NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN AD HOC WIRELESS MOBILE COMMUNICATIONS MODEL FOR SPECIAL OPERATIONS FORCES

By

Cetin Ogut

September 2000

Thesis Co-Advisors : James Bret Michael
John Arquilla

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE September 2000	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE An Ad Hoc Wireless Mobile Communications Model For Special Operations Forces	5. FUNDING NUMBERS
6. AUTHOR(S) Ogut, Cetin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

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

13. ABSTRACT

The digitization of the battlefield enables special operators to use improved communications supported by computer networks across a range of missions. The communications paradigm is evolving toward mobile wireless ad hoc networks. This development enables an autonomous system of mobile nodes supporting peer-to-peer communications in forward-deployed military networks. Ad hoc networks have to establish a reliable, secure, instant, and usually temporary, communication infrastructure and to be able to access in a global communications infrastructure.

Our model describes a global communication network supporting the special operator in mobile wireless communications. The main purpose is to provide a handheld wireless communications node which is capable of transferring voice, data, and imagery to and from parallel and vertical command structures within an environment replete with electronic countermeasures. The model will support the representation of requirements such as throughput, quality of service with low power consumption, and low probability of detection/interception. Special Forces are moving toward using commercial-off-the-shelf products and services based on availability and cost effectiveness.

Using GloMoSim tool, we run simulations for a direct action scenario and compared the efficiency of on-demand and table-driven routing protocols under different bandwidths and communications loads.

14. SUBJECT TERMS Special Operation Forces, Ad hoc, wireless, mobile communications, information operations, electromagnetic pulse weapons, EMP	15. NUMBER OF PAGES 290
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A WIRELESS MOBILE COMMUNICATIONS MODEL FOR SPECIAL OPERATIONS FORCES

Cetin OGUT
First Lieutenant, Turkish Army
B.S., Turkish Military Academy, Ankara, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

and

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
September 2000

ABSTRACT

The digitization of the battlefield enables special operators to use improved communications supported by computer networks across a range of missions. The communications paradigm is evolving toward mobile wireless ad hoc networks. This development enables an autonomous system of mobile nodes supporting peer-to-peer communications in forward-deployed military networks. Ad hoc networks have to establish a reliable, secure, instant, and usually temporary, communication infrastructure and to be able to access in a global communications infrastructure.

Our model describes a global communication network supporting the special operator in mobile wireless communications. The main purpose is to provide a handheld wireless communications node which is capable of transferring voice, data, and imagery to and from parallel and vertical command structures within an environment replete with electronic countermeasures. The model will support the representation of requirements such as throughput, quality of service with low power consumption, and low probability of detection/interception. Special Forces are moving toward using commercial-off-the-shelf products and services based on availability and cost effectiveness.

Using GloMoSim tool, we run simulations for a direct action scenario and compared the efficiency of on-demand and table-driven routing protocols under different bandwidths and communications loads.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. James Bret Michael and Dr. John Arquilla for their guidance with this thesis. I greatly appreciate the gracious patience they maintained while I was working on this project.

I am grateful to all faculty members of the Computer Science Department and Special Operations Academic Group who have turned my education at NPS into a unique and joyful experience.

Finally, I would like to thank the Turkish Army and Turkish Special Forces for the opportunity they gave me to pursue this higher education.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The nature of warfare has evolved in parallel with advances in human culture. Ongoing novelties in tactics, doctrine, weapons, and technologies compose a continuing cycle that progresses with each new step in their component elements. Each new advance in turn causes the nature of warfare and the conduct of the military operations to become more complex. As complexity increases, the forces included in these operations must be better prepared, trained, and equipped than before. Carl von Clausewitz summarized the complex nature of military operations in his paramount work, *On War*: "The conduct of war resembles the working of an intricate machine with tremendous friction, so that combinations which are easily planned on paper can be executed only with great effort."[1]

The complex nature of modern conflicts sometimes require covert solutions. In a world of increasing levels of global interaction, Special Operations Forces (SOF) might prove to be a unique mechanism for quelling conflicts. Increased volatility throughout the world, reduced permanently deployed conventional forces and bases, and diminishing resources force decision-makers to find unconventional, asymmetric solutions to resolving conflicts. In this context, the SOF will provide access to national goals and promote stability with an affordable force for supporting political and military strategies.

---

[1] Carl von Clausewitz, *On War*, Edited and Translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, New Jersey, 1984, 577

The SOF are specially trained, equipped, and organized units with specialized, highly focused capabilities. The unique qualifications and capabilities of the SOF provide, to both "national and theater level decision-makers, a great range of options and flexibility in responses through their rapid adaptability and strategic advantage."[2] The SOF serve three strategic purposes that are important in the current and future global environment. "First, they offer a range of options to decision makers confronting crises and conflicts below the threshold of war, such as terrorism, insurgency, and sabotage. Second, they are force multipliers for major conflicts, increasing the effectiveness and efficiency of ... military effort. Finally, they are the forces of choice in situations requiring regional orientation and cultural and political sensitivity, including military-to-military contacts and noncombatant missions like humanitarian assistance, security assistance, and peace keeping operations."[3]

The SOF are different from conventional military forces. They possess unique characteristics that allow them to accomplish missions that conventional forces are unable to perform either effectively or efficiently. These elite forces generally play a role as a strategic asset of a nation. In his report to the President, the Secretary of Defense made the following comment:

> Special operations differ from traditional military operations in degree of political risk, often unconventional mode of employment, independence from friendly support, and dependence on detailed intelligence and indigenous assets. For these reasons, some of the missions carry an exceptionally high degree of physical risk. Political sensitivities surrounding many of SOF missions require close coordination at the interagency level.[4]

---

2 Commander in Chief, USSOCOM, Special Operations Forces: The Way Ahead; 1998, 1.

3 Cohen, W. S., Secretary of Defense, Annual Report to the President and to the Congress, 1998, 1

4 Ibid, 3.

The five principal missions of the SOF are: unconventional warfare, direct action, strategic reconnaissance, foreign internal defense, and counterterrorism. "While SOF provide unique, versatile, and flexible forces designed primarily to meet these missions, conventional forces may be required for support, depending upon mission circumstances."[5]

The revised C4I doctrine stresses the need for rapid movement to access the infosphere, taking full advantage of the national information infrastructure. The following five C4I fundamental principles represent the vision for effective employment of the SOF in consonance with a national security policy:

- Global
- Secure
- Mission Tailored
- Value Added
- Joint[6]

U.S. SOF currently rely on over twenty systems and networks for global deployment. The USSOCOM Command Network, commonly referred as to the Command LAN/WAN, is a command, control, and communications network providing data services to the USSOCOM Headquarters and locations serviced by SCAMPI (not an acronym), including tactical connections to forward operating locations. This system "allows special operators access to the same applications in the field as those used in the garrison. Currently it is functioning on Windows NT and Unix servers on a 100Mbps fiber-optic backbone. The Windows NT network operating system environment will enhance office automation over the network by providing access to the latest in

---

[5] Joint Pub 3-05, 1992.

commercial off-the-shelf (COTS) software. The Unix servers make it possible to run any of the existing, and planned, UNIX based government off-the-shelf (GOTS) software system. Using the two different operating systems together increases capability and functionality by allowing access to the office automation and command and control (C2) on the same terminal."[7]

Most of the current C2 used by the lower level commanders is still accomplished over a push-to-talk radio, much as it was in World War II. Ongoing digitization efforts of the battlefield are seeking to harness the power of the computer to help the commander and his forces better understand their situation, improve force synchronization, and enhance combat effectiveness. As a result, there is a crucial need for a seamless integration of wireless and mobile digital communications. The primary reason for wireless communications is to enable mobility, and this is also the principal benefit for the military. However, "mobility" means different things in the commercial and military worlds. Within the Internet community, the current notion of supporting host (user) mobility is via "mobile IP." In the near term, this is a technology for supporting host "roaming," where a roaming host may be connected through various means to the Internet. However, at no time is a host more than "one hop" from the fixed network. Supporting host mobility requires addressing management and protocol interoperability enhancements. However, core network functions, such as a routing, still occur within the fixed network.

A great effort has been made for a whole system that supports wireless mobile

---

[6] USSOCOM, USSOCOM C4I STRATEGY INTO THE 21ST CENTURY, 1996, 6.

[7] Ibid.,14.

networking. A long-term vision of mobile IP is to support host mobility in wireless networks consisting of mobile routers. Such networks are envisioned to have dynamic, often rapidly changing, mesh topologies consisting of bandwidth-constrained wireless links. "These characteristics create a set of underlying assumptions for protocol design which differ from those used for the higher-speed, fixed topology Internet. These assumptions lead to somewhat different solutions for implementing core network functionality such as routing, resource reservation, etc."[8]

B. MOTIVATION

The motivation for our research stems from the need to ensure that the SOF remain the best informed forces on the battlefield. To accomplish this goal, the special operator must swiftly obtain all of the most current, relevant data. The future digital battlefield will have a mix of terrestrial and space-based communications to handle voice data, and imagery. As the battlefield becomes digitized, the amount of operational, intelligence, and logistical information that may be of interest to the special operators can potentially overload the capacities of the existing networks.

The USSOCOM C4I strategy represents a radical change for the SOF community. The strategy is well on its way to being implemented. "Its requirement for systematic technological enhancements will allow USSOCOM to fully exploit the infosphere and maximize interoperability with national, joint, and combined information assets in support of special operations missions worldwide."[9]

Although current-generation commercial and military ground-based mobile

---

[8] Carson, S., Macker, J., *Architectural Considerations for Mobile Mesh Networking*, IETF Network Working Group, May 1996.

[9] USSOCOM, USSOCOM C4I STRATEGY INTO THE 21ST CENTURY, 1996, 11.

wireless networks might seem on the surface to be providing similar functionality, they are in fact fundamentally different types of networks; future generations of these ground-based wireless networks may diverge even further. Commercial wireless networks, which are perhaps best exemplified by the cellular telephone system, depend on a fixed supporting infrastructure of base stations interconnected by high-speed trunk lines. The topology of the supporting network is fixed, which greatly simplifies the routing of the connections. Military ground-based mobile wireless networks cannot depend on a static supporting network for several reasons; the most important of these are (1) highly mobile forces need networks that move with them, (2) fixed assets are more vulnerable to attack, and (3) the military needs networks that will continue to function even when some nodes are destroyed and some links are jammed.

Today's internetwork technology has been extremely successful in linking large numbers of computers and users. However, to date, this technology has been oriented toward computer interconnection in relatively stable operational environments, and thus cannot adequately support many of the emerging civilian and military uses that require a more adaptive and more easily deployed technology. In particular, multihop packet radio networks are ideal for establishing ad hoc on-demand communication infrastructures in supporting military doctrine for reliable, secure infrastructures for communication among all tiers down to the special operators on-the-move, and extending the global communication infrastructure to the wireless, mobile environment.

There are ongoing parallel governmental efforts to support research for future needs. "The Defense Advanced Research Projects Agency (DARPA) is sponsoring the development of the Wireless Internet Gateways (WINGs) as part of the DARPA Global

Mobile (GloMo) Information System program."[10] This system also targets an integration of commercial systems. "The notion of scalable untethered system means developing technology for a product line approach to wireless systems, allowing military to enhance commercial products with military required features and still retain most of advantages of working with commercially available hardware."[11]. The associated risk might be the sharing of sensitive military technology with the commercial world. In addition, it might be undesirable, if everybody –terrorists, criminals, hostile nations- has easy access to the robust wireless systems encouraged by the military and designed by commercial groups.

SOF are prepared to operate worldwide across a broad spectrum of conflict. Moreover, there is a great tendency –and benefit- toward working together with allied and friendly forces. Technological improvements and systems have to be interoperatable within a coalition. There must at least be some common ground to connect different national infrastructures while keeping each participant's confidentiality private.

In recent years, there has been increasing pressure to cut down the defense budget. One outcome of the weakening defense budget is that increased use of commercial-of-the shelf (COTS) products in the military operations needs further attention. Most of the COTS are produced for a potential target market without specific military use in mind. However, it turns out that military operators are important customers. In fact, if military analysts were to be included in the design and development of potential commercial products, some special requirements of military systems such as

---

[10] Garcia-Luna-Aceves, J. J., Fullmer, C.L., Madruga, E., Beyer, D., Frivold, T.; "Wireless Internet Gateways (WINGS)," MILCOM '97 Proceedings, Volume 3, 1997, Pages 1271-1276.

[11] Ruth, Robert, Program Manager, GloMo BAA Outreach Brief, Global Mobile Information Systems, DARPA, http://www.darpa.mil/ato/programs/glomo/outreachbrief.

security and low probability of detection/interception could be embedded into the system from its early phases as optional packages. This will decrease the huge R&D burden in the military defense budget, but not all commercial producers will be willing to let the military take part in their development plans. In fact, the military's share in the high-tech communication devices is decreasing with time. In the 1970s almost 90% of the R&D efforts were supported by military funds throughout the U.S. Today, this share is about 10%. In short, the military might inform commercial producers of its requirements which will not increase the cost of the unit product, if the requirements are embedded early enough into the development phase. For this reason, the military has to define its future needs and publicize its requirements for future products.

At the end of this thesis, we will suggest a mobile wireless networking model for the Special Operations Forces that meets national requirements and supports allied operations.

C. METHODOLOGY

The methodology employed in this thesis will consist of the following:

Conduct a thorough literature survey and analyze different approaches on global wireless communication and routing of information along the networks.

- Review current USSOCOM doctrine, policy, and guidance on mobile communications.
- Examine current mobile communications capabilities of the SOF and based on these capabilities, determine the future need for mobile communications in the SOF.
- Develop a network model for the SOF which enables global mobile communications including wireless, satellite and, Internet opportunities.

- Construct a GloMoSim simulation for the battalion level of the model.
- Analyze the results of the simulation.
- Examine different routing schemas in wireless mobile communications.
- Examine the information warfare (IW) aspects of the mobile wireless communication of the SOF.

D. ORGANIZATION

This thesis is divided into eight chapters. Chapter II provides an overview of characteristics and current mobile communication capabilities of SOF. Next, the future needs, and opportunities for the use of the public communication infrastructure are discussed. Chapter III provides information about modeling and simulation of the networks. The GloMoSim simulation tool is also introduced in this chapter. Chapter IV describes a network model based on the future needs discussed in Chapter II. Chapter V contains the analysis of the results of the simulation based on the model. Information Warfare issues are covered in Chapter VI. Security measures for mobile wireless communication, low probability of detection (LPD), low probability of interception (LPI), and dangers of traffic analysis by the enemy are some of the topics covered in this chapter. The final chapter contains recommendations for future work and presents a summary of our findings.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SPECIAL OPERATION FORCES

A. CHARACTERISTICS OF THE SOF

Under the so-called "New World Order" it became apparent that, under new circumstances, the threat of full-scale conflicts has dramatically diminished. At the same time there is a continuing danger of local conflicts, often of ethnic background, such as in Chechnya and East Timor. Each conflict has a long escalation period, gradually crossing the threshold of open hostilities. On the other hand, it is easy to observe a growing number and intensity of various military activities that are commonly known as peace operations in the post-Gulf War era. During the past decade, the nature of international terrorism and trans-national crimes were changing. While the number of incidents were decreasing, there has been an increase in the lethality. Under these conditions the use of military forces becomes a sensitive option. In addition, the political aspect of military operations is gaining key importance.

Many of the current challenges are better addressed using smaller, especially trained forces rather than the traditional deployment of the conventional forces of the past. "Unlike unconventional forces, where mass and fire power are measures of effectiveness, the SOF comprise very small teams. Formed of skilled operators, trainers, and teachers, the SOF staff serve in remote locales, often behind unfriendly lines."[12]

A popular misconception of special operations is that they are accepted as "a phenomenon of the post-World War II era."[13] Actually "special operations have been

---

[12] C4I Handbook for Integrated Planning, Appendix K, USSOCOM, C4I Systems and Networks, December 1997, 1-3.

[13] Cohen, A., *Commandos and Politicians*, Center for International Affairs Harvard University,1978, 18.

present from the earliest stirrings of the organized conflict."[14] From the wooden horse of the Trojan War to Rogers' Rangers raid on St. Francis, there are many examples of special operations throughout history. That is, from the very beginning of warfare, commanders sought to use unconventional means on the battlefield. However, modern and organized Special Forces found their place in military concepts as a separate category of military operations during and after WWII. "Special operations (SO) are operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or informational objectives by unconventional military means in hostile, denied, or politically sensitive areas."[15] SO are a form of warfare characterized by a unique set of objectives, weapons, and forces. Special operations differ from conventional military operations. Some of the key differences include the degree of risk involved, both political and physical as well as the means by which they achieve their objectives. They are inherently more complex and require more detailed planning than conventional military operations. USSOCOM has developed five requirements that "distinguish special operations from conventional military operations: 1. Unconventional training and equipment; 2. Political sensitivity; 3. Unorthodox approaches; 4. Limited opportunity; and 5. Specialized intelligence."[16]

SOF missions can be divided into three main areas: special operations, psychological operations, and civil affairs. Of these, "the area of special operations further subdivides into mission activities and collateral activities. Mission activities include direct action, special reconnaissance, unconventional warfare, foreign internal

---

[14] Arquilla, J., *From Troy to Entebbe*, University press of America, Inc., Lanham, 1996, 1.

[15] Joint Pub 3-05, *Doctrine for Joint Special Operations*, Joint Staff, 28 Oct 1992, GL-20.

defense, and counterterrorism. Less traditional collateral activities include humanitarian assistance, counterdrug missions, personnel recovery, counterproliferation, security assistance, antiterrorism, and information operations."[17]

Three types of motivations lead politicians and soldiers to create, nurture and deploy elite units. "The first type is military utility. The second type consists of the irrational and romantic sources of support for elite units. The final type of motivation stems from the increased politicization of war and military actions in the past half-century."[18]

The unique qualifications and capabilities of the SOF provide, to both national and theater level decision-makers, a greater range of options and flexibility in responses through their rapid adaptability and strategic advantage. These elite forces serve as one of the strategic assets of a nation. The SOF have ability to access remote, denied or politically sensitive regions of the world that conventional forces cannot access. The inaccessibility of a particular area may be due to political, logistical, or operational constraints. The SOF offer extended options to the decision-maker and this ability is a highly valuable strategic asset. The SOF have repeatedly demonstrated an ability to apply their skills to a variety of tasks and each deal with complex issues. This characteristic is another reason that the SOF offer extended choices to the decision-maker. Innovation, unconventional approaches, organizational flexibility, and personnel quality cause this adaptability.

---

[16] SOF Posture Statement, USSOCOM, 1998.

[17] C4I Handbook, 1-5.

[18] Cohen, 29.

As SOF activity increases in this critical arena, planners must understand the command, control, communications, computers and intelligence (C4I) systems and networks that contribute to their capabilities and play an important part in accomplishing their missions.

B. CURRENT DOCTRINE AND COMMUNICATION CAPABILITIES OF SOF

An important aspect of current special operations is their need for a high quality C4I system during operations. We will not separate communications from C4 capabilities, because it is already included there and has a doctrinal meaning within C4. Units may operate independently for weeks, but they still depend on radio communications to receive updated orders and report intelligence information back to the command. In the case of foot units, these facilities must be available from a package that can be carried by one man. This equipment should meet the requirements such as lightweight, low power consumption, ease of use and information security. These necessities are supported by the Joint Pub doctrine as follows: "C4 support to SO must be jointly interoperable, reliable, secure, redundant, lightweight. Flexible (capable of being mission tailored), and highly mobile and must provide low probability of interception/detection (LPI/D)." [19]

C4 systems must provide the rapid, reliable, and secure flow and processing of data to ensure continuous information exchange throughout the whole force. "An unbroken chain of communications must be extended from the National Command

[19] Joint Pub 3-05, V-5.

Authorities (NCA), through the Chairman of the Joint Chiefs of Staff (CJCS), to the combatant commanders."[20]

C4 systems must be **global**. They support the full range of diverse special operations missions worldwide and make maximum use of existing national capabilities, as well as commercial, tactical, and allied or friendly nation resources. The lowest possible tactical level has to be given the access to the infosphere.

C4 systems are directed against high value, critical targets. Their offensive nature brings physical and political risk. For this reason, C4 systems must be conducted in a **secure** way, using the latest technology, procedures, and standards to ensure that an enemy cannot exploit them.

SOF C4 systems must be **tailored to the projected operational environment**. As a result, the deployed special operator will have methods for communicating, reporting, and querying available resources, regardless of geographic location.

Every communications systems used by SOF must **add value** to their mission, continually improving their mission capability. Smaller, lighter, and more capable C4 equipment will add value by reducing the number and size of resources.

The special operations are becoming more and more **joint** and **multinational** in nature. Acquiring and transporting large amounts of data reliably, securely, and in near-real time must support these joint activities.

Current trends in military systems are primarily based on providing voice communications in mobile environments. Data is typically overlaid on systems designed for voice. Networks such as cellular are fixed base-station oriented. Such networks with

---

[20] Joint Pub 6-0, I-7.

large immobile infrastructure are not suitable for rapid deployment. End-to-end service is typically voice oriented, so even though the wireline nets can support higher levels of service, it is difficult to tie them together with wireless networks at the end. Moreover, applications need the ability to negotiate for bandwidth and other resources and be informed as to the extent to which requests can be serviced.

The C4I for the Warrior concept, which currently guides the military's adoption of information technologies, integrates commercial and military networks. The provision of vastly increased access to information at all echelons is made possible by the use of modern high-speed computer networks. This overarching doctrine has placed the procurement and deployment of computer networks into the mainstream of industry driven standards and procedures.

The widespread nature of the USSOCOM's mission requires global communications coverage. The command's main focus is military systems down to team level. "The command operates an intricate, full spectrum, and robust network of satellite and terrestrial systems."[21] Most of the current systems and networks interconnect command, operations, and intelligence centers that, in turn, connect with numerous globally deployed forces. Moreover, these assets allow efficient planning and decision making.

SCAMPI is a National Security Agency approved communications network of services that allows information of multiple security classification levels to travel over a single commercial or government provided transmission path. It is a robust, seamless, C4I system, which takes advantage of commercial and government off-the-shelf

---

[21] C4I Handbook, 5-3.

equipment and utilizes bandwidth on demand technology. The system provides an exceptional variety of multimedia services for the SOF community, including C2 voice and data services as well as intelligence voice, data, and imagery services.

Deployable SCAMPI was the next step for USSOCOM. This tactically oriented system allows field deployed units to have the same capabilities that garrison units now enjoy via SCAMPI. "The first Deployable SCAMPI systems were delivered to the Joint Communications Support Element (JCSE) in November 1995 and to the Joint Special Operations Command (JSOC) in January 1996. Further fielding of SCAMPI capability will continue until units down to the Army battalion, Navy SOF task unit, and Air Force SOF detachment levels have access to this network of services."[22]

C. FUTURE COMMUNICATION NEEDS FOR SOF

1. Future Vision

The world environment continues to change and presents more complex challenges in the nature of the threats. These threats make the defense planners expand the capabilities of their SOF. Joint Vision 2010 provides the basics for the continuing development and advancement of US warfighting capability into the future by suggesting the following four operational concepts: "**dominant maneuver, precision engagement, full dimensional protection,** and **focused logistics**. Technological superiority has been crucial in prior successes in combat, and will continue to be so in the foreseeable future. Therefore, continuing advances in information and systems integration technologies must be aggressively developed to provide decision-makers with accurate and timely

---

[22] USSOCOM C4I Strategy into The 21st Century,USSOCOM,1996, 12.

information to gain dominant battlespace awareness."[23]

USSOCOM also has a vision for the future that expands on the concepts outlined in Joint Vision 2010 and applies them to the nature of special operations and the role of SOF. "SOF Vision 2020 provides a long-range strategy for SOF missions, force structure, equipment, and capabilities into and beyond 2020. It outlines defining characteristics that focus on quality, well-trained personnel with a superior technological edge who provide military capabilities not available with conventional forces."[24]

From the five doctrinal principles, previously discussed, the following planning considerations are derived: (1) SOF communication must be digital, (2) C4I support must depend on national systems to the maximum extent possible, (3) Access to the infosphere must be driven down to the lowest possible tactical level, (4) Communications systems do not have to follow the chain of command.

The C4I systems that support new architecture employ the latest standards and technology in transitioning to full integration with the whole information assets. "C4I architecture provides a smooth transition between operations other than war and war by utilizing the five tenets:

- Seamless: There must be a seamless connectivity in garrison, in transit, and while deployed. A capability to reach back from any location to sources of information normally available in garrison is essential. Multiple entry points into the infosphere, high-speed networks, and worldwide-assured connectivity are critical elements of this tenet.

Robust: SOF C4I systems must support a robust architecture that is flexible and adaptable to the changing needs of the special operator. This architecture assures that

---

[23] Chairman of the Joint chiefs of Staff, *Joint Vision 2010*, Chairman of the Joint Chiefs of Staff, 1996.

[24] Commander in Chief, USSOCOM, Joint Vision 2020, USSOCOM, 1996.

operational and intelligence information is successfully transmitted to the appropriate user. Robust networks feature:

- multiple routing
- alternative sources of connectivity
- bandwidth on demand
- modularity and scalability

- Automated: Maximum use of automated tools is essential for optimization. Achieving a fully automated architecture requires simplified human-computer interfaces, standard data elements, distributed interactive databases, local and wide area networks, digital switching nodes combined with dynamic bandwidth and a client-server environment. Full automation will facilitate the exchange of information with all players in the mission.

- Full spectrum: Special operations mission requirements demand exploitation of the full frequency spectrum. This harnesses the energy and resources of the global infosphere, providing robust and ready access to systems required by elements conducting special operations.

- Standard compliant: The special operations community must comply with commercial, international, federal, and DoD standards to achieve a seamless, robust, automated system."[25]

Tactical military communications heavily depend on wireless systems. On the present battlefield, it is necessary to combine wireless systems with mobility supported by computers. One of the main concerns in the mobile wireless communications would be mobility of the supporting network. For this reason, it is necessary to develop self-configuring networks to decrease the time period from days to minutes for a supporting backbone network

The SOF generally operate in a hostile environment, often in the enemy's rear area. Recent technological innovations have mostly concentrated on perfecting communications between high level users such as headquarters and a deployed

operational center. One good reason might be the need for a powerful backbone system to support the mobile end-users. With the enhancements in satellite communications, wide use of SCAMPI, implementation of Global Command and Control System (GCCS) and Global Broadcast System (GBS), the need for a powerful backbone supporting the lower echelons is almost met. Although there have been improvements in the special force team's communication support, it has not exploited the current technology enough. When we compare a hand-held push-to-talk radio and a cellular phone, we can easily understand the technological diversity that is available to the ordinary commercial user versus special operator.

D. GLOBAL MOBILE INFORMATION SYSTEMS (GLOMO) PROGRAM

DARPA's Advanced Technology Office is currently running the Global Mobile Information Systems (GloMo) Program to solve the communication problems of the future digital battlefield. This program's goal is to "develop technology for robust end-to-end information systems in a global, mobile environment."[26] They are planning to reach this goal by integrating the commercial components into flexible, robust, multihop, and high-bandwidth military systems. These specifications of ARMY are not different from requirements for SOF communications. Due to the nature of the Special Forces Units' wide-ranging and specialized missions, SOF-specific hardware needs are often unique within their particular service or military structure. However, the additional need for cost efficiency in current "minimized defense budget" forces the military to enhance the uses of commercial products with military required features. As a result, there will be

---

[25] USSOCOM C4I Strategy into The 21st Century,USSOCOM,1996, 7.

[26] Ruth, Robert, Program Manager, *GloMo BAA Outreach Brief, Global Mobile Information Systems*, DARPA, http://www.darpa.mil/ato/programs/glomo/outreachbrief.

more integrated use of commercial of-the-shelf (COTS) products in the battlefield. We will continue to investigate the use of the COTS versus military-only products, and will stress potential vulnerabilities of COTS in depth in the following section.

DARPA's suggested global information structure, which supports mobile wireless communications of end-users, has three levels: bitways (providing the communicational paths), services (providing the communications and distributed information services that support distributed applications), and the applications themselves. The basic infrastructure technology to support mobile operation can be thought of as four levels as shown in the Figure 1[27]. The lowest level consists of low-power, highly capable hardware and software to allow mobile communications. These are improved radios with sufficient processor power to support wireless networking. At the second level, the untethered nodes are robustly tied together in a wireless-networking environment. At the next level, end-to-end communications across both wireless and fixed networks is supported. Finally, to entirely use the mobile communications capability, an effective computing environment is needed to support changing and sporadic connectivity.

The critical elements in the mobile wireless architecture will be the nodes. These nodes should support the required bandwidth, range, networking, mobility, and battery lifetime. Nodes that can provide multi-megabit data rates at ranges in excess of 10 km and a battery life in excess of 24 hours would be a good first step for encouraging the potential manufacturers. These nodes should also provide frequency and media agility through a flexible and adaptive front end and have sufficient processing power to support a highly capable system of networking algorithms and management. They should be

[27] Ruth, R., http://www.darpa.mil/ato/programs/glomo/outreachbrief.

pocketsize, with a minimum possible cost. Further detailed features of these kinds of nodes are given in Figure 2.[28]

In order to evaluate the future communications systems, one must examine thoroughly the patterns that today's communications have followed. In fact, the pace of the technology is so fast that our evaluations will be limited to the near future of the next five to ten years at most. The early mobile wireless communications equipment began

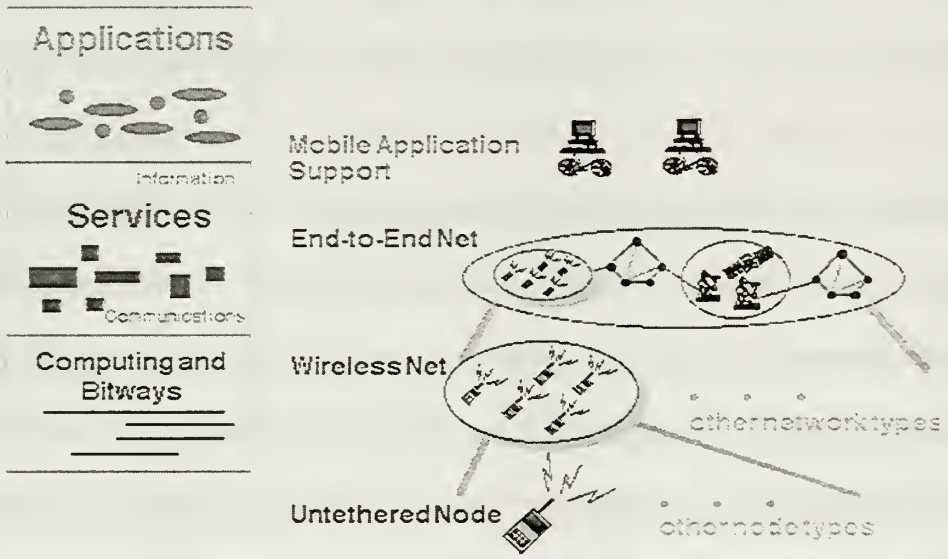


Figure 1. Mobile Wireless Architecture.

[28] Ruth, R., http://www.darpa.mil/ato/programs/glomo/outreachbrief.

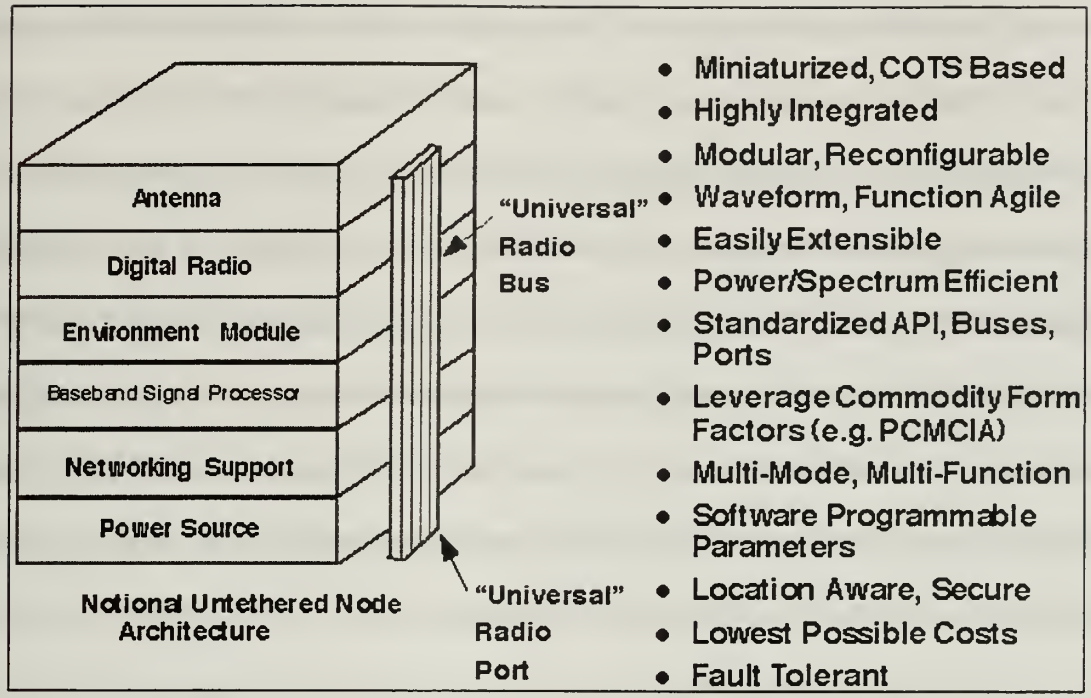


Figure 2. Untethered Node Desirable Features.

using analog techniques with push-to-talk radios. Those radio devices were very clumsy, and performed poorly against electronic countermeasures like jamming. They were easy to determine and intercept. Quality of service was very low, hardly allowing more than one-way traffic. They were mainly line-of-sight devices with very limited ranges.

For many years, developers had concentrated on the range improvements. By increasing output power, using new antennas, and projecting waves from the atmospheric layers, they had managed to send the information up to several thousand kilometers. However, increasing ability to intercept and detect the communication had made them concentrate on dispersing signals throughout the frequency band. Thus, frequency-hopping devices were introduced during WWII. Meanwhile, early use of codes in the message was replaced by encryption, including the introduction of the digital techniques. The use of digital communications introduced the use of high throughput for bursty

sending against detection/interception, and channel access methods for allowing many users be able to use the same media without colliding with each other. The improvements in the last two decades occurred very quickly, usually on an order of magnitude higher with respect to previous periods. Today, the level of data rate, global coverage, battery life, sizes and output power are very developed in comparison to the early 1990s. This speed of change frightens researchers because it is possible that their model might be outdated before going into effect. For this reason, military system designers and planners have a critical need for simulation tools that can accurately predict the performance and behavior of mobile wireless networks.

After having these improved nodes, wireless networking technology can be built upon the untethered node technology to support mobile operations. The networking technology must be easy to deploy and require little network management through self-organization. The same networking technology should also support peer-to-peer wideband communications, multi-hop network algorithms, effective bandwidth utilization, high performance services (e.g. real-time image transferring), and compatibility with National Information Infrastructure networking technologies (e.g. Internet). This last area has requires further attention.

The Internet is an information infrastructure that is almost globally used. Although it was not developed with security-in-mind during its early years in the 1970s, recently there has been an increasing concern about information security on the net. The use of the Internet by the military, at least in some light cases, will decrease the burden of the global military communications. The main concern of the military is to control resources on the Internet. Since the sender cannot control all the routers on the path, the

message can be caught by malicious personnel or the enemy, or the enemy at least may configure the message traffic to reach some military patterns used by the friendly forces.

The Internet has grown enormously in the last decade. Prior to this decade, it was accepted slowly and mostly used in academia. However, recent improvements have showed us its future potential. Improved security has enabled the Internet to be widely used for commercial and personal communications. The introduction of Virtual Private Networks (VPN) has improved the opportunity for secure and private communications. Moreover, with the introduction of the Mobile IP, user mobility was supported throughout global networks such as the Internet. Next, recent innovations in wireless personal communications forced the Internet to support wireless connections and communications. Current users are able to make wireless mobile communications through the Internet, but further research and investments are needed to improve the quality. While the commercial world is continuing its profit-in-mind way, the governmental and military foundations might direct them towards a combination of profit-in-mind and security-in-mind innovations. Thus, the vast amount of expenses that are spent on R&D will be reduced, and big cost savings can be obtained.

E. AVAILABILITY OF PUBLIC COMMUNICATION INFRASTRUCTURE FOR SPECIAL OPERATORS

In this section, we will try to evaluate the suitability of commercial wireless technology for military applications. The wireless communication revolution is bringing fundamental changes to data networking and telecommunications. Furthermore, an integrated network is becoming a reality. By freeing the user from the cord, personal communications networks, wireless LAN's mobile radio networks and cellular systems, promise fully distributed mobile computing and communications anytime, anywhere.

It is nothing new that commercial products are used by the military. The current SCAMPI is "a robust, seamless, C4I system which takes advantage of commercial and government of-the-shelf equipment" and is widely used in the SOF. On the other hand, there are fundamental differences between commercial and military mobile wireless networks, although they provide similar functionality. "Commercial wireless networks, which are perhaps best exemplified by the cellular phone systems, depend on a fixed supporting infrastructure of base stations interconnected by high-speed trunk lines. The topology of the supporting network is fixed, which greatly simplifies the routing of connections. Military ground-based mobile wireless networks cannot depend on a static-supporting network for several reasons; the most important of these are;

- Highly mobile forces need networks that move with them,
- Fixed assets are more vulnerable to attack,
- The military needs networks that will continue to function even when some nodes are destroyed and some links are jammed."[29]

Commercial mobile wireless services include cellular telephony, personal communications services (PCS), paging, wireless data services, interactive and low/high rate data over low earth orbit (LEO) satellites. The military's major concern about the use of these services is that their waveforms are not designed against jamming or to provide low probability of detection (LPD). Moreover, detailed waveform characteristics of them are mostly available to the public. "With the military systems, potential adversaries cannot begin to collect information about the system and develop countermeasures until the system is fielded and used. Developing jammers or direction-

[29] Feldman, P.M., Emerging Commercial Mobile Wireless Technology and Standards, RAND, 1998, xi.

finding equipment that is optimized for use against the system can thus be delayed by several years. With standards-based systems, developers of the systems and developers of the countermeasures both begin to work at the same time."[30]

Cellular telephony, PCSs, paging and wireless data services might be the first group of alternative communications systems offered by the commercial world. In comparison with the military-only equipment, the service price and cost of the equipment is very low. On the other hand, these systems have similar disadvantages when used by the military. The military needs systems and services that can be used anywhere they may need to operate. However, most of these systems will be available in populated areas, and along the major highways. These systems heavily depend on wired structures that might be destroyed by the enemy. Since these systems are open to the public, military users have to compete with general users for access to the resources. They do not support secure end-to-end encryption. The lack of worldwide standards causes different equipment to be used for communications. Moreover, different frequency allocations in different regions of the world prevent the use of a single phone in all of the different locations. "Tactical use of existing cellular telephone networks makes sense only for peace keeping ... operations in the urban and suburban areas."[31] Since SOF have a wide area of operational responsibility, it may be more possible to use these systems than conventional military forces. Firstly, they are available during peacetime, and give an alternative for communications. During exercises or training, these systems may be used as an emergency means of communications. Secondly, it is becoming more

---

[30] Ibid., 46.

[31] Ibid., 62.

and more difficult to control private commercial life. Thus, during an operation in a hostile environment which has enough coverage for the recalled systems, it will be difficult for the authorities to decide to shut down the whole system, since these systems are used by the target nations as well. Briefly, the enemy will have difficulties in applying electronic countermeasures against commercial systems, especially during situations short of war. However, it is still a viable course of action, and in some cases the national security policy of the target nation might force it to shut down the communications systems regardless of whether or not the system is vital. For example, let us assume a global system such as the Iridium were successful. If an operation is using the Iridium communications system as its main and contingency communications system then there is a risk of not finding the Iridium resources available during the critical seconds of the operations. On the other hand, one must not forget that the ability to track the user and obtain the content of the communications is still mostly available to the enemy.

The other set of choices might be the use of the medium earth orbit (MEO) or low earth orbit (LEO) satellite systems, which covers most of the world. This second group costs more than the first group of systems. Their main services would be interactive voice, low-rate data and high-rate data. There are several alternatives to this group, such as Teledesic, Iridium, Globalstar. However, their future success seems uncertain due to the lack of enough users to make all proposed investments profitable. These systems also have certain drawbacks for military users. They are far from supporting enough capacities in every region of the world. Like cellular systems, there is no user prioritization, so military users have to compete with others. Most of them depend on

regional Earth stations that can be destroyed as a target. Each individual sovereign state has to accept the use of these systems in its country. Without this agreement, the use of the systems will be illegal. For pricing, each handset is given an identification number and home location. Each device is tracked to appropriately price the communication and the device's unique information is sent without encryption. This might cause security problems for military purposes. All of these systems are very susceptible to jamming.

In the area of commercial satellite use, we see the SOF ahead of the rest of the military. Since they are generally involved in contingency operations, no single means of connectivity would support enough capacity and reliability all over the world. For this reason, the SOF uses commercial satellites as an additional means of communications. INMARSAT, International Maritime Satellite Organization, is "one of first communications links established by special operations deployed forces."[32]

Although the needs of the military are significantly different (Figure 3) from the commercial world, consultations with a standards working group might help establish future capabilities. The dialogue and active exchange of information between the military and the commercial world might create new techniques and services that are mainly planned for commercial use but also suitable for military purposes.

