2005, 1883- 1886.

[51] Kennedy, J., "Small worlds and megaminds: Effects of neighborhood topology on particle swarm performance," in: *Proceeding of the 1999 Conference on Evolutionary Computation*, 1999, 1931-1938.

[52] Kennedy, J. and Eberhart, R. C. "Particle swarm optimization," in: *Proceedings of IEEE international conference on neural networks*, 4, 1995, 1942-1948.

[53] Kennedy, J., Eberhart, R. C., Swarm intelligence, Morgan Kaufmann Series in Evolutionary Computation, 2001.

[54] Kwak, B.J., Song, N.O. and Miller, L.E., "A standard measure of mobility for evaluating mobile ad-hoc network performance," *IEICE Transactions on Communications E86-B* (2003) 3236-3243.

[55] Lee, S-J., Hsu, J., Hayashida, R., Gerla, M. and R. Bagrodia., "Selecting a routing strategy for your ad-hoc network," *Computer Commnications* 26(7) 723-733.

[56] Lekovic, B., Mieghem, P. V., "Link state update policies for quality of service routing," in: *Proceedings of 8th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT2001)*, Delft, The Netherlands, 2001, 123-128

[57] Libicki, M., What is information warfare?, Institute for National Strategic Studies, 1995.

[58] Lin, G., Noubir, G. and Rajaraman, R., "Mobility models for Ad-hoc network simulation," in: *Proceedings of the 23rd Conference of the IEEE Communications Society (INFOCOM)*, 2004.

[59] Luddy, J., "The challenge and promise of network-centric warfare," Lexington Institue: 2005, Accessed on December 12, 2008; Available at: http://www.lexingtoninstitute.org/docs/521.pdf .

[60] Macker, J., Corson, M. S., "Mobile ad-hoc networking and the IETF," *ACM Mobile Computing and Communications Review* 2(1) (1998) 7-9.

[61] Masip-Bruin, X., Yannuzzi, M., Domingo-Pascual, J., Fonte, A., Curado, M., Monteiro, E., Kuipers, P., Mieghem, V., Avallone, S., Ventre, G., Aranda-Gutiérrez, P., Hollick, M., Steinmetz, R., Iannone, L. and Salamatian, K., "Research challenges in QoS routing, Computer Communications Journal," *Elsevier* 29 (5) (2006) 563-581.

[62] Murthy, S. and Garcia-Luna-Aceves, J. J., "An efficient routing protocol for wireless networks," *Mobile Networks and Applications* (Hingham, MA: Kluwer Academic Publishers) 1(2) (1996) 183 – 197.

[63] NIST, Shortest path, Accessed on July 26, 2008; Available at: http://www.nist.gov/dads/HTML/shortestpath.html

[64] Office of Force Transformation, The implementation of network-centric warfare, Accessed on January 22, 2009; Available at: http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf

[65] Oliveira, C. A. and Pardalos, P. M., An optimization approach for cooperative communication in ad-hoc networks, Technical report, School of Industrial Engineering and Management, Oklahoma State University, 2005.

[66] ORACLE, Building a network-centric warfare architecture, White paper, 2004, Available at: http://www.oracle.com/industries/government/ncwwhitepaperr1.pdf.

[67] Parsopoulos, K. E. and Vrahatis, M. N., "Recent approaches to global optimization problems through particle swarm optimization," *Natural Computing: an International Journal* 1(2-3) (2002) 235-306.

[68] Pazand, B. and McDonald, C., "A critique of mobility models for wireless network simulation," in: *Proceedings of Computer and Information Science, ICIS, 6th IEEE/ACIS International Conference on*, 2007, 141-146.

[69] Peacock, B. A., Connecting the Edge: Mobile Ad-Hoc Network (MANETs) for network centric warfare, Blue Horizons paper, Center for Strategy and Technology, USAF Air War College, 2007.