---

[32] C4I Handbook, 5-5.

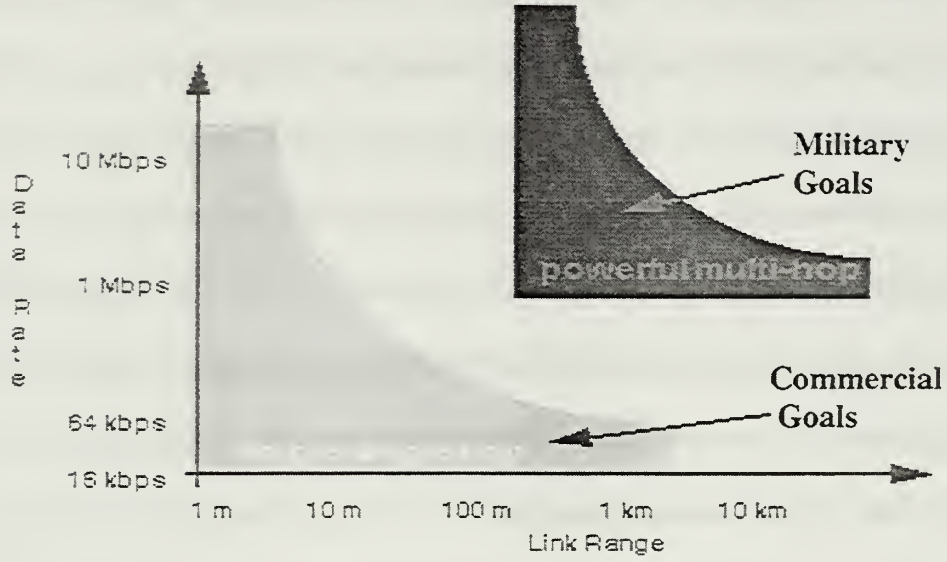


Figure 3. Different Goals of the Military and Commercial Worlds on their Specifications for Wireless Nodes.[33]

One last point to remember will be the overall security concerns about a robust, secure, commercially available and affordable communications system. Due to increasing threats from transnational criminal organizations and terrorist groups, such communications systems will give malicious users new opportunities to violate security. Therefore, it is not necessary to build uniform systems for all users. Special licenses or equipment might give law enforcement and the military forces access to those required specifications while regular users have enough already available for modern communications. One example would be the use of GPS. Currently it is used all over the world. However, certain users, like the military or aviators, have different security measures and robustness built-in to their equipment via special equipment and software which does not exist in the ordinary user machine.

[33] Ruth, R., http://www.darpa.mil/ato/programs/glomo/outreachbrief.

Government policies supporting the development of appropriate defense technologies have always been a special case. In the past, when defense requirements generally guided commercial sector technology advances, government investments in R&D were not disputable. Now sophisticated consumer and industrial products are developed independent of defense requirements, and thus the need for federal investments may seem less pressing. The government influences commercial sector technology development in a variety of ways. The instruments of government policy may include indirect methods such as decrease in taxes, or direct methods such as funding for R&D. Sometimes these policies are implemented to accelerate the development of strategically important technologies; at other times the motive is to ensure that equipment will be available at the right time.

Current public communication infrastructure (such as the Internet) has not been developed with security in mind. This infrastructure might not be convenient for military purposes, but the implementation of encryption techniques and use of VPNs could add leverage to the current system until more secure systems (such as Internet II) could be developed. In the case of the Special Operations Forces, the current infrastructure can be used for communication purposes given certain enhancements such as encryption. If we categorize the content of the communications, some information, which is valid for a very limited time or not as vital as other categories, might be transferred via public systems. This will reduce the burden of the real communications channel and will increase their quality of service. For future developments, the military could urge the commercial world to meet its requirements starting in the early phases of the development cycle. This possible consultation system will benefit both sides while the

military is cutting huge R&D resources. On the other hand, the commercial world will have the military among its customers as usual. "With commercial demand for wireless technology growing worldwide and defense budgets flat or falling, incentives for future commercial-military cooperation need to be provided by the military side."[34]

[34] National Research Council, *The Evolution of Untethered Communications*, National Academy Press, Washington, D.C. 1997, http://www.nap.edu/readingroom/books/evolution/index.html .

III. MODELING AND SIMULATION

A. MODELING

"Performance evaluation is required at every stage of in the life cycle of a computer system, including its design, manufacturing, use, and upgrade."[35] Performance evaluation can be done by three different techniques: analytical modeling, simulation, and measurements. For a new concept, analytical modeling and simulation are the only available techniques. "In general, analytical modeling requires so many simplifications and assumptions that if the results turn out to be accurate, even the analysts are surprised. Simulation can incorporate more details and requires less assumptions than analytical modeling and, thus, more often are closer to reality."[36]

Simulation is the process of mimicking – or approximation - reality. It involves designing a model of a system and carrying out experiments on it as it progresses through time. It can be accepted that "one deals with a real thing while working with an imitation. In operations research the imitation is a computer model of simulated reality."[37] A wireless mobile communication model may be simulated to determine the performance of the system. "The simulation analyst develops the skills to observe and translate events, ideas, and attributes of pertinent surroundings into a model."[38]

Simulation modeling involves testing ideas by conducting what-if analyses. In each scenario, the inputs are altered and the output parameters are observed at the end of

---

35 Jain, R., The Art of Computer Systems performance Analysis, 1, 1991.

36 Ibid., 31.

37 Arsham, H., *System Simulation*, http://www.cs.sun.ac.za/~lynette/simulation/harsham.html.

38 Avni, T., Simulation Modeling Primer, IIE Solutions, Sep 1999, 39.

the simulation run. Simulations may be performed manually. Most often, however, the system model is written either as a computer code or as some kind of input into simulator software. "A key characteristic of simulation modeling is the ability to incorporate the behavior of key system elements into a computer "mock-up" of the area under investigation."[39] The repeating and computationally intense nature of simulation analysis lends itself to the use of computer software. Computer simulation modeling has evolved over the last two decades into a powerful tool for understanding operational issues in communications networks.

Why do we use simulations? It is much cheaper and safer to fly a simulated model than the real aircraft. It is very costly, dangerous or often impossible to conduct experiments with real systems. After being validated, models as the adequate descriptions of the real system, can save money, suffering and time if the experiments are conducted using them. With the use of a proper simulation model, "an analyst can:

- Predict the course and result of certain actions
- Understand why observed events occur
- Identify problem areas before implementation
- Explore the effects of modifications
- Confirm that all variables are known
- Evaluate ideas and identify inefficiencies
- Gain insight and stimulate creative thinking
- Communicate the integrity and feasibility of his/her plans"[40]

---

[39] Zilm, F., *Simulation Modeling*, http://www.zilm.com/simulati.htm.

[40] Rivera, J., Diamond, P., EXTEND user Manual, 4,1997, 4.

By using simulation modeling one can manage change and minimize the risk. Change is a process that we experience continuously. In every change process there is uncertainty. This uncertainty creates risk for the planner and analyst. The use of what-if analyses enables us to test various alternatives and chose the best one before any action is taken. The result is the attainment of goals in an efficient manner. With the reduction of risk, the flow of ideas gains momentum, and brainstorming results in creativity. Without the presence of simulation modeling, breakthrough changes may never even be proposed.

"The development and implementation of a simulation model typically moves through three phases:

- Model definition and data collection
- Model validation
- Simulation of proposed plans and outcome analysis"[41]

A model is the expression of reality in a controlled environment. It possesses the prominent characteristics of the object, concept, or the system it represents and logically describes how a system performs. A model fighter jet, for example, has geometric attributes similar to a real one but on a reduced scale. A communication networks model may contain interdependent elements and events. "One of the principal benefits of a model is that you can begin with a simple approximation of a process and gradually refine the model as your understanding of the process improves. This 'step-wise refinement' enables you to achieve good approximations of very complex problems surprisingly quickly. As you add refinements, your model becomes more and more

[41] Zilm, http://www.zilm.com/simulati.htm.

accurate."[42] While defining and developing a model one has to decide continuous-time vs. discrete-time, continuous-state vs. discrete-state, deterministic vs. probabilistic, static vs. dynamic, linear vs. nonlinear, open vs. closed, and finally stable vs. unstable.

Models are either static or dynamic. The increased computational power and speed of today's computers, coupled with the need for more exact answers, has vaulted dynamic modeling ahead of static modeling as the method of choice.

1. Static Models

Static models describe a system mathematically, in terms of equations, where the potential effect of each alternative is ascertained by a single computation of the equation. The variables used in the computations are averages. The performance of the system is determined by summing individual effects. Spreadsheets are static models. Static models ignore time-based variances. For example, you cannot use them to determine the impact of when something occurs in relation to other incidents. Also, static models do not take into account the synergy of the components of a system, where the actions of separate elements can have a different effect on the total system than the sum of their individual effects would indicate.

2. Dynamic Models

Dynamic modeling (also known as simulation) is a software representation of the dynamic or time-based behavior of a system. While a static model involves a single computation of an equation, dynamic modeling, on the other hand, is iterative. A dynamic model constantly recomputes its equations as time changes. Dynamic modeling can predict the outcomes of possible courses of action and can account for the effects of

---

[42] Rivera, J., Diamond, P., EXTEND user Manual, 4,1997, 5.

variances or randomness. You cannot control the occurrence of random events. You can, however, use dynamic modeling to predict the likelihood and the consequences of their occurring.

During the development of the simulation model, one must ensure that the model is correctly implemented and that it is representative of the real system. After model development is complete, it must be verified and validated. "Since a number of assumptions about the behavior of real systems are made in developing the model, there are two steps in measuring the goodness. The first step is whether the assumptions are reasonable, and the second step is whether the model implements those assumptions correctly. These two steps are called *validation* and *verification*. Validation is concerned with the representativeness of the assumptions, and the verification is related to the correctness of the implementation."[43]

The last phase of the simulation modeling is the analysis of the output data and presentation of the results. "In many simulation studies a great deal of time and money is spent on model development, but little effort is made to analyze the simulation output data appropriately."[44] Statistical techniques are used to analyze the output data from the production runs. Typical goals are to construct a confidence interval for a measure of performance for one particular system design or to decide which simulated system is best relative to some specified measure of performance. Since simulation models are often used for more than one application, it is important to document the assumptions that went into the model. Finally, a simulation study whose results are never implemented is most

---

[43] Jain, 413.

[44] Law, A.M., Kelton, W.D., *Simulation Modeling & Analysis*, McGraw-Hill, New York, 1982, 522.

likely a failure. Furthermore, results from highly credible models are much more likely to be used.

Military analysts have been using the simulation modeling techniques from the beginnings of computerized simulation. Simulation has played an important role in both the design process and in training personnel to use advanced technologies. New concepts can be implemented in virtual environments and tested at relatively low cost. It will be less expensive to model a new system with a simulator than to physically build a demonstration prototype. It is possible to use different values of parameters, loads or configurations using computerized simulation tools. This allows the analyst to assess the performance of the system under different scenarios and plan or change the configuration of the system accordingly. Simulators allow users to examine emerging system's interfaces with current military, commercial and joint networks, and they provide a method for testing future technologies and capabilities. Moreover, they enable the users to evaluate communications network performance, to test the effects of system outrages, to stress under high load, and to see how a network behaves under an agile special operations environment. The cost of building a user-specific simulation model is very high nowadays. For this reason, most simulation studies are conducted using commercial-of-the-shelf (COTS) software packages. "Dynamic modeling tools greatly facilitate the model-building process. A good modeling tool is flexible enough to fit a specific project, company, or industry. It should provide benchmark figures for comparing current 'as is' processes to future 'to be' processes, allow you to explore alternative approaches, help you determine how to prudently use resources, and show

where to eliminate tasks that add no value. Dynamic modeling tools abound. They range from general purpose to specialized applications"[45]

There are specialized tools for various applications such as manufacturing and communications. Although the software is becoming more user-friendlier by employing graphical interfaces, some amount of programming is still required to manage complex problems. On the other hand, there are some complaints about the quality and fitness of the COTS software packages for military purposes: "Military system designers and planners have a critical need for simulation tools that can accurately predict the performance and behavior of mobile wireless networks operating in realistic tactical environments. Existing tools tend to concentrate on either the middle protocol layers or the lower physical layer, and they do not simultaneously model all of the layers with sufficient details and accuracy to yield useful results."[46]

B. NETWORK SIMULATION AND MODELING TOOLS

Network performance analysis can take three forms: mathematical analysis, experimental trials, or system simulation. Mathematical analyses can incorporate only a limited range of realistic phenomena, and field trials are expensive as well as difficult to set up under repeatable conditions. Consequently, simulation is often the best tool for optimizing system design and predicting performance.

Network-level simulation tools are used to simulate the dynamic behavior of routing, flow, and congestion-mitigation schemes in packet-switched data networks. These tools can model arbitrary network topologies, link-error models, router scheduling

---

[45] http://www.imaginethatinc.com/pages/case_studies.html#Anchor-Simulation-47857.

[46] Feldman, P.M., Emerging Commercial Mobile Wireless Technology and Standards, xii, Santa Monica, CA, RAND,1998.

algorithms, and traffic. Network simulators have been used to investigate new link-layer algorithms for packet scheduling and retransmission, new mechanisms within routers for determining local congestion conditions and sending this information to transmitters and receivers, and transport-layer algorithms for retransmission and rate control. Performance tools can also help troubleshoot problems in real networks by collecting statistics about the throughput of the various nodes and links. This information can be used to identify bottlenecks and develop remedial strategies such as changing the topology of the network.

To model mobile networks accurately, simulators require special features, some of which have yet to be developed. They need to model the nature of errors on the wireless link precisely because errors are not uniformly distributed but rather tend to cluster. They also need to model node mobility, especially in the case of packet radio networks. Existing simulation technology consists of good models of radio propagation at microwave frequencies but only standard teletraffic models and little abstract mobility models. Some proprietary tools integrate geographical modeling, propagation, and cellular networking behavior, but no integrated tools are available commercially to predict the performance of the next generation of wireless technologies, such as smart radios.

Similarly, existing tools can simulate the creation of relatively narrowband waveforms at the transmitter and analyze the effects of radio propagation on the received signal, but they cannot model the antenna radiation or reception properties of a signal that spans more than 1 GHz of spectrum. No existing tool can model the propagation performance of urban, suburban, rural, or free-space radiation of wideband signal-

containing components with diverse propagation characteristics. No tool can analyze the effects of the motion of network elements on the received signal's multipath characteristics, such as spectral nulls and Doppler shift over wide bandwidths. No widely available tools allow for the geographical or topological analysis of specific network deployments. Finally, no analysis tool is sophisticated enough to examine the performance of software radios or radio networks in the presence of interference sources common to wideband mobile communications. The evaluation and optimization of mobile wireless networks would be enhanced by the development of sophisticated, flexible models of communications traffic and node mobility.

The following section includes an evaluation for four different COTS simulation software packages; EXTEND, COMNET III, OPNET and GloMoSim. The selection of the packages is based on availability to us and the suggested use of the software packages in wireless mobile communications networks.

1. Extend

Extend, developed by Imagine That Inc., is an advanced simulation tool designed to develop dynamic models for real-life processes. It is a dynamic, iconic simulation environment with a built-in development system for extensibility. It enables the user to simulate discrete event, continuous, and combined discrete event/continuous processes and systems. By using EXTEND, the user can predict the course and results of certain actions, and can understand why observed events occur. Moreover, the user can identify problem areas before implementation and explore the effects of modifications.

EXTEND uses icons or building blocks to build models. There are fifteen libraries of various building blocks included with EXTEND. These building blocks

represent the smallest level of function of a model. The user can build communications network requirements based on the building blocks. However, this requires the user to be good at modeling. "Since each EXTEND block has a predefined functionality, the user merely need to enter parameters into each block's dialog box. Data can be entered directly into block dialogs, interactively using controls, or read in from files as the simulation runs. For example, clicking a button can select a probability distribution or change a queue from LIFO to FIFO. Dialog boxes also provide the user with other vital simulation information like utilization rate, number of items entering or leaving the block, queue length, etc."[47]

EXTEND is written in ModL, a C-based language. The tool is very user friendly with its graphical user interface (GUI). The user can quickly and easily create models by selecting building blocks from the menu of libraries, and connecting building blocks to simulate the basic functions and flows of the system. The product supports Monte Carlo and batch mode simulations. The data can be inserted via two means; input random number menu and input data menu. The first provides the user with a distribution selection, and the second enables the user to enter specific data values such as a trace. The tool provides results consistent with the input parameters and the model. The user's ability to create building blocks could effect the behavior of the model. EXTEND's degree of accuracy is based on the user design. A properly designed model will produce plausible results.

Due to EXTEND's purpose of modeling real life processing, many of its features are not communications network specific. On the other hand, it is the generic structure of

---

[47] http://www.imaginethatinc.com/frame_products.html.

the package that enables the user to model communications and computer networks by expanding the user's area of choice.

2. COMNET III

COMNET III, developed by CACI Products Company, is a network-planning tool with an object-oriented environment. It supports the modeling of a wide range of communications networks such as LAN and WAN. Using a drag-and-drop tool palette and libraries of hardware and protocols, users graphically create a hierarchical model of their proposed network. COMNET III simulates the network's detailed operation producing dynamic animation and reports describing the network performance. COMNET III allows the user to:

"Predict end-to-end delays, throughputs, and utilization of links, buffers and processors.

Reproduce random and bursty traffic patterns

See peak and valleys of traffic- not just snapshots and averages

Pinpoint sources of delays and bottlenecks"[48]

The source software code is unavailable to the user. The product is a simple drag-and-drop icon and menu based application. It enables the user to further detail the simulation by using simple if-then code blocks in modules.

The package has user-friendly features. The network topologies are quickly developed using drag-and-drop icons and a menu driven environment. Double clicking on the various network objects alter parameters quickly.

---

[48] COMNET III User Manual, 1997.

The product supports discrete and continuous random variable data through tables. The discrete data is based on inputs from the user and a step distribution. The continuous data is based on a selected user probability distribution function. The tool reliably provides results consistent with the input parameters. COMNET Baseliner, an add-on feature, enables the user to model existing networks with realistic external data.

The basic steps to build a model using COMNET III are to define the topology, and establish traffic and computer loads. Upon competition of the model, the product does a quick verification of the network connections. The user can easily alter the simulation clock and run duration. Reports, selected by the user, are automatically generated during the run.

The Satellite and Mobile Module is a different package supporting satellite and mobile communications. "Not limited strictly to satellites, the Satellite and Mobile Module can assess the time-varying parameters of various mobile nodes such as airplanes and land vehicles. The Satellite and Mobile Module gathers data that helps the user visualize each satellite's location in time, determine when it has access to a ground station, and study what its sensor can 'see'. This 'physical view' of the mobile nodes can then be imported into COMNET III with the Satellite and Mobile Module's interface software."[49]

The user is provided with the "logical" or "network layer" view of how data is transmitted. It is possible to perform capacity planning scenarios to examine network performance. With each changing scenario, the Satellite and Mobile Module and COMNET III interface with one another to determine whether or not modules and nodes

[49] http://www.caciasl.com/comnet/netperform/satellite_main.cfm.

can communicate. Using the Satellite and Mobile Module with COMNET III allows the user to assess the effect of moving nodes on end-to-end performance of the communications network.

COMNET III is a simple network-planning tool with an additional module supporting wireless mobile communications. It provides a good method for performance and network analysis of computerized communications networks.

3. OPNET

OPNET Modeler is a COTS tool for the modeling and simulation of communications networks, devices, and protocols. Its object-oriented modeling approach and graphical editors mirror the structure of actual networks and network components. Originally developed at MIT, and introduced in 1987 as the first commercial network simulator, OPNET Modeler has the following important features:

- "Hierarchical network models. Manage complex network topologies with unlimited subnetwork nesting.
- Object-oriented modeling. Nodes and protocols are modeled as classes with inheritance and specialization.
- Clear and simple modeling paradigm. Model the behavior of individual objects at the process level and interconnect them to form devices at the "Node Level"; interconnect devices using links to form networks at the "Network Level".
- Comprehensive support for protocol programming. 400 library functions support and simplify writing protocol models.
- Wireless, point-to-point and multipoint links. Link behavior is open and programmable.
- Geographical and dynamic mobility modeling (for mobile and satellite networks)."[50]

[50] http://www.mil3.com/products/modeler/home.html.

The source code of the tool is unavailable to the user. The user can program input and exit criteria for simulation by using Proto-C, a language very similar to C. It has the most complicated aspects among the available COTS. Due to its detailed nature, it is difficult for an inexperienced user to understand all of its qualities in a short period of time. OPNET modeler enables the user to model events at the process and states level. The user adds the nodal model and then combines all of them into a network. This enables the user to have very powerful modeling capabilities.

OPNET allows users to use built-in Generator Modules. Moreover, it enables the use of "stochastic traffic sources, based on a user selected probability function, for creating message inter-arrival times, and uses deterministic sources to specify exact times for message/packet generation."[51] External model Access includes the capability to extract data from another model.

The product allows the user to execute iterative runs. Various probes can be set up for each of the runs. Separate output data files must be established prior to execution. The results are consistent with the input parameters and models. It is easy to validate a sample model, by simulating the model with measurement data. This must provide results consistent with real data.

OPNET Modeler/Radio includes the added capability of modeling radio links and mobile communications nodes. This additional tool allows user to specify transceiver frequency, bandwidth, and power, as well as optional spread-spectrum characteristics. The analysis capabilities of the radio tool include the recording of standard statistics such

---

[51] OPNET Unix Online Manual.

as channel utilization, received power levels, signal-to-noise ratio, and bit and packet error rates.

The OPNET modeler is a sophisticated tool for modeling and simulating communications systems. Although it possesses a user-friendly environment, it is not for beginners because of its complexity. However, this is the powerful aspect of the product.

4. GLOMOSIM

The GloMoSim is an application developed for simulating large-scale wireless systems using the Parsec[52] simulation language. The GloMoSim was developed by UCLA and it is a continuing effort. The goal is to build a library of paralleled models that can be used for the evaluation of a variety of wireless network protocols. The proposed protocol stack includes models for the channel, radio, MAC, network, transport, and higher layers. The simple approach to designing a network simulation would be to initialize each network node in the simulation as a Parsec entity.

Different entity initializations can be viewed as being separate logical processes in the system. Therefore each entity initialization requires its own stack space in the runtime. With GloMoSim, the developers are trying to build a simulation that will scale to thousands of nodes. If one has to instantiate an entity for each node in the runtime, the memory requirements would increase dramatically. The performance of the system would also degrade rapidly. Since there are so many entities in the simulation, the runtime would need to constantly context switch among the different entities in the system. This will cause significant degradation in the performance of the simulation.

---

[52] Parsec (PARallel Simulation Environment for Complex systems), http://pcl.cs.ucla.edu.

Hence initializing each node as a separate entity will inherently limit the scalability and performance of the simulation.

Given these limitations, the developers at UCLA decided to integrate the various GloMoSim layers into a single entity. Each entity now encompasses all the layers of a simulation. Instead, each layer is now implemented as functions in the new design. An initialization function that will be called for each layer of each node at the beginning of the simulation is provided. Moreover, the developers provide functions that can be used to send messages between the layers. When a layer receives a particular message, it will automatically invoke a function that is provided by the developer of that particular layer. Based on the contents of the message, the function can then execute the appropriate instructions. At the end of the simulation, a function is also called for each layer of each node. A layer can use this function to collect any relevant statistics. An actual implementation of a particular layer will be shown shortly.[53]

The simulation language used for GloMoSim is PARSEC and it is a C-based discrete-event simulation language. It adopts the process interaction approach to discrete-event simulation. A logical process represents an object or set of objects in the physical system. Interactions among physical processes are modeled by timestamped message exchanges among the corresponding logical processes.

The source code of all the entities is available for research purposes. Users can make modifications and recompile the code to test different parameters for the protocols and applications.

---

[53] For latest information about GloMoSim, visit UCLA's related web site: http://pcl.cs.ucla.edu/projects/glomosim/GloMoSimManual.html.

We will use GloMoSim for testing different routing protocols using different scenarios. A detailed procedure for using GloMoSim in our study will be given in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. WIRELESS AD HOC NETWORKS

We will explore specifications of wireless mobile communication and necessities for developing ad hoc network. "The present situation recalls previous epochs in which breakthroughs in hardware – aircraft carrier, jet aircraft, tactical missiles, nuclear weapons- have lead to a radical revision of military doctrine. The next great revolution in military affairs could be shaped by information technology: global communications, ubiquitous sensors, precision location, and pervasive information processing."[54]

"Wireless systems, especially those serving mobile users, are extremely complex. A network needs to be capable of rerouting information seamlessly and effectively as users move, and sophisticated digital signal processors and antennas are needed to minimize the interference, distortion, jamming, and interception without undue power burdens on portable devices."[55]

The ideal wireless communications system would provide high data rates with high reliability and yet use limited bandwidth and power. It would perform well in wireless propagation environments despite multiple channel impairments such as signal fading and interference. The ideal system would accommodate hardware constraints such as imperfect timing and nonlinear amplifiers. The mobile units will have low power requirements and yet still provide adequate transmit power and signal processing.

We are interested in those capabilities that must be put in place to support nomadicity. The desirable characteristics for nomadicity includes independence of

---

[54] National Research Council, *The Evolution of Untethered Communications*, National Academy Press, Washington, D.C. 1997, http://www.nap.edu/readingroom/books/evolution/index.html.

[55] Ibid, http://www.nap.edu/readingroom/books/evolution/index.html.

location, motion, computing platform, communication device, and communication bandwidth, and widespread presence of access to remote files, systems and services. Some of the key system parameters of concern include bandwidth, latency, reliability, error rate, delay, storage, processing power, interference, version control, file synchronization, access to services, and interoperability. These are the usual concerns for any computer communication environment. What makes them of special interest for us is that the values of these parameters change dramatically as the mobile user moves from location to location. In addition, some totally new and primary concerns arise for the mobile users such as weight, size, and battery life of the portable devices, in addition to the unpredictability and wide variation in the communication devices and channels.

There are fundamental research problems that arise in the development of a mobile wireless architecture and system. Kleinrock expresses[56] one of them as developing a reference model for mobility. This model should characterize the view of the system as seen by the user and the view of the user as seen by the system. The dimensions of this reference model might include system state consistency, functionality and local awareness. The system has to be consistent in different levels such as link layer, network layer and application layer. This is important for the robustness of the communications. In addition, the system should offer different functionality in bandwidth and quality of service. Finally, the mobile user is able to aware of the resources offered by its current environment.

Among several wireless mobile architectures, our interest will be on ad hoc infrastructures. These mobile multihop radio networks are expected to fulfill a critical

---

[56] Kleinrock, L., *Nomadic Computing and Communications*, UCLA,

role in applications in which a wired backbone network is not available or not economical to build. These networks, also known as peer-to-peer networks, provide a good solution in situations where instant infrastructure is needed and no central system backbone and administration (like wired backbone and base stations in a cellular system) exist. For example, disaster relief, emergency operations, special operations, and clandestine operations are all cases where no base station infrastructure can be assumed. In the case of operating without base stations, maintaining communications is considerably more difficult. For example, it may be that the destination for a given reception is not within range of the transmitter, and some form of relaying (multihop routing) is required. In the tactical arena, the hostility of the environment prevents the application of a fixed backbone network. In our research, a peer-to-peer mobile network consists of a large number of mobile radio nodes that create a network on demand and may communicate with each other via intermediate nodes in a multihop mode, that is to say every node acts as a router.

Since there are no fixed-location base stations, the connectivity of the network is subject to considerable change as devices move around and/or as the medium changes its characteristics. More simple scenarios such as static topology with one-hop communications, and static topology with multihop communications have their own well-known network algorithm. In the case of dynamic topology with multihop, the devices are allowed to move, which causes the network connectivity to change dynamically. Location Control, Adaptive Topology Control, and Adaptive Base Station Control algorithms have to be implemented to manage a successful ad hoc wireless network.

---

http://stills.nap.edu//html/whitepares/ ch-40.html.

A. WIRELESS ARCHITECTURE

The choice of architecture for a two-way wireless network involves numerous issues dealing with the most fundamental aspects of network design. The primary issue is whether to use a peer-to-peer or a base-station-oriented network configuration. In a peer-to-peer architecture, communication flows directly among the nodes in the network and the end-to-end process consists of one or more individual communication links. In a base-station-oriented architecture, communication flows from network nodes to a single central hub. In cellular networks with base stations connected into a wired backbone, the handling of mobility (such as handoffs, paging, user tracking, etc.) has been a well studied problem in the last decade, and many good solutions have been proposed. In these networks the wireless part of the communication is reduced to a single-hop problem because mobile nodes communicate directly with the fixed base stations.

The choice of a peer-to-peer or base-station-oriented architecture depends on many factors. Peer-to-peer architectures are more reconfigurable and do not necessarily have a single point of failure, thus enabling a more dynamic topology. The multiple hops in the typical end-to-end link offer the advantage of extended communication range, but if one of the nodes fails, then the localized link path needs to be reestablished. Base-station-oriented architectures tend to be more reliable because there is only one hop between the network node and the central hub. In addition, this design tends to be more cost-effective because centralized functions at the hub station can control access, routing, and resource allocation. Another problem with a peer-to-peer architecture is the significant co-site interference that arises for multiple users in close proximity to each

other—a problem that can be averted in a base-station-oriented architecture by the coordinated use of transmission frequencies or time slots.

The wireless base-station-oriented architecture is exemplified by cellular telephone systems, whereas the most common peer-to-peer architecture for wireless systems is a multihop packet radio. Fundamental differences between the two types of systems are indicated in Table 1.

Feature	Cellular System	Multihop Packet Radio
Topology	Static	Dynamic
Number of hops	One	Multiple
Network control	Centralized	Distributed
Link distance	Fixed (by cell size)	Variable

Table 1. Comparison of Cellular and Multihop Packet Radio Architectures.

It has been recognized that the reuse of existing cellular architectures in multihop peer-to-peer networks is desirable and will be helpful for seamless communication across fixed and mobile networks. Chlamtac and Farago suggest[57] mapping a cellular architecture into the multihop network via the *Virtual Cellular Architecture* (VCA) concept. This concept is based on *clustering* in packet radio networks.

The architecture of an ad hoc network can be either *flat* or *hierarchical*. In a hierarchical network, the network elements are partitioned into several *clusters*. In each cluster, there is a clusterhead, which is selected to manage all other nodes within the cluster. The depth of the network can vary from a single tier to multiple tiers. Examples of a flat network and a two-tier hierarchical network are shown in Figures 4 and 5.

[57] Chlamtac, I., Farago, A., A New Approach to the Design and Analysis of Peer-to-Peer Mobile Networks, Wireless Networks 5, 1999, 149-156.

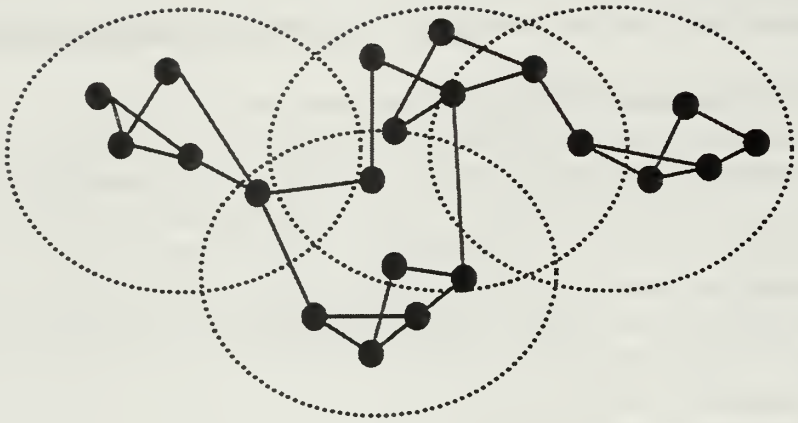


Figure 4. A Flat Ad Hoc Network.

In the case of a flat network, each terminal in the network also has the role of the router, but the frequent changes in the terminal locations results in a waste of time, energy, and computing power for updating the routing tables. This also will induce call droppings due to the disconnection between routing terminals.

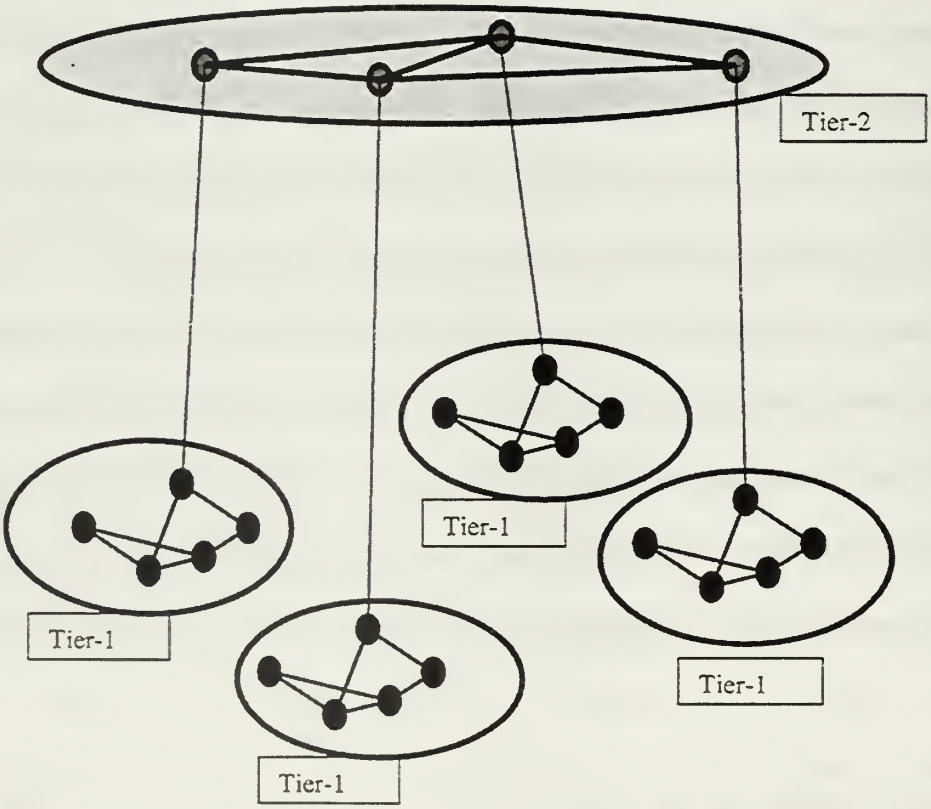


Figure 5. A Two-Tier Hierarchical Ad Hoc Network.

A hierarchical network architecture can be used to accomplish the mobility management process more easily because clusterheads can manage to keep track of their mobile users in a less costly manner. In this way, not all nodes in the communication have to be aware of the whole topology and handovers can be coordinated more efficiently. Since routing is often inefficient because of the lack of direct connectivity between two different cluster heads. The most important advantage of the flat network is that there are multiple paths between source and destination. This helps reduce traffic congestion and provides the best route to satisfy quality-of-service requirements. While flat addressing may be less complicated and easier to use, there are doubts as to its scalability.

To overcome the aforementioned problems, nodes in the network can be classified as *low-echelon terminals* and *high-echelon terminals*. In the defense community, this classification goes in parallel with the organization. For example, in a SOF unit, the team commander would carry the high-echelon terminal while the remainder of the team members would carry low-echelon terminals while operating as a whole team. At the next level, in a SOF battalion, the battalion commander would be the high-echelon node while team commanders would be the low-echelon nodes. This logical abstraction of nodes will prevent frequent updates of routing tables, as we will see in the next section. On the one hand, this approach introduces new problems to the system. Clustering nodes under a high-echelon node might create a single point of failure and choke point along the communication lines. Once the clusterhead is destroyed, the low-echelon nodes might stay out of touch. This might be prevented by implementing fault tolerance for the

role of the clusterhead. A low-echelon node, typically the executive officer's Type-1 device, might take over the communication routing when the clusterhead does not operate properly. On the other hand, this classification will enhance the adaptation of cellular technology via a *Virtual Cellular Network* (VCN). VCN is a well-studied architecture among the academics. Chamlac and Farago describe VCN in the following paragraph.

The basic concept of a VCN is the creation of a cellular network type architecture for networks which are totally mobile, to allow for the use of a standard cellular network software infrastructure. In a VCN, clusterheads are selected among the nodes to play the role of the mobile base stations. Any node can become a clusterhead if it has the necessary functionality, like processing and transmission power or storage capacity. The rest of the nodes can then communicate as in a cellular networks, using the selected clusterheads as base stations, similar to a stationary cellular network. In this package, a mobile node which is not a clusterhead registers with the nearest clusterhead. The set of nodes registered with a given clusterhead forms a virtual cell or cluster in the network. Clusters may change dynamically, reflecting the mobility of the underlying network. Once the VCN is established, these changes can be handled using handoff protocols borrowed from regular cellular networks.[58]

In order to allow continuous operation of the virtual cellular network, clusterheads have to be selected so that in the neighborhood of any non-clusterhead node, there will be at least one clusterhead. In this way, clusterheads will cover the network. As Chlamtac and Farago point out in their article, it is natural to want to create a VCN in which network coverage is obtained by assigning the clusterhead role to an optimum number of

[58] Ibid, 150.

nodes that are spread over the entire network. This optimization can be achieved by preventing two clusterheads from being direct neighbors. This requirement satisfies the effective VCN condition and provides efficient routing.

In a fully mobile environment, the role of the clusterhead may need to be updated from time to time. For example, if two clusterheads become neighbors, then one of them should resign. This may leave some nodes without a clusterhead neighbor. In order to exploit the ability of cellular communication, new clusterheads have to be promoted or nodes in the resigned clusterhead's region have to be handed over to the new clusterhead. All clusterheads in a VCN need to be connected into a backbone. Since in a peer-to-peer network no wired backbone exists, a virtual backbone (VB) has to be formed and updated as the nodes' locations change.

B. ROUTING AND MOBILITY MANAGEMENT

1. Multihop Routing

The routing of messages through a multihop packet-radio network requires the identification of existing communication links and an assessment of their relative quality. Routing protocols perform these tasks. The best route is the one with the smallest number of hops providing acceptable connectivity; the link quality can be determined by measuring signal strength, SNR, or BER. Poor link quality can be improved to some extent through the use of higher transmission power, wider spreading codes, aggressive hop-by-hop error correction, or retransmission schemes. However, link capacity is also a function of the traffic on nearby links; it may be necessary to route around nodes experiencing heavy congestion.

In general, network topologies change rapidly in mobile packet radio networks, with links constantly being lost and new ones established. Therefore, the network management component needs to distribute connectivity information more rapidly than is necessary in wired networks. The network also needs to be able to handle in a graceful manner any network partitions caused by link outages, which are more likely to occur in mobile packet radio networks than in a conventional wired network.

Routing algorithms choose a hop-by-hop path based on information about link connectivity. The simplest scheme is flooding, in which a packet is transmitted on all links from the source to neighboring nodes, which then repeat the process. Flooding is inefficient but can be the best strategy when a network topology changes rapidly. Another scheme, connection-oriented routing, maintains a sequence of hops for communications between a single source and specific destination in the network. Given rapid topology changes, network partitions, and large numbers of nodes, keeping this information updated and available to all nodes is difficult at best. A third scheme is connectionless routing, which requires no knowledge of end-to-end connections. Packets are forwarded toward their destination, with local nodes adapting to changes in network topology.

Connection-oriented and connectionless approaches require that routing information be distributed throughout the network. In small networks this distribution was originally accomplished by a centralized routing server. By now and especially in large networks, distributed algorithms with improved scaling behavior have largely replaced centralized servers. Each node independently determines the best hop in the

direction of the destination, and updated routing tables are periodically exchanged among neighboring nodes.

Routing schemes have also been used that combine elements of the centralized and distributed approaches. For very large multihop packet radio networks, such schemes impose a hierarchy on the network topology, hiding changes in the distant parts of the network from local nodes (the next-hop routes to distant network nodes are not likely to change as rapidly as are routes within each cluster). A combined strategy is to use a centralized route server, known as a clusterhead, to maintain routes between clusters in the direction of "border radios."

A final routing issue relates to packet forwarding, which is initiated when several transmission attempts fail to deliver a message to the next node. In these cases a node engages in localized rerouting and broadcasts the message to any node that can complete the route. Packet forwarding can cause flooding if multiple nodes hear the request and choose to forward the packet. The process can be optimized by filtering based on overheard traffic: if a node has a packet in its send queue and hears the same packet being forwarded from a second node, then the first node assumes that the packet has been sent and removes it from the queue.

Existing routing protocols for ad hoc wireless networks can be classified as table-driven or on-demand. Table-driven protocols continuously evaluate the routes within the network, so that when a packet needs to be forwarded, the route is already known and can be immediately used. In contrast, on-demand routing protocols invoke a route-discovery procedure on an on-demand basis. The advantage of the table-driven schemes is that the route information is available when needed, resulting in little delay prior to data

transmission at the cost of keeping the routes updated in a highly mobile environment. On the other hand, on-demand schemes may produce significant delay in order to determine a route when route information is needed. In the following section we describe some existing protocols, compare the protocols, and suggest one schema for our wireless mobile communication model.