[70] Pearlman, M.R., Haas, Z. J. and Samar, P., The zone routing protocol (ZRP) for Ad-hoc networks, Internet Draft, draft-ietf-manet-zone-zrp-04.txt, 2002.

[71] Pearlman, M.R. and Haas, Z. J., "Determining the optimal configuration for the zone routing protocol," *IEEE Journal on Selected Areas in Communications* 17 (8) (1999) 1395–1414.

[72] Peng, B., Kemp, A. H. and Boussakta, S., "QoS routing with bandwidth and hop-count consideration: A performance perspective," *Journal of Communications* 1 (2) (2006). 1-11.

[73] Perisa, D., Allwright, A. and Pourbeik, P., "Structural dynamics of war game MANETs," in: *Proceedings of Communications and Information Technologies, ISCIT '07. International Symposium*, 2007, 830-835.

[74] Perkins, C.E. and Bhagwat, P., "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers," *Computer Communications Review* 24 (4) (1994) 234–244.

[75] Perkins C.E., Royer, E. M., Das, S. R. and Marina, M. K, "Performance comparison of two on-demand routing protocols for Ad-hoc Networks", *IEEE Pers. Commun* 8(1) (2001) 16-28.

[76] Perkins, C.E. and Royer, E. M., "Ad-hoc on-demand distance vector routing," in: *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, 90–100.

[77] Poli, R., Kennedy, J. and Blackwell, T., "Particle swarm optimization," *Swarm Intelligence* 1(1) (2007) 33-57.

[78] Raby, M, Wireless networks jump in popularity: survey, 2007, Accessed on May 24 2009; Available at: http://www.tomshardware.com/news/wireless-networks-survey,4372.html.

[79] Quintero, A., Pierre, S. and Macabeo, B., "A routing protocol based on node density for ad-hoc networks," *Ad-hoc Networks* 2 (3) (2004) 335-349.

[80] Raghavan, V. N., Venkatesh, T., Peer, M. L., Praveen, D. P., "Evaluating performance of quality-of-service in large networks," in: *Proceedings of World Academy of Science, Engineering and Technology*, vol.20, 2007.

[81] Rani, K. N. A. and Sharif, B. S., Particle Swarm Optimization (PSO): Fundamental concepts and applications in mobile communications, University of Newcastle upon Tyne, United Kingdom, 2008.

[82] Robert F. Dillingham, Communicating on the Move: Mobile ad-hoc networks, SRA International, Inc. the Journal of Defense Software Engineering, Accessed on September 27, 2008; Available at: http://www.stsc.hill.af.mil/crosstalk/2007/07/0707DillinghamNathans.html.

[83] Royer, E. M., Melliar-Smith, P. M., Moser, L. E., "An analysis of the optimum node density for ad-hoc mobile networks," in: *Proceedings of the IEEE International Conference on Communications*, 2001, 857–861.

[84] Roux, N., Pegon, J. S., Subbarao, M. W., "Cost adaptive mechanism to provide network diversity for MANET reactive routing protocols," in: *Proceedings of IEEE MILCOM*, 2000, 387-391.

[85] Sahin, C. S., Urrea, E., Uyar, M. U., Conner, M., Self-deployment of mobile agents in MANETs for military applications, 2008, Accessed on March 22, 2009; Available at: http://asc2008.com/manuscripts/B/BP-22.pdf.

[86] Salmanian, M., Military wireless network information operation scenarios, Defense R&D Canada Ottawa Technical Memorandum DRDC Ottawa TM, 2003, 2003-241.

[87] Sanchez, M, Mobility models, 2001, Accessed on Feb 7 , 2009; Available at http://www.disca.upv.es/misan/mobmodel.htm.

[88] Satyanarayanan, M., "Fundamental challenges of mobile computing," in: *Proceddings of 15th ACM symposium. Principles of dist. Comp*, 1996.

[89] Schechtmann, G., Manipulating the OODA loop: the overlooked role of information resource management in information warfare, Master's Thesis, Faculty of the graduate school of logistics and acquisition management of the Air Force Institute of Technology, 1996.