2. Table Driven Routing Protocols

In table-driven routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables to maintain a consistent and up-to-date view of the network. When the network topology changes, the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. The following sections discuss some of the existing table-driven ad hoc routing protocols.

a. Dynamic Destination-Sequenced Distance-Vector Routing Protocol

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm[59] is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements.

Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number

[59] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, Comp. Comm. Rev., Oct. 1994, pp. 234-244.

assigned by the destination node. The sequence number is used to distinguish old routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. Thus, the update is both time-driven and event-driven. The routing table updates can be sent in two ways: a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets, whereas in an incremental update only those entries from the routing table are sent that produce a metric change since the last update and it must fit in a packet. If there is space in the incremental update packets then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dumps are relatively infrequent.

In a fast-changing network, incremental packets can grow in size so that full dumps will occur more frequently. Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e., most recent) sequence number is used. If two routes have the same sequence number, then the route with the best metric (i.e. shortest route) is used. Based on past history, the stations estimate the creation time of routes. The stations delay the transmission of a routing update by creation time so as to eliminate those updates that would occur if a better route were found very soon.

b. The Wireless Routing Protocol (WRP)

The Wireless Routing Protocol[60] (WRP) is a table-based distance-vector

[60] S. Murthy and J. J. Garcia-Luna-Aceves, *An Efficient Routing Protocol for Wireless Networks*, ACM

routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify it if the entry is a simple path, a loop, or invalid. Storing the predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission List (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message.

Nodes exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of the update message (formed using MRL) are required to acknowledge the receipt of the update message. If there is no change in the routing table since the last update, then the node is required to send an idle "Hello" message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables. The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a

---

Mobile Networks and App. J., Oct.1996, pp. 183-97.

change in link of any of its neighbors. Consistency checking in this manner helps eliminate looping situations in a better way and also has fast convergence.

c. Global State Routing

Global State Routing[61] (GSR) is similar to DSDV described in Section 2.2.1. It takes the idea of link-state routing but improves it by avoiding flooding of routing messages.

In this algorithm, each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table. The Neighbor list of a node contains the list of its neighbors; here all nodes that can be heard by a node are assumed to be its neighbors. For each destination node, the Topology table contains the link-state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node.

The routing messages are generated on a link change as in link-state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors.

d. Fisheye State Routing

Fisheye State Routing[62] (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In

---

[61] Tsu-Wei Chen and Mario Gerla, Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks, Proc. IEEE ICC'98.

[62] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, *Scalable Routing Strategies for Ad Hoc*

FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes, thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from the node increases. Figure 6 defines the scope of the fisheye for the center node. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has the most accurate information about all the nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination. FSR scales well to large networks as the overhead is controlled in this scheme.

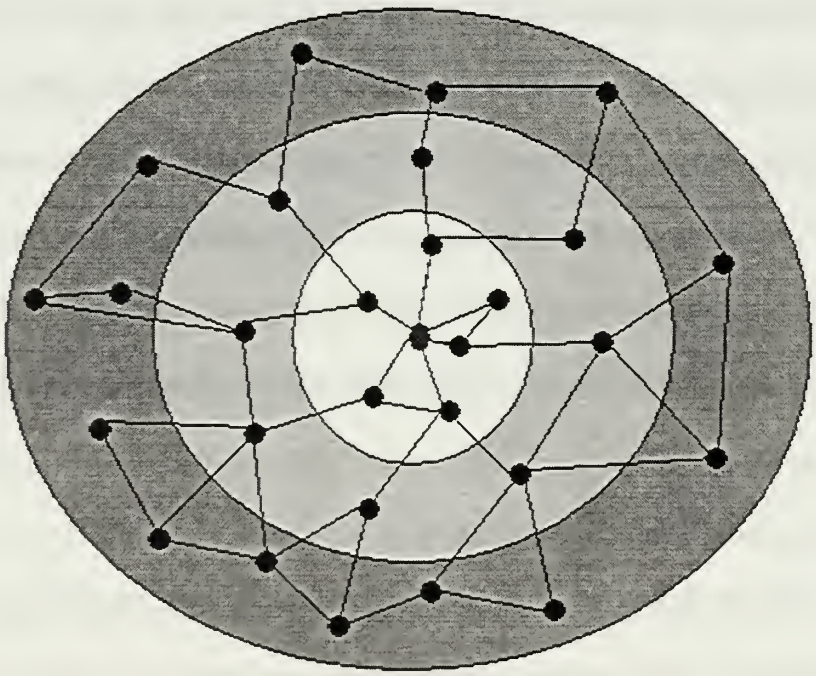


Figure 6. Accuracy of information in FSR.

Wireless Networks, IEEE Journal, Aug. 1999, pp.1369-79.

e. Hierarchical State Routing

The characteristic feature of Hierarchical State Routing[63] (HSR) is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. The nodes of a physical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighboring cluster-heads via a gateway. As shown in Figure 7, these clusterheads are members of the cluster at the next higher level and they exchange their link information as well as the summarized lower-level information among each other and so on (e.g., ATM PNNI). A node at each level floods to its lower level the information that it obtains after the algorithm has run at that level. So the lower level has a hierarchical topology information. Each node has a hierarchical address. One way to assign a hierarchical address is the cluster numbers on the way from the root to the node as shown in Figure 7. A gateway can be reached from the root via more than one path, so the gateway can have more than one hierarchical address. A hierarchical address is enough to ensure delivery from anywhere in the network to the host.

In addition, nodes are also partitioned into logical subnetworks and each node is assigned logical address <subnet, host>. Each subnetwork has a location management server (LMS). All the nodes of that subnet register their logical address with the LMS. The LMS advertises its hierarchical address to the top levels and the information is sent down to all of the LMSs also. The transport layer sends a packet to the network layer

---

[63] Ibid, 1372.

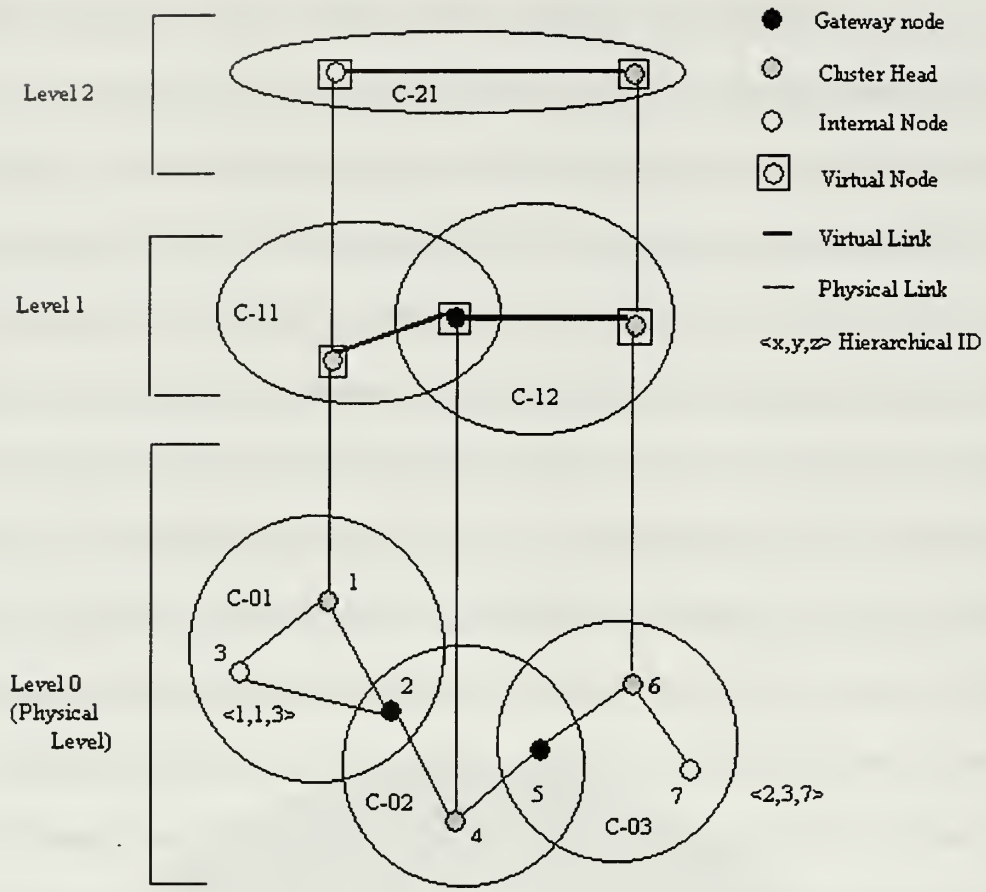


Figure 7. An example of clustering in HSR.

with the logical address of the destination. The network layer finds the hierarchical address of the hierarchical address of the destination LMS from its LMS and then sends the packet to it. The destination LMS forwards the packet to the destination. Once the source and destination know each other's hierarchical addresses, they can bypass the LMS and communicate directly. Since the logical address/hierarchical address is used for routing, it is adaptable to network changes.

f. Zone-based Hierarchical Link State Routing Protocol

In Zone-based Hierarchical Link State Routing Protocol[64] (ZHLS), the network is divided into non-overlapping zones. Unlike other hierarchical protocols, there is no zone-head. ZHLS defines two levels of topologies - node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some node of the other zone. Zone level topology tells how zones are connected together. There are two types of Link State Packets (LSP) as well - node LSP and zone LSP. A node LSP of a node contains its neighbor node information and is propagated with the zone whereas a zone LSP contains the zone information and is propagated globally. Thus, each node has full node connectivity knowledge about the nodes in its zone and only zone connectivity information about other zones in the network. Therefore, given the zone id and the node id of a destination, the packet is routed based on the zone id until it reaches the correct zone. Then in that zone, it is routed based on the node id. A <zone id, node id> of the destination is sufficient for routing so it is adaptable to changing topologies.

g. Clusterhead Gateway Switch Routing Protocol

Clusterhead Gateway Switch Routing[65] (CGSR) uses as a basis the DSDV Routing algorithm described previously. The mobile nodes are aggregated into clusters and a clusterhead is elected. All nodes that are in the communication range of the

---

[64] M Joa-Ng and I.-T. Lu, *A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks*, IEEE Journal, Special Issue on Ad-Hoc Networks, Aug. 1999, pp. 1415-25.

[65] C.-C. Chiang, *Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*, Proc. IEEE SICON'97, Apr.1997, pp.197-211. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf.

clusterhead belong to its cluster. A gateway node is a node that is in the communication range of two or more clusterheads. A dynamic network clusterhead scheme can cause performance degradation due to frequent clusterhead elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In the LCC, a clusterhead change occurs only if a change in network causes two clusterheads to come into one cluster or one of the nodes moves out of the range of all the clusterheads.

The general algorithm works in the following manner. The source of the packet transmits the packet to its clusterhead. From this clusterhead, the packet is sent to the gateway node that connects this cluster-head and the next clusterhead along the route to the destination. The gateway sends the packet to that clusterhead and so on until the destination clusterhead is reached in this way. The destination clusterhead then transmits the packet to the destination. Figure 8 shows an example of the CGSR routing scheme.

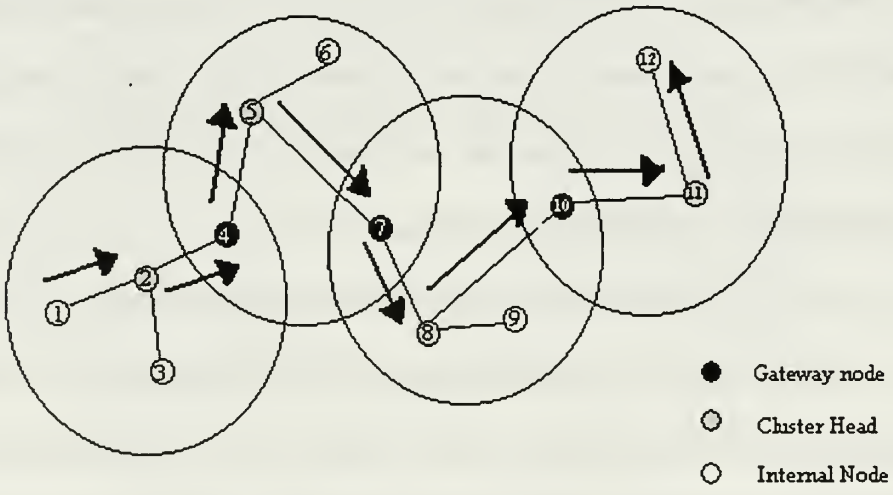


Figure 8. Example of CGSR Routing from Node 1 to Node 12[66]

[66] Ibid, 10 (based on the example given in the page).

Each node maintains a cluster member table that maintains a mapping from each node to its respective cluster-head. Each node broadcasts its cluster member table periodically and updates its table after receiving other node broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster.

On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

3. On-Demand Routing Protocols

These protocols take a lazy approach to routing. In contrast to table-driven routing protocols, all up-to-date routes are not maintained at every node. Instead, the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid until the destination is reachable or until the route is no longer needed. This section discusses a few on-demand routing protocols.

a. Cluster based Routing Protocols

In the Cluster Based Routing protocol[67] (CBRP), the nodes are divided into clusters. To form the cluster, the following algorithm is used. When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a “Hello” message. When a cluster-head gets this “Hello” message it responds with a triggered hello message immediately. When the undecided node gets this message, it sets its state to "member."

If the undecided node times out, then it makes itself the cluster-head if it has a bi-directional link to some neighbor; otherwise it remains in an undecided state and repeats the procedure again. Clusterheads are changed as infrequently as possible.

Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A clusterhead keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has an entry that contains the gateway through which the cluster can be reached and the clusterhead of the cluster.

When a source has to send data to a destination, it floods route-request packets to the neighboring cluster-heads. On receiving the request, a clusterhead checks to see if the destination is in its cluster. If yes, then it sends the request directly to the destination; else it sends it to all of its adjacent clusterheads. The clusterheads address is recorded in the packet so a cluster-head discards a request packet that it has already seen. When the destination receives the request packet, it replies back with the route that had been recorded in the request packet. If the source does not receive a reply within a timeout period, it backs off exponentially before trying to send the route request again.

In CBRP, routing is done using source routing. It also uses route shortening, or on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet, if a node detects a broken link it sends back an error message to the source and then uses a local repair mechanism. When using a local repair mechanism, when a node finds the

next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if the hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

b. Ad hoc On-demand Distance Vector Routing

Ad hoc on-demand Distance Vector Routing[68] (AODV) is an improvement on the DSDV algorithm discussed in Section 2.2.1. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors until it reaches an intermediate node that has recent route information about the destination or until it reaches the destination (Figure 9a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

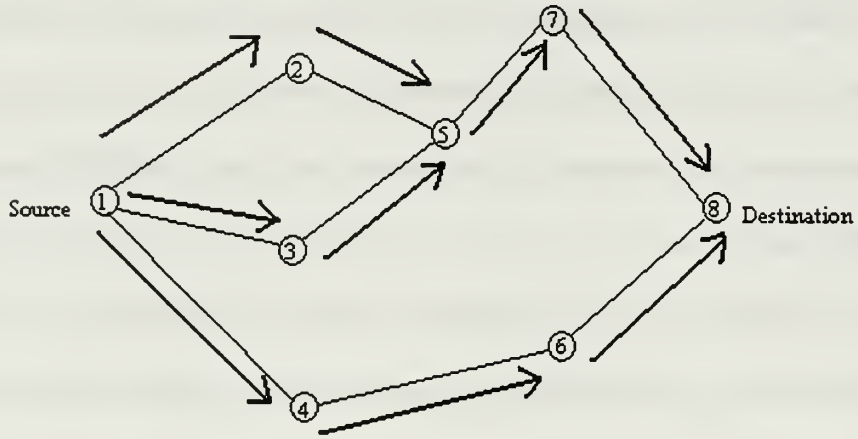
When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of the route request packet. As the route reply packet traverses back to the source (Figure 9b), the nodes along the path enter the forward route into their tables.

If the source moves, then it can reinitiate route discovery to the destination. If one of the

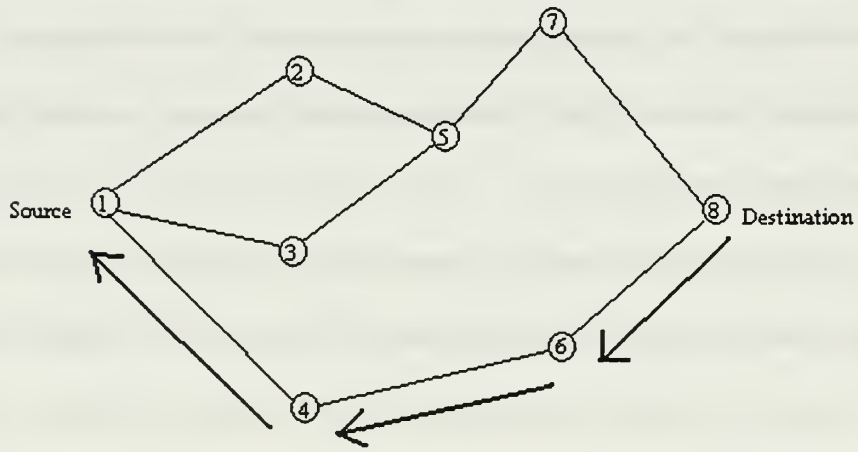
---

[68] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, *Ad Hoc On-demand Distance Vector Routing*,

intermediate nodes move, then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on until it reaches the source. Then the source can reinitiate route discovery if needed.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Figure 9. Route Discovery in AODV.

October 99 IETF Draft.

c. Dynamic Source Routing Protocol

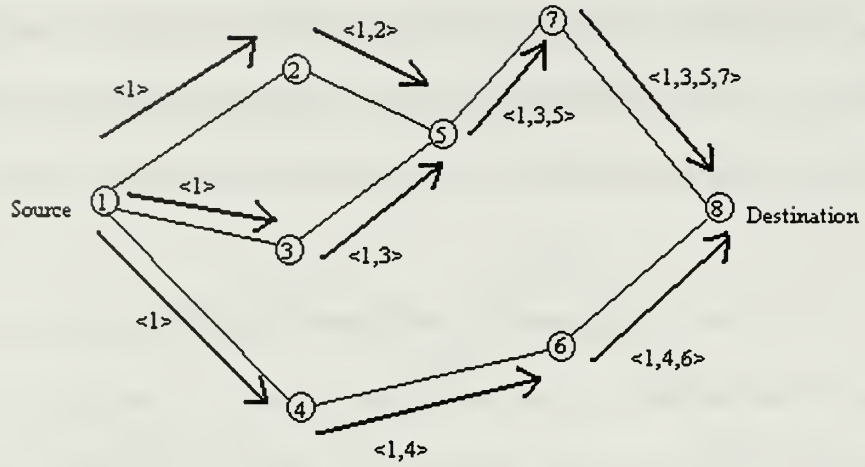
The Dynamic Source Routing Protocol[69] is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes of which it is aware. The node updates entries in the route cache as and when it learns about new routes.

The two major phases of the protocol are route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. If the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. In order to limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and its address is not present in the route record of the packet.

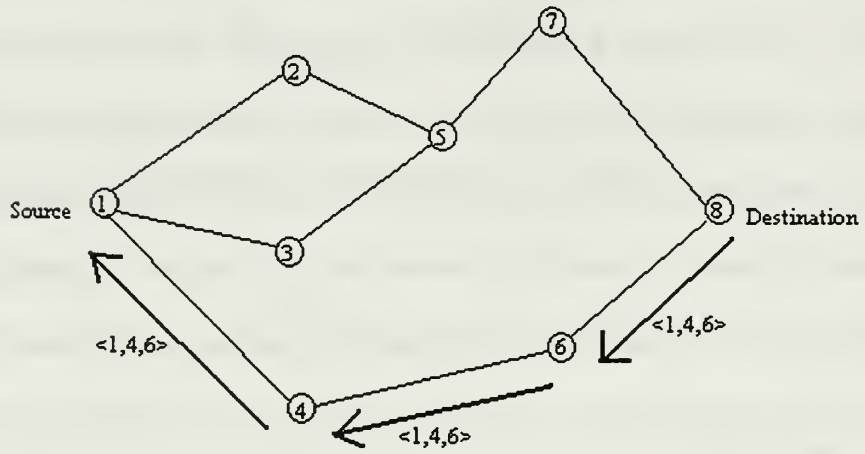
A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.

---

[69] Johnson, D.B., Maltz, D.A.; *Protocols for Adaptive Wireless and Mobile Networking*, IEEE Personal Communications in 1996, Volume :31, Feb 1996, pp. 34-42.



(a) Building Record Route during Route Discovery



(b) Propogation of Route Reply with the Route Record

Figure 10. Creation of Record Route in DSRP.

As the route request packet propagates through the network, the route record is formed as shown in Figure 10a. If the route reply is generated by the destination, then it places the route record from the route request packet into the route-reply packet. On the other hand, if the node generating the route reply is an intermediate node, then it appends its cached route-to-destination to the route record of the route-request packet and puts that into the route-reply packet. Figure 10b shows the route-reply

node, then it appends its cached route-to-destination to the route record of the route-request packet and puts that into the route-reply packet. Figure 10b shows the route-reply packet being sent by the destination. In order to send the route-reply packet, the responding node must have a route to the source. If it has a route to the source in its route cache, it can use that route. The reverse of route record can be used if symmetric links are supported. In case symmetric links are not supported, the node can initiate route discovery to the source and piggyback the route reply on this new route request.

DSRP uses two types of packets for route maintenance: Route Error packet and Acknowledgements. When a node encounters a fatal transmission problem at its data link layer, it generates a Route Error packet. When a node receives a route error packet, it removes the hop in error from its route cache. All routes that contain the hop in error are truncated at that point. Acknowledgment packets are used to verify the correct operation of the route links. This also includes passive acknowledgments in which a node hears the next hop forwarding the packet along the route.

d. Temporally Ordered Routing Algorithm

"The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal."[70] TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The critical

[70] Park , V.D., Corson, M.S., A highly adaptive distributed routing algorithm for mobile wireless networks,

destination without new path information. New path requests are triggered automatically but this process will require additional time that, in turn, will delay the real-time applications.

The protocol has three basic functions: Route creation, Route maintenance, and Route erasure. Each node has five attributes: Logical time of a link failure, the unique ID of the node that defined the new reference level, a reflection indicator bit, a propagation ordering parameter and the unique ID of the node.

"The first three elements collectively represent the reference level. A new reference level is defined each time a node loses its last downstream link due to a link failure. The last two values define a delta with respect to the reference level."[71]

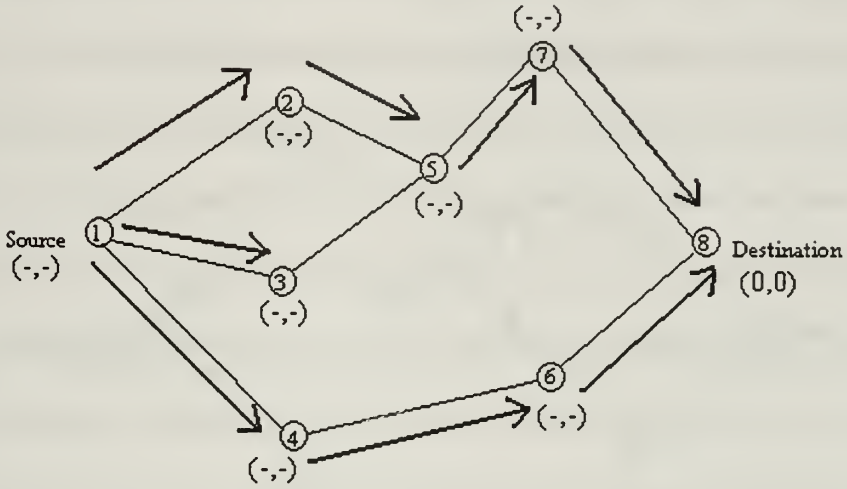
Route Creation is done using query (QRY) and update (UPD) packets. The route creation algorithm starts with the height (propagation ordering parameter in the quintuple) of destination set to 0 and all other node's height set to NULL (i.e., undefined). The source broadcasts a QRY packet with the destination node's id in it. A node with a non-NULL height responds to a UPD packet that has its height in it. A node receiving a UPD packet sets its height to one more than that of the node that generated the UPD. A node with higher height is considered upstream and a node with lower height downstream. In this way a directed acyclic graph is constructed from the source to the destination. Figure 11 illustrates a route creation process in TORA. As shown in Figure 11a, node 5 does not propagate a QRY from node 3, as it has already seen and propagated a QRY message from node 2. In Figure 11b, the source (i.e., node 1) may have received

---

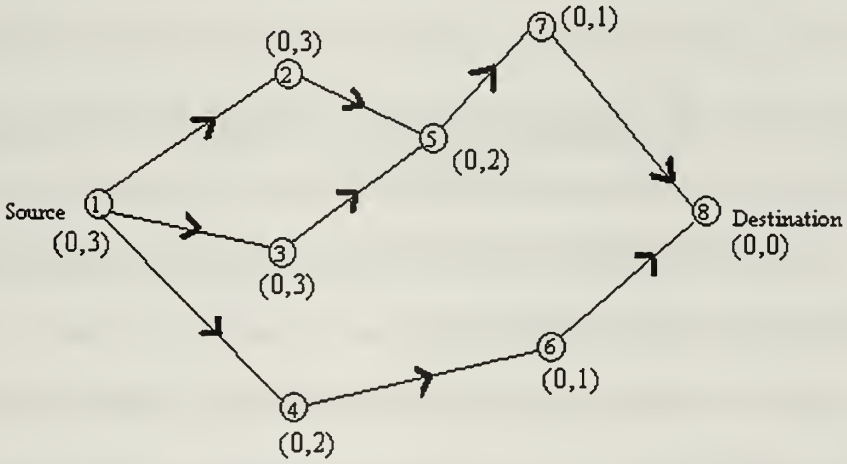
Proc. INFOCOM'97, Apr. 1997, 1405-1413.

[71] Ibid, 1409.

a UPD each from node 2 or node 3, but since node 4 gives it lesser height, it retains that height.



(a) Propogation of QRY message through the network



(b) Height of each node updated as a result of UPD messages

Figure 11. Route Creation in TORA. (Numbers in parentheses are reference level, height of each node).[72]

When a node moves, the DAG route is broken and route maintenance is needed to reestablish a DAG for the same destination. When the last downstream link of

[72] Ibid, 1410 (based on the example given in the page).

a node fails, it generates a new reference level. This results in the propagation of that reference level by neighboring nodes as shown in Figure 12. Links are reversed to reflect the change in adapting to the new reference level. This has the same effect as reversing the direction of one or more links when a node has no downstream links.

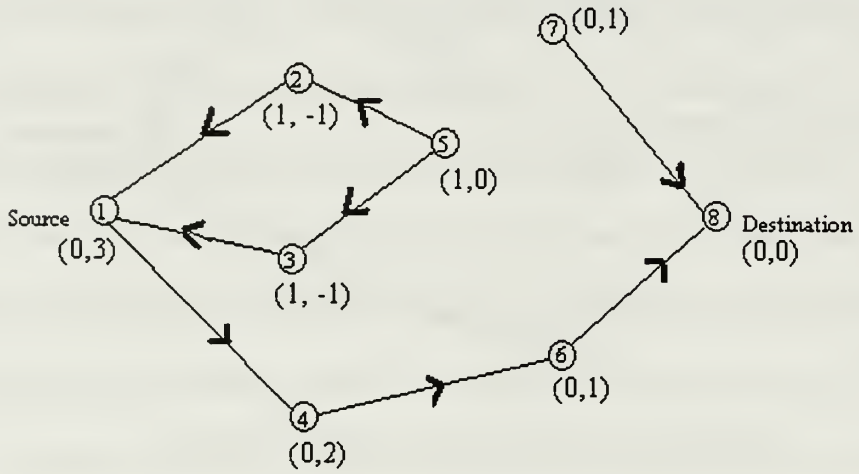


Figure 12. Re-establishing Route Failure of Link 5-7. The New Reference Level Node is 5.

In the route erasure phase, TORA floods a broadcast clear packet (CLR) throughout the network to erase invalid routes.

In TORA, there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Since TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will ultimately occur.

e. Associativity Based Routing

The Associativity Based Routing (ABR) protocol is a new approach to routing.[73] ABR defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are likely to be long-lived. All nodes generate periodic beacons to signify their existence. When a neighboring node receives a beacon, it updates its associativity tables. For every beacon received, a node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are Route discovery, Route reconstruction (RRC), and Route deletion.

The route discovery phase is a broadcast query and await-reply (BQ-REPLY) cycle. The source node broadcasts a BQ message in search of nodes that have a route to the destination. A node does not forward a BQ request more than once. On receiving a BQ message, an intermediate node appends its address and its associativity ticks to the query packet. The next succeeding node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. Each packet arriving at the destination will contain the associativity ticks of the

[73] Chai-Keong Toh, *A novel distributed routing protocol to support Ad hoc mobile computing*, Proc. 1996

nodes along the route from the source to the destination. The destination can now select the best route by examining the associativity ticks along each of the paths. If multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. Once a path has been chosen, the destination sends a REPLY packet back to the source along this path. The nodes on the path that the REPLY packet follows mark their routes as valid. All other routes remain inactive, thus avoiding the chance of duplicate packets arriving at the destination.

The RRC phase consists of partial route discovery, invalid route erasure, valid route updates, and new route discovery, depending on which node(s) along the route move. Source node movement results in a new BQ-REPLY process because the routing protocol is source-initiated. The route notification (RN) message is used to erase the route entries associated with downstream nodes. When the destination moves, the destination's immediate upstream node erases its route. A localized query (LQ [H]) process, where H refers to the hop count from the upstream node to the destination, is initiated to determine if the node is still reachable. If the destination receives the LQ packet, it selects the best partial route and REPLYs. Otherwise, the initiating node times out and backtracks to the next upstream node.

A RN message is sent to the next upstream node to erase the invalid route and informs this node that it should invoke the LQ [H] process. If this process results in backtracking more than halfway to the source, the LQ process is discontinued and the source initiates a new BQ process.

IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480-86.

When a discovered route is no longer needed, the source node initiates a route delete (RD) broadcast. All nodes along the route delete the route entry from their routing tables. The RD message is propagated by a full broadcast, as opposed to a directed broadcast, because the source node may not be aware of any route node changes that occurred during RRCs.

f. Signal Stability Routing

The Signal Stability-Based Adaptive Routing protocol[74] (SSR) is an on-demand routing protocol that selects routes based on the signal strength between nodes and a node's location stability. This route selection criterion has the effect of choosing routes that have "stronger" connectivity. SSR is comprised of two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

The DRP maintains the Signal Stability Table (SST) and Routing Table (RT). The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either recorded as a strong or weak channel. All transmissions are received by DRP and processed.

After updating the appropriate table entries, the DRP passes the packet to the SRP. The SRP passes the packet up the stack if it is the intended receiver. If not, it looks up the destination in the RT and forwards the packet. If there is no entry for the destination in the RT, it initiates a route-search process to find a route. Route-request packets are forwarded to the next hop only if they are received over strong channels and have not been previously processed (to avoid looping). The destination chooses the first arriving route-search packet to send back as it is highly likely that the packet arrived over

[74] R. Dube et al., Signal Stability based adaptive routing for Ad Hoc Mobile networks, IEEE Pers.

the shortest and/or least congested path. The DRP reverses the selected route and sends a route-reply message back to the initiator of the route-request. The DRP of the nodes along the path update their RTs accordingly.

Route-search packets arriving at the destination have necessarily arrived on the path of strongest signal stability because the packets arriving over a weak channel are dropped at intermediate nodes. If the source times out before receiving a reply, then it changes the PREF field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated.

When a link failure is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then sends an erase message to notify all nodes of the broken link and initiates a new route-search process to find a new path to the destination.

4. Comparison and the Proposed Protocol

The advantage of a table-driven scheme is that there is little delay until the route is determined, but this scheme is not appropriate for an ad hoc network environment due to excessive network capacity to keep the routing information, since both bandwidth and battery power are scarce resources in mobile computers. In on-demand schemes, the delay to determine a route can be quite large. Thus, it cannot be applicable to real-time communication. Some of the protocols mentioned above are compared in the Table 2.

In our research, we will suggest a hybrid protocol combining table-driven and on-demand routing techniques. There exists high-echelon nodes in the hierarchical architecture and these low-mobility terminals will use the table-driven approach.

Comm., Feb. 1997, pp. 36-45.

	DSDV	AODV	DSR	ZRP	TORA	CBRP
Loop-free	Yes	Yes	Yes	Yes	No	Yes
Multiple routes	No	No	Yes	No	Yes	Yes
Distributed	Yes	Yes	Yes	Yes	Yes	Yes
Reactive	No	Yes	Yes	Partly	Yes	Yes
Unidirectional link support	No	No	Yes	No	No	Yes
QoS Support	No	No	No	No	No	No
Multicast	No	Yes	No	No	No	No
Security	No	No	No	No	No	No
Power conservation	No	No	No	No	No	No
Periodic Broadcasts	Yes	Yes	No	Yes	No	Yes
Requires reliable or sequenced data	No	No	No	No	Yes	No

Table 2. Comparison of Different Routing Protocols.

In fact, Cho and Kim introduced this routing schema.[75] The candidate terminals as routers are only low-mobility terminals. Similar to the conventional on-demand schemes, when the source node does not find the destination node in the cluster of itself, the routing path discovery procedure is started. The difference between conventional on-demand schemes and proposed scheme is that the paging signals to the nodes in the cluster are received by only low-mobility terminals (high-echelon nodes). When the low-mobility terminal receives the paging signals, there exist two possible schemes to make the routing path. One is table-driven approach. The updating rates of routing tables between low-mobility terminals are comparatively low. Hence, the prepared routing table can be used without paging to find the routing path. Each high-mobility terminal is registered in the memory of low-mobility terminals when high-mobility terminals (low-echelon nodes) entered into the cluster of the low-mobility terminal. If one of the low-mobility terminals receives the paging signals from the source node, then the low-mobility terminal multicasts the node-search signal to all of the low-mobility terminals in

[75] Ryu, J., Kim, Y., Cho, D., A New Routing Scheme Based on the Terminal Mobility in Mobile Ad Hoc Networks, Vehicular Tech. Conf., 1999, IEEE VTS 50th, V:2 1255.

the prepared routing table, and the low-mobility terminal looks for the destination from the memory. With this approach, the routing time can be shortened but the capability of each low-mobility terminal to manage the memory is also needed. The other approach is on-demand. Each low-mobility node receiving the paging signals for routing finds the destination node in its cluster, and if the finding fails, then it forwards the routing signal to the low-mobility nodes in its neighborhood. This approach is simpler than the first approach, but the amount of the paging to find the route is greater than in the case of the first approach.

5. Terminal Mobility Support on the INTERNET

The mobile internetworking routing protocols (Mobile IP) were designed to accommodate the mobility of Internet users. There is some disagreement concerning whether Mobile IP was originally designed for an individual user moving from one fixed location to another or for on-the-move wireless operations. In any case, the Internet Engineering Task Force (IETF) has addressed the issue of full mobility, and Mobile IP is now suited for highly mobile users. On the Internet, every node (fixed or mobile) has a unique identifying address- its IP address. Mobile IP has to circumvent the association of IP addresses with specific networks because mobile nodes can attach to and detach from multiple networks as they roam. Changing an IP address on the fly is not always possible. If a node has an open TCP connection when its IP address changes, then the TCP connection will fail. If the node requires an accurate Domain Name System (DNS) entry, then the entry will need to be updated as the address changes, and in today's implementation of DNS, such an update can be very slow.

Communications take place between a sender and receiving mobile host (MH). In the Mobile IP specifications, every MH has a home network and its IP address is called the home address. A router called the home agent, which resides in the MH's home network, is responsible for intercepting each packet destined for the home address of a roaming MH. The packet is placed inside another IP packet through a process called "IP encapsulation." The source address in the encapsulating packet is that of the home agent. The packet is usually sent "in care of" another agent, the foreign agent, which resides in the network in which the MH is roaming. Conventional IP routing to the foreign agent sends the packet, where the contents (i.e., the original packets) are removed and delivered to the MH. The MH can transmit information directly to the sender but the sender always directs its own communications to the home network. The MH can also request a locally assigned care-of IP address in its roaming domain by invoking the dynamic host configuration protocol. This address could be used by the home agent directly and thus eliminate the foreign agent.

When a MH enters a new mobile subnetwork, it needs to obtain a care-of address. It can find a foreign agent using a process built on top of the existing Internet control message protocol (ICMP) capabilities for router discovery. Once accepted by the local network, the MH registers its new care-of address with its home agent. All registration attempts need to be authenticated to prevent a malicious user from hijacking the packets simply by furnishing another care-of address. The Mobile IP specifications use a message authentication code (similar to a digital signature) based on a secret key shared by the MH and home agent. Only the MH that knows the secret key can provide the

digital signature expected by the home agent. Replay protection is required to prevent a malicious user from falsely registering a MH with a stale care-of address.

The major performance challenge is to circumvent the indirect routing among the sender, home agent, and foreign agent. This path can be eliminated if the sender caches bindings between the MH's home and care-of addresses. The management of these bindings is called route optimization. For example, when a sender first sends a packet to an MH through its home agent, the home agent could send a binding-update message to the original sender. Until the binding expires (i.e., times out), the sender can use the care-of address directly. If the MH moves to a new subnetwork, then it can ask its former foreign agent to forward packets to the new care-of address while also alerting senders of that new address.

C. WIRELESS OVERLAY NETWORKS

No single network technology can simultaneously offer wide-area coverage, high bandwidth, and low latency. In general, networks that span small geographical areas (e.g., LANs) tend to support high bandwidth and low latency, whereas networks that span large geographical areas (e.g., satellite networks) tend to provide low bandwidth and high latency. In order to provide flexible connectivity over wide areas, a wireless internetwork needs to be formed from multiple wide-, medium-, and local-area networks interconnected by wired or wireless segments. This internetwork is called a wireless overlay network because the WANs are laid on top of the medium- and local-area networks to form a multilayered network hierarchy. A user operating within the LAN enjoys high bandwidth and low latency, but when communicating outside the local

coverage area the user accesses a wider-area network within the hierarchy, typically sacrificing some bandwidth or latency in the process.

Future mobile information systems will be built on heterogeneous wireless overlay networks, extending traditional wired and internetworked processing "islands" to hosts on the move over a wide area. The critical vulnerability of the “islands” approach would be whether they are capable of suggesting alternative routes or not because damage in one “island” can create a gap among the nodes. For this reason, the overlay networks must be dynamically self-configuring and have to implement the fault tolerance for critical nodes in the communications system. Overlay technologies are used in buildings (wireless LANs), in metropolitan areas (packet radio), and regional areas (satellite). The software radio, with its capability to change frequencies and waveforms as needed, is a critical enabling technology for overlay networks.

Handoffs may take place not only "horizontally" within a single network but also "vertically" between overlays. If each overlay network assigns the MH a different IP address, then the Mobile IP needs to be extended to correlate all the addresses for one user. Alternatively, the mobile node can treat each new IP address as a new care-of address. The home agent maintains a table of bindings between the home and locally assigned addresses. The applications running on the MH may participate in the choice of route. For example, an application might specify that high-priority traffic traverse an overlay with low latency. Less-critical traffic might travel over higher-latency connections.

Under certain conditions, such as the transmission of urgent data, a slow-speed overlay with strong signal strength might be preferred to one with a higher bandwidth but a weaker signal.

D. END-TO-END SYSTEM DESIGN ISSUES

Most end-to-end system design issues, such as security, design tools, and interoperability with other systems, are applicable to any wireless application. However, some end-to-end design issues depend on the application to be supported by the network. For example, videoconferencing is an extremely challenging application for a wireless system because of its high bandwidth requirement and strict constraints on delayed end-to-end transmissions. To support this application, the capability to adapt to channel conditions, perhaps through a slight degradation in image quality, might be built into the end-to-end system protocols. Similarly, many military command-and-control operations require the capability to assign priorities to certain messages, and this flexibility needs to be built into the system. The following sections deal with three key end-to-end design issues for wireless systems: application-level adaptations, quality of service and system security.

1. Application-Level Adaptation

A system can adapt to the variability in mobile client applications in three ways. One approach is to exploit data-type-specific lossy (i.e., involving some distortion) compression mechanisms and use data semantics to determine how information can be compressed and prioritized en route to the client. A second approach is on-the-fly adaptation involving the transcoding of data into a representation that can be handled by the end application. The third approach is to push the complexity away from the mobile

clients and servers into proxies, which are often used in wired networks but are not currently optimized for wireless applications.

Introduced in response to security concerns, the proxy approach is a new paradigm for distributed applications. A proxy is an intermediary that resides between the client and server—outside the client's security firewall—to filter network packets on behalf of the client. Proxies provide a convenient place to change data representations en route to the client, perform type-specific compressions, cache data for rapid re-access, and fetch data in anticipation of access. By supporting the adaptation to network variations in bandwidth, latency, and link error rates as well as to hardware and software variations, proxies enable client applications running on limited-capability end nodes to appear as if they were running on high-end, well-connected machines. Low-end clients (e.g., PDAs) have limited processing capabilities due to small displays and memory, relatively slow processors, and limited-capability software and run-time environments.

2. Quality of Service (QoS)

Quality of service refers to traffic-dependent performance metrics—bandwidth, end-to-end latency, or likelihood of message loss—that a connection must have or can tolerate for the type of data transmitted. A network's admission-control mechanisms, which are invoked whenever a new connection is initiated, provide assurance that QoS requirements will be met; a new connection is aborted if its QoS requirements cannot be met. Attention to QoS issues is increasing because of at least two converging trends: the growing market for applications (e.g., video) that require real-time service, and the evident interest in using the Internet for a range of activities that are critical to both the public and private sectors.

It is difficult to provide QoS in an ad hoc network due to its dynamic nature. The overhead of QoS routing in an ad hoc network is likely to be higher than that in a wireline network because the available state information is less precise, and the topology changes in an unpredicted way. There are three main QoS parameters which are important in wireless mobile networks supporting real-time applications: end-to-end delay, bandwidth, and jitter.

The provision of QoS relies on resource reservation. Therefore data packets of a QoS connection are likely to flow along the same network path on which the required resources are reserved. Routing is the first step in resource reservation. The goal of QoS routing is two fold: a) selecting network paths that have sufficient resources to meet the QoS requirements of all admitted connections and b) achieving global efficiency in resource utilization. Lin and Gerla[76] proposed an algorithm that introduces the bandwidth constraint to traditional routing protocols. This bandwidth routing algorithm keeps track of the shortest paths for all bandwidth values. "To compute these paths each node periodically broadcasts to its neighbors the {bandwidth, hop distance} pairs for the preferred paths to each destination. ... If a node receives a real-time packet with a bandwidth request, which cannot be satisfied by the currently available paths to the intended destination, it drops the packet without ACK. Eventually, the sender will reroute the call on other path."[77]

---

[76] Lin, C. R., *Real-time Support in Multihop wireless Networks*, Wireless Networks 5, 1999, 125-135.

[77] Ibid, 129.

A better algorithm for satisfying QoS requirements is studied by Chen and Nahrstedt.[78] They proposed a ticked-based distributed QoS routing scheme for ad hoc networks. The existing single path routing algorithms have low overhead but do not have the flexibility of dealing with imprecise state information. On the other hand, the flooding algorithms can handle information imprecision but have high overhead. Proposed ticket-based probing scheme achieves a balance between single-path routing algorithms and the flooding algorithms. It does multihop routing without flooding. The basic idea is to achieve an optimal performance with low overhead by using a limited number of tickets and making intelligent hop-by-hop path selections.

The basic idea of ticket-based probing is outlined as follows:

> A ticket is the permission to search one path. The source node issues a number of tickets based on the available state information. One guideline is that more tickets are issued for the connections with tighter requirements. Probes (routing messages) are sent from the source toward destination to search for a low-cost path that satisfies the QoS requirement. Each probe is required to carry at least one ticket. At an intermediate node, a probe with more than one ticket is allowed to be split into multiple ones, each searching a different downstream subpath. The maximum number of probes at any time is bounded by the total number of tickets. Since each probe searches a path, the maximum number of paths searched is also bounded by number of tickets.[79]

Due to the mobility of nodes, paths are broken frequently. A broken path is thought of as a fault and uses the *path redundancy* for fault tolerance. There is a tradeoff between the overhead of redundancy and the performance of the QoS provision. Chen and Nahrstedt propose a multilevel redundancy scheme to meet the diversity of user requirements.

---

[78] Chen S., Nahrstedt K., *Distributed Quality of Service Routing in Ad Hoc Networks*, IEEE Journal on Selected Areas in Comms, V: 17, No: 8, 1999, 1488-1505.

[79] Ibid, 1491.

First-level redundancy is used for the most critical connections. The idea is to establish multiple routing paths for the same connection. Every data packet is sent along each path independently. If the destination receives the same packet from more than one path, it keeps the first copy and discards the rest. The required QoS is guaranteed as long as one of the paths remain unbroken.

Second-level redundancy is used for ordinary connections that allow certain degree of QoS disruption. It is similar to first-level redundancy, except that among the multiple established paths, one is selected as the primary path, and the others are secondary paths. Data packets are sent only along the primary path. Although resources are reserved on the secondary paths as well, they are not used. In case a primary path is broken, the source node detects this fault and promotes one of the secondary paths to be the primary path.

The ordinary connections may also use the third level of redundancy which has the lowest overhead. It is similar to the second-level redundancy except that no resource is reserved on the secondary paths. When the primary path is broken, control messages are sent along the secondary paths to check the current resource availability. If some of the secondary paths remain feasible, one is selected as the new primary path, and the resources are reserved. If none of them is feasible, rerouting is activated.

a. Approaches to Quality of Service on the INTERNET

Within the Internet, three categories of QoS are currently defined: guaranteed, predictive, and best-effort service. Guaranteed service is achieved if the connection conforms to a well-specified traffic specification. If the network determines that it can support this traffic, then it allows the connection to be established and

guarantees that its requirements will be met. Guarantees of this type are necessary when the application requires tight, real-time coupling between the end points of the connection. An example of guaranteed service is the telephone system, which is designed to meet the level of perceived audio/speech quality, end-to-end switching delays, and likelihood of call blocking required for telephone calls. Certain values for these metrics are determined and the network is designed to offer the desired number of simultaneous connections. Another example of guaranteed service is that provided by an ATM; a transmission protocol that handles voice, data, and video. If absolute guarantees are too expensive, then it is often sufficient to provide predictive service, indicating that the application's requirements are highly likely to be met.

The Internet as it exists today does not provide explicit QoS to different packet flows; instead it is based on a best-effort model that makes no performance guarantees. Flows are groups of packets that share common characteristics, including the tolerated delay. Best-effort services are appropriate for applications that do not demand real-time performance and that can adapt gracefully to the bandwidth available in the network. Best-effort service tolerates simple network components and is a good match for data transmitted in interactive bursts, interactive bulk transfer, and asynchronous bulk transfer. The common Internet data transfer applications are sensitive to losses but tolerant of latency. However, the reverse is true for emerging real-time Internet applications, which are tolerant of losses but sensitive to latency. The IETF is working to provide guaranteed services on the Internet.

The Internet carries two broad classes of applications: delay tolerant and delay intolerant. The former application, such as file transfer, tolerates some packet

losses and delays. For these services, which are common today, the network does not reserve resources or limit the number of transfers in progress at any one time. Instead, the network shares the available bandwidth among all the active applications as best it can. This is the so-called best-effort service. Delay-intolerant applications require data that is delivered with little or no delay. For these applications, different services are being developed. The components of these services consist of traffic and network descriptions, admission control procedures, resource reservation protocols, and packet scheduling mechanisms. These specifications are associated with flows. Given a service specification, the network can admit a new flow or deny access when the specifications exceed what the network can provide. The network can also police a flow to ensure that it meets the traffic specification.

Real-time Internet applications are developed on top of the real-time protocol (RTP). With RTP, a node moderates its transmission rate based on periodic reports of successfully received data at the receiver. If the sender's rate exceeds that which is reported as received, then the sending rate is reduced. Periodically the sender probes the network by attempting to increase the rate to see if a higher rate can be supported. In this way, the sender and receiver adapt to the available bandwidth without requiring any special support from the network itself. The RTP protocol is appropriate for real-time data streams, such as video and audio, that can tolerate some losses.

The real-time Internet services proposed by the IETF use the resource reservation protocol (RSVP), which enables dynamic changes in QoS and permits receivers to specify different QoS requirements. The RSVP protocol is closely integrated with multicast services in which receivers determine a path through the network on which

senders distribute their traffic specifications and receivers distribute their network service requirements. These sender-directed path messages and receiver-directed reservation messages are built on top of the existing multicast protocols. Senders and receivers are responsible for periodically signaling the network about their changing specifications. Once the reservations have been made, the final step is to implement them in every router on the path from sender to receiver through packet classification and scheduling. The router implementation achieves the performance specified by the network end points. The classification process maps packets on flows into their associated reservation, and scheduling drives queue management to ensure that the packets obtain their requested service.

Proponents of ATM networks view such networks as the foundation of integrated voice, video, and data services because they combine flexibility with performance guarantees. The ATM approach involves breaking up data into short packets of fixed size called cells, which are interspersed by time division with data from other sources and delivered over trunk networks. An ATM network can scale up to high data rates because it uses fast switching and data multiplexing based on these fixed-format cells, which contain 48 bytes of traffic combined with a 5-byte header defining the virtual circuits and paths over which the data are to be transported.

The virtual circuits need to be established before data can flow. In setting up connections, the network makes resource allocation decisions and balances the traffic demands across network links, thereby separating data and control flows and enabling switches to be simple and fast.

Two types of guaranteed service are available on ATM networks: constant bit rate (CBR) and variable bit rate (VBR). The CBR service is appropriate for constant-rate data streams that demand consistency in delay. An example of such a data stream is telephone traffic that uses constant-bit-rate encodings for audio and places bounds on delivery latency. The VBR service is appropriate for traffic patterns that have a fairly sustained rate but also may feature short bursts of data at the peak transmission rate.

Burst-type traffic tolerates higher delays and higher variations in delay than does constant-rate traffic. Two types of best-effort traffic classes are available on ATM networks: available bit rate, which guarantees zero losses (but makes no other guarantees) if the source follows the traffic management signals delivered by the network; and undefined bit rate, which provides no performance guarantees.

The connection orientation of the ATM presents problems when dealing with network mobility. Movement between cells requires existing connections to be reestablished. Even brief transmissions invoke the full latency of connection setup. In addition, the ATM is not appropriate for lossy links because there is no agreed-upon mechanism for error recovery or retransmission at the link layer.

Considerable controversy exists as to whether the ATM will be used throughout a system or only at the link or subnetwork level. Full ATM connectivity, from one end of a system to the other, is required to take advantage of the service guarantees. Many believe that it will be necessary to run TCP/IP over the ATM to ensure interoperability across heterogeneous subnetworks. Debate continues over how to interface the ATM's performance guarantees with the emerging Internet capabilities for predictive service.

Wireless communications introduce additional QoS issues. The QoS guarantees for expected loss rates, latencies, and bandwidths were developed based on the assumption that switched, fiber-optic wired networks would be used. Such networks feature low link-error rates, easily predicted link bandwidths, and QoS parameters that are largely determined by how the queues are managed within the switches. As a result, losses are due almost entirely to congestion-related queue overflows. Wireless links, on the other hand, have high bit-error rates, high latencies due to link layer retransmissions, and unpredictable link bandwidths.

Furthermore, the quality of a wireless link varies over time, and connections can be lost completely. Two wireless end nodes sharing the same link can experience vastly different link bandwidths depending on their relative proximity to the base station, location in a radio fade, or loss of receiver synchronization in a multipath environment. Link quality can also be degraded by interference from a nearby transmitter. In addition, hidden terminals cause time-consuming back-off (i.e., waiting before resending) that further degrades network performance.

Since link quality varies over short time intervals, it is difficult to improve a wireless link through error coding or increased transmit power. Moreover, attempts to improve a link for one user can adversely affect other users. Guarantees are elusive in this complex environment. The ATM end-to-end QoS model is difficult to implement when the limiting link is wireless. In general, however, approaches such as adaptive spreading codes and transmit-power control can be used at the media access control and link layers to improve the QoS provided by higher protocol layers in a wireless environment.

b. Transport-Layer Issues

The most widely used reliable transport protocol is TCP, a connection-oriented protocol that combines congestion control with "sliding-window" flow control at the sender and cumulative acknowledgments from the receiver. As each segment is received in sequence, the receiver generates an acknowledgment indicating the number of bytes received. In the current generation of TCP, congestion is controlled by the sender, which maintains a variable called the congestion window that regulates how much data the sender transmits across the network at any one time. The sender adjusts the congestion window in response to perceived network conditions. When a TCP connection first starts, or after a major congestion event, the congestion window is set to one packet, which means the sender cannot send a second packet until it receives an acknowledgement of the first. The sender then adjusts the congestion window by doubling it for each round-trip across the net. This part of the algorithm is called slow-start. Once a certain threshold is crossed, the congestion-avoidance phase is triggered and the window size grows in increments of a single packet for each round-trip. The sender uses these mechanisms to probe the network to discover how much data can be in flight.

A lost packet creates a gap in the sequence number of data arriving at the receiver. When this occurs, the receiver generates a duplicate acknowledgment for the last segment received in order. When a threshold number of duplicate acknowledgments is received, the sender retransmits the lost segment and reduce the window to half of its original size; this part of the algorithm is known as fast retransmission and recovery. A more serious congestion event can cause the loss of so many packets that the receiver

generates no duplicate acknowledgments. The sender detects and corrects this situation using a timer. The TCP protocol sets time-outs as a function of the mean and standard deviation of the round-trip time. If no acknowledgment is received within this interval, then the sender retransmits the first unacknowledged segment, sets its window to one packet, and reenters the slow-start phase. This event causes a major reduction in throughput until the window opens and also can cause a silent period until the timer expires.

Fast retransmission works well in many circumstances today. However, other issues arise in wireless systems. When a packet is lost or damaged because of bit errors on the wireless link, this loss is detected and corrected by the fast-recovery algorithm.

However, fast retransmission reduces the window size as a side effect, thus keeping throughput low. These problems can be mitigated through a TCP-aware link layer, in which the base station triggers local retransmissions of lost segments. By intercepting the duplicate acknowledgments, the base station shields the sender from the effects of local losses that would have the effect of shrinking the congestion window and reducing throughput. More seriously, burst errors on the wireless link can cause the loss of several packets, which will trigger the slow-start algorithm even though there is no congestion.

Asymmetric connections, in which the bandwidth in one direction far exceeds that available for the opposite path, can present problems for transport-layer connections because the effective bandwidth on the forward path is limited by the amount of acknowledgment traffic that can be sent along the reverse path. An example of

asymmetry is direct-broadcast satellite, which sends data to the user at several hundred kilobits per second but uses substantially smaller-bandwidth technologies (such as a conventional telephone or wide-area wireless) for the return path at tens of kilobits per second. Asymmetries also arise because of the nature of data traffic patterns. For example, Web access involves much more data transmitted from servers to users than in the opposite direction. Yet poor performance on the acknowledgment path moderates the performance on even a high-bandwidth forward path. One solution to is to compress the acknowledgment packets; another is to delay acknowledgments so that each one acknowledges an expanded range of received data.

Asymmetries can undermine reliability in the application of TCP to wireless links. The TCP protocol can adapt the duration of its time-outs as long as the round-trip time estimate is not highly variable. Asymmetries in the connection bandwidth, coupled with differential loss rates and congestion effects on the forward and reverse paths, increase the variability in estimated round-trip time. This means that when losses do occur, the retransmission time-outs can become very large, significantly degrading a connection if losses occur often.

3. Security

Wireless communication systems are inherently less private than are wired systems because the radio link can be intercepted without any physical tap, and be undetected by the transmitter and receiver. Wireless networks are therefore especially vulnerable to eavesdropping, usage fraud, and activity monitoring. These threats will grow as wireless military applications become available. In addition, both wired and wireless networks need to be designed to maintain the integrity of data and systems and

assure the appropriate availability of services. For purposes of this discussion, which considers key aspects of the information security but is not comprehensive, the issues can be divided into three categories: network security, radio link security, and hardware security.

Network security encompasses end-to-end encryption and measures to prevent fraudulent network access and monitoring. One user-oriented framework distinguishes several levels of end-to-end encryption. Level 0 has no encryption which means that anyone with a scanner and knowledge of the communication link design can intercept a transmission.

Analog cellular telephones offer this level of security, which has been a problem and has motivated security upgrades in digital cellular standards. Level 1 provides low-level security such that individual conversations might take a year or more to decrypt. This level is probably secure enough for commercial telephony applications, provided that an equivalent effort would be needed to decrypt subsequent conversations ("perfect forward secrecy"). Level 2 provides increased (perhaps by a factor of 10) security for sensitive information related to electronic commerce, mergers and acquisitions, and contract negotiations. Level 3 provides the most stringent level of security and meets government and military communications requirements as defined by the appropriate agencies.

Radio link security prevents the interception of radio signals, ensuring the privacy of user location information and, for military applications, anti-jamming (AJ) and low-probability-of-detection-and-interference (LPD/I) capabilities. However, link security does not prevent traffic analysis. Link security was primarily a military concern before

commercial wireless communications became prevalent. Military systems are designed to avert the detection of radio signals, jamming of communication links, and interception and decoding of messages. Many military radios are based on spread-spectrum technology, which provides both AJ and LPD/I capabilities. However, because knowledge of the spread-spectrum code would enable an adversary to intercept a spread signal, encryption is usually applied as well to prevent signal interception and message recovery. Many military techniques for reducing interception and detection are classified.

For commercial systems, the primary link-level issue is privacy, which is cannot be assured. Conversations on analog cellular telephones are accessible to anyone with an FM scanner, as demonstrated by the recent publication of communications involving public figures. Moreover, the location of a cellular user can be determined by triangulating the signal from two or more base stations, a feature that has been exploited successfully by law enforcement authorities. It is difficult to prevent the interception of commercial radio signals, not only because communications protocols are publicized in patents and standards but also because most communications devices have a "maintenance" mode for monitoring calls (a capability intended for testing purposes that could also be used to eavesdrop).

It is unlikely that commercial devices will ever require a level of security equivalent to military systems and may not even provide the "hooks" enabling the addition of LPD/I capabilities. Similarly, although the growing use of wireless systems and growing dependence on networked communications have heightened concerns about the possible denial of service in commercial contexts, there is probably a greater

tolerance of private-service outages than of jamming with regards to a military situation at this time.

Hardware security also has different implications for commercial and military applications, although encryption keys typically need to be protected in both contexts. Commercial systems require sufficient security to prevent the fraudulent use of information in the event of theft or loss, and user databases need to be secured against unauthorized access. The military has similar requirements but at a much higher security level. It also has additional requirements: military devices need to be protected so that opening them will not reveal any of the specialized hardware or software technology.

THIS PAGE INTENTIONALLY LEFT BLANK

V. WIRELESS AD HOC NETWORKS MODEL

A. BUILDING THE MODEL

Ongoing digitization efforts of the battlefield are seeking to harness the power of the computer to help the commander and his forces better understand their situation, improve force synchronization, and enhance combat effectiveness. As a result, there is a need for seamless* integration of wireless and mobile digital communications.

In the military arena, the SOF are prepared to operate worldwide across a broad spectrum of conflict. Moreover, there is a great tendency –and benefit- toward working together with allied and friendly forces. Technological improvements and systems have to be interoperable within a coalition. There must at least be some common ground to connect different national infrastructures while keeping each participant's confidentiality private.

As stated in Chapter I, the motivation for our research stems from the need to ensure that the SOF remain the best informed forces on the battlefield in order to accomplish this goal, the special operator must immediately obtain all of the most current, relevant data. This is important because SOF teams often operate behind enemy lines with limited resources. New and detailed information about their operational area increases the likelihood of mission success and survivability.

We use the following planning considerations, which are based on the five doctrinal principles previously discussed in Chapter II:

---

* "Seamless" refers to the transportation of data, whether across one or multiple networks that is transparent to the user.

- SOF communication must be digital
- C4I support must depend on national systems to the maximum extent possible,
- Access to the infosphere must be driven down to the lowest possible tactical level
- Communications systems do not have to follow the chain of command

Moreover, we need to think about organizational issues as well. The information revolution is changing the nature of the conflict. This revolution "is favoring and strengthening networks forms of organization, while simultaneously making life difficult for old hierarchical forms."[80] The network concept in which every node is connected to every other node shifts power traditional, hierarchical, state actors to nonstate actors. It is likely that networks will wage the future conflicts more than hierarchies. Those who control the network will get the major advantages.

The SOF is part of the military hierarchy, but the communication of SOF units might be in a networked fashion where the traditional chain of command can be skipped.[81] In this way the SOF can cope with multinational, networked, nonstate enemies who will be appearing frequently in the future.

We can express networks in three topologies: the chain network, the star network, and the all-channel network (Figure 13). Different adversaries can be found in different forms: "e.g., the chain in smuggling operations; the star among criminal syndicates; and

---

[80] Ronfeldt, D., Arquilla, J., Fuller, G.E., Fuller, M., *The Zapatista Social Netwar in Mexico*, RAND Arroyo Center, Santa Monica, CA, 1998, 7.

[81] This idea is supported by the military in *USSOCOM C4I Strategy Into The 21st Century*, Macdill AFB, FL,1996, 6.

the all-channel among militant groups that are highly internetted and decentralized."[82] There may also be hybrids of these networks and this makes many combinations possible.

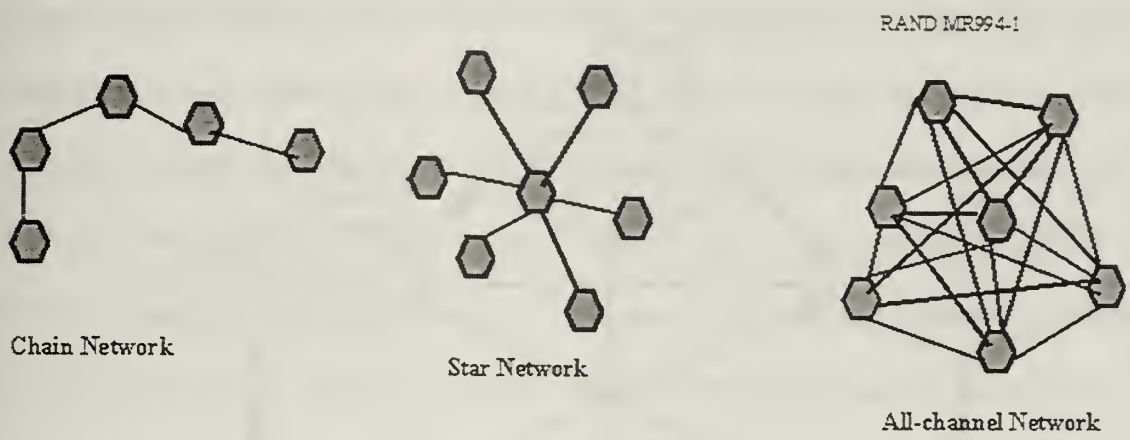


Figure 13. Types of Networks.

The all-channel type seems to be the most complicated network topology to organize and maintain. It requires a vast amount of communications. "But this is the type that gives the network form its new, high potential for collaborative undertakings. It is the type that is gaining new strength from the information revolution."[83] Our communications model will also follow this topology in order to meet requirements of future battlefields and potential adversary profiles.

To satisfy requirements for rapidly deployable and robust information systems, it is critical that the underlying technologies be available to support operations in the mobile environment. The Global Mobile Information Systems (GloMo), sponsored by the Defense Advanced Research Projects Agency (DARPA), is tasked with creating a detailed list of enabling technologies for robust wireless environments (Figure 14). In order to develop a global communications system, three critical components are needed:

---

[82] Ronfeldt, Arquilla, *Zapatista*, 12.

untethered nodes, wireless networking, and mobile application support. Table 3 briefly describes each focus area.

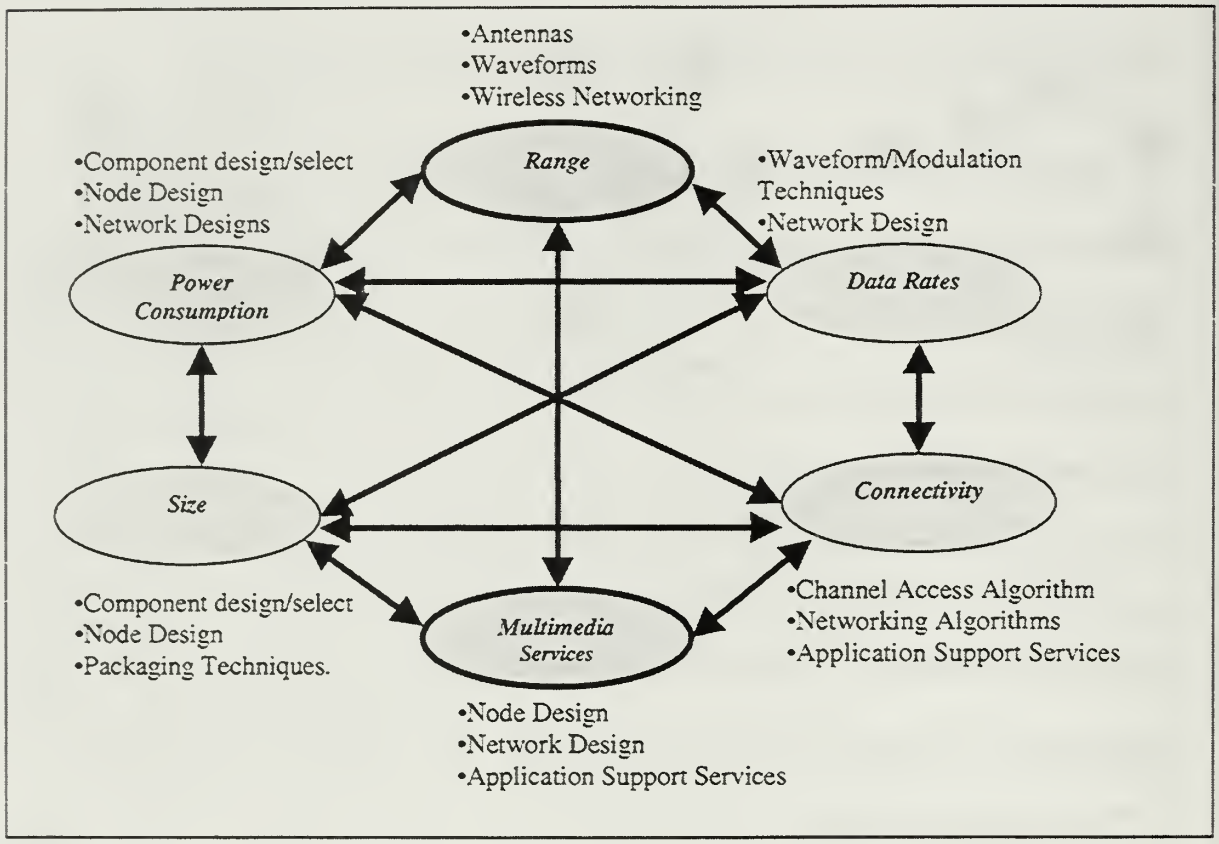


Figure 14. Required Technologies for a Wireless Mobile Network.

Untethered Nodes	Scalable, adaptable untethered systems exploiting low-power technology.
Wireless Networking	Networking techniques that support rapid deployment and robust networking service in a hostile and dynamic environment.
Mobile Application Support	New distributed computing techniques supporting mobile operation (e.g., file systems, locality awareness) in an environment characterized by sporadic connectivity and varying QoS.

Table 3. Main Focus Areas for a Global Mobile Communications System.

[83] Ibid., 13.

The objectives of the system are to provide real-time information collection and management for generating tactical understanding; automated planning, dynamic planning, and tasking; and robust, wireless communication with voice, data, video/graphics, and geo-location capability. The system is to be flexible and adaptable to environments and missions, and optimized for restrictive environments (such as urban, forest, and mountainous). Important aspects of the system include long-range (global via relays) communications, low probability of intercept (LPI), low probability of detection (LPD), anti-jam (AJ), internetting, and efficient use of the electromagnetic spectrum.

Our simulation model will depend on a direct action (DA) scenario. According to the DA scenario, there is a SOF battalion consisting of six teams. Each team consists of a total of twelve personnel, two officers and ten non-commissioned officers (NCO). Two teams are used in the actual raid and four teams stand ready as a reserve force in case of an emergency.

As to the nation building mission, a SOF battalion of six SOF teams operates in a friendly country, and trains and advises armed forces of the country in their fight against a separatist guerilla movement. The country is divided into four operational districts and the battalion serves as twelve half-teams with three in each district. Half teams operate under a Region Command Center (RCC). The first region also serves as the National Command Center (NCC). Each RCC is connected to the NCC via wireless communication channels.

1. Untethered Nodes

Each team member carries a hand-held communications device, which will be called an untethered node in wireless networking. It is wise to give each member of the

team the same type of device. For the sake of cost efficiency, we will assume that the team commander and his deputy (second officer) has more capable devices (Type-1) than the rest of the team, who carry Type-2 devices, in terms of range, memory capacity, and output power. This organizational and hierarchical approach is parallel to virtual cellular architecture, which exploits today's state-of-the-art cellular communications technology.

On the other hand, we are following the all-channel network topology also. In this model the twelve-man team can be thought as a node. Each team commander might communicate with another one. Once every special operator is promoted to owning a Type-1 device, each member of the team becomes the node of the all-channel network. Until then, the first described model resembles a hybrid network topology. At the team commander's level the SOF communications follows the all-channel topology. Inside the team a star topology exists. The advantage of the star topology is that it controls communications. The down side is that it is a single point of failure and there are congestion points in the network.

Developments in commercial cellular technology impel producers and designers to develop cost-efficient devices for market use. As shown in Table 4, there are differences in the fundamental design and vision issues between commercial handheld wireless devices and those used by the SOF. Shrinking defense budgets, and rapidly changing technologies, force military customers to gain leverage from using commercial technology and systems, while getting involved in standardization and technology setting.

Commercial	Military
Ubiquitous, uniform, open information access	Highly structured C2, team centered, mission specific, non-uniform
Consumer cost determines features (competitive)	Performance at lowest cost
Personal/consumer feature set	Dynamic situation-dependent functionality
Government legislated waveforms, frequencies	Waveform/frequency/range agility, programmability
Focus on emerging frequency bands and service overlays (e.g. PCS, GSM, CDPD)	Leverage tech. for very high bandwidth, high frequency, unregulated bands
High volume production	Lower volume, ruggedized against EMP threat
Data security	LPI, LPD, multi-level security
Operating modes synchronization	Burst packet synchronization

Table 4. Commercial vs. Military Untethered Nodes.

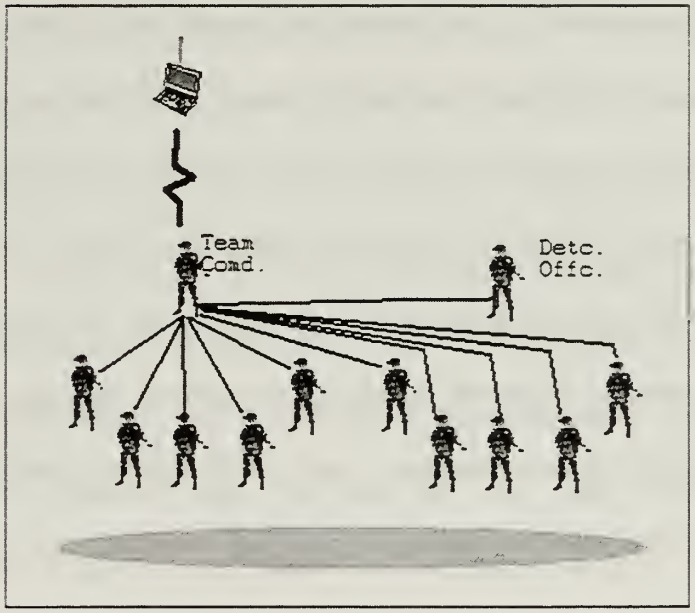


Figure 15. SOF Team Working as a Whole*

A twelve-man team has the ability to operate in two independent teams of six members each with the same capabilities. For this reason, each team will have at least two highly capable untethered nodes (Type-1), which relay communications between the lower echelon and the higher echelon. Under normal conditions, a team operates as a

* Each special operator can communicate with his fellow team friends within the range of the communications device. These links are not shown in the figures for graphical simplicity.

whole during the mission. Intra-team communication is held among team members in a direct way.

Each team member needs to be able to send messages (voice, data, and image) to the other members of the team (including the team commander) within the rules of operation. Since communications systems do not have to follow the chain of command under the SOF doctrine, a team member might send/receive a message to/from a higher echelon device. In order to manage this connection, a highly capable device (Type-1) carried by a team commander acts as a router for packets sent in between. Under normal conditions, the second Type-1 node carried by a deputy officer who acts as a Type-2 node checks for a heartbeat from the main device carried by the team commander. In order to provide a rudimentary level of fault tolerance, the second Type-1 node takes over the routing mission of the main node when the main node fails. On the other hand, if the team is divided into two half-teams operating in different physical areas, the second Type-1 node can be promoted to become a router node under the new topology. Figures 15 and 16 illustrate the possible topologies in a SOF team carrying Type-1 and Type-2 nodes.

In a nation building mission, each six-person team carries one Type-1 and five Type-2 devices. The RCC and NCC also carry Type-2 devices. In any region, a team member can communicate with the NCC directly. In this case, interim Type-2 devices route the packets. Moreover, special operators can exchange intelligence, weather and logistic information among themselves. In case of an emergency, close air support and naval support might be coordinated using the same devices.

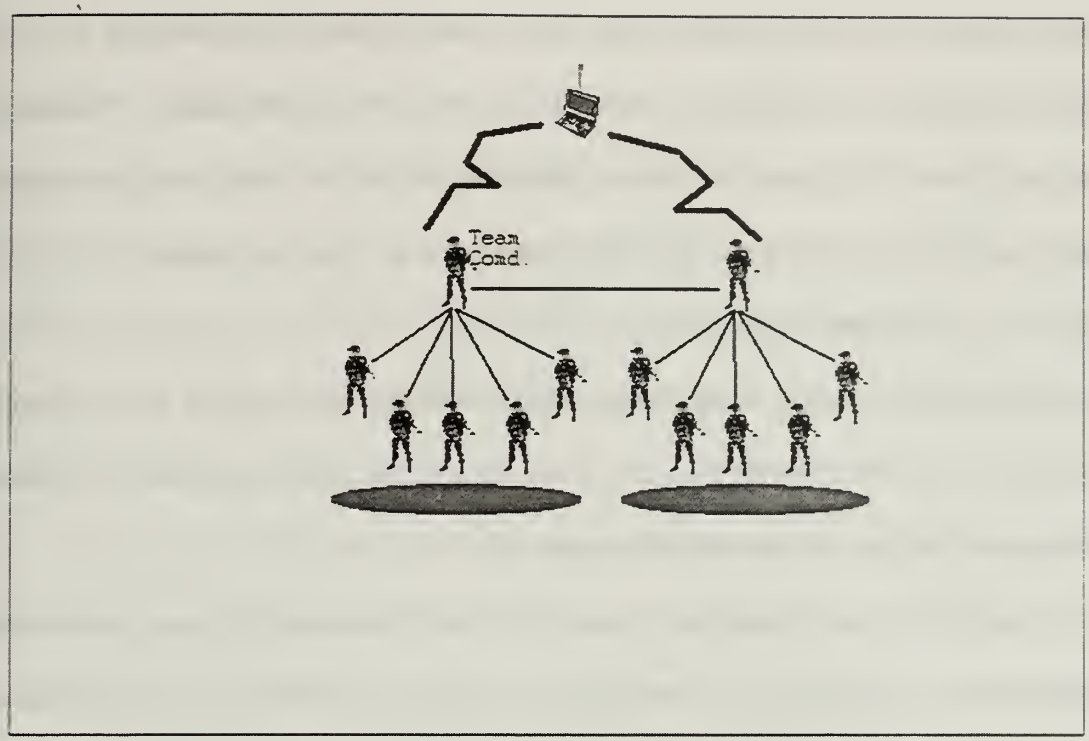


Figure 16. SOF Team Working as Two Half-Teams.

Power consumption is a major driver for the requirement of untethered nodes. The use of a single battery and careful power management is essential. Variable receiver/transmitter dynamic range, low receiver duty cycle (stand-by), and burst transmissions are desired approaches to minimize power consumption for communications. The system needs to weigh less than 1 kg, consumes less than 5 W*, have a user-friendly interface without a keyboard, and be compromised of a minimum number of wires.

The situational awareness system provides reliable connectivity for the twelve-man team in a range up to 2 km*, between teams in a 10 km X 10 km area, and the forward operations center at ranges of up to 200 km. Variable processing gain and

* 5 W transmit power is a required standard set by DARPA in the GloMo project, in order to provide LPI/LPD.

transmit power are to be employed to maximize the transmission bandwidth, minimize power consumption, and provide high LPI at very low bandwidths. "Notionally, communications will support 10 MHz to 2 GHz and 10 bps[<] to 2 Mbps. High processing gain waveforms (e.g., 50 db) and low-power software encryption are desired."[84]

2. Wireless Networking

Our model supports a peer-to-peer mobile network consisting of a large number of mobile radio nodes that create a network on demand and may communicate with each other via intermediate nodes in a multihop network.

For efficiency and cost effectiveness, the reuse of existing cellular architectures in multihop peer-to-peer networks is desirable and clearly very helpful. As mentioned in the previous chapter, a workable solution might be obtained by mapping a cellular architecture onto a multihop network via the Virtual Cellular Architecture (VCA) concept suggested by Chlamtac and Farago[85]. In fact, this method has been presented in the literature as *clustering* in wireless mobile networks. Chlamtac and Farago point out that prior research has been focused on finding clusterheads and forming the clusters. At the end of their study, they manage to efficiently interconnect the clusterheads via a virtual backbone network found in cellular systems. They also show that global backbone connectivity can be provided by building local clusterheads connections among nearby clusterheads, without the knowledge of the global network topology.

[•] Team members can provide fire support for each other in this range.

[<] This low capacity is required for "legacy" systems.

[84] DARPA Information Tech. Office, Recommendations for Tech. Transfer from GloMo Area to Small Unit operations (SUO) Program, 27 Jan 1998, 1-12.

[85] Chlamtac, Farago, 149.

In fact, the defense community is familiar with the idea of clustering. Its hierarchical organization fits well with a clustered topology. As an example, Saas mentions the Near-Term Digital Radio (NTDR) project in his study[86]. The NTDR system architecture employs a two-tier hierarchical network concept, where an intercluster backbone channel is used to relay packets between users in local clusters. One NTDR in each channel is designated as a clusterhead and operates on both the backbone channel and the local cluster channel.

Our model will support a tactical organizational clustering. A SOF team or half-team is the lowest level cluster and the Type-1 node is the clusterhead. In the upper level (battalion), each battalion forms a cluster and improved Type-1 nodes act as clusterheads. One may think that this hierarchical system might create choke points in the communications. We assume that it provides more capability in terms of resources and resource reservation for the clusterheads as the level of the cluster goes up. This is required to prevent potential choke-points at the clusterheads. The highway system might be a good analogy for illustrating the necessity of providing more capacity as complexity of the system grows. Residential areas two-lane roads can be sufficient to sustain the proper flow of traffic. However, when the vehicles are on the freeway the additional lanes in each direction can help to minimize congestion. As the drivers approach the city center, main arteries become multi-lane roads. In addition, this assumption is plausible when we compare the resources held by a forward operations commander, battalion commander, team commander, and single special operator. For example, one phone line might be enough for a team commander, but for a continuous uninterrupted

[86] Saas, P., *Communications networks for the Force XXI Digitized Battlefield*, Mobile Networks And

communication with the battalion commander, it is necessary to have at least two lines one for the upper command and one for his teams. Figures 17 and 18 summarize the wireless networking topology for different hierarchical levels.

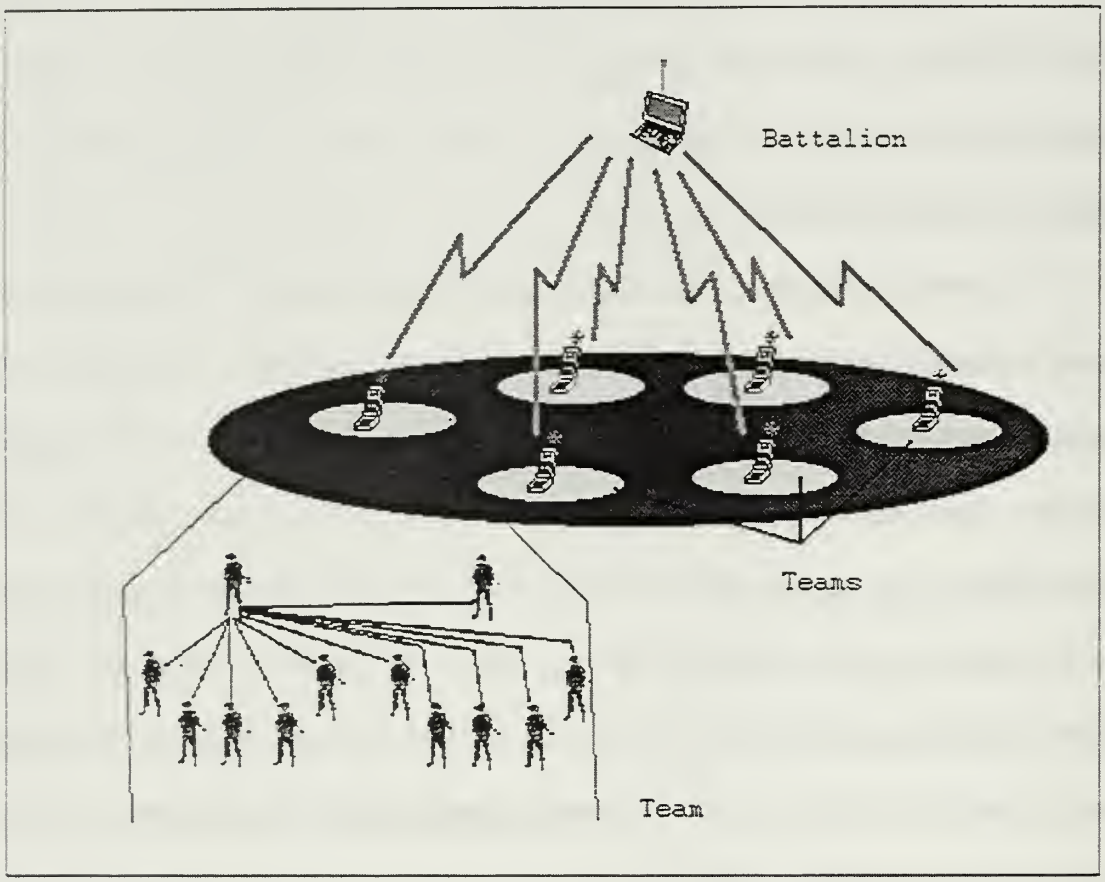


Figure 17. Communications between Different Levels.