[90] Shaikh, A., Rexford, J. and Shin, K., "Evaluating the impact of stale link state on quality-of-service routing,"*IEEE Trans. Networking* 9 (2001) 162–176.

[91] Shi, Y. and Eberhart, R. C., "Parameter selection in particle swarm optimization," in: *Proceedings of Evolutionary Programming VII (EP 98)*, 2001, 591-600.

[92] Shi, Y., "Particle swarm optimization," *IEEE Neural Networks Society* (2004) 8-13.

[93] Shukla, D, Mobility models in ad-hoc networks, Master's Thesis, KReSIT-IIT, Bombay, 2001.

[94] Smith, A. E., Effects-based operations: applying network-centric warfare in peace, crisis, and war, DoD CCRP, Washington, DC, 2002.

[95] Smith, A. E., Network-centric warfare, Naval War College Review, 2001, Accessed on March 24, 2009; Available at: http://findarticles.com/p/articles/mi_m0JIW/is_1_54/ai_75762213.

[96] Sridhar, K.N. and Chan, M. C., "Stability and hop-count based approach for route computation in MANET," in: *Proceedings of IEEE ICCCN*, 2005, 25-31.

[97] Stepanov I., Maron, P. J. and Rothermel, K., "Mobility modeling of outdoor scenarios for MANETs," in: *Proceedings of the38th Annual Simulation Symposium (ANSS'05)*, 2005, 312-322.

[98] Sun, T, The art of war, Filiquarian Publishing, LLC., 2006.

[99] Ted, M., "Developers of net-centric warfare battle complexity," *Journal of Electronic Defense*, 7 (2005) 23.

[100] Walter, M., "Technology for a naval revolution in military affairs," Second Navy RMA Round Table, Science Applications International Corportation, Tysons Corner, Virginia, 1997.

[101] Wang, N-C., and S-W. Chang, "A reliable on-demand routing protocol for mobile ad-hoc networks with mobility prediction," *Computer Commnications* 29(1) (2005) 123-135.

[102] Warren Ferster, Military bandwidth demand energies market, SpaceNews, 2003, Accessed on March 1, 2009; Available at: http://www.spacecom/spacenews/archive03/militaryarch_090203.html

[103] Wikipedia, Partical Swarm Optimization, Accessed on July 24, 2008; Available at: http://en.wikipedia.org/wiki/Particle_swarm_optimization

[104] Wikipedia, Shortest path problem, wikepedia, Accessed on August 17, 2008; Available at: http://en.wikipedia.org/wiki/Shortest_path_problem#Applications.

[105] Wikipedia, Telecommunication network Wikipedia.org, Accessed on July 15, 2008; Available at: http://en.wikipedia.org/wiki/Telecommunication_network.

[106] Wikipedia,Wi-Fi, Accessed on June 27, 2009; Available at: http://en.wikipedia.org/wiki/Wi-Fi

[107] Wilson J. W, The importance of mobility model assumptions on route discovery, data delivery, and route maintenance protocols for ad-hoc mobile networks, Virginia Polytechnic Institute and State University, 2001.

[108] Zheng, Y.-L., Ma, L.-H., Zhang, L.-Y., and Qian, J.-X., ”On the convergence analysis and parameter selection in particle swarm optimization,” in: *Proceedings of the IEEE International Conference on Machine Learning and Cybernetics*, 2003, 1802–1807.

[109] Zhou, B., Xu, K. and Gerla, M., “Group and swarm mobility models for Ad-hoc network scenarios using virtual tracks,” in: Proceedings of *Military Communications Confrerence*, *MILCOM2004*, IEEE 1, 2004, 289-294.

[110] Zitlzler E., Laumanns, M., Bleuler, S., ”A tutorial on evolutionary multiobjective optimization,” *Metaheuristics for Multiobjective Optimization*, 2004, 3-37.