The Operations Center –and sometimes the forward operations center also - is usually supported by wireline network systems. One enhancement to application support systems is to develop a comprehensive proxy architecture that mediates constrained bandwidths of the wireless link and well connected bandwidth of the wireline network. The proxy chooses an appropriate representation and degree of compression for transport

---

Applications, Vol: 4, Issue 3, 1999, pages 139-155.

over the wireless link, while performing fetching and caching operations on behalf of the mobile end node.

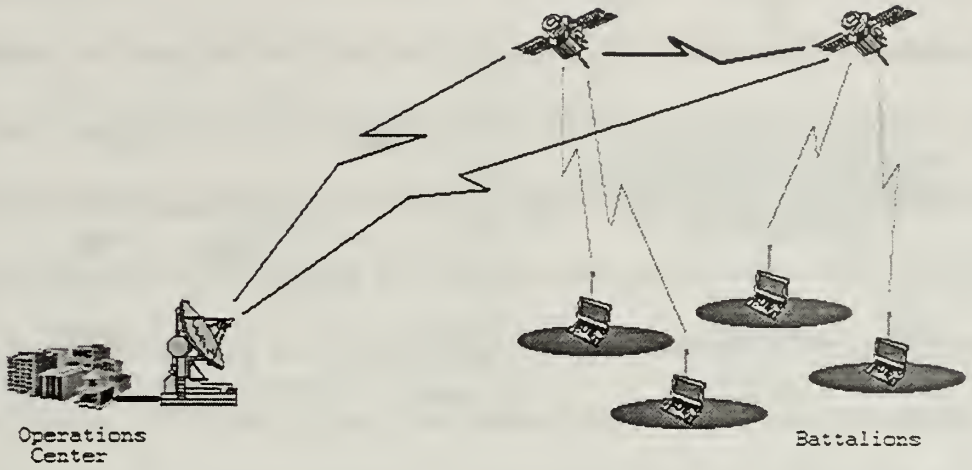


Figure 18. Connections from Battalions to Ops. Center.

In addition, the proxy performs-processing intensive tasks on the behalf of the computationally less improvised Type-1 and Type-2 devices. Nam and Park propose a buffering method including a proxy, which is located between the server and the client[87]. The proxy acts as an agent for a mobile host. The idea of delegating mobile nodes via proxy supports communications at different levels. For example, during humanitarian aid operations or nation building missions, the conditions might not be as limiting as direct actions. The ability to use local wired networks or having enough resources for power and processing makes the use of a proxy beneficial for the mobile end nodes.

In a nation-building mission, availability of the host nation's communications infrastructure enhances the quality of overall communications because the burden of wireless mobile communication can be shared by the local infrastructure and the quality

[87] Nam, D., Park, S., *Adaptive Multimedia stream presentation in Mobile Computing Environment*,

of service in both wired and wireless channels increases. Doctrinally, it is essential to use national assets in the SOF communications. However, multinational coalitions, humanitarian aid operations, and nation-building missions are hosted by friendly and allied nations. The use of the available communication infrastructure of host nations after taking necessary security measures- for example, 128-bit encryption and VPN implementation- leverage the shortcomings of the wireless mobile communications in the near future. The same cluster-based architecture is planned for the nation-building mission. The only difference from direct action missions will be the use of a wired communications infrastructure –supposedly the Internet due to its global coverage. Figure 19 demonstrates the communications of SOF teams in a potential nation-building mission.

TENCON'99, proceedings of the IEEE Region 10 Conference, 1999, Vol: 2, Pages: 966-969.

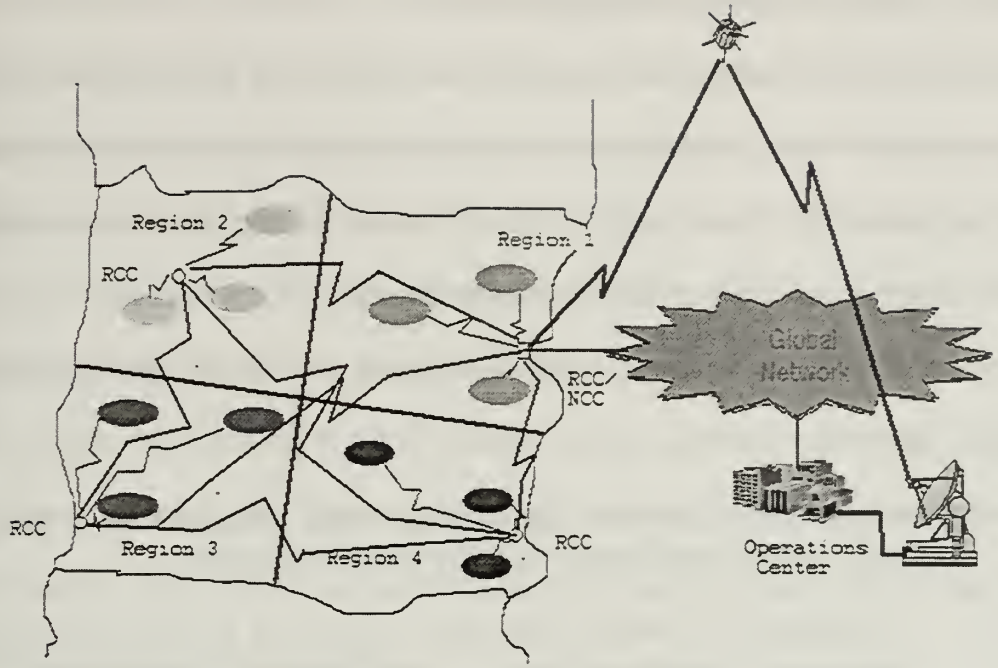


Figure 19. Communications of SOF in a Nation-Building Mission.

During training and exercises, necessary files might be downloaded from national resources. The use of visual training documentaries might increase the quality of the training while lessening the time and resources required. Host nation's wired infrastructure plays an important role when distance learning might be an available choice in training and physiological warfare. The wireless mobile communication supports image transfer and video conferencing but it might not have adequate resources for distance training. In this case, host nations infrastructure and even international resources (i.e, the Internet) can be helpful under the prerequisite of enhanced security.

3. Vulnerabilities of Wireless Systems

The world is becoming more dependent on wireless and mobile services but the ability of wireless network infrastructures to handle the growing demand is questionable, as wireless and mobile systems play greater roles in the military arena and emergency response network failures take on life or death significance.

For ad hoc wireless networks, a network's ability to avoid or cope with failure is measured in three ways:

- Reliability is a network's ability to perform a designated set of functions under certain conditions for specified operational times.
- Availability is a network's ability to perform its functions at any given instant under certain conditions. Average availability is a function of how often something fails and how long it takes to recover from failure.
- Survivability is a network's ability to perform its designated set of functions given network infrastructure component failures, resulting in a service outage, which can be described by the number of services affected, the number of users affected, and the duration of the outage.

Military operations heavily depend on communications for coordination, reporting and for the continuation of the operations. This is especially true of the SOF which operates behind enemy lines. Contingency plans might respond to critical communications failures. Careful and detailed planning will decrease the need for excessive communications, which in turn increases the probability of detection. However, these tactical and technical approaches will not reduce the degree of reliability, availability and survivability of SOF communications.

In ad hoc wireless networks, the most important network component is the hand-held devices carried by the users. Since these types of networks do not have fixed infrastructures, the failure of these hand-held devices are critical for communications. As

stated before, due to impressive cellular network applications, using the cellular network approach makes use of the current technology as much as possible. Virtual cellular networks create virtual cells with clusterheads managing their cells. While this approach benefits the state-of-the-art cellular technology, it also creates a single point of failure. The node assuming the role of the clusterhead becomes vulnerable to attacks as well as operational failures. Since the clusterheads function as the routers in their cells, their failure affects intercellular and intracellular communications. Varying degrees of redundancy decreases the failure of frequency. Powerful fault tolerance algorithms which can promote a similar device to the role of clusterhead make use of quantitative redundancy of the same type devices.

Our model consists of two types of devices. Type-1 devices are used for intra-team communications and these devices have limited routing and range capability. Type-2 devices, on the other hand, are capable of communicating with satellites and have longer line-of-sight ranges. If the network consisted of homogeneous nodes, then it would be very easy and effective to promote the first available node to be the next clusterhead in case of failure. There would be enough redundancy and fault tolerance algorithms would work quickly. However, supplying all personnel with complex and expensive devices will not be cost effective and might not be necessary at all. Thus, heterogeneous systems consisting of devices but having been networked efficiently might operate as well as expensive homogeneous systems. On the other hand, in the long term, with the improvements in the technology, all nodes in the system might be the same powerful type devices.

B. BUILDING THE SIMULATION

As stated in Chapter III, UCLA's GloMoSim simulation tool for simulating our mobile wireless communications model will be used. In this section, a procedure for using GloMoSim in conjunction with the scenarios described in Appendix A is discussed.

1. Environment

GloMoSim supports a wide range of platforms. Our simulations are run on a Windows NT 4.0 Workstation. Microsoft's Visual C++ 6.0 is used to convert Parsec based entities into C. JDK 1.2.2 is used for running the graphical user interface (GUI) of the GloMoSim. The hardware consists of a Pentium II 166 CPU with 64 K RAM of memory and 4.3 Gbyte of storage memory.

2. GlomoSim Components

A typical GloMoSim software packet contains the following directories and files:

/application contains code for the application layer
/bin for executable and input/output files
/doc contains the documentation
/include contains common include files
/mac contains the code for the mac layer
/main contains the basic framework design
/network contains the code for the network layer
/radio contains the code for the physical layer
/transport contains the code for the transport layer

Most of our interaction with the simulation takes place via input/output files under the "bin" directory. These files are used to define the configuration of the simulation model, the physical terrain, initial locations of the mobile nodes, the mobility trace of each node throughout the simulation, and the traffic that is to be generated among the nodes. The user can configure different protocol stacks and probe statistics from each node. The input/output files of interest are defined briefly below:

config.in: This is the main configuration file for the simulation. The terrain, the number of nodes, bandwidth, communication range of each node, protocols for radio, mac, network layers and the routing algorithm are specified in this file.

nodes.in: The nodes on the terrain can be distributed randomly or in groups. In those cases, it is specified in the config.in file. The "nodes.in" file is used when the user wants to initialize nodes at specific locations.

mobility.in: Just like locating nodes, it is possible to make nodes move randomly via the "config.in" file. The "mobility.in" file is used when it is necessary to define different paths for each node. The user can move any node to any point on the terrain at a specific time during the simulation.

apps.in: The generation of the traffic among the nodes is configured by using this file. Currently available applications are FTP, TELNET, CBR (Constant Bit Rate), and HTTP. It is possible to define a communication payload between any two nodes, at any given time during the simulation. Moreover, the user can define the size of the payload and the duration of the session whenever available.

.stat: This is the output file. The statistics approved in the config.in file are collected via this file.

A detailed format of the aforementioned files is given in Appendix C.

3. Preparing the Configuration

Our simulation models were configured with respect to out scenarios. Twenty-five nodes represent the tactical elements in the scenario. These nodes communicate via radio links. The terrain is a 1000-meter by 600-meter rectangular. The two operational teams form their position next to the target areas. Team commanders are connected to

the operations center (OC). In our model two different devices – Type-1 and Type-2 – are defined. Due to the homogenous nature of the GloMoSim, it is assumed that the OC is out of reach of the team elements except for the team commander and the executive officer who are using the Type-1 devices. The team commander's device will relay messages addressed to the team elements from outside and vice versa. As stated earlier, our model envisages a fault tolerance via the execution of the officer's Type-1 devices. This fault tolerance provision can prevent the single point of failure while operating as a whole team. However, when the team splits into the two groups, it is not sufficient. For this reason, all Type-2 devices will be required to be Type-1 devices in the future. Each Type-2 device is capable of relaying messages among the team members. That is, when a team member is not covered by the team commander's device, the packets for/from him are routed through neighboring nodes.

Discrete-event models deal with events and specific time intervals. An example of the discrete events includes computer-performance evaluation. In discrete-event models, the occurrence of an event drives the model, whereas in continuous models, the passing of time drives the model. The events and the other specifications are included in the configuration file of the GloMoSim. The configuration file for a typical simulation run looks as follows:

SIMULATION-TIME	1600S
SEED	1
PARTITION-NUM-X	1
PARTITION-NUM-Y	1
TERRAIN-RANGE-X	1000
TERRAIN-RANGE-Y	600
NUMBER-OF-NODES	25
NODE-PLACEMENT	FILE
NODE-PLACEMENT-FILE	../bin/nodes.input
MOBILITY-TRACE	
MOBILTIY-TRACE-FILE	../bin/mobility.in
MOBILTIY-POSITION-GRANULARITY	0.5
PROPAGATION-FUNCTION	FREE-SPACE
RADIO-TYPE	RADIO-CAPTURE
POWER-RANGE	250
BANDWIDTH	(250000 to 2000000 with a stepsize of 250000)
MAC-PROTOCOL	(CSMA/802.11)
PROMISCUOUS-MODE	YES
NETWORK-PROTOCOL	IP
ROUTING-PROTOCOL	(DSR/WRP)
TRANSPORT-PROTOCOL-TCP	YES
TRANSPORT-PROTOCOL-UDP	YES
APP-CONFIG-FILE	../bin/app.conf
APPLICATION STATISTICS	YES
ROUTING STATISTICS	YES
MAC STATISTICS	
YES	

The traffic is generated according to the scenario, and each time, one of the simulation parameters is changed. The routing protocol, MAC protocol and the bandwidth were chosen as changing parameters.

Both table-driven and on-demand protocol kinds are used for the routing protocols. Using a simulation with different routing protocols, the most efficient routing protocol in the wireless systems will be reached.

C. TESTING

Multiple runs of our simulator using DSR and, WRP routing protocols and CSMA, and 802.11 MAC layer protocols were conducted. We initially validated our basic model using only a single data generation source and channel. We validated our design and ensured the correctness of the values generated by the simulation. After verifying the correctness of the basic model, additional simulations varying the parameters and using small data sets as reflected by the small size of the load were run.

We varied the bandwidth of the system in different simulations. Eight different bandwidth values are used. The smallest value was 250000 bps, then the bandwidth was increased with a stepsize of 250000 bps until 2 Mbps was reached. All channels among the nodes have the same capacity because of the homogenous nature of the GloMoSim.

Another simulation parameter is the load on the system. Different message sizes were used for comparison and sensitivity analysis. In the first set of run simulations, the message size was kept in small. Then, in the second runs, the message size was increased by doubling the original message size in order to see the effects of the load on the overall system. Small data sets are used to determine the sensitivity of our simulations to changes in certain parameters. Next, real message sizes were reached by multiplying the original sizes by four. Additional runs were conducted to determine whether our analysis of the smaller data sets holds for larger data sets ("app.conf" file. See Appendix C).

Finally, in order to see the performance of the system under high loads, the load was increased to six and eight folds of the original load.

In order to compare the performance of the on-demand and table-driven routing algorithms, the protocol type was changed, and the simulation for the same parameters was run each time.

D. RESULTS

In Figure 20, the results of our testing for DSR and WRP routing protocols are provided. All data are taken from the first node, which is one of the most active communicating nodes during the scenario. Node 1 is the team detachment officer in the eastern operational area. Similarly, Node 13 assumes the same role in the western operational area. Since the messages used in both areas are almost identical (Appendix B) the data collected from Node 1 and Node 13 are similar. In order to prevent redundancy, the results of Node 1 are included. Figure 20 consists of 4 different tables. Each table demonstrates different combinations of routing and MAC layer protocols (e.g., DSR and CSMA, or WRP and 802.11). Each row in the tables represents different bandwidth values. The first columns show the packets generated by the protocols for the same size of communications. The second columns give the power consumption under given protocol combinations. The third columns are the representation of the control overheads for the systems.

After comparing routing protocols, the performance of the system under different message loads was studied. Figure 21 provides the results of our testing for the DSR routing protocol with the CSMA Mac layer protocol. Finally, Figure 22 provides the results of the DSR routing protocol with the 802.11 MAC layer protocol. Each table

represents different load values. Both figures share the same row and column types as described for Figure 20.

NODE 1	DSR	CSMA		
	MAC	COLL.	POWER	CTRL
0.25	40	35	164.45	19
0.5	42	44	163.29	18
0.75	44	47	162.91	19
1	35	11	162.64	13
1.25	37	10	162.51	14
1.5	35	9	162.44	13
1.75	34	8	162.38	12
2	35	7	162.4	13
AVE	37.75	21.375	162.878	15.125

NODE 1	DSR	802.11		
	MAC	COLL.	POWER	CTRL
0.25	188	73	166.38	28
0.5	276	25	165.04	41
0.75	257	22	164.27	45
1	248	22	163.59	42
1.25	174	8	163	19
1.5	171	10	162.9	18
1.75	197	26	163.66	22
2	199	16	162.9	23
AVE	213.8	25.25	163.968	29.75

NODE 1	WRP	CSMA		
	MAC	COLL.	POWER	ROUTIN G
0.25	806	157	237.61	778
0.5	825	91	199.94	797
0.75	823	42	187.92	795
1	831	44	181.77	803
1.25	802	22	178.03	774
1.5	825	41	175.82	797
1.75	822	42	174.58	792
2	822	28	172.95	794
AVE	819.5	58.375	188.578	791.25

NODE 1	WRP	802.11		
	MAC	COLL.	POWER	ROUTING
0.25	951	204	249.95	825
0.5	888	60	204.32	768
0.75	926	54	190.94	809
1	902	50	184.3	786
1.25	933	38	180.13	813
1.5	929	38	177.51	813
1.75	937	40	175.58	821
2	919	34	174.03	800
AVE	923.1	64.75	192.095	804.375

Figure 20. Test results of the DSR and WRP Routing Protocols.

LOAD_X			
	NO. PK	POWER	CTRL
0.25	40	164.45	19
0.5	42	163.29	18
0.75	44	162.91	19
1	35	162.64	13
1.25	37	162.51	14
1.5	35	162.44	13
1.75	34	162.38	12
2	35	162.4	13
AVE	37.75	162.878	15.1

LOAD_2X			
	NO. PK	POWER	CTRL
0.25	62	166.6	20
0.5	68	164.38	18
0.75	70	163.62	19
1	59	163.16	14
1.25	57	162.97	13
1.5	56	162.83	12
1.75	57	162.81	13
2	57	162.63	13
AVE	60.75	163.625	15.25

LOAD_4X			
	NO. PK	POWER	CTRL
0.25	141	172.44	19
0.5	122	166.59	20
0.75	122	165.03	19
1	101	164.27	13
1.25	101	163.94	13
1.5	101	163.53	13
1.75	101	163.31	13
2	100	163.16	12
AVE	111.125	165.284	15.3

LOAD_6X			
	NO. PK	POWER	CTRL
0.25	172	176.17	19
0.5	195	169.75	18
0.75	175	166.5	21
1	171	165.6	14
1.25	145	164.89	13
1.5	145	164.47	13
1.75	145	164.08	13
2	145	163.89	13
AVE	161.62	166.919	15.5

LOAD_8X			
	NO. PK	POWER	CTRL
0.25	208	179.62	19
0.5	239	171.1	18
0.75	225	167.8	19
1	189	166.47	13
1.25	207	165.62	14
1.5	189	165.05	13
1.75	189	164.63	13
2	189	164.39	13
AVE	204.375	168.085	15.3

LOAD_10X			
	NO. PK	POWER	CTRL
0.25	275	185.36	19
0.5	315	174.06	18
0.75	277	169.36	19
1	233	167.63	13
1.25	274	166.8	14
1.5	234	165.69	14
1.75	274	165.63	14
2	233	165.07	13
AVE	264.37	169.95	15.5

Figure 21. The DSR and CSMA with Different Communication Loads.

LOAD_1x	DSR		
	NO. PK.	POWER	CTRL
0.25	188	166.38	28
0.5	276	165.04	41
0.75	257	164.27	45
1	248	163.59	42
1.25	174	163	19
1.5	171	162.9	18
1.75	197	163.66	22
2	199	162.9	23
AVE	213.75	163.968	29.8

LOAD_2x	DSR		
	NO. PK.	POWER	CTRL
0.25	772	176.52	22
0.5	386	168.34	23
0.75	385	165.75	23
1	387	164.57	22
1.25	388	164.13	21
1.5	380	164.34	21
1.75	382	163.92	21
2	382	163.41	21
AVE	432.75	166.3725	21.8

LOAD_4x	DSR		
	NO. PK.	POWER	CTRL
0.25	577	182.72	27
0.5	535	175.54	31
0.75	553	168.56	23
1	622	166.98	23
1.25	530	166.36	22
1.5	621	166.78	23
1.75	624	165.51	25
2	618	165.83	23
AVE	585	169.785	24.6

LOAD2_6x	DSR		
	NO.PK	POWER	CTRL
0.25	1101	193.34	27
0.5	930	175.88	30
0.75	1192	178.59	28
1	1095	171.37	24
1.25	1093	171.76	20
1.5	1112	171.98	30
1.75	1095	170.51	22
2	1094	168.13	24
AVE	1089	175.195	25.6

LOAD_8x	DSR		
	NO. PK.	POWER	CTRL
0.25	2048	213.32	33
0.5	1051	178.99	24
0.75	1037	171.43	22
1	1073	173.31	21
1.25	1324	174.44	25
1.5	1025	169.21	22
1.75	1096	172.01	23
2	1030	168.33	24
AVE	1210.5	177.63	24.3

Figure 22. The DSR and 802.11 with Different Communication Loads.

E. ANALYSIS

This section provides the analysis of the testing.

1. Table-driven versus On-demand Routing Protocols

In table-driven routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables to maintain a consistent and up-to-date view of the network. When the network topology changes, the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. Wireless Routing Protocol (WRP) is a typical table-driven routing protocol.

In on-demand routing protocols, in contrast to table-driven routing protocols, all up-to-date routes are not maintained at every node. Instead, the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid until the destination is reachable or until the route is no longer needed. Dynamic source Routing (DSR) protocol is one of the effective on-demand protocols.

Figure 23 uses the data from Figure 20 and shows the performance of the routing protocols with respect to packets generated by the protocols. There is a substantial difference in the number of packets created by two different protocols. While the DSR generates very few packets, the WRP generates more packets and increases the load of the networks system. In fact, both protocols use same amount of messages, but the substantial difference is due to control overhead embedded by the routing protocol in the system.

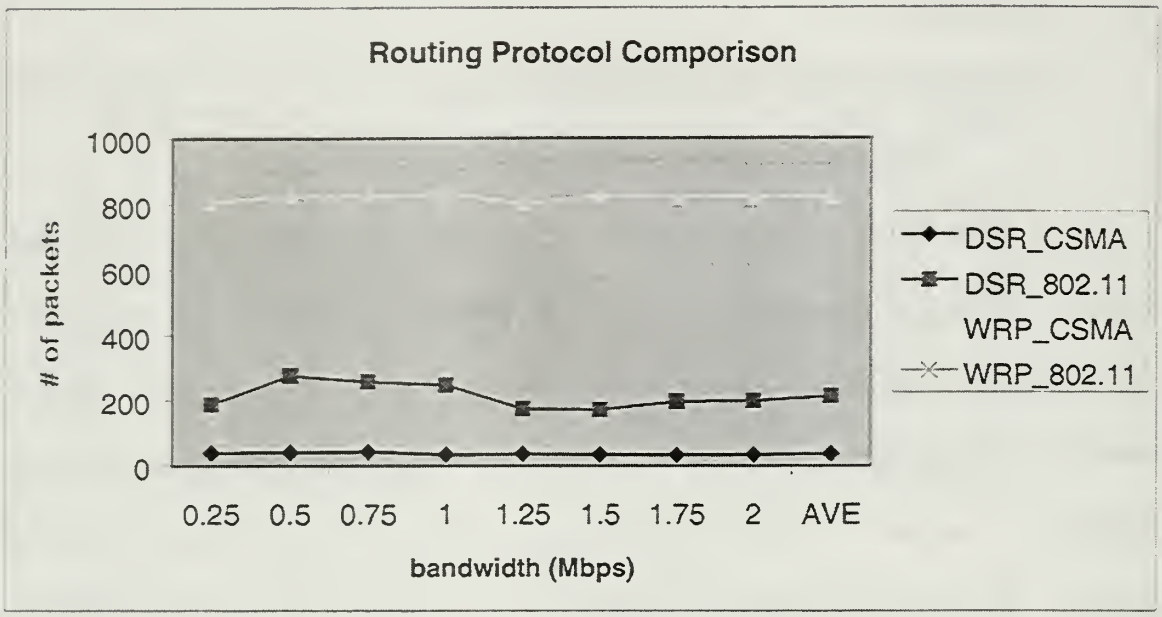


Figure 23. The DSR and WRP Comparison.

Figure 24 demonstrates this fact more clearly. While the DSR creates very few overhead packets, the WRP generates more control packets due to the nature of the table-driven routing protocols' update mechanism. In both cases, the results show that the system is independent of the bandwidth changes. This is true because the number of packets generated is not the function of the bandwidth but the message load on the network.

On the other hand, Figure 25 shows the power consumption is slightly related to the bandwidth. The WRP consumes more power than the DSR. The difference is high at low bandwidth values – i.e., 0.25 to 1 Mbps- and decreases as the bandwidth supported by the system approaches the 2 Mbps value.

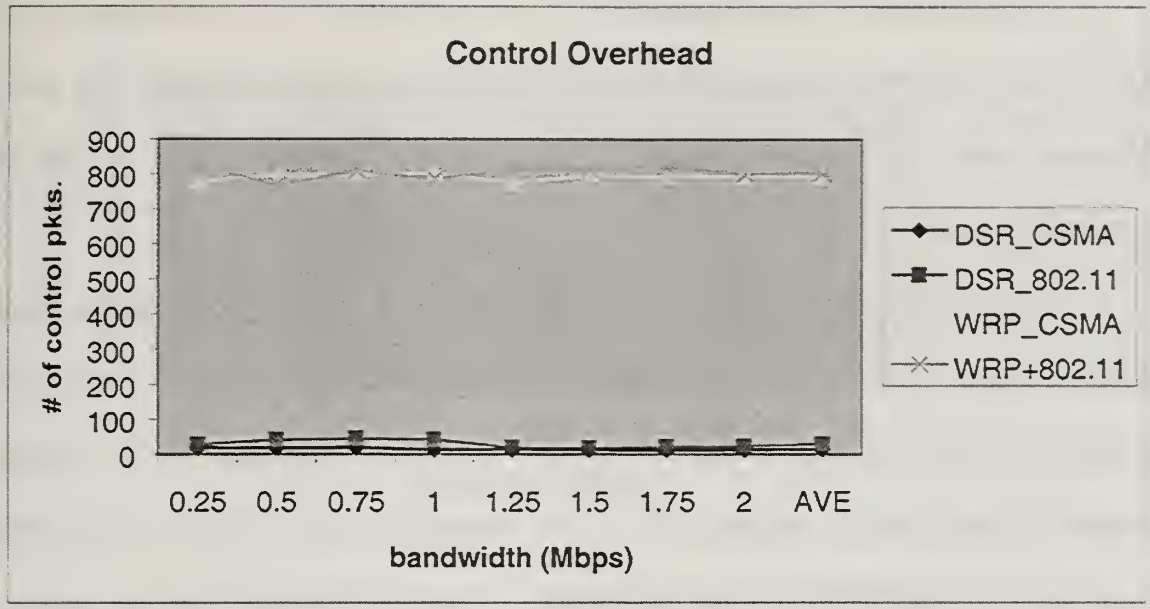


Figure 24. Control Overhead Comparison.

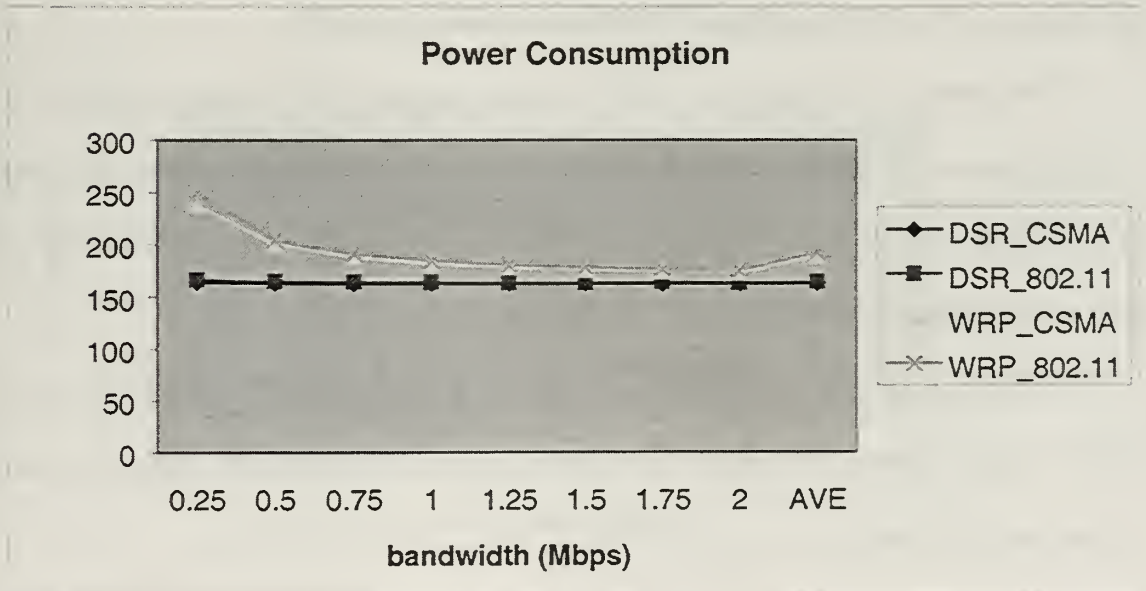


Figure 25. Power Consumption Comparison.

2. CSMA versus 802.11 MAC Layer Protocols

After deciding on the performance of the routing protocol, we concentrated on the MAC layer protocols. The CSMA and 802.11 protocols were chosen for our tests. Moreover, the communication load of the system was varied in order to see its consistency under high level loads.

Figure 26 shows the performance of the DSR and the CSMA combination under different loads. Each line represents a different communication load value. One of the interesting results obtained is that the number of packets generated by the routing protocol is not directly proportional to the increasing load. That is, when the communication load was doubled, the number of packets generated did not double. Figure 27 shows the number of packets generated by the DSR and the 802.11 combination. The values in both figures indicate that the CSMA protocol enhances the performance of the DSR better than the 802.11 protocol.

The control overhead of the DSR routing protocol with different MAC layer protocols does not differ substantially. Figures 28 and 29 show these results. Although the difference between the CSMA and 802.11 is not substantial, the CSMA follows a more stable trend than the 802.11.

The power consumption of both the CSMA and the 802.11 protocols under the DSR are almost identical and stable for different communication loads. Figures 31 and 32 represent these results.

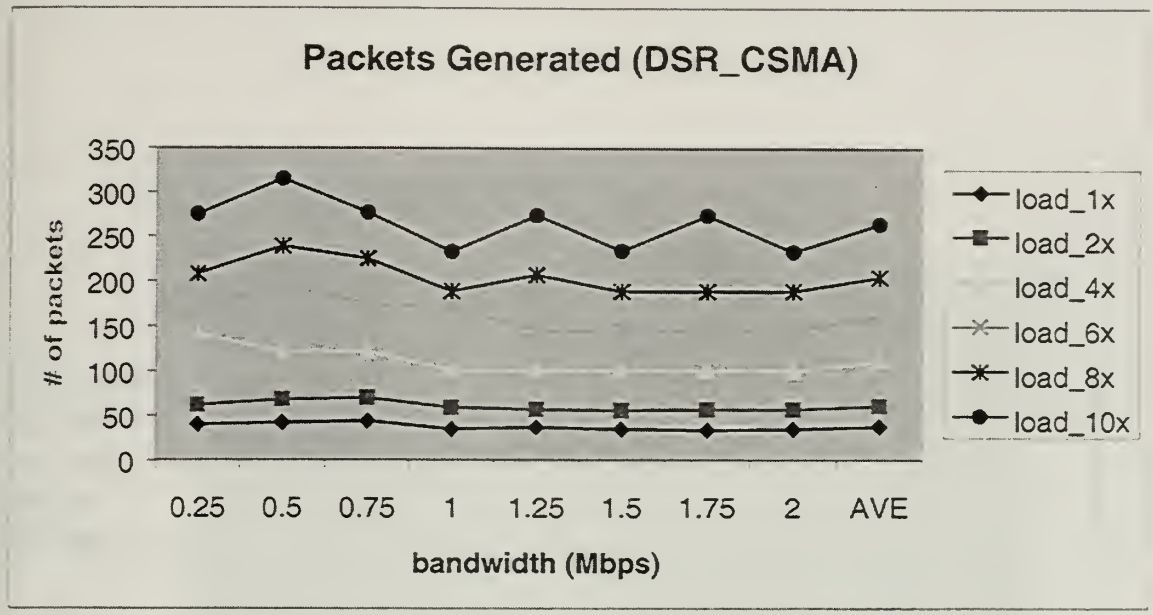


Figure 26. DSR/CSMA Packets Generated for Different Loads.

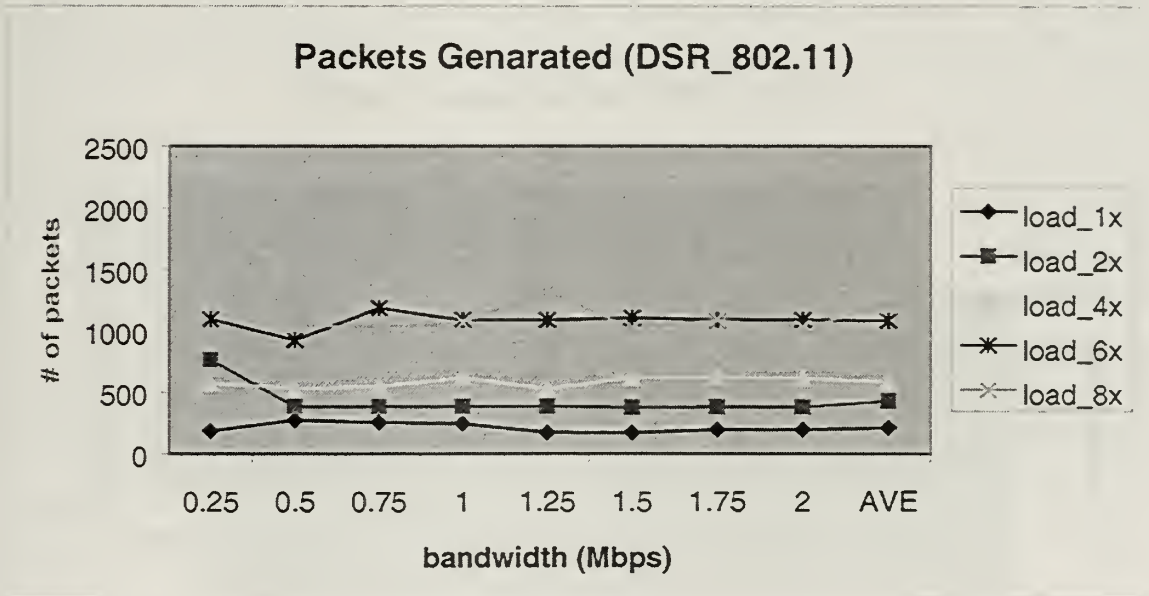


Figure 27. DSR/802.11 Packets Generated for Different Loads.

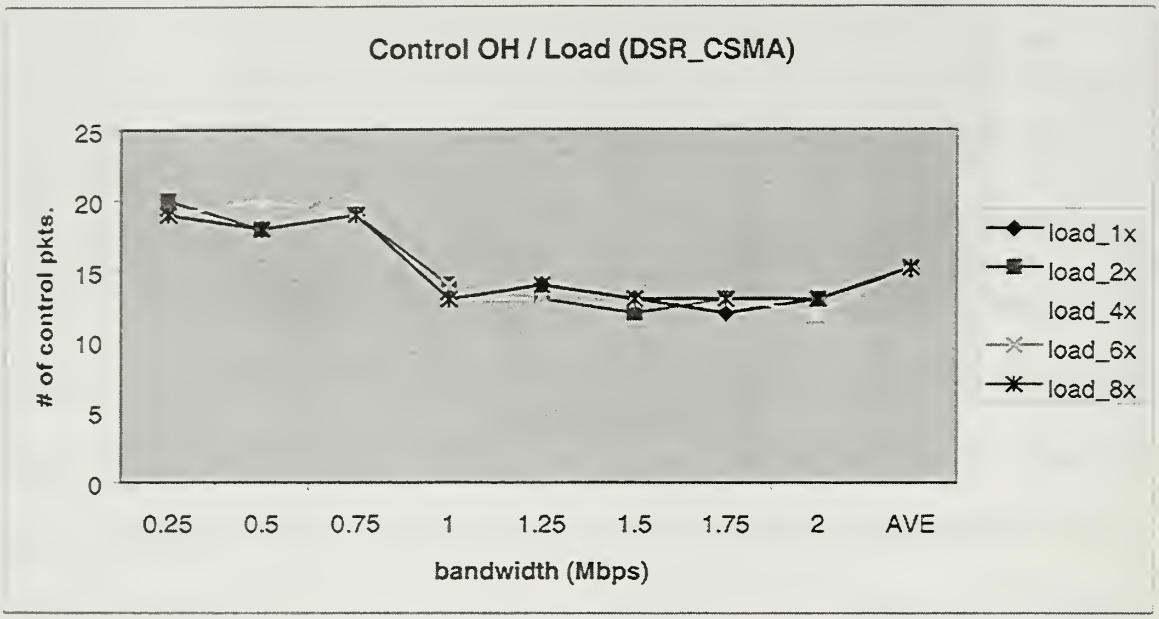


Figure 28. DSR/CSMA Control Packets for Different Loads.

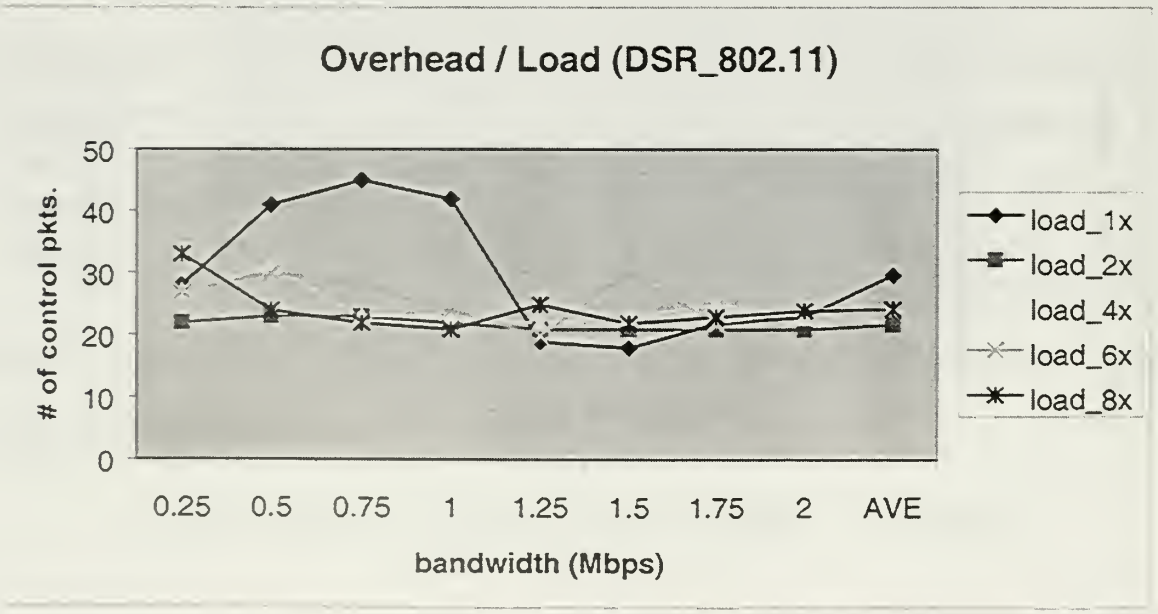


Figure 29. DSR/802.11 Routing Overhead for Different Loads.

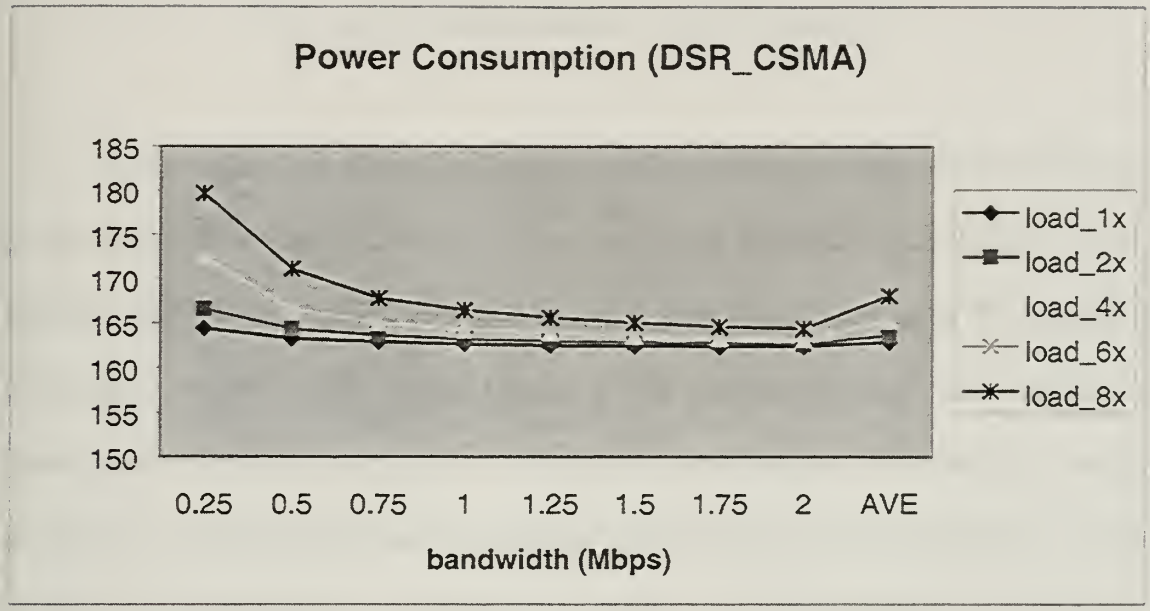


Figure 30. Power Consumed by DSR/CSMA for Different Loads.

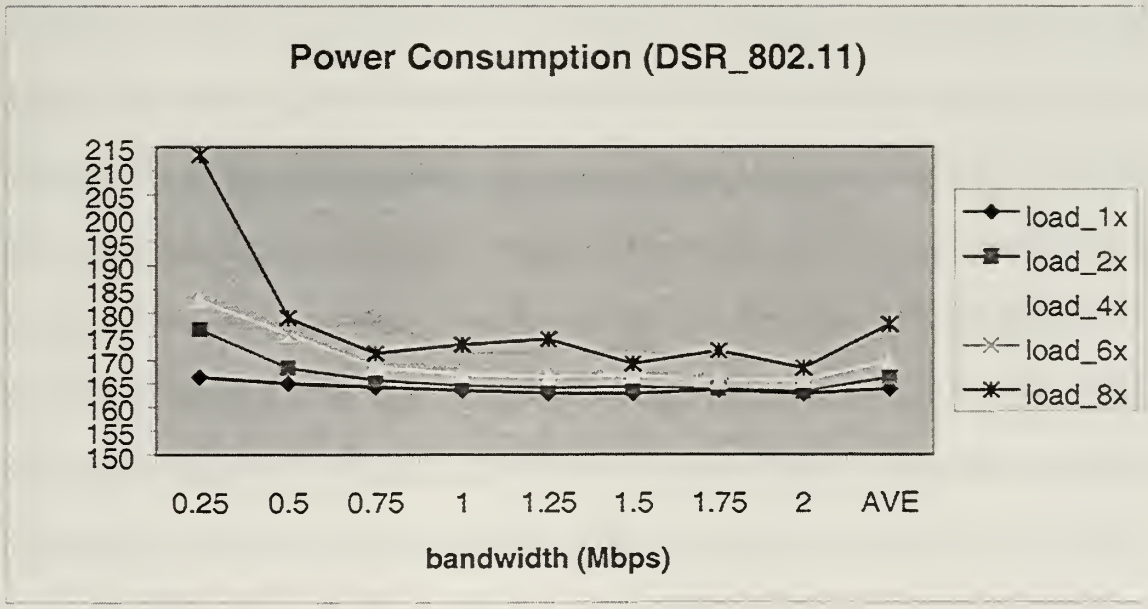


Figure 31. Power Consumed by DSR/802.11 for Different Loads.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. INFORMATION OPERATIONS

Today, many feel that the world is on the edge of one of the periodic changes in the fundamental conduct of war, which may be causing a Revolution in Military Affairs (RMA). The changes behind this RMA consist primarily of advances in information technology, which in turn enable gains in the precision, range and lethality of conventional weapons. As a part of this RMA, development of information warfare depends on technological changes, systems development and the adaptation of new operational approaches and organizational structures. This is necessary in order to take advantage of this new capability. Modern information warfare is heavily based on the use of information technology. With such use comes dependency, which in turn creates vulnerabilities, which may be attacked and, which must be defended. The process of attacking an enemy's information and information technology vulnerabilities for any political or military purpose and the protection of one's own information and information technology is the essence of information warfare. There is a continuing effort to describe the content and scope of information warfare. Martin Libicki points out this fact by an analogy of the attempts of three blind men to discover the nature of an elephant.[88] Dr. Shen Weiguang –one of the first Chinese authors to write about the topic of IW- defined information warfare as "command and control warfare or decision control warfare, using information as the main weapon to attack enemy's cognitive and information systems,

[88] Libicki, M., *What is Information Warfare?,* National Defense University Press, Washington, D.C., 1995, 3.

and to influence, check or change the decision of enemy policymakers and their consequent hostile actions."[89]

IW is not a new concept. "It is not a third-wave phenomenon or a byproduct of the computer revolution. Take the cuckoo bird. This information warrior has duped as many as 180 different species into foster parenthood by laying its eggs in the nets of other birds. To avoid detection, it adjusts the egg's morphology to that of the host. Through its behavior, it destroys the integrity of the information environment of its host. Visual appearance of an egg is no longer a reliable source of information."[90] Examples of information warfare can be found throughout human history. In 1200 BC, the Greeks infiltrated Troy by compromising the integrity of the visual systems used by the Trojans. In the twelfth and thirteenth centuries, the Mongols succeeded in overthrowing the great armies of China, Islam, and Christendom by learning the exact locations of their enemies while keeping their own location secret. In the campaign against the Polish-Prussian coalition forces at the battle of Liegnitz, they defeated an enemy four times their size. They maintained superior knowledge of the coalition order of battle as they drew the enemy into chasing after small detachments, which brought them into the Mongol main force.[91] Although information warfare is not new, new information media and technologies have transformed it. Also, there are new attempts to redefine the whole issue with a new term: "Information operations (IO)"

---

89 http://call.army.mil/call/fmso/fmsopubs/isues/chinarma.htm.

90 Denning, D.E., *Information Warfare and Security*, Addison-Wesley, 1999, Berkeley, Ca, 13 The author refers to Loyal Rue, by *The Grace of Guile: The Role of Deception in Natural History and Human Affairs*, Oxford University Press, New York, 1994, 120-122.

91 Arquilla, J., Ronfeldt, D., *In Athena's Camp*, RAND, Santa Monica, CA, 1997, 34.

The concepts of IW and IO represent new strategies for using emerging technologies. Are they different? Yes, there is a difference in scope. "The recent adaptation of the term 'information operations' signals a recognition of the fact that many people believe that the term 'information warfare' is too restrictive. 'Warfare connotes open, armed conflict and leaves out operations conducted during peacetime and conflicts short of war. It also excludes operations related to national security but conducted in cooperation with other government agencies."[92] As a result, IO points out that information can be exploited for strategic advantage during peacetime, conflicts or wars by different actors. This also implies that information warfare is a subset of IO, the IO in the battlefield.

The concept of information operations is wide open. "Its impact is affecting the definition of operational success, the interaction of different and assignment of levels of expertise up the chain of command."[93] Over the past two decades, information systems have been on the leading edge of change in military operations. Traditionally, the objective of warfare was to win over an enemy. Success was defined by the achievement of strategic or geopolitical goals. The cost of waging warfare was determined by weighing it against the gains brought by success. Today's environment has changed that equation. Military operations are planned and executed with an eye toward reducing casualties to the point of elimination. This growing zero tolerance towards lethality, as opposed to winning a war regardless of its cost, relies mainly on information technologies.

---

[92] Mitchell, M.E., Strategic Leverage: Information Operations and Special Operations, Thesis, NPS, 24 Monterey, CA, March 1999.

[93] Wood, C. N., Information Operations Change the Map of Conflict, SIGNAL, March 2000, 14.

There is some uncertainty about the technical requirements for communications during future confrontations with unsophisticated adversaries. "Recent U.S. actions in Haiti and Somalia are examples of these types of operations, which may become more common as the United States plays an expanding role in peacekeeping and peacemaking missions. These countries tend to have little modern communications infrastructure, although this situation is changing as worldwide markets evolve for advanced technology."[94]

It is mostly probable that in the future, there will be a dynamic engagement environment with numerous non-state actors, i.e. transnational terrorist and crime organizations. The SOF is already the force of choice for combating some of these threats and this tendency will continue with an increasing demand. On the other hand, the SOF must understand the realities of limited resources and increasing demand. A potential solution to this dilemma might be found in the RMA. New approaches to warfare like Information Operations (IO) are beginning to emerge from the RMA.

IO is one of the missions of the SOF included under the special operations. These "missions disrupt or destroy the electronic or physical communications and information systems of hostile nations to preclude their use for command and control during a conflict."[95] One of the IO missions is to evaluate potential hostile nations and how they would use their information systems against allied forces. In short, IO "comprises the actions taken to defend the integrity of one's own information and to achieve information superiority in a given situation by affecting an adversary's understanding of events. IO

---

[94] http://www.nap.edu/readingroom/books/evoluation/3.html. *The Evalution of Untethered Communications.*

[95] C4I Handbook, 1-6.

applies to peaceful military/government endeavors as well as to more traditional military conflict and war activities."[96]

IO is vital due to its potential for conceptual, strategic, and integrative use of IW concepts and innovative application of emerging technologies. For SOF, IO presents an opportunity to balance the resource limitations and demand by enhancing the current forces.

Dependency and Risk

Using technological innovations is not risk-free. Becoming high tech dependent brings its own risks. Arquilla points out that "the pursuit of radical advances might actually lead to the erosion of the current position of relative advantage."[97] A potential adversary might attack these dependencies with asymmetric methods and can damage temporarily or permanently the communication infrastructure. With its tremendous benefits, a global mobile wireless communication infrastructure will raise new security problems. While setting a totally secure communications backbone is demanding the use of such systems will depend on the risk assessments done prior to the mission or conflict. Some of the potential attacks are related to the nature of the wireless communications such as interception, detection and jamming. Some attacks are general for all communications such as traffic analysis, authentication, and use of public services in a secure way. A new maturing trend, which has been studied in the last five decades, is becoming a real danger to electronic devices: use of electromagnetic pulse bombs. These possible security issues will be studied in the following sections.

---

[96] Ibid., 4-30.

[97] Arquilla, J., *The "Velvet" Revolution in Military Affairs*, World Policy Journal, Winter 1997/98 Vol.XIV, No. 4,34.

A. EMP

The prosecution of a successful IW campaign against an industrial or postindustrial opponent will require a suitable set of tools. As demonstrated in the Desert Storm air campaign, air power has proven to be a most effective means of inhibiting the functions of an opponent's vital information processing infrastructure. Air power allows concurrent or parallel engagement of a large number of targets over geographically significant areas.

While Desert Storm demonstrated that the application of air power was the most practical means of destroying an opponent's information processing and transmission nodes, the need to physically destroy these with guided munitions absorbed a substantial proportion of available air assets in the early phase of the air campaign. Indeed, the aircraft capable of delivering laser-guided bombs were largely occupied with this very target set during the first nights of the air battle.

The efficient execution of an IW campaign against a modern industrial or postindustrial opponent will require the use of specialized tools designed to destroy information systems. Electromagnetic bombs built for this purpose can provide, where delivery is by suitable means, a very effective tool for this purpose.

Use of electromagnetic pulse (EMP) bombs or high-energy radio frequency (HERF) guns is not a new threat to communications. In general, these are referred to by different names in academic groups. An electromagnetic pulse or EMP device is a generic term applied to any device, nuclear or conventional, which is capable of generating a very intense, but short, electromagnetic field. For weapons applications, this field must be sufficiently intense to produce electromagnetic power densities, which are

lethal to electronic and electrical equipment. Electromagnetic weapons are electromagnetic devices specifically designed as weapons. The term 'electromagnetic bomb' or 'E-bomb' will be used to describe both microwave and low frequency non-nuclear bombs. It might be considered science fiction in the not so distant past, but not so today. Parallel to this fact, the SOF are also vulnerable to attacks from these kinds of weapons. Their high-tech equipment and communications devices have certain weaknesses against high electromagnetic waves. On the other hand, use of these weapons by the SOF in IO against potential adversaries will add a new dimension, which may increase the efficiency and military utility of the SOF greatly. SOF teams might be used as the means of delivery for EMP weapons against hidden or mobile communications nodes of the enemy.

From unclassified sources, it is well known that "Russia, the Ukraine, the United Kingdom, China, Australia and France are well ahead in this field, while Germany, Sweden, South Korea, Taiwan and Israel are emerging."[98] Without going into any classified matters one may reasonably infer that some nations or even organizations have similar interests and some certainly have the financial resources to develop or produce EMP weapons. "Beijing is developing high-power microwave sources that could form the basis for radio frequency weapons applications.... It is still unclear whether this weapon to negate electronics at a greater range than does can produce sufficient microwave energy blast damage caused by the same size high-explosive warhead."[99]

---

[98] Schweitzer, R. L., Statement before Joint Economic Committee U.S. Congress, June 17, 1997 http://www.house.gov/ jec/hearings/espionag/schweitz.htm.

[99] Robinson, C.A., "China's Military Potency Relies On Arms Information Content", SIGNAL, NOV 1999, 22.

Users of the new weapons can be criminals, individuals or organized gangs of narcotics or domestic terrorists. According to published reports, British military officials suspect that these devices are already in the arsenal of the Irish Republican Army. The tendency toward "irregularization" and asymmetric capabilities of adversaries make EMP weapons a valuable tool.

A French scientist, Jean-Claude Amblard, has the following vision for these weapons: "Will we one day see a high power microwave (HPM) radiation that can take out the radar and electronic system of fighter planes or that can blind and deafen observation satellites flying over enemy territory? In other words, are we on the brink of a new age where new style weapons can remotely destroy the vital functions of electronic systems? The answer is yes."[100] Recent engineering advances in very high power frequency sources give increasing plausibility to the idea of microwave pulse weapons. High power microwave weapons direct electromagnetic power that can drastically disrupt or if not destroy equipment electronics, by coupling with the antennas, wire links or the structure of the weapon systems.

Today, postmodern, highly "informatized" nations' vulnerability arises from the fact that they are the most advanced nation electronically and the greatest user of the electricity in the world. As General (Retired) Robert L. Schweitzer reminds us of this fact in his speech before the U.S. Congress: "All of our military doctrine assumes extensive use of sophisticated electronics and communication systems to ensure information dominance and overwhelming battlefield success.... Because our battlefield success and the well being of our civilian economy are so dependent on the effectiveness

[100] http://www.adit.fr/produits/TF/Anciens?TF37a.html.

of our microelectronic-based systems, we should fully understand any technology that might be used to defeat our systems. This is particularly true of the newly emerging threat of radio frequency weapons. And even more importantly, we must develop countermeasures before such weapons are used against us."[101] This statement shows us the overall threat caused by EMP weapons against both civilian and military communications and electronics. This might mean that what Sun Tzu wrote about 2000 years ago: to conquer an enemy without fighting, becoming possible to do. Why are these new weapons becoming so popular? They are suggesting certain advantages to the user:

- "Low cost per engagement
- All weather
- Instantaneous engagement times
- Simplified pointing and tracking
- Possible to engage multiple targets
- Deep magazines – simplified logistics (can "fire" or pulse as long as there is power in the generator)
- Non-lethal to humans when properly adjusted
- Well suited to covert operations because of lack of signature; deniability
- Not able to detect attacks; silent when used without explosive devices"[102]

While the devices are problematic for planners, experts say countermeasures

---

[101] Schweitzer, R. L., Statement before Joint Economic Committee U.S. Congress, June 17, 1997 http://www.house.gov/ jec/hearings/espionag/schweitz.htm.

[102] Schweitzer, http://www.house.gov/ jec/hearings/espionag/schweitz.htm.

exist, including specialized building construction materials and unique voltage protectors. In addition, fiber optics, which are immune to most pulses, could replace cabling in buildings. Before going into countermeasures, though, it would be wise to detail the effects of EMP.

1. The EMP Effect

The Electro Magnetic Pulse (EMP) effect was first observed during the early testing of high-altitude airburst nuclear weapons.[103] The effect is characterized by the production of a very short (hundreds of nanoseconds) but intense electromagnetic pulse, which propagates away from its source with ever diminishing intensity, governed by the theory of electromagnetism. The electromagnetic pulse is in effect an electromagnetic shock wave.

This pulse of energy produces a powerful electromagnetic field, particularly within the vicinity of the weapon burst. The field can be sufficiently strong to produce short-lived transient voltages of thousands of Volts (i.e. kilovolts) on exposed electrical conductors, such as wires or conductive tracks on printed circuit boards.

It is this specialty of the EMP effect, which is important for the military as it can result in a large amount of damage to a wide range of electrical and electronic equipment, particularly computers and radio or radar receivers. According to the electromagnetic hardness of the electronics and the intensity of the field produced by the weapon, the equipment can be totally damaged or in effect electrically destroyed. The damage caused is not unlike that experienced through exposure to close proximity lightning strikes, and may require complete replacement of the equipment, or at least substantial portions.

---

[103] Glasstone, S., Dolan, P. J., (Editors), The Effects of Nuclear Weapons, US AEC, April, 1962, Third

Commercial computer equipment is particularly vulnerable to EMP effects, as it is largely built up of high-density Metal Oxide Semiconductor (MOS) devices, which are very sensitive to exposure to high voltage transients. What is significant about MOS devices is that very little energy is required to permanently damage or destroy them. Even if the pulse is not powerful enough to produce thermal damage, the power supply in the equipment will readily supply enough energy to complete the destructive process. Damaged devices may still function, but their reliability will be seriously impaired. Shielding electronics by equipment chassis provides only limited protection, as any cables running in and out of the equipment will behave very much like antenna, in effect guiding the high voltage transients into the equipment.

Computers used in data processing systems, communications systems, displays, industrial control applications, including road and rail signaling, and those embedded in military equipment, such as signal processors, electronic flight controls and digital engine control systems, are all potentially vulnerable to the EMP effect.

Other electronic devices and electrical equipment may also be destroyed by the EMP effect. Telecommunications equipment can be highly vulnerable, due to the presence of lengthy copper cables between devices. Receivers of all varieties are particularly sensitive to EMP, as the highly sensitive miniature high frequency transistors and diodes in such equipment are easily destroyed by exposure to high voltage electrical transients. Therefore, radar and electronic warfare equipment, satellite, microwave, communications equipment and television equipment are all potentially vulnerable to the EMP effect.

Edition by DoD and DoE, 1977,514.

It is significant that modern military platforms are densely packed with electronic equipment, and unless these platforms are well hardened, an EMP device can substantially reduce their function or render them unusable.

2. Coupling Modes

In assessing how power is coupled into targets, two principal coupling modes are recognized in the literature:

Front Door Coupling occurs typically when power from an electromagnetic weapon is coupled into an antenna associated with radar or communications equipment. The antenna subsystem is designed to couple power in and out of the equipment, and thus provides an efficient path for the power flow from the electromagnetic weapon to enter the equipment and cause damage.

Back Door Coupling occurs when the electromagnetic field from a weapon produces large transient currents or electrical standing waves on fixed electrical wiring and cables interconnecting equipment, or the telephone network.[104] Equipment connected to exposed cables or wiring will experience either high voltage, which can damage power supplies, and communications interfaces if these are not hardened. Moreover, if the transient penetrates the equipment, damage can be done to other devices inside.

A low frequency weapon will couple well into a typical wiring infrastructure, as most telephone lines, networking cables and power lines follow streets, building risers and corridors.

---

[104] Taylor C. D., Harrison C. W., *On the Coupling of Microwave Radiation to Wire Structures*, IEEE Transactions on Electromagnetic Compatibility, August 1992, Vol. 34, No. 3, 183.

Communications interfaces and power supplies must typically meet electrical safety requirements imposed by regulators. Isolation transformers usually protect such interfaces with ratings from hundreds of Volts to about 2 to 3 kV.

HPM weapons operating in the centimetric and millimetric bands, however, offer an additional coupling mechanism to Back Door Coupling. This is the ability to directly couple into equipment through ventilation holes, gaps between panels and poorly shielded interfaces. Under these conditions, any hole in the equipment behaves much like a slot in a microwave cavity, allowing microwave radiation to directly excite or enter the cavity. Components situated within the anti-nodes within the standing wave pattern will be exposed to potentially high electromagnetic fields.

Since microwave weapons can couple more readily than low frequency weapons, and can in many instances bypass protection devices designed to stop low frequency coupling, microwave weapons have the potential to be significantly more lethal than low frequency weapons.

The diversity of likely target types and the unknown geometrical layout and electrical characteristics of the wiring and cabling infrastructure surrounding a target makes the exact prediction of lethality impossible.

A general approach for dealing with wiring and cabling related back door coupling is to determine a known lethal voltage level, and then use this to find the required field strength to generate this voltage. Once the field strength is known, the lethal radius for a given weapon configuration can be calculated.

A trivial example is that of a 10 GW 5 GHz HPM device illuminating a footprint of 400 to 500 meters diameter, from a distance of several hundred meters. This will

result in a field strength of several kilovolts per meter within the device footprint which in turn is capable of producing voltages of hundreds of volts to kilovolts on exposed wires or cables. This suggests lethal radii on the order of hundreds of meters, subject to weapon performance and target set electrical hardness.

3. Defense Against Electromagnetic Bombs

The most effective defense against electromagnetic bombs is to prevent their delivery by destroying the launch platform or delivery vehicle, as is the case with nuclear weapons. This however may not always be possible, and therefore systems, which can be expected to suffer exposure to the electromagnetic weapons effects, must be electromagnetically hardened.

The most effective method is to enclose the equipment in an electrically conductive enclosure, termed a Faraday cage, which prevents the electromagnetic field from gaining access to the protected equipment. However, most such equipment must communicate with and be fed with power from the outside world, and this can provide entry points via which electrical transients may enter the enclosure and effect damage. While optical fibers address this requirement for transferring data in and out, electrical power feeds remain an ongoing vulnerability.

Where an electrically conductive channel must enter the enclosure, electromagnetic arresting devices must be fitted. A range of devices exist. However, care must be taken in determining their parameters to ensure that they can deal with the rise time and strength of electrical transients produced by electromagnetic devices.

Reports indicate that hardening measures adjusted to the behavior of nuclear EMP bombs do not perform well when dealing with some conventional microwave

electromagnetic device designs.

It is significant that hardening of systems must be carried out at a system level, as electromagnetic damage to any single element of a complex system could inhibit the function of the whole system. Hardening new build equipment and systems will add a substantial cost burden. Older equipment and systems may be impossible to harden properly and may require complete replacement. In simple terms, hardening by design is significantly easier than attempting to harden existing equipment.

An interesting aspect of electrical damage to targets is the possibility of wounding semiconductor devices thereby causing equipment to suffer repetitive intermittent faults rather than complete failures. Such faults would tie down considerable maintenance resources while also diminishing the confidence of the operators in the equipment's reliability. Intermittent faults may not be possible to repair economically, thereby causing equipment in this state to be removed from service permanently, with considerable loss in maintenance hours during damage diagnosis. This factor must also be considered when assessing the hardness of equipment against electromagnetic attack, as partial or incomplete hardening may in this fashion cause more difficulties than it would solve. In fact, shielding which is incomplete may resonate when excited by radiation and thus contribute to damage inflicted upon the equipment contained within it.

Other than hardening against attack, facilities, which are concealed, should not radiate readily detectable emissions. "Where radio frequency communications must be used, low probability of interception (i.e. spread spectrum) techniques should be employed exclusively to preclude the use of site emissions for electromagnetic targeting

purposes."[105]

Communications networks for voice, data and services should employ topologies with sufficient redundancy and fail over mechanisms to allow operation with multiple nodes and links inoperative. As a result, hardening in addition to redundancy of key system elements represent a better choice for defending communication networks. This will deny a user of electromagnetic bombs the option of disabling large portions if not the whole of the network by taking down one or more key nodes or links with a single or small number of attacks.

4. Limitations of Electromagnetic Bombs

Weapon implementation and means of delivery determine the limitations of electromagnetic weapons. Weapon implementation will determine the electromagnetic field strength achievable at a given radius, and its spectral distribution. Means of delivery will affect the accuracy with which the weapon can be positioned in relation to the intended target.

In the context of targeting military equipment, it must be noted that thermionic technology (i.e. vacuum tube equipment) is substantially more resilient to the electromagnetic weapons effects than solid state (i.e. transistor) technology. Therefore, a weapon optimized to destroy solid state computers and receivers may cause little or no damage to a thermionic technology device, for instance early 1960s Soviet military equipment. Therefore, a hard electrical kill may not be achieved against such targets unless a suitable weapon is used.

---

[105] Dixon R. C., *Spread Spectrum Systems*, John Wiley and Sons, New York, 1984, 264.

This underscores another limitation of electromagnetic weapons, which is the difficulty in *kill assessment.* Radiating targets such as radar or communications equipment may continue to radiate after an attack even though their receivers and data processing systems have been damaged or destroyed. This means that equipment, which has been successfully attacked, may still appear to operate. Conversely an opponent may shut down an emitter if attack is imminent and the absence of emissions means that the success or failure of the attack may not be immediately apparent.

Assessing whether an attack on a non-radiating emitter has been successful is more problematic. A good case can be made for developing tools specifically for the purpose of analyzing unintended emissions, not only for targeting purposes, but also for kill assessment.

An important factor in assessing the lethal coverage of an electromagnetic weapon is atmospheric propagation. While the relationship between electromagnetic field strength and distance from the weapon is one of an inverse square law in free space, the decrease in lethal effect with increasing distance within the atmosphere will be greater due to quantum physical absorption effects. This is particularly so at higher frequencies, and significant absorption peaks due to water vapor and oxygen existing at frequencies above 20 GHz. These will therefore contain the effect of HPM weapons to shorter radii than are ideally achievable in the K and L frequency bands.

Means of delivery will limit the lethality of an electromagnetic bomb by introducing limits to the weapon's size and the accuracy of its delivery. If the delivery error is on the order of the weapon's lethal radius for a given detonation altitude, lethality will significantly disappear. This is particularly important when assessing the lethality of

unguided electromagnetic bombs, as delivery errors will be more substantial than those experienced with guided weapons such as GPS guided bombs.

Therefore, accuracy of delivery and achievable lethal radius must be considered against the allowable collateral damage for the chosen target. Where collateral electrical damage is a consideration, accuracy of delivery and lethal radius are key parameters. An inaccurately delivered weapon of large lethal radius may be unusable against a target if the likely collateral electrical damage beyond acceptable limits. In this sense, SOF teams may become a critical means of delivery with all risk involved in the mission.

5. Doctrinal Use of Conventional Electromagnetic Bombs

A fundamental principle of IW is that complex organizational systems such as governments, industries and military forces cannot function without the flow of information through their structures. Information flows within these structures in several directions, under typical conditions of function. A trivial model for this function would see commands and directives flowing outward from a central decision-making element, with information about the state of the system flowing in the opposite direction. Real systems are substantially more complex.

This is of military significance because stopping this flow of information will severely debilitate the function of any such system. Stopping the outward flow of information produces paralysis, as commands cannot reach the elements, which are to execute them. Stopping the internal flow of information isolates the decision-making element from reality, and thus severely inhibits its capacity to make rational decisions, which are sensitive to current of information at hand.

The recent evolution of strategic (air) warfare indicates a growing trend toward targeting strategies, which exploit this most fundamental vulnerability of any large and organized system. The Desert Storm air war of 1991 is a good instance. "Indeed, the model used for modern strategic air attack places leadership and its supporting communications in the position of highest targeting priority."[106] Modern Electronic Combat concentrates upon the disruption and destruction of communications and information gathering sensors used to support military operations. Again, the Desert Storm air war provides a good illustration of the application of this method.

A strategy, which stresses attack upon the information processing and communications elements of the systems, which it is targeting, offers a very high payoff, as it will introduce an increasing level of paralysis and disorientation within its target.

6. Strategic Air Attack Operations Using Electromagnetic Bombs

Electromagnetic bombs are a powerful tool in the implementation of such a strategy. The modern approach to strategic air warfare reflects in many respects aspects of the IW model, in that much effort is expended in disabling an opponent's fundamental information processing infrastructure.

Modern strategic air attack theory is based upon Warden's Five Rings model[107], which identifies five centers of gravity in a nation's war fighting capability. In descending order of importance, these are:

- leadership and supporting C3 system

---

[106] Warden J. A. III, Col USAF, *Air Theory for the Twenty-first Century, Chapter 4 in Schneider B.R, Grinter L. E., Battlefield of the Future*, 21st Century Warfare Issues, Air University Press, Maxwell AFB, September 1995, 23.

[107] Ibid., 28.

- essential economic infrastructure
- transportation network
- population
- fielded military forces

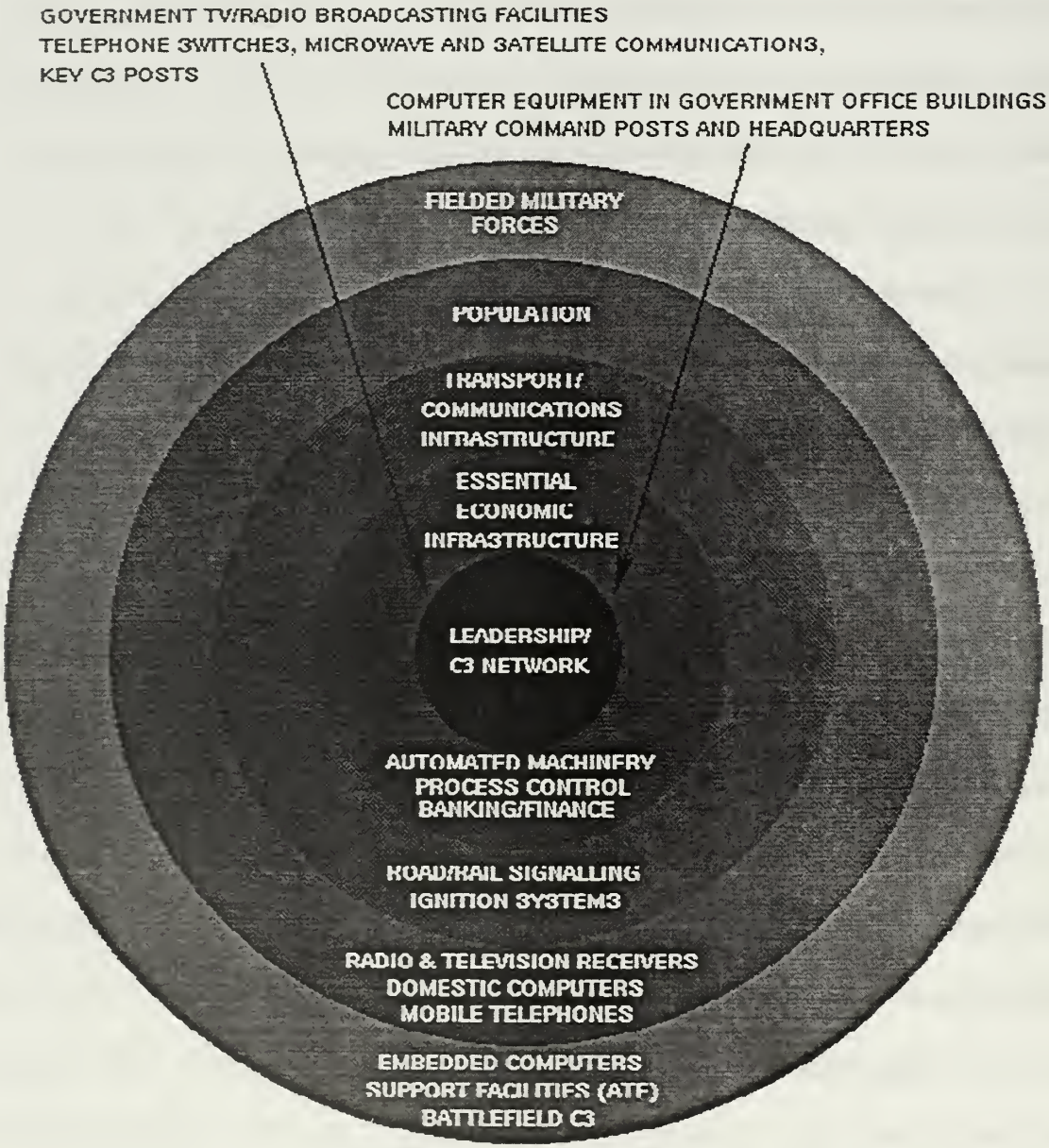


Figure 32. Warden's "Five Rings" Strategic Air Attack Model in the Context of Electromagnetically Vulnerable Target Sets.[108]

[108] Carlo Kopp, The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction,

Electromagnetic weapons may be productively used against all elements in this model, and provide a particularly high payoff when applied against a highly industrialized and geographically concentrated opponent. Of particular importance in the context of strategic air attack, is that while electromagnetic weapons are lethal to electronics, they have little if any effect on humans. This is a characteristic which is not shared with established conventional and nuclear weapons.

This selectivity in lethal effect makes electromagnetic weapons much more readily applicable to a strategic air attack campaign, and reduces the political pressure which is experienced by the leadership of any democracy which must commit itself to warfare. An opponent may be rendered militarily, politically and economically ineffective with little if any loss in human life.

The innermost ring in the Warden model essentially comprises government bureaucracies and civilian and military C3 systems. In any modern nation these are heavily dependent upon the use of computer equipment and communications equipment. What is of key importance at this time is an ongoing change in the structure of computing facilities used in such applications, as these are becoming increasingly decentralized. A modern office environment relies upon a large number of small computers, networked to interchange information, in which respect it differs from the traditional model of using a small number of powerful central machines.

This decentralization and networking of information technology systems produces a major vulnerability to electromagnetic attack. Whereas a small number of larger computers could be defended against electromagnetic attack by the use of

---

www.hut.fi/zam/ew/mirror/apjemp.html.

electromagnetic hardened computer rooms, a large distributed network cannot. Moreover, unless optical fiber networking is used, the networking cables are themselves a medium via which electromagnetic effects can be efficiently propagated throughout the network to destroy machines. While the use of *distributed* computer networks reduces vulnerability to attack by conventional munitions, it increases vulnerability to attack by electromagnetic weapons. On the other hand, this vulnerability might be limited. In the case of a distributed network, the attacker would not effect the entire network, unless a vital hub was attacked. Then, the important issue in attacking distributed computer networks is evaluating and hitting the right target. In this way, the damage inflicted will be high with correct targeting. Certainly, the countermeasure for these types of attacks will be providing enough fault tolerance and redundancy in the distributed network.

The targeting of government buildings with electromagnetic weapons will result in a substantial reduction in a government's ability to handle and process information. The damage inflicted upon information records may be permanent should inappropriate backup strategies have been used to protect stored data. It is reasonable to expect most data stored on machines which are affected will perish with the host machine, or become extremely difficult to recover from damaged storage devices.

The cost of hardening existing computer networks is very expensive, as is the cost of replacement with hardened equipment. While the use of hardened equipment for critical tasks would provide some measure of protection, the required discipline in the handling of information required to implement such a scheme makes its utility outside of military organizations questionable. Therefore, the use of electromagnetic weapons against government facilities offers an exceptionally high payoff.

Other targets, which fall into the innermost ring, may also be efficiently attacked. Satellite links, and importantly control facilities, are vital means of communication as well as the primary interface to military and commercial reconnaissance satellites. Television and radio broadcasting stations, one of the most powerful tools of any government, are also vulnerable to electromagnetic attack due the very high concentration of electronic equipment at such sites. Telephone exchanges, particularly later generation digital switching systems, are also highly vulnerable to appropriate electromagnetic attack.

In summary, the use of electromagnetic weapons against leadership and C3 targets may provide highly profitable, in that a modest number of weapons appropriately used might include a state of strategic paralysis, without the substantial costs incurred by the use of conventional munitions to achieve the same effect.

Essential economic infrastructure is also vulnerable to electromagnetic attack. The finance industry and stock markets are almost wholly dependent upon computers and their supporting communications. Manufacturing, chemical, petroleum product and metallurgical industries rely heavily upon automation, which is almost universally implemented with computers. Furthermore, most sensors and telemetry devices used are electrical or electronic.

Attacking such economic targets with electromagnetic weapons will halt operations for the time required to either repair the destroyed equipment, or to reconfigure for manual operation. Some production processes, however, require automated operation, either because hazardous conditions prevent human intervention, or a human operator in real time cannot carry out the complexity of the control process

required. A good instance is larger chemical, petrochemical and oil/gas production facilities. Destroying automated control facilities will therefore result in substantial loss of production, causing shortages of these vital materials.

Manufacturing industries, which rely heavily upon robotic and semiautomatic machinery, such as the electronics, computer and electrical, precision machine and aerospace industries, are all key assets in supporting military capability. They are all highly vulnerable to electromagnetic attack. While material-processing industries may in some instances be capable of functioning with manual process control, the manufacturing industries are almost wholly dependent upon their automated machines to achieve any useful production output.

Historical experience during WWII against Germans suggests that manufacturing industries are highly resilient to air attack as production machinery is inherently mechanically robust and thus a very high blast overpressure is required to destroy it. The increasing number of electronic and computer controlled machinery has produced a major vulnerability, for which a historical precedent does not exist. Therefore, it will be necessary to reevaluate this orthodoxy in targeting strategy.

The finance industry and stock markets are a special case in this context, as the destruction of their electronic infrastructure can yield, unlike manufacturing industries, much faster economic dislocation. This can in turn produce large systemic effects across a whole economy, including elements, which are not vulnerable to direct electromagnetic attack. This may be of particular relevance when dealing with an opponent which does not have a large, and thus, vulnerable manufacturing economy. Nations which rely on agriculture, mining or trade for a large proportion of the their gross domestic product are

prime candidates for electromagnetic attack on their finance industry and stock markets. Since the latter are usually geographically concentrated and typically electromagnetically "soft" targets, they are highly vulnerable.

In summary, there may be a large payoff in striking at economic essentials with electromagnetic weapons, particularly in the opening phase of a strategic air attack campaign, as economic activity may be halted or reduced with modest expenditure of the attacker's resources. An important aspect is that centers of gravity within the target economy must be properly identified and prioritized for strikes to ensure that maximum effect is achieved as quickly as possible.

Transport infrastructure is the third ring in the Warden model, and also offers some useful opportunities for the application of electromagnetic weapons. Unlike the innermost rings, the concentration of electronic and computer equipment is typically much lower, and therefore considerable care must be taken in the selection of targets.

Railway and road signaling systems, where automated (mostly in the U.S. and Europe), are most vulnerable to electromagnetic attack at their control centers. This could be used to produce traffic congestion by preventing the proper scheduling of rail traffic, and disabling road traffic signaling, although the latter may not yield particularly useful results.

Significantly, most modern automobiles and trucks use electronic ignition systems, which are known to be vulnerable to electromagnetic weapons effects, although opportunities to find such concentrations to allow the profitable use of an electromagnetic bomb may be scarce.

The population of the target nation is the fourth ring in the Warden model, and its morale is the object of attack. The morale of the population will be affected significantly by the quality and quantity of the government propaganda it is subjected to, as well as being affected by living conditions.

Using electromagnetic weapons against urban areas provides the opportunity to prevent government propaganda from reaching the population via means of mass media, through the damaging or destruction of all television and radio receivers within the effective range of the weapon. On the other hand, it may be counterproductive, as it will prevent the target population from being subjected to friendly means of psychological warfare such as propaganda broadcasts.

The use of electromagnetic weapons against a target population is therefore an area which requires careful consideration in the context of the overall IW campaign strategy. If useful objectives can be achieved by isolating the population from government propaganda, then the population is a valid target for electromagnetic attack. Forces constrained by treaty obligations will have to reconcile this against the applicable regulations relating to denial of services to non-combatants.

The outermost and last ring in the Warden model are the fielded military forces. These are by all means a target vulnerable to electromagnetic attack, and C3 nodes. Fixed support bases as well as deployed forces should be attacked with electromagnetic devices. Fixed support bases which carry out depot level maintenance on military equipment offer a substantial payoff, as the concentration of computers in both automatic test equipment and administrative and logistic support functions offers a good return per expended weapon.

Any site where more complex military equipment is concentrated should be attacked with electromagnetic weapons to cause the equipment to become unserviceable and hence reduce the fighting capability, and where possible also mobility of the targeted force. As discussed earlier in the context of Electronic Combat, the ability of an electromagnetic weapon to achieve hard electrical kills against any non-hardened targets within its lethal footprint suggests that some target sites may only require electromagnetic attack to render them both undefended and non-operational. Whether to expend conventional munitions on targets in this state would depend on the immediate military situation.

In summary, the use of electromagnetic weapons in strategic air attack campaigns may offer a potentially high payoff, particularly when applied to leadership, C3 and vital economic targets, all of which may be deprived of much of their function for substantial periods of time. The massed application of electromagnetic weapons in the opening phase of the campaign would introduce paralysis within the government, which would be deprived of much of its information processing infrastructure as well as paralysis in most vital industries. This would greatly reduce the capability of the target nation to conduct military operations of any substantial intensity.

Since conventional electromagnetic weapons produce negligible collateral damage, in comparison with conventional explosive munitions, they allow the conduct of an effective and high tempo campaign without the loss of life which is typical of conventional campaigns. This will make the option of a strategic bombing campaign more attractive to a Western democracy, where mass media coverage of the results of conventional strategic strike operations will adversely affect domestic civilian morale.

The long-term effects of a sustained and concentrated strategic bombing campaign using a combination of conventional and electromagnetic weapons will be important. The cost of computer and communications infrastructure is substantial, and its massed destruction would be a major economic burden for any industrialized nation. In addition, it is likely that poor protection of stored data will add to further economic losses, as much data will be lost with the destroyed machines.

From the perspective of conducting an IW campaign, this method of attack achieves many of the central objectives sought. Importantly, the massed application of electromagnetic weapons would inflict attrition on an opponent's information processing infrastructure very rapidly, and this would arguably add a further psychological dimension to the potency of the attack.

7. Effects of EMP on SOF

Availability of EMP weapons introduces both usability and hardening difficulties for the SOF. Communications are vital to a special operator operating behind the far rear of the front lines. Also, its importance will increase as the time dedicated for the mission increases because the continuation of the mission might depend upon updated intelligence reports or follow-up orders from high command. Thus, any threat to the availability of communications channels will affect the overall mission. For this reason, all equipment used by these elite troops must be armed against EMP weapons whatever the added cost.

The use of EMP bombs delivered by the Air Force poses the prospect of air campaigns that do more disruption without the need for more destruction. Embedding smart bombs and EMP technology might be a viable and less risky way for direct action

missions and limit the use of SOF in these areas. SOF missions are for short duration. This fact also might encourage the enemy to use EMP weapons even in its own backyard.

On the other hand, currently available EMP weapons cannot distinguish friend from foe. Therefore, an EMP weapon used in the theater might affect the friendly forces in the field if they are in the effective range of the weapon. Since the SOF operates behind enemy lines, potential enemies will hesitate to use EMP weapons in its own backyard. However, if the SOF are operating among an insurgent group in a rural area, the enemy will be more willing to use EMP weapons. Even the enemy might use some simple techniques such as shutting down critical electronic devices prior to an EMP attack on their own territory. Then, one can assess the vulnerability of the SOF against EMP weapons if they do not have enough protection and redundancy for their critical communications.

In the light of those vulnerabilities, the SOF still make use of these weapon systems. While air force and guided munitions might be ideal during open war scenarios, in the case of operations other than war, the SOF will be a viable delivery means of the weapons systems.

8. Conclusions

Electromagnetic bombs are Weapons of Electrical Mass Disruption with applications across a broad spectrum of targets, spanning both the strategic and tactical. As such, their use offers a very high payoff in attacking the fundamental information processing and communication facilities of a target system. The massed application of these weapons will produce substantial paralysis in any target system, thus providing a decisive advantage in the conduct of Electronic Combat, Offensive Counter Air and

Strategic Air Attack.

Since E-bombs can cause hard electrical kills over larger areas than conventional explosive weapons of similar mass, they offer substantial economies in force size for a given level of inflicted damage, and are thus a potent force multiplier for appropriate target sets.

The non-lethal nature of electromagnetic weapons makes their use far less politically damaging than that of conventional munitions, and therefore broadens the range of military options available.

E-bombs can be an affordable force multiplier for military forces that are under post Cold War pressures to reduce force sizes, increasing both their combat potential and political utility in resolving disputes. Given the potentially high payoff derived from the use of these devices, it is incumbent upon such military forces to appreciate both the offensive and defensive implications of this technology. It is also responsible to governments and private industry to consider the implications of the proliferation of this technology, and take measures to safeguard their vital assets from possible future attack. Those who choose not to may become losers in any future wars.

B. TRAFFIC ANALYSIS

On the first night of the bombing campaign in the Gulf, pizza deliveries to the Pentagon increased something like 12,000%. Soldiers had to manage the war, soldiers had to eat and pizza delivers. With Pizza Hut and Domino's trucks behaving like bumper cars in the Pentagon parking lot the media got a pretty good clue something was afoot in Iraq. This is called traffic analysis. It is concerned with masking the frequency, length, and origin-destination patterns of the message traffic.

At the telecommunication level, traffic analysis is a form of passive attack in which an intruder observes data being transmitted and makes inferences from the calling numbers, and the frequency and length of the calls. For example, a corporate merger might be deduced from the amount of traffic between two companies.

On the network level it is about the same. Let's assume a network usually operates its T-1 to the Internet at 30% utilization, with burst to 85%. Then one night it sits at 72% for hours on end. It means that something is happening at both ends of the network. Suspicion is raised by the behavior detected through traffic analysis, not the actual contents of the communications. Traffic analysis tools make an ideal detection mechanism if the basic profiles are reasonably set and the reaction channel can be whatever management chooses it to be.

Traffic analysis can be used to infer who is talking to whom over a public network. For example, in a packet switched network, packets have a header used for routing, and a payload that carries the data. The header, which must be visible to the network, reveals the source and destination of the packet. Even if the header were obscured in some way, the packet could still be tracked as it moves through the network. Encrypting the payload is similarly ineffective, because the goal of the traffic analysis is to identify who is talking to whom, not (to identify directly) the content of that conservation. "Traffic analysis allows the eavesdropper to identify relationships and changes in the communication activity. This can be useful when the content is scrambled and undecipherable."[109]

---

[109] Denning, D. E., *Information Warfare and Security,* Addison-Wesley, Berkeley, Ca, 1999, 176.

Another aspect of traffic analysis is its use for deceptive purposes. If we are sure that our enemy is analyzing our traffic and sometimes we might want it to be so, we can feed them with false information to diverse their attention from our main operational avenues. Carefully planned deceptions hide real intentions. For example, in the battle area, increased communications among the units can be a pointer to the upcoming movement of the troops. Let's assume A is attacking B. and there are three potential avenues of approach for A. If A can simulate a brigade level communication profile prior to the main attack on one of the possible approaches, B's attention toward that avenue will increase. Along with careful planning and coordination, A can deceive B about the main attack avenue. In this overall plan, fake communication is an important indicator when B is analyzing the traffic of A.

Although communicating parties usually identify themselves to one another, there is no reason that the use of a public network ought to reveal to others who is talking to whom and what are they talking about. The first concern is traffic analysis and the second one is eavesdropping. If we protect a communication channel against both eavesdropping and traffic analysis, and remove identifying information from the data stream, the new channel has an anonymous and private communication. "Appropriate link encryption techniques can mask the frequency, length and origin-destination patterns of the message traffic. End-to-end techniques can limit the precision of the origin-destination analysis but cannot entirely prevent it. The precision depends on the layer in which encryption is performed. Encrypting transport layer would limit the attacker to

observing patterns at the network-address level. On the other hand masking host-level patterns is more difficult."[110]

A mainly unsolved security problem in packet-oriented networks is the analysis of the network traffic flow for the purpose of deducing information that is useful to an unauthorized third party. The Navy Research Lab is currently working on a project called Onion Routing. The primary goal of this project is to provide private, traffic analysis resistant communications over a public network for a reasonable cost and efficiency. "Onion Routing uses well known networking and cryptographic techniques to protect both the privacy and anonymity of the communication against both eavesdropping and traffic analysis.... Onion Routing works in the following way: An application, instead of making a (socket) connection to an Onion Routing Proxy. That Onion Routing Proxy builds an anonymous connection through several other Onion Routers along the route. Before sending data over an anonymous connection, the first Onion Router adds a layer of encryption for each Onion Router in the route. As data moves through the anonymous connection, each Onion Router remove one layer of encryption, so it finally arrives as plaintext. This layering occurs in the reverse order for data moving back to the initiator. Data passed along the anonymous connection appears different at each Onion Router, so data cannot be tracked en route and compromised Onion Routers cannot cooperate. When the connection is broken, all information about the connection is cleared at each Onion Router."[111]

---

[110] http://www.cs.nyu.edu/~yingxu/privacy/0203/0203_kamijo.html.

[111] http://www.onion-router.net/Solution.html.

Onion Routing differs from other anonymity services in three ways:

- Communication is real-time and bi-directional
- The anonymous connections are application independent
- There is no centralized trusted component

Onion Routing's anonymous connections are protocol independent and exist in three phases: connection setup, data movement, and connection teardown. Its overhead is relatively small. "Connection setup overhead is typically much less than one second and appears to be more noticeable than other delays associated with normal web connection setup. Computationally expensive public-key cryptography is used only during his connection setup phase... The data movement phase uses only secret-key (symmetric) cryptography, which is much faster... Data latency is affected by the number of onion-routers along the connection and can vary with route length." [112]

One study, done in Spain, is also capable of capturing and analyzing the traffic on the network. This system is called MEHARI and consists of a low cost hardware traffic capture platform, and several traffic analysis software modules running on the top of this platform. "The MEHARI capture and processing capabilities can be expanded in modules by increasing the number of hardware elements in the system configuration. The MEHARI analysis functionality can be extended or modified both by configuration and by adding on new analysis software modules. Three examples of the type of information that can be obtained from the current implemented traffic analysis modules are the following:

---

[112] Goldschlag, D., Reed, M., Syverson, P., *Onion routing for anonymous and Private Internet Connections*,IEEE, Jan 28, 1999.

- A classification of the traffic in academic, commercial, leisure, and undetermined categories
- A classification of the traffic according to its origin and destination
- The verification of port assignment applications"[113]

Routine behaviors can be tracked easily. If a traffic analyzer can understand the traffic pattern of the opposite side, without knowing the content of the communication, an analyzer might predict the purpose. For example, let's assume A is communicating with B over a secure channel and with encrypted formats. X, the analyzer, follows the traffic between A and B for a while. Daily, weekly or monthly periodic reports would follow almost the same template, so there will be a similarity. After a while X will be able to differentiate them. Also, during a crisis or prior to an upcoming crisis, the volume of the communication will increase. Even this limited information can give the analyzer an idea about the possible outcome. If this information is combined with other intelligence resources, it is highly probable that "the big picture" will be revealed when the different pieces come together. Then, it is important to behave in a random fashion; doing fewer amounts of routine facilities. Also, the level of communication might always be at certain levels. In this way, we can hide the increased traffic level during a crisis or preparation period. One disadvantage of this approach might be wasting network resources by pumping unnecessary information onto the network. The use of bursty transmit techniques in wireless communication will lessen this disadvantage.

1. Mobile IP and Traffic Analysis

In mobile environments, protection against traffic analysis particularly means

[113] Lizcano, P.J., Azcorra, A., *MEHARI: a system for analyzing the use of the internet services,* Computer Networks, Vol 31, Issue 21, 10 Nov 1999, 2293-2307.

enabling location privacy, which up to now has not been solved practically. By wire-tapping network links, or by an active attack against routers, an intruder is able to retrieve sender and recipient address from the message headers, which are usually transmitted in plaintext. The additional ease of eavesdropping on wireless links makes this problem even more important for mobile environments.

"The IP Security Architecture RFC explicitly states that protection from traffic analysis is not provided by the proposed security mechanisms. They suggest traditional methods like bulk link encryption and generating false traffic to hide the communication partners. The Mobile IP draft specifies that protection from traffic analysis is an important topic. They propose link encryption and the establishment of bi-directional tunnels."[114]

Link encryption transmits a message as ciphertext between source and destination. The message is deciphered and enciphered at the intermediate routers with link specific keys. At the routers the messages are processed as plaintext, where the data may be exposed to secrecy and authenticity threats. "Therefore, link encryption is not secure enough to prevent intruders from traffic analysis. Moreover, the encryption and decryption procedures impose delays at each intermediate router and do not allow the user to scale the level of security according to his demands."[115]

Bi-directional tunnels can be used to establish a connection between networks, where the addresses of the communicating hosts are hidden from examination by intermediate routers, as original source and destination addresses are invisible. However,

---

[114] Fasbender, A., Kesdogan, K., Kubitz, O., Variable and Scalable Security: Protection of Location in Mobile IP, IEEE, 1996, 964.

[115] Ibid, 964.

"the traffic between the two corresponding networks (that provide the tunnel) is observable. This may give sufficient knowledge to an attacker, even if he does not know which nodes are communicating."[116]

In order to overcome these difficulties Chaum presents a method that allows messages to be sent anonymously through a "mix" node. In his model "a number of messages with equal length is collected from many distinct senders, repeats are discarded and their sequence is shuffled to obscure the flow through the network. A sender ***S*** first encrypts the message ***M*** with the public key of the receiver ***R*** (end-to-end encryption). Then, it encrypts this message plus the address of the ***R*** using the public key of the mix (i.e. sort of link encryption). The message is send to the mix, which decrypts the received message and forwards it to the recipient ***R***. A single mix station can ensure the security of the messages. However, if the output of the one mix were used as input of a second mix then both would have to conspire to trace any message. Thus, a cascade of mixes increases the security of the system and ensures untraceable traffic flow, provided that not all mixes are insecure or conspire."[117]

IP enables encapsulation to enhance the Mobile IP's security features. The Mobile IP normally uses tunneling only to forward a packet reaching the Home Agent (HA) but destined to a mobile node (MN) currently visiting a foreign network. The reverse direction does not use tunneling. To hide the location of a mobile node from the network, the registration messages as well as all other packets between MN and HA sent on unsecured networks, are tunneled using Secure IP (SIP) in IP protocol. "SIP in IP is

---

[116] Ibid, 965.

[117] Chaum, D., *Untraceable Electronic Mail*, Communication of the ACM, 24/2, 1981, 84-88.

an encapsulation protocol. Instead of tunneling a packet directly from one node to another (disclosing the end points of the tunnel and therefore the communicating hosts), several security agents (SA) in between are addressed, dividing the tunnel independent subtunnels. A SA- only knowing the addresses of its predecessor and successor- is unable to disclose the entire tunnel's end-points."[118] Secure encapsulation may be performed by the MN itself, the Foreign Agent (FA) or any other node the MN is connected to over a secure communication link, hiding IP addresses from observers.

Traffic analysis on a communication network becomes an important issue if the communication is among military entities. As the British and US coalition forces intercepted and defined the German organization prior to Normandy, successful traffic analysis exposed the organization, size and location of the communicating parts even though the communications were encrypted. This issue becomes more vital when it comes to the SOF. Since they engage in long-range actions behind the enemy lines, they are more susceptible to the enemy effect. During peacetime missions such as nation building and counterdrug operations, the SOF may use the available public data communication networks such as the Internet. In this case, preventing methods like Onion Routing will be a powerful tool against the potential traffic analysis efforts of the adversaries.

Another method might be a deception scenario, which would produce fake communications between nodes imitating a real communication and may end up being somewhat beneficial. Firstly, with devices simulating the communication of the teams in one area, the attention of the adversary might be diverted from the real target area.

---

[118] Fasbender, 965.

Secondly, if one can maintain a certain amount of traffic on a data network at all times, there will not be peaks during real crises or mission communications. There are tools available that can simulate fake communications among the nodes and the use of these tools might mask the amount of real data sent.

While proposing different techniques against traffic analysis, the best way might be to prevent or minimize the seizing of signals in the media by adversaries. Without a signal to analyze or the lack of complete signal information, traffic analysis would be unavailable. This leads us to low interception and detection capabilities of signals used in communications.

C. AVAILABILITY OF COMMERCIAL COMMUNICATION INFRASTRUCTURE FOR SOF

Global or wide regional projection of the SOF will require a capable communication infrastructure. For DoD, it is essential that this infrastructure be owned and controlled by national resources. It might be the most appropriate way for information security but availability of such an infrastructure will depend on vast amounts of capital and resource investment. In fact, this vision is on the way to becoming a reality for USSOCOM.

A network of interlocking HF base stations will allow special operators access to the infosphere from anywhere in the world. "This network is designed to ensure a deployed SOF team is always within the footprint of at least two base stations regardless of the location of the team or its headquarters. It operates by automatic link establishment techniques to provide highly reliable, low-power, long-range connectivity between team radios and base stations. Both team radios and base stations will employ

NSA-approved COMSEC equipment to secure the communications link. Phased upgrades of the network include embedding Global Positioning System (GPS) receivers and adding support for features such as secure voice/data, video, voice activation, global paging, and uninterruptable power supplies. In order to maintain a responsive network, a team of network controllers will keep the system operationally responsive while working with other infosphere systems."[119]

Although this is a thoughtful vision of having one's own controllable communications network, it would be wise to investigate the availability of commercial communications network infrastructure, due to the current unavailability of base station systems, which might be dependent upon the allowance of host nations. Among the commercial alternatives, our research choice will be the Internet, due to its almost worldwide availability and allowance of data transmissions. There will be ample opportunities for special operators to use the Internet for communications purposes. This partition of communication among the nationally owned infrastructure and commercial Internet will decrease the limitations such as bandwidth of the national infrastructure. If some communications can be moved to the Internet, then the burden of traffic on the national infrastructure will be less, and thus improve the overall quality of service for communications.

There are, however, some risks associated with this. Without securing the Internet for custom use sharing, the burden will be too heavy. On the other hand, "network security is a contradiction in terms, like the classic references to *jumbo shrimp* and *military intelligence*. True security can only be achieved when the information is

[119] USSOCOM C4I STRATEGY INTO THE 21ST CENTURY, USSOCOM, 1996, 12.

isolated, locked in a safe surrounded by guards, dogs and fences, and rendered inaccessible. Some would argue that even then, there is not absolute security. It is simply not possible, therefore to render a network system completely secure, and any reader ... must understand and accept this basic tenet in order to be successful. In spite of this managers of network systems must strive to attain this unreachable goal simultaneously."[120]

Prevention of security attacks is an essential step in network communication. Such attacks may be passive or active. "The passive attacks cause the release of data to an eavesdropper. The active attacks cause an unauthorized modification of the data. The best safeguard against any of these attacks is encryption. For this purpose, encryption can be applied either at an individual communication link known as link encryption, or from the source to destination known as *end-to-end encryption*."[121] Encryption is a huge topic to explore. We will not delve too deeply into encryption, but will investigate one application of encryption or virtual private networks (VPN), which provide connectivity via an encrypted tunnel through the public Internet.

1. Virtual Private Networks

A VPN connects the geographically dispersed networks of an establishment (government, military or commercial) over a public network such as the Internet. It essentially provides a secure global communications across the whole establishment without the need for private leased lines. The VPN can be implemented with dedicated hardware or software, or it can be integrated into a firewall and used to provide firewall-

---

[120] http://www.techguide.com/int/sec_html/intsec.shtml.

[121] Hatefi, F. G., Golshani, F., *A new framework for Secure Network Management*, Computer Communications, Vol.22, Issue 7, 15 May 1999, 633.

to-firewall communications or firewall-to-remote user communications.

Most VPN products support a technique known as *tunneling* which encrypts both the header and payload and then encapsulates them in new headers before transmitting. VPNs might be used in either of two ways. In one case, the tunnel through the Internet is between two private networks, such as main headquarters on one end and a remote forward-deployed unit on the other, or between two forward-deployed units. In the latter case, the management of the tunnel on each end is performed by a dedicated VPN server, or by an existing Internet firewall.

The other way of using VPNs is to connect an individual mobile computer across the Internet to a private network. The VPN function is implemented as software within the mobile computer. The mobile user then uses a local dial-up connection to access the Internet and reach the private network.

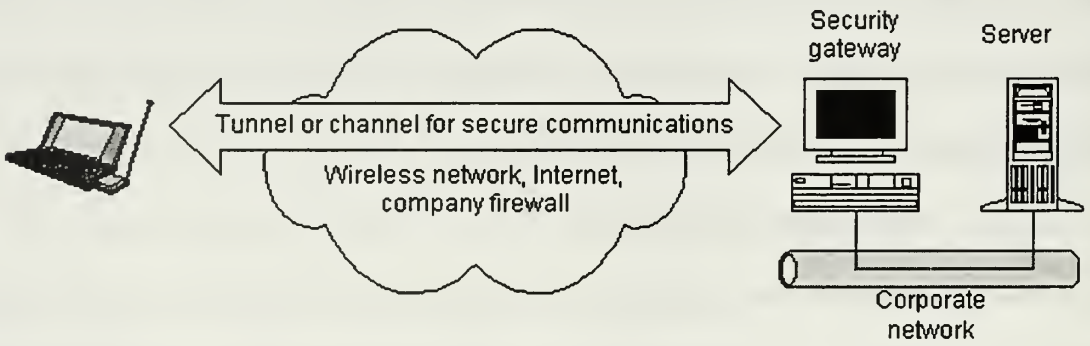


Figure 33. Secure Tunnel with a VPN.

a. Advantages

VPNs offer several advantages over traditional dedicated private networks such as cost savings, flexibility and convenience.

VPNs partially eliminate the modem banks, access servers, phone lines,

and other type of hardware that organizations must install to provide remote access to traditional private networks. In addition, VPNs can let remote users access networked resources via local telephone calls rather than, for example, via more expensive leased lines. They would be particularly cost-effective over longer distances, where leased lines are more expensive and over multiple connections, where the additional cost of leased lines adds up. On the other hand, savings could be consumed because large VPN traffic volumes could cause processing bottlenecks as systems spend time encrypting and decrypting the packets. To reduce these bottlenecks, the user would have to buy more hardware.

VPNs can be more flexible and convenient than traditional networks in their ability to permit remote entry to any authorized user with Internet access. This might eliminate the need for special equipment, which may limit the mobility of the user. VPNs also may let deployed special operators access networked resources via the Internet, thus providing a strong "backbone" for communications. This would be difficult with traditional dedicated private networks, because of the difficulties caused by the interoperability between remote networks. This would be an issue especially in peace keeping operations and humanitarian operations, where the availability of the local networks is good but the chance of compatibility with national systems is not.

b. Disadvantages

VPNs face obstacles to widespread implementation, including questions about security, reliability, performance, and the lack of open standards.

As with many Internet-related technologies, the security of communications and data transmission is an important issue for VPNs. Two key issues

are user authentication, which can be accomplished with passwords or tokens, and the security of the VPN's encryption tunnel. Since VPNs use the Internet, they can cause reliability and performance problems due to congestion, dropped packets, and other factors. This could cause problems for real-time applications, such as live voice transmission and video teleconferencing. The lack of open standards is a significant barrier to the widespread use of VPNs. Without standards, it will be difficult to invest in VPN technology because the products could quickly become obsolete and unsupported. For this reason, the industry is moving rapidly toward developing open standards. One of them is the Internet Engineering Task Force (IETF)'s IP Security Protocol, a set of open standards for authentication and encryption of IP packets. Another approach is Layer 2 Tunneling Protocol (L2TP), which combines Microsoft's Point-to-Point Tunneling protocol and Cisco Systems' Layer 2 Forwarding protocol. This proposal establishes a set of protocols by which compliant Internet components can create their own *channel* inside the Internet. This channel is protected by authentication and encryption countermeasures. This ensures that even though the traffic is being transmitted over the public Internet, individual sessions can be established which are private to those members allowed to work within the channel.

D. LOW PROBABILITY OF INTERCEPTION/DETECTION

The environment is constantly full of electrical and magnetic energy. It is what allows us to see and hear everything around us. It allows doctors to see inside our bodies and pilots to fly at night and through storms. It carries the TV shows we watch and radio stations we listen to.

Electromagnetic signals are essentially waves that propagate through some medium- air, water, copper wires, fiber optics and so forth. The entire range of frequencies make up what is called the electromagnetic spectrum. Low-frequency radio can go through deep water, is hard to jam, and is highly resistant to the interference produced by nuclear explosions. Higher frequencies generally allow higher bandwidths, so more information can pass over the medium in a given unit of time. Intelligence agencies use the term "signal intelligence" (SIGINT) to refer to the broad range of operations that involves the interception and analysis of signals across the electromagnetic spectrum.

Parallel to improvements in communications, countermeasures are also improved. The use of an air channel as the transmission media allows the communication to be detected and intercepted. In this way, the enemy has the capability of understanding the existence, content and origin of the message, which might pose fatal to friendly forces, especially the SOF which are very sensitive about the loss of covertness of the operation, and which could be detected and destroyed without reaching their tactical goals. For this reason there must be techniques which will prevent or at least decrease the detection and interception of the communication such as using frequency-hopping spread-spectrum techniques or burst transmissions. On the other hand, there is a certain trade-off for applied techniques. For example, to have a low probability of intercepting the transmission, one must use low output power, which will limit the range of the communication. For this reason, while developing systems, these trade-offs must be taken into account.

"A low probability of interception exists where there are burst transmissions, frequency-hopping, chip transmissions and spread-spectrum techniques. Burst transmissions compress the data before it is sent in the form of a short pulse, or burst. This reduces transmission time and also enlarges the frequency bandwidth due to physical relationships. Typical transmission periods for burst techniques are in the region of a few to many hundreds of milliseconds."[122]

With frequency-hopping techniques, the transmitter sends the information in a single burst. The bursts are transmitted consecutively on different frequencies. Modern transmitters do not hop a second time to the same frequency within the transmission. The transmitter and the receiver use a synchronous random key running via a high-precision time base. The approach allows the receiver to promptly change to the transmission frequency.

Wartime always creates a need for secrecy, especially in the communications area, and World War II gave birth to a method known as spread spectrum to prevent enemy intelligence from intercepting or jamming messages. "Although spread spectrum was not developed during the war due to the lack of an enabling technology, it became practical in the 1950s with the growth of digital technology. An interesting sidelight to spread spectrum is that the concept was the brainchild of an Austrian woman, Hedy Lamarr, who later gained fame as a Hollywood movie star. Together with musician George Antheil, she holds US patent number 2,292,387 for a Secret Communications system. The idea grew out of the need for a way to guide torpedoes to their targets without being jammed and driven off course. The system involved sending radio

[122] Clarence A. R., Position-fixing methods use broadband direction finders, Signal, Oct 1998.

messages between a transmitter and receiver over multiple frequencies in a random pattern. The message would skip so quickly among the different frequencies that a receiver tuned to a specific frequency would pick up just a blip that could not be intercepted or jammed. Today's frequency-hopping-spread spectrum (FHSS) technology is based on this original idea."[123]

Spread spectrum has evolved into the predominant wireless-modulation technique in a wide range of communications applications, from digital cellular and satellite to wireless local area networks (WLANs) and wireless local loops (WLLs). By spreading the data over a wide bandwidth, it minimizes the impact of noise and disturbances on transmitted data. Its key assets in commercial use parallel those for military applications-good interference-rejection capability (anti-jamming), low probability of interception, simultaneous multiple transmission over the same frequency bandwidth (efficiency and conservation of communications bandwidth) and low-power output for transmission (small, lightweight equipment).

While FHSS is a spin-off of the original spread-spectrum concept, most modern applications are based on the direct-sequence versions (DSSS). This is because DSSS supports the technique of code-division multiple access (CDMA) which does not require that users be separated into different channels or time slots. Simultaneous communications links are created by assigning them different spreading codes, so an increase in the number of users does not require a decrease in data transmission rate. CDMA, in general, is a more efficient technique for using the available frequency spectrum.

---

[123] "Military Technology Gets a Commercial Look," *Microwaves & RF*, Cleveland, Sep 1998.

1. Satellites and LPI

Today's sophisticated sensors and weaponry require the transmission of ever-growing amounts of data, as does the need to maintain situational awareness of tactical, highly mobile air, land, and sea forces during what will probably be involving joint coalition forces. The traditional method of long-range communications is high frequency (HF) radio, a technique that is dependent on ionospheric conditions and offers only limited bandwidth. Satellite communications is the only technique able to move such large amounts of data over global ranges. Currently, the satellite communications have some limitations especially due to latency issues. Real time communications via satellites still require further development. In addition, satellite communications have vulnerability against EMP weapons. High-altitude EMP bombs can effect the satellite itself. The earth stations are also vulnerable to EMP bombs.

Satellite systems operate in the ultra-high frequency (UHF), superhigh frequency (SHF) and extremelyhigh frequency (EHF) bands. Each of these bands has their own advantages and disadvantages. We will discuss the use of the EHF band, which is critical for LPI. "The 30 to 300 GHz EHF band is the most survivable and secure band of the three, and provides users good anti-jam and low probability of detection/interception. Primarily used for Time Division Multiple Access (TDMA) services, it can support low and medium data rates and has the potential to provide high data rates. However its terminals are expensive, and the service can be degraded by heavy rain, snow, hail, and other weather conditions."[124]

---

[124] Richardson, D., "Military Satcoms poised for expansion," *Armada International*, Zurich, Feb/Mar 1999.

One example of hand-held satellite communications is Iridium. Iridium users have voice, paging, fax, and data capability by using a hand-held phone and pager from almost anywhere in the world. The system forms a digital packet switch network that is accessible from virtually anywhere in the world. Defense Information Systems Agency (DISA) has installed a dedicated ground station in Honolulu, HI, to act as a terrestrial gateway for the Iridium system. "The location of the DoD Iridium users will be protected and a low probability of interception will be provided via secure hand-held telephones (which incorporate security chips developed by the National Security Agency) that link users to the gateway."[125] If this only gateway is disabled (by accident or sabotage), there will be a mobile gateway available to serve as a standby system. Due to its low data rate capability, an Iridium system promises secure digital voice transmission for users. The SOF is also capable of using this commercial system as a contingency asset in its communications. One must remember that the uncontrollable sources of the Iridium system might cause problems in the future. The high cost of maintaining the current system requires high user profiles, but Iridium could not reach the requisite numbers yet. Thus, this points to the importance of using controllable national resources.

By June 1999, the Iridium satellite system was bankrupt due to the high cost of service maintenance. On December 31, 1998, there were approximately 3,000 activated subscribers to the Iridium system – a far cry from the 200,000 the company had expected by year's end.[126] Beyond launching nearly 80 router satellites in orbit, the system was challenged by 130 to 150 different countries because of licensing issues. The Iridium

---

[125] "Iridium Network to serve defense personnel," *Microwave Journal*, Dedham, Feb 1999.

[126] "Iridium Report Reveals Five New Losses," *Communications Today*, Potomac, Jan 26, 1999R.

system example shows the potential dangers of being dependent on international resources and the business world. Yet when it is available, using these kinds of systems eases the burden of the other vital communications channels. The commercial systems are in danger of being shot down during a crisis and do not have measures against A/J, LPD/ LPI and the EMP effect. They might, however, be viable means during the humanitarian operations and among the well-organized coalition forces.

2. Examples

A German-South African joint communication initiative is developing a new HF tactical radio system, designated "Phoenix." According to the manufacturef, Grintek, the Phoenix design emphasis is on data transmission, and it has superior functionality to equivalent Racal and Tadiran manpacks. "In the long term, Grintek is expected to offer an alternative CDMA/LPI wireless handset giving full remote control and patrol intercommunication facilities."[127]

To handle data transmission needs during its Task Force XXI battlefield digitization experiment, the US Army created the tactical internet communication architecture by interconnecting existing communications equipment. "The Surrogate Digital Radio was an attempt to obtain the most sophisticated technology industry had to offer on a timescale that matched the needs of Force XXI. Intended for use as a 'data hauler' (that is, a higher capacity mobile data radio), it is secure (LPI) version the GEC-Marconi Hazeltine PRC-118 low-cost packet radio."[128]

---

[127] Coulsdon, "German-South African HF radio under development," *Jane's International Defense Review*, Feb 1, 1999.

[128] Richardson, D., "Battlefield radio after Bowman," *Armada International*, Zurich, Apr/May 1998.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The Special Operations Forces (SOF) have a unique and extended role as a national strategic asset. The conjecture of a changing political and security environment and new technologies present both challenges and opportunities for the SOF.

With today's limited defense budgets, the leverage of the SOF is increased even more. Likewise, fast technological change might bring the next Revolutions in Military Affairs (RMA). This potential new RMA encourages the development of new concepts like Information Operations (IO). When IO and the SOF are used cooperatively, their leverage will be even greater in the world of limited resources, providing economy of force.

Special operators have to be one of the best informed forces on the battlefield. This goal can be achieved with digital communications depending on national systems to the maximum extent possible. Doctrinally, these communications systems do not have to follow the traditional chain of command and access to the infosphere has to be available down to the single operator on the field. Wireless ad hoc networks are becoming the essential part of the battlefield as the digitalization efforts continue. The SOF members have to reach the infosphere individually and continuously. In order to support such a requirement, a global communications system including the satellites and various-capacity hand-held devices is needed. This system has to support tactics and techniques used by the SOF. Moreover, it has to provide fault tolerance avoiding single points of failure.

Among several wireless mobile architectures, ad hoc infrastructures will be more convenient for the SOF. These architectures are more configurable and do not necessarily have a single point of failure, enabling more dynamic topology. In our research, we established an ad hoc peer-to-peer network, which is capable of supporting a large number of mobile radio nodes. Each node may communicate with each other via intermediate nodes in a multihop node. That is, every node acts as a router in the network.

The issue of multihop routing requires special attention to the routing of packets throughout the network. The routing algorithm used in the system has to support the dynamic nature of the wireless mobile networks with the least possible control overhead. Especially, the implementation of multihop packet radios benefits the special operators conducting operations behind enemy lines where updated and qualitative data flow is needed the most.

Since every node participates in a routing mechanism, it is viable to choose the most efficient routing algorithm for the mobile wireless network system. The efficiency of the routing protocol will be reflected by the limitations of the communications system. Limited resources such as bandwidth, battery life, and quality of service have to be take into account, while deciding on the use of existing routing protocols or designing a new one. The dynamic nature of the mobile wireless communications supports use of on-demand (reactive) routing protocols, which have less control overhead then table-driven static (proactive) routing protocols. Since control information uses the same resources available in the system, more control information means less available resource for the actual communications.

No single network technology can simultaneously offer wide-area coverage, high bandwidth, and low latency. In general, networks that span small geographical areas (e.g., LANs) tend to support high bandwidth and low latency, whereas networks that span large geographical areas (e.g., satellite networks) tend to provide low bandwidth and high latency. In order to provide flexible connectivity over wide areas, a wireless internetwork needs to be formed from multiple wide-, medium-, and local-area networks interconnected by wired or wireless segments. This internetwork is called a wireless overlay network. Future mobile information systems will be built on heterogeneous wireless overlay networks.

Electromagnetic pulse (EMP) weapons have potential use in future battlefields. As the burden of digitalization of the battlefield increases, the vulnerability of equipment and devices on that battlefield against EMP weapons also increases. Vital hubs on the communications network will be a good target for EMP weapons. Hardening of the material from the early design phases and building enough redundancy in the network for fault tolerance can be potential solutions. Special operators who use the most advanced communications means, will be the main targets of the enemies and transnational criminal organizations. EMP weapons' easy delivery methods and high payback increases their appeal. On the other hand, the SOF can include these weapons in their arsenal. These weapons can be used by the SOF against targets and there is little remaining signature left behind.

Cyberspace is a field that is not controlled by a single nation. When national resources are not available, it is beneficial to use a public communications infrastructure by a special operator. Shifting some of the available traffic over public infrastructure will

also lighten the burden of the vital communications links. However, most of the public communications infrastructures are not designed with security in mind. Embedding this into military communications system requires the implementation of powerful encryption of the content. Moreover, potential adversaries must not be able to analyze traffic on the network. Applications such as Onion Routing help hide the real identity of the source and destination nodes. Implementation of special techniques such as virtual private networks (VPN) increases the use of public infrastructure for secure communications among dispersed nodes physically. With the use of VPNs, the high cost of maintaining a dedicated private network is eliminated. Since this technology is still in its evolutionary phase, additional security, reliability, and performance problems can arise.

Government policies supporting the development of appropriate defense technologies have always been a special case. Increasing demand from the public market decreased the share of the military in the overall communications market. In addition, commercial and military goals for the communications requirement are different in technical and design specifications. A possible consultation system between the military and the commercial world will handle the differences from the early phases of the development cycles. As a result, while the military is cutting the huge R&D budgets, the commercial market will get its loyal patron.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

A particularly short avenue for future research is the application of the concepts to different scenarios in order to evaluate their impact more carefully. In the scope of a huge overall system, we conducted the simulations for the tactical part of the model.

Due to the homogenous nature of the GloMoSim, the specifications of the individual nodes on the wireless network could not be defined. Powerful simulation tools such as OPNET and COMNET III might be used for further improvements to our model. Since GloMoSim does not have a built-in statistical analyzer, we have to transform the statistics collected by GloMoSim to different tools. Most of the commercial simulation tools do not have this problem. They have powerful statistical and graphical tools to represent results.

Mobile IP will be widely used in the future by wireless and mobile users. IETF obtained major improvements for supporting mobile and wireless users on the Internet. The use of standard routing protocols will increase the ability of using existing networks. In order to implement this system, a military internet can be established and the wireless network used by the SOF can be part of that military internet.

After adding necessary security perimeters such as authentication, integrity, and confidentiality, this military internet can be connected to the commercial internet. The advantage of this approach will be the ability to use commercially available resources for some –limited- military communications. In order to implement such a system, the Mobile IP has to be improved and secured.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. LITERATURE REVIEW

Before beginning our research, we made a through survey of the latest articles published by various scientific organizations, such as IEEE and ACM. Our initial concern was about the different access and routing mechanisms used or proposed in wireless mobile communications. As we examine further, we have chosen articles that especially include military applications and their simulations. It was amazing to find a lot of concern for military wireless communications in the publications. Moreover, we tried to select articles that covered other hot issues such as security, mobile IP, power consumption and quality of services. With this review work, we laid the basis of our future work for developing a model for mobile wireless communications, which would be used particularly by SOF behind the enemy lines. On the other hand, it was difficult to find a complete model that can support not only the team level or the high headquarters level, but also all special operations forces at all levels. As we discussed before, the nature of these forces requires special tools, which will overrun their disadvantages such as being totally in the rear of the enemy, or lacking in heavy firepower. Powerful communications is one of those special tools that have to be given to the special operators.

A. ACCESS METHODS

Radio communications use the same channel, air, as their communication medium. This medium is perfect for broadcasting, all receivers in the range of transmitter can receive the signals. "Although this high connectivity is very useful in some applications, like broadcast radio or television, it requires stringent access control in

wireless communication system to avoid, or at least to limit, interference between transmissions."[129]

Multiple access in wireless communications is based on insulating signals used in different connections from each other. "The support of parallel transmissions on the uplink and downlink, respectively, is called multiple access, where as the exchange of information in both directions of a connection is referred to as duplexing."[130] The necessary channel utilization is achieved by assigning to each transmission different parts of the domains that contain the signals. The signal domains commonly used to provide multiple access capabilities include the following: time domain, frequency domain, and code domain. Their respective access methods are time-division multiple access (TDMA), frequency-division multiple access (FDMA), and code-division multiple access (CDMA). There are further methods based on improvements to these basic mechanisms.

First generations systems (analog systems) used FDMA for the user traffic in the air interface. TDMA and CDMA are both used with digital signaling. "Digitization of the signal enables encryption..., and error checking and error correction... In conventional analog systems, the RF channel is allocated to one user; in a digital system, the RF channel is allocated to more than one user."[131]

In choosing the best access method, we might have some difficulties. FDMA is only suited for applications such as cordless telephone with very small cells. Then for personal communications, the solution reduces to TDMA or CDMA. "In terms of

---

[129] Paris, B., Access Methods, article appears in the book edited by Gibson, J.D., The Mobile Communications Handbook, IEEE, 1999, 17-1.

[130] Ibid., 17-2.

[131] Black, U., Second Generation Mobile & Wireless Networks, 1999, 6.

complexity, TDMA receivers require adaptive, nonlinear equalizers when operating in environments with large delay spreads. CDMA systems, in turn, need ... sophisticated power control algorithms."[132] When results are checked from Table 8*, it is easy to see the recent CDMA variations are covering an important place in the research world. CDMA is especially advantageous for cell-based networks because it does not need for frequency and timeslot coordination among cells and allows carrier-frequency reuse in adjacent cells.

One of the new mechanisms is the Orthogonal Domain multiple Access (ODMA) is the combination of TDMA and FDMA. It has ability to dynamically adapt the slots, which have both time and frequency assigned to them, to prevent interference.

B. ROUTING

In general, the term routing is referred as all the things that are done to discover and advertise the paths from source to destination and in between, and actually move information packets from here to there when necessary. So, routing is a characteristic of connectionless communications where as switching is used in connection-oriented communications.

There are two basic ways of routing; *source* routing and *hop-by-hop* routing. In *source routing*, all information about how to get from source to destination is first collected at the source, then the path information is put into the packets that is sent toward the destination. The job of the nodes between the source and destination is simply to read the routing information from the packets and act on it correctly. In hop-by-hop

---

[132] Paris, 17-11.

routing, the source is not expected to know all information about the path to destination. It is sufficient for the source to know only how to get to the "next hop". The job of the interim nodes is more complicated in this case. They only have the address of the destination and have to figure out the best "next hop" for each packet. During our review we saw that Dynamic Source Routing (DSR) is fitting due to its complete on-demand nature. In this way, the scarce resources are used effectively by using DSR in the mobile wireless communications.

One thing that we observe from the Table 8 is that the exclusion of access methods and routing mechanisms. In fact, each article concentrates in one aspect of the wireless communications. Generally, the articles about the access methods are assumes the wireless model as of one-hop, just like cellular communications. In this one hop system, mobile node directly reaches to the base station and after this phase, packets are switched to the destination. More complex models consisting of multi-hops will definitely need an effective routing schema. In this research, we will suggest both the access method and the routing mechanism for our global wireless mobile network model.

C. REFERENCES

In the following section, we will present brief summaries of the articles that we studied during the review.

1. Bittel, R., Caples, E., Young, C.D., Loso, F.; "Soldier Phone: An Innovative Approach to Wireless Multimedia Communications," paper appears MILCOM '98 Proceedings, IEEE, Volume:3, 1998, Pages 903-907 in 1998 and ASSET '99 Proceedings, IEEE Symposium, 1999, Pages 264-268 in 1999

---

*Page 236.

This article describes a newly developed, wireless military communication system known as "Soldier Phone." The Soldier Phone system meets the need for high data rate, multimedia, and adaptive networking in highly dynamic operation environments. It is a half-duplex transceiver that operates over multiple channels in a single RF band using line-of-sight (LOS) propagation modes and includes modem and networking functions which permit a terminal powered by Wireless Network Engine (WNE) to communicate without the need for central base stations or cell sites. The network is fully distributed with each node capable of being a source of multimedia information.

The WNA provides all of the hardware and software processing for handling traffic and system management, filtering, error control, transmit and receive signal processing, voice encoding, and information security functions.

In order to provide dynamic bandwidth management, WNE uses Orthogonal Domain Multiple Access (ODMA). ODMA is a combination of TDMA and FDMA resulting in slots that have both an assigned time and frequency.

There are four basic system concepts that are important to understand the Soldier Phone system;

- Self-organizing capability
- Switching, routing, and resource management
- Status monitoring
- Interoperability with other networks and systems

The concepts underlying the Soldier Phone networking, synthesized in hardware and software, have been successfully demonstrated in a laboratory test-bed.

2. Stehle, R.H., Lewis, M.G.; "Wireless Networks of Opportunity in Support of Secure Field Operations," paper appears in MILCOM '97 Proceedings, IEEE, Volume:2, 1997, Pages 676-681, in 1997

This article summarizes a demonstration of the DARPA-funded Information Technology (InfoTech) project. This project developed a basic capability for secure, wireless, voice, data, and video information transfer, using a combination of both commercial and military networks.

The InfoTech project had to meet several goals, including timely information transfer, universal coverage, ease of use, multimedia with voice and image, and security. No matter where a field user (mobile) is working, it is desired that the mobile user have access to on-line submittal and retrieval tools. This requirement places a special emphasis on wireless networks.

A series of networks (LANs, MANs, AMPS, Satellite links) are used for connectivity of different operational purposes. The Internet formed the primary backbone for center-to-center communications and served as a vehicle for a number of wireless communication services. Wireless LAN technology was used for rapid deployment in field operations centers. Cellular telephone networks served as a connection medium using a data modem to send data over analog AMPS network. The satellite system was integrated into the architecture to provide communications for a rapidly mobile command. The system can be used for voice and data communications.

Security was an important aspect of the demonstration. It is ensured that the data to be transported is protected by encryption and other security services provided by the FORTEZZA card. During the demonstration, following FORTEZZA-supported applications are also tested: Secure WWW browser, hard-drive bulk encryption,

encrypted motion video and voice, firewall and file transfer, network tunneling.

The demonstration provided an opportunity to test the maturity and availability of wireless networks and security elements that could support the information needs of both law enforcement and the military.

3. Tendre, M.L., Macauley D., Sudnikovich M.; "Routing and Internetworking Within The Tactical Internet," paper appears in MILCOM '95 Conference Record, IEEE , Volumu:3, Pages 921-924 in 1995

In this article the authors describe an application of commercial internetworking technology for use in providing a framework for a Tactical Internet (TI).

It is known that tactical systems can be robust, but they are generally bandwidth limited, operate in a high-noise environment, are subject to nodal and link outages and are highly mobile in nature. The US Army's goals of seamless communications include routing and internetworking. Seamless communications are defined as communications between two computers where transport of data, whether across one or multiple networks, is transparent to the user. Routers, both commercial and tactical, allow for the seamless transport of data across multiple heterogeneous networks.

The TI is based upon three networks. The lowest level network is the primary user network for forward echelon units. The second level network will be the primary general purpose data traffic backbone from the maneuver brigade to lower echelon units and direct support units. The third level will be a backbone from brigade to higher echelon units.

Two different tactical routers will provide routing through interconnected communications systems. While one will connect first and second levels, the other will connect second and third level networks. Both routers use a commercial standard

protocol called Open Shortest Path First (OSPF).

Three different modules; WAN Manager, LAN Manager, and Network Server will provide desired network management.

The authors propose an ambitious plan for the fielding of the TI, its capabilities, and optimum performance of commercial protocols within the tactical environment.

4. Agrawal, P., Famolari, D.; "Mobile Computing in Next Generation Wireless Networks," paper appears in Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications , 1999, Pages 32 - 39

In this paper the authors describe the evolving status of wireless communications and its impact on the future of mobile computing. They present a historical perspective and explain the technical challenges facing the next generation of mobile computing technology and applications.

Wireless data traffic is expected to account for over seventy percent of the global wireless revenues by 2003. To meet this expectation, the next generation of wireless networking needs to offer improvements in terms of bit rates, advanced Medium Access Control (MAC) layers, power saving techniques, and data transmission capabilities.

Some examples of systems in current use are Analog Mobile Phone System (AMPS), Interim Standard 136 (IS-136), Global System for Mobile (GSM), and Interim Standard 95 (IS-95). Second generation systems have improved the capacity, security and quality of AMPS. However, these systems were not suited for full blown high-speed network access. Systems, protocols, and devices were designed primarily for voice applications.

Three kind of wireless data services are deployed on top of the current wireless systems to improve wireless computing. Despite these improvements, there are some problems with the current state of mobile computing such as slow networking, wasteful protocols, disconnections, weak terminals, immature IP access to networks, and poorly optimized operating systems for mobile applications.

SERVICES	SYSTEMS	DATA RATE (KBPS)
CDPD	AMPS	19.2 (total in a cell)
GPRS	GMS	100
EDGE	GMS	300
CIRCUIT SWITCH	GMS, IS-136	9.6

Table 5. Different Wireless Data Services.

The third generation (3G) is fast approaching. One of the main goals of the 3G is to provide universal coverage and to enable terminals to be capable of seamless roaming between networks that may be different in type. The current project for 3G is the International Mobile Telecommunication 2000 (IMT-2000) project. This project offers 2 Mbps for indoor low mobility, 384 Kbps for the pedestrian situation, and 144 Kbps for a high-speed environment. New air interfaces will be CDMA2000 in the U.S., Wideband CDMA (W-CDMA) in Europe and Japan, and third generation TDMA which uses higher modulation.

In IMT-2000 compliant systems, mobile users will be able to access the internet, make voice calls, receive streaming audio and video, and transfer large data files while on the go and away from their home networks. This will be facilitated by the interoperability of disparate network domains, secure tunneling of information across

foreign networks, and through IP-enabled mobility schemes such as Mobile IP (MIP).

It is clear that 3G systems will not solve all problems with mobile computing. The authors point out some of the challenging problems such as optimal radio resource use in a crowded medium, efficient power saving algorithms, and the most efficient use of limited spectrum. On the other hand, availability of appropriate end devices and internet-enabled mobile terminals by using Wireless Access Protocol (WAP) still could not reached a maturity level of being practical. Data rate, migration, and guaranteed QoS still need to be improved upon.

As a result, it is expected that the next generation cellular systems will provide fertile ground for new applications, never before imagined, and provide innovative anytime, anyplace, and anymedia service to customers roaming the globe.

5. Torrieri, D.; "Future Army Multiple Access Communications," paper appears in MILCOM 97 Proceedings Volume: 2 , 1997 , Page(s): 650 -654 vol.2

In this article the author discusses the future use of *frequency-hopping* (fh) CDMA systems for the Army's mobile multiple-access communications.

Multiple access is sharing a common transmission medium with other users. Wireless multiple-access communications are possible if the transmitted signals are orthogonal or separable in some sense. CDMA separates the signals by using the unique code of the sender. CDMA is realized by using spread-spectrum modulation while transmitting signals from multiple users in the same frequency band at the same time.

CDMA has some advantages with respect to air interface channel utilization techniques like TDMA or FDMA. Firstly, CDMA does not need frequency and timeslot coordination among cells. Second, it allows adjacent cells to reuse carrier-frequencies because each mobile unit in the system has a unique code. Third, a transmitter is

activated only when the user is talking. And last, CDMA increases system capacity by exploiting intermitted voice signals or multi-beamed arrays. This last advantage is the result of the combination of CDMA with multi-beamed antenna arrays that are either adaptive or have fixed patterns covering cell sectors. Since digitalization of signals is used, this technique has resistance to jamming, interception, and multiple path interference.

The two types of CDMA techniques are direct-sequence (ds) CDMA and frequency-hopping (fh) CDMA. The ds-CDMA suffers from, near-far problem, and the suggested solution is power control. But the accuracy of the power control is a crucial issue. The author explains the difficulties that will be encountered at high frequencies with power control, and points out the limits of ds-CDMA for future military use.

Frequency-hopping CDMA networks avoid the near-far problem by continually changing the carrier-frequency, so that frequency collisions become unusual. Another advantage is that the signal can be spread over a much larger spectral band than ds-CDMA.

Under identical conditions, fh-CDMA systems have lower bit error rate probabilities than ds-CDMA systems.

The article addresses some problems of the fh-CDMA. Spectral splatter which is the interference on frequency channels other than the one being used by fh pulse is one of them, and spectral efficient modulations are proposed as a solution to such interference.

The author concludes that, for the future Army wireless networks, fh-CDMA is attractive due to its significant advantages over ds-CDMA.

6. Alagar, S., Venkatesan, S., Cleveland, J.R.; "Reliable Broadcast in Mobile Wireless Networks," paper appears in Military Communications Conference, MILCOM '95, Conference Record, IEEE Volume: 1 , 1995 , Page(s): 236 -240 vol.1

This article contains a description of a model for wireless networking that supports reliable communications between nomadic hosts engaged in distributed computing and collaborative conferencing.

According to the authors, this model addresses the need to provide reliable information exchange, mitigate bottlenecks, avoid excessive traffic, and offer scalable services without the benefit of static base stations or fixed backbone support. This network model supports the needs of subscribers to mobile command posts and satellite ground entry points.

In this network concept, the cell of a mobile host is the geographical area within which the mobile hosts can directly communicate with other mobile hosts. Host mobility and terrain prevents a priori knowledge of any host location and optimum path. Message broadcasting, or flood routing, provides the means for reliable delivery of information in the presence of uncertain connectivity and node locations. Flooding ultimately involves transmitting the message to every node in the network, which is a disadvantage, particularly for large networks. The main advantage of flooding is that there is little explicit overhead and network management. Instead, hosts keep track of individual messages received and determine whether or not to transmit the message.

Each host detects neighbors by periodically broadcasting a probe message. Each mobile host retains a history of messages broadcasted to and received from its neighbors. A host, which receives a message, broadcasts an acknowledgement to the sender, updates

its local history, and then retransmits the message if it is not a duplicate message. Duplicated messages are discarded. When a host detects a new neighbor, a "handshake" procedure results in the exchange of active messages not common to the respective history of each host. Using handshake procedures, mobile hosts receive messages that they did not receive previously due to link disconnection.

The authors built a protocol model designed to achieve assured delivery of information in a multi-hop nomadic wireless network that has limited bandwidth and is subject to changes in link connectivity. They also address some methods to improve protocol efficiency such as reducing the buffer size.

7. Corson, M.S., Macker, J.P., Cirincione G.H.; "Internet-Based Mobile Ad Hoc Networking," paper appears in IEEE Internet Computing in 1999, Volume 34, July-Agu 1999, Pages 63-70

Mobile ad hoc networking technology enables the operation of autonomous systems consisting of mobile nodes. Each node in a Mobile Ad Hoc Network (MANET) logically consists of a router with possibly multiple IP-addressable hosts and multiple wireless communications.

In a MANET, routers can be mobile, and interrouter router connectivity can change frequently during normal operation. Moreover, end devices are mobile, meaning that they can change their point of attachment to the fixed infrastructure. This causes a change in the routing topology as well. An end user's association with a mobile router determines its location in the MANET.

The emerging mobile Internet can be divided into layers: the mobile host and mobile router layers. The mobile router layer consists of mobile routers and mobile hosts with each mobile host permanently or temporarily affiliated with a mobile router. The

mobile router layer does not require routing support from the fixed network, as it forms a mobile infrastructure parallel to the fixed infrastructure.

The resource constraints in MANET are somewhat opposite to those in the fixed Internet, that cause a decrease in some of the horizontal communication requirements (which expands bandwidth) and increases some of the vertical communication requirements with in the protocol stack. The increased two-way communication permits upper-layer protocols to bind more closely with lower-layer protocols, thereby retaining some of the inefficiencies that might result in additional horizontal communication.

Several perceived benefits of IP-based networking for mobile wireless systems – cost effectiveness, flexibility, interoperability, and physical media independence go hand-in-hand with a view that connectionless datagram forwarding is a robust and sensible technology approach for building mobile networks. The hardware advancements, coupled with the increased use of IP technology in both commercial and military systems are resulting in a shift from closed, proprietary systems to Internet -compatible standards-based systems.

Large-scale, mobile, multihop wireless networking systems pose many challenges to the designer of IP-based networking systems. Such systems must operate in environments with highly mobile nodes, bandwidth-constrained, unreliable communications, high levels of interference, and accompanying potential electronic information threats. One additional challenge with potential large-scale, wide-area use of this technology is the relatively low performance achievable over "strictly terrestrial" mobile, multihop wireless networks. A *vertically networked*, hybrid system composed of terrestrial, aerial, and satellite nodes may best serve mobile users. In the long term,

MANET technology appears well suited for internetworking these diverse, heterogeneous networks.

8. GARCIA-LUNA-ACEVES, J.J., FULLMER, C.L., MADRUGA, E., BEYER, D., FRIVOLD, T.; "WIRELESS INTERNET GATEWAYS (WINGS)," paper appears in MILCOM '97 Proceedings, Volume 3, 1997, Pages 1271-1276

Multihop packet-radio networks (or ad hoc networks) are an ideal technology to establish an instant communication infrastructure for military and civilian applications in which both hosts and routers are mobile and can have multiple points of attachments to the global IP Internet. In the multihop packet-radio networks, there are no dedicated base stations as in commercial cellular networks, and all nodes interact via packet forwarding. Since packet-radio networks can be entirely deployed and operated by the end users, there is no reliance on wireless service providers or a stable backbone infrastructure.

The Wireless Internet Gateways (WINGs) project has introduced and demonstrated an architecture and protocols for mobile wireless internetworking, in which packet-radio nodes are wireless IP routers and the global IP Internet is extended to the mobile wireless environment in a seamless manner. Like an IP router, a WING accomplishes its routing functions at the IP layer. However, in contrast to wired IP routers, WINGs must also adopt to the dynamics of ad hoc networking in which routers can move frequently, and must schedule their transmissions to maximize utilization of the available spectrum. Meanwhile they avoid interference with other transmissions that they may not even be able to detect. (The hidden terminal problem)

The differences between a WING and a traditional router are the following: (a) Wireless Internet Routing Protocol (WIRP), improved from RIP and RIPv2, can far more effectively handle the topological dynamics and broadcast radio channel of the wireless

links; (b) the routing protocol interacts with the link-layer protocols in order to reduce control traffic needed to maintain routing tables; (c) uses a new set of protocols for link control and channel access designed for ad hoc networks – solves the hidden terminal problem.

In the WING protocol architecture WIRP runs at the top of UDP and it can be functionally divided into three main components: reliable exchange of updates; neighbor discovery mechanism; and its path-finding routing algorithm (PFA).

Reliable transmission of update messages is implemented by means of multicasting of update messages that are acknowledged with update messages carrying both updates and acknowledgements to one or more other messages.

Every WING checks its connectivity with its neighbors periodically. A WING transmits a HELLO packet if it does not have any data packet or routing-table update message to transmit during a HELLO interval, which is three seconds currently.

Each WING communicates to its neighbors a hierarchical routing tree in an incremental fashion. The tree reported by a WING consists of all the WING's preferred shortest paths to each known IP network and IP host, where an IP host is typically a WING. An entire remote IP network is simply a node in the routing tree.

In the next part of the article, the authors show that using the FAMA-NCS (floor acquisition multiple access with non-persistent carrier sensing) protocol, a given station and its neighbors are able to utilize at least one third of the channel capacity in the worst case.

In the last part, the authors represent their simulation results about the average throughput of FAMA-NCS and the effectiveness of WIRP.

9. Murthy, U.; Bukhres, O.; Winn, W.; Vanderdez, E.; "Firewalls For Security in Wireless Networks," paper appears in Proceedings of the Thirty-First Hawaii International Conference, 1998 , Page(s): 672 –680, Vol.7

This article discusses the firewall and other security tools used to provide security for the wireless networks and offers a methodology to protect the wireless networks.

Users of wireless network users do not have the same physical constraints that users of wired-networks have. The wireless medium allows users to move about freely while they are connected to the network and its users from various locations. But this freedom of wireless networks does not come without risks. The very medium which frees users from their homes and offices increases the security risks of the network.

The approach offered by the authors adopts the concept of "defense in depth;" meaning that if one component of the firewall system is compromised, there will be other components that will stop the intruder, or at least slow the intruder until the system administrator notices the security breach.

The suggested system consists of three main parts, each part of a defense-in-depth design. The external screening router is the first line of defense. This router will reject all connections except from those machines with approved IP addresses. The next line of defense is the bastion host. This is the single most important component of the firewall. The bastion host performs the tasks of user authentication, machine verification, and logging of all security events to an internal host. In short, the primary function of the bastion host is to act as a proxy server for various services. The internal screening router, the last line of defense, is configured in much the same way as the external screening router. The only difference is the internal router will accept connections from the bastion

host only. This is done to protect the internal network in case the bastion host is compromised.

The proposed implementation is a fairly standard firewall implementation used by fixed-wire networks. However, with the wireless network comes the need to protect against the rogue users assuming the identity of currently active users and the need to guard against the danger of mobile computers being stolen. At this point, the authors add machine verification and user authentication via challenge-response mechanisms. These mechanisms may be encountered in three different occasions: (a) at the initial connection, (b) an attempted use of a protected operation/service, and (c) at random time intervals.

The authors have made some assumptions in their analysis. First, it is assumed that all data in the communications is encrypted with a strong key. Second, their approach does not take into account the limited bandwidth problem encountered in the wireless networks. Third, they assume that a mobile IP addressing scheme is used. With these assumptions in mind, it is apparent that the model has limitations. The performance of the firewall against the growth in the number of the users, and the cost of the authentication devices-smart cards, tokens- are to name a few.

The authors point out a protection application by the implementation of introduced firewall system and a well designed security policy. This will minimize the effects of potential attacks.

10. Martin, J.N.; Colella, N.J.; "Broadband wireless communications via stratospheric HALO/sup TM/ aircraft," paper appears in Military Communications Conference, 1998. MILCOM 98 Proceedings., IEEE Volume: 1 , 1998 , Page(s): 45 -49

In this article, the authors describe the conceptual design of a "bandwidth-on-demand" wireless network whose data rates to and from the user will be measured in multi-megabits per second ranges.

The High Altitude Long-Range Operation (HALO) Network will offer access to any subscriber within a "super metropolitan area" from an aircraft operating at high altitude. The aircraft will serve as the hub of the HALO network. Each subscriber will be able to communicate at multi-megabits per second data rates through a simple-to-install subscriber unit. In fact, this wireless service is evolutionary, not revolutionary, because most of the technology already exists.

The HALO Network can be thought of as a "tall-tower" approach that provides better line-of-sight to customers without the high cost of deploying and operating a satellite constellation. Unlike satellite systems, the airborne system concentrates all of the spectrum usage in certain geographic areas, which minimizes frequency coordination problems and permits sharing of frequency with ground-based systems.

Operations at millimeter wave (MMW) frequencies enables broadband systems to be realized by providing spectrum bandwidth of one to six GHz. MMW systems also permit very narrow beamwidths to be realized with small aperture antennas.

The HALO Network can utilize a cellular pattern on the ground. The entire bandwidth will be reused many times to achieve total coverage throughout a 2800 square

mile area served by the airborne platform. The total capacity of the network supported by a single airborne platform could be greater than 100 Gbps.

The network architecture of the system is described as follows: the payload of the HALO aircraft becomes the hub of the star topology network for routing data packets between any two subscribers possessing necessary equipment within the service coverage area. Information created outside the service area is delivered to the subscriber's consumer necessary equipment through business necessary equipment operated by businesses, Internet service providers, and through the HALO Gateway equipment directly connected to the distant metropolitan areas via leased trunks.

The authors end by stressing that the HALO Network is capable of providing high rate communications to users of the multimedia and broadband services.

11. Maltz, D.A.; Broch, J.; Jetcheva, J.; Johnson, D. B.; "The effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks," paper appears in Selected Areas in Communications, IEEE Journal on Volume:17, Aug.1999, Pages: 1439-1453

In this paper the authors present a detailed examination of the performance of on-demand routing protocols. They analyzed the latency of route discovery, the cost of route discovery, and the effect of on-demand behavior on routing cache consistency, drawing on their examples for study from the Dynamic Source Routing (DSR) protocol.

As communicating nodes, or those between them that are forwarding packets, move about, the routing protocol in use in the network must adapt its routing decisions to enable continued communication between the nodes. The rate of topology change, and thus the rate of routing protocol reaction, may be different. A number of protocols are described as based on on-demand behavior, providing for dynamic adoption to the level

of routing protocol activity required to correctly handle the offered traffic. By on-demand behavior, the authors mean approaches based on reaction to the presence of data packets. The use of strictly periodic or time-based activity, such as typical router advertisements, is not considered here.

The authors pose three questions that apply in general to any wireless ad hoc network routing protocol based on on-demand behavior.

- *What effect does on-demand routing have on packet latency?*

An on-demand routing protocol attempts to discover a route to a destination only when it is presented with a packet for forwarding to that destination. This discovery must be completed before the packet can be sent, which adds to the latency of delivering the packet. Indeed, some mechanisms used to reduce the overhead cost of discovering a new route may result in an increase in latency for some route discovery attempts.

- *What is the overhead cost of on-demand routing behavior?*

Without additional information, a protocol using on-demand routing must search the entire network for a node to which it must send packets, but does not know how to reach. Optimizations to the protocol may reduce the cost of initiating communication, but discovering a new route is likely to remain a costly operation.

- *When caching the results of on-demand routing decisions, what is the level and effect of caching and cache correctness on the routing protocol?*

Any on-demand routing protocol must utilize some type of routing cache in order to avoid the need to rediscover each routing decision for each individual packet. However, the cache itself may contain out-of-date information indicating that links exist between nodes that are no longer within wireless transmission range of each other. This stale data

represents a liability that may degrade performance rather than improve it.

The DSR protocol is based entirely on-demand behavior. It is composed of two mechanisms: route discovery and route maintenance, each of which relies on on-demand behavior. When a node in the ad hoc network attempts to send a packet to some destination, if it does not already know a route to that destination, it uses route discovery to dynamically discover one. The route is cached and used as needed to send subsequent packets, each of which utilizes the route maintenance mechanism to detect if the route has broken, for example, due to two nodes along the route moving out of wireless transmission range of each other. Route discovery is only invoked when needed, and route maintenance operates only when actively using the route to send individual packets.

The routes that DSR discovers and uses are source routes. That is, the sender learns the complete ordered sequence of network hops necessary to reach the destination, and each packet to be routed carries this list of hops in its header. The key advantage of a source routing design is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they forward, since the packets themselves already contain all the routing decisions. This fact, coupled with the on-demand nature of the protocol, eliminates the need for the periodic route advertisement and neighbor detection packets present in other protocols.

Route Discovery works by flooding, and three optimizations are suggested for this mechanism: Nonpropagating route request that is only sent to the neighboring nodes, replying from cache that reduces latency and prevents ROUTE REQUESTS from flooding through the entire network, and gratuitous ROUTE REPLIES provide shorter routes to the source. Likewise, salvaging and gratuitous ROUTE ERROR are suggested

for the optimization of route maintenance. Finally, snooping and tapping are suggested for caching strategies.

The authors also described their methodology for simulation. They test the affects of latency, affects on overhead cost, and affects on cache consistency via simulation.

The simulation results indicate the twin techniques of using route caches to answer route requests and using nonpropagating requests to limit the search performed by the routing protocol can reduce the overall latency. Finally, they found that the cache is able to acquire useful information about the overall network topology solely by extracting routing information from packets that pass through and near it. Finally, they pointed out that efficient route maintenance is critical in all systems with route caches.

12. Zygmunt J.H., Tabrizi, S.; "On Some Challenges And Design Choices in Ad-Hoc Communications," paper appears in Military Communications Conference in 1998, MILCOM 98 Proceedings., IEEE Volume:1, 1998, Pages : 187-192

In this article, the authors discuss some of the challenges and choices that need to be made while designing an ad hoc network. They particularly address hierarchical vs. flat network architectures, proactive vs. reactive (on-demand) routing protocols vs. a hybrid approach, and sensing-based vs. dialog-based medium access control issues.

Three main challenges in the design and operation of the ad hoc networks stem from the following: the lack of a centralized entity, the possibility of rapid platform movements, and the fact that all the communication is carried over the wireless medium. Lack of these entities in the ad hoc networks requires more sophisticated distributed algorithms to perform these functions.

Because of the possibly rapid movement of the nodes and fast changing propagation conditions, network information such as routing becomes quickly obsolete. Additionally, as the wireless bandwidth is limited, its use should be minimized. Finally, as some of the mobile devices are expected to be hand-held with limited power, the required transmission power should be minimized as well.

The configuration of ad hoc networks can be either hierarchical or flat. In a hierarchical network, routing traffic between two nodes that are in two different clusters is always through the cluster heads of the source and destination. In a flat ad hoc network, all nodes are equal. Connections are established between nodes that are in close enough proximity to allow sufficient radio propagation conditions to establish connectivity.

One of the biggest advantages of the flat networks of is in the existence of multiple paths between a source and a destination, reducing congestion and eliminating possible traffic "bottleneck" in the network. In addition, QOS-based routing is possible. Nodes in flat networks transmit at a significantly lower power than the transmission power of the cluster heads in the hierarchical networks. This maintains low output power of nodes, the reuse of the wireless spectrum, and both a low probability of interception and low probability of detection. On the other hand, routing in hierarchical networks is often sub-optimal. The main advantage of the hierarchical ad hoc network is the ease of mobility management.

As the nodes become more mobile, the lifetime of a link decreases. Thus, the period in which the routing information remains valid decreases as well. In general, the existing routing protocols can be classified either as proactive or as reactive. Proactive

protocols attempt to continuously evaluate the routes within the network, so that when a packet needs to be forwarded, the route is already known and can be immediately used. Reactive protocols, on the other hand, invoke a route determination procedure on demand only. Thus, when a route is needed, some sort of global search procedure is employed. The classical flood search algorithms are reactive protocols. Because of long delay and excessive control traffic, pure reactive routing protocols may not be applicable to real-time communication. However, pure proactive schemes are likewise not appropriate for the ad hoc network environment, as they continuously use a large portion of the network capacity to keep the routing information current.

What is needed is a protocol that initiates the route-determination procedure on-demand, while minimizing the search cost. The Zone Routing Protocol (ZRP) is a hybrid reactive/proactive routing protocol. It limits the scope of a proactive procedure only to the node's local neighborhood. The search throughout the network, although it is global, is done by effectively querying only selected nodes in the network, as opposed to querying all network nodes.

Because of the possible large size of ad hoc networks, much larger than the transmission range of a single transmitter, single shared channels will not perform well in this environment. What is required is a protocol that resolves the collision based on the state of the channel at the receiver but provides a constant indication of the status of the channel, so that when a mobile node migrates within range of the transmitting/receiving node, the mobile node's transmission does not interfere with the transmission in progress. The Dual Busy Tone Multiple Access (DBTMA) protocol supports exactly this type of operation.

While the interest in the ad hoc networks continues to grow both in the military and the commercial markets, it is expected that the three basic issues addressed in this article will provide some guidance in the making choices for implementing such networks.

13. Johnson, D.B., Maltz, D.A.; "Protocols for Adaptive Wireless and Mobile Networking," paper appears in IEEE Personal Communications in 1996, Volume :31, Feb 1996, Pages: 34-42

The authors' work will enable mobile hosts to communicate with each other and with stationary or wired hosts, transparently making the most efficient use of the best network connectivity available to the host at any time.

With hierarchical addressing and routing, packets sent to a mobile host can only be routed to the mobile host's home network regardless of the host's current location, possibly away from home. A mobile host could perhaps change its address as it moves from one network to another, but it requires all existing transport-level network connectivity be restarted or the host to be rebooted.

Each mobile host must have a home agent on its home network, which forwards IP packets to the mobile host while it is away from home. Each mobile host must have a care-of address, when visiting any network away from home. Normally, the care-of address is the address of a foreign agent. The foreign agent delivers packets forwarded for the mobile host to it on the local network. Optionally, if a mobile host can acquire a temporary IP address within the local subnet as its care-of address. Packets tunneled to the mobile hosts are tunneled to this temporary address, while the mobile host continues to use its home address for all other functions.

To find a foreign agent with which to register, an agent discovery protocol is used. Agent discovery also provides a means for a mobile host to detect when it has moved within the range of different wireless networks. When moving to a new location, a mobile host must have registered with its home agent so that the home agent always knows the mobile host's current care-of address. The association between a mobile host's home address and its care-of address is called a mobility binding. Each binding has associated with it a lifetime period, after which the registration is deleted.

While a mobile host is registered with a care-of address away from home, the mobile host's home agent must intercept any packets on its home network address to the mobile host. For each such packet that is intercepted, the home agent encapsulates the packet and tunnels it to the mobile host's care-of address. The encapsulated packet reaches the foreign agent and the foreign agent removes the added header and transmits the packet to the mobile host over the local network interface on which the mobile host is registered.

The indirect routing through the home agent generally causes unnecessary overhead on the home network and on the portion of the internet leading to and from the home network, and causes unnecessary latency in the delivery of each packet to the mobile host. The authors suggest a route optimization mechanism that permits other hosts or routers sending packets to a mobile host to dynamically learn and cache the mobile host's current location; the sending node can then tunnel its own packets directly to the mobile host, bypassing the trip to and from the home agent. In this procedure, when a home agent intercepts and tunnels a packet to a mobile host away from home, the home agent also returns a binding update message to the original sender of the packet.

This allows the sender to cache the current binding of the mobile host and to tunnel its own packets to the mobile host in the future. The main challenge will be to address cache consistency. When a mobile host moves to a new location, all cached copies of its binding at the corespondent host become out of date. In this case, the mobile host sends it new care-of address via a binding update to its previous foreign agent. The previous foreign agent forwards incoming packets to mobile host's new address, and it also sends a binding warning message to the mobile host's home agent to request it to send a binding update message to the correspondent host.

A further challenge in the route optimization is that of authentication. It is managed by key a distribution mechanism on the Internet. Without sharing secret keys, the communicating units will not allowed to use routing optimization.

Unlike stationary routing, host mobility and wireless networks require us to rethink design strategies and decisions at every level of the protocol strategy.

14. Broch, J., Maltz, D.A., Johnson, D.B; "Supporting Hierarch and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks," paper appears in Parallel Architectures, Algorithms, and Networks, 1999, Proceedings Fourth International Symposium, Pages: 370-375

In this article, the authors describe a technique that allows a single ad hoc network to span across heterogeneous link layers. Using this technique, it is possible to both integrate ad hoc networks into the hierarchical Internet and support the migration of mobile nodes from the Internet into and out of ad hoc networks via Mobile IP.

In an ad hoc network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct transmission range of each other.

The Dynamic Source Routing (DSR) protocol works by discovering and using source routes. That is, the originator of a packet first learns the complete, ordered sequence of network hops necessary to reach the destination, and each packet sent carries this list of hops in its header.

Among the most basic properties of a network is the manner in which the nodes of the network are assigned the addresses by which other nodes will communicate with them. In the most general case, each node in an ad hoc network will be acting as an independent router. This implies that the addressing scheme inside an ad hoc network should ideally be flat, meaning that each address serves only as an identifier and does not convey any in formation about where one node is topologically located with respect to any other node.

In the addressing architecture, the authors suggest that each node in the ad hoc network should have a single identifier by which it is known to all other nodes in the network. This allows each node to be recognized by all other nodes in the network as a single entity regardless of which interface they use to communicate with it. Under the suggested addressing architecture, each node locally assigns a unique interface index to each of its network interfaces. These index values are local to each node, and the index values chosen by a node have no meaning outside of that node except to represent a unique network interface. This eliminates the need to agree globally on a mapping between interface indices and interface types and allows nodes to encode extra information that is locally significant into an index value.

The home addresses are assigned from the same legal IP subnet. In this way, although it is flat, a single ad hoc network acts as a subnet within the hierarchy of the IP

Internet. This addressing architecture gives DSR the ability to treat the overall network as a single routing domain since the use of interface indices allows a source route, and thus a route discovery, to traverse interface types.

The suggested addressing architecture handles heterogeneous interfaces on the nodes. Moreover, it solves the problem of connecting an ad hoc network to the Internet. Since routing within the ad hoc network is flat, and routing within the Internet is hierarchical, it is necessary to provide the illusion to the outside world that the ad hoc network is simply a normal IP subnet. Local delivery within the ad hoc subnet is accomplished using the DSR protocol while standard IP routing mechanisms decide which packets should enter and leave the subnet. According to the mechanism described by the authors, nodes inside the ad hoc network can discover routes that allow them to send packets to nodes outside the networks. Each gateway can act as a proxy replier for nodes in their cloud. This decreases the latency of route discovery.

According to the authors, it is also possible to integrate this addressing architecture with Mobile IP. Consider an ad hoc wireless network that is connected to the Internet, and a mobile node whose home network is not the ad hoc network. The mobile node will keep its network interface in promiscuous receive mode and understands that it has entered a DSR network. After completing the classical Mobile IP procedures –agent advertisement, registration- the mobile node's home agent will use Mobile IP to tunnel packets destined for the mobile node to a multi-homed gateway (foreign agent); this gateway will deliver the packets locally to the mobile node using DSR.

The suggested scheme works well under the conditions of overlapping ad hoc clouds, wandering nodes, and cooperating ad hoc clouds to obtain the best performance.

The techniques described in the article successfully enable the use of heterogeneous interfaces, the integration of an ad hoc network into the Internet as a subnet, and the movement of mobile nodes into and out of an ad hoc network using Mobile IP. However, there are still some unresolved issues. The communication between different administrative domains and the complete destruction of home agents are but two of them, and the authors remark that they are currently addressing these issues.

15. Iwata,A.;Ching-ChuanChiang; Guangyu Pei; Gerla, M.; Tsu-Wei Chen ; "Scalable routing strategies for ad hoc wireless networks," paper appears in Selected Areas in Communications, IEEE Journal on Volume: 17 8 , Aug. 1999 , Page(s): 1369 -1379

In this article, the authors investigate routing strategies that scale well to large populations and can handle mobility. In addition, they address the need to support multimedia communications, with requirements for low levels of for latency interactive traffic and quality-of-service (QoS) support for real-time streams (voice/video).

A fundamental assumption in ad hoc routing networks is that all nodes are "created equal," and therefore any node can be used to forward packets between arbitrary sources and destinations. The routing strategies suggested by the authors focus on scalability for large number of nodes and mobility of these nodes. The problem is particularly challenging because of the presence of both large numbers of nodes and their mobility. If nodes are stationary, the large population can be managed using conventional hierarchical routing. In contrast, when nodes move, the hierarchical partitioning must be continuously updated—a significant challenge and source management overhead. Mobile IP solutions work well if there is a fixed infrastructure supporting the concept of the "home agent." When all nodes move (including the home

agent), such a strategy cannot be directly applied.

Before describing their solution, the authors refer to current routing schemes. They classify prior work into three broad categories: global precomputed routing, on-demand routing, and flooding. Global precomputed routing schemes can be subdivided into two further categories: flat and hierarchical. On-demand routing is the most recent entry in the class of scalable wireless routing schemes. It is based on a query reply approach. Flat routing schemes do not scale well to large networks. On-demand routing does scale, but has limitations in terms of latency and QoS support. Hierarchical routing is overhead prone and quite complex to maintain.

The authors' proposed approach is based on the applications of hierarchical routing principles (implicit or explicit) onto a global routing algorithm. They explore two different schemes, namely: 1) Fisheye State Routing (FSR) and 2) Hierarchical State Routing (HSR).

FSR scales well to large networks, by keeping Link State (LS) exchange overhead low without compromising route computation accuracy when the destination is near. By retaining a routing entry for each destination, FSR avoids the extra work of "finding" the destination (as in on-demand routing) and thus maintains low single packet transmission latency. As mobility increases, routes to remote destinations become less accurate. However, when a packet approaches its destination, it finds increasingly accurate routing instructions as it enters sectors with a more frequent refresh rate.

HSR maintains a hierarchical topology, where elected cluster heads at the lowest level become members of the next higher level. These new members in turn organize themselves in clusters and so on. The goals of clustering are the efficient utilization of

radio channel resources and the reduction of network-layer routing overhead (i.e., routing-table storage, processing, and transmission). In addition to multilevel clustering, HSR also provides multilevel logical partitioning. While clustering is based on a geographical (i.e., physical) relationship between nodes (hence, it will be referred to as physical clustering), logical partitioning is based on logical functional affinity between nodes (e.g., employees of the same company, members of the same family, etc.). Logical partitions play a key role in location management.

In real-time applications (e.g., IP telephony) it is beneficial for the source to know, prior to call set up, not only the path to the destination, but also the average data rate available/achievable on such path. In an ad hoc wireless network, the MAC layer is generally responsible for monitoring channel quality and available bandwidth. For example, consider a network with MAC-layer clustering and token access protocol. The cluster head can monitor both local and transit traffic in the cluster. It can also monitor channel quality (error rate, etc.). It can distinguish between real-time and data traffic and can determine the amount of bandwidth still available for voice (high priority) traffic. In ad hoc networks that do not use clustering, the monitoring of available resources is more complex, but can still be accomplished. In order to include QoS monitoring in the routing process, it suffices to extend the definition of LS by also adding the link entry bandwidth and channel quality information. In this regard, both FSR and HSR are "QoS ready" in that they are both based on the LS routing model.

The home addresses are assigned from the same legal IP subnet. In this way, although it is flat, the single ad hoc network acts as a subnet within the hierarchy of the IP Internet. This addressing architecture gives DSR the ability to treat the overall

network as a single routing domain since the use of interface indices allows a source route, and thus a route discovery, to traverse interface types.

16. Lee, S., Gerla M., Toh, C.; "A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks," paper appears in IEEE Network, Volume: 134, July-Aug. 1999, Pages:48-54

In this article, the authors compare table-driven and on-demand routing protocols in a common network environment. They find Associatively-Based Routing (ABR) as a strong candidate for a multihop wireless environment along with Dynamic Source Routing (DSR).

The authors, first, review the key properties of three distinct routing mechanisms. They briefly described Distributed Bellman-Ford (DBF) and DSR protocols. Then, they provide overview of the ABR protocol.

ABR is an on-demand routing protocol like DSR. The uniqueness of this scheme is the route selection criteria. By exploiting the spatial and temporal relationship of mobile hosts, ABR introduces the following new routing metrics:

- Longevity of a route based on associativity
- Route relaying load of intermediate nodes supporting existing routes
- Link capacities of the selected route

ABR has a route discovery and a route reconstruction phase. These phases are similar to the route discovery and route maintenance phases of DSR. In each node three different kinds of tables are stored during the operation. *Routing table* contains routing information for nodes that are actually required by the source. *Neighbor table* maintains

the node's associativity relationship with surrounding neighborhood. *Seen table* prevents a mobile node from processing and forwarding the same message multiple times.

Key characteristics and properties of DBF, DSR, and ABR are summarized in the following Table 6:

PROTOCOLS	DBF	DSR	ABR
Route establishment	Proactive	On-demand	On-demand
Routing metric	Shortest path	Shortest path	Associativity, load, delay, etc.
Periodic messages	Routing tables	None	Beacons
Loop-free	No	Yes	No

Table 6. Comparison of DBF, DSR, and ABR Routing Protocols.

Performance evaluation of the three schemas is done by simulation. The authors used the Global Mobile Simulation (GloMoSim) library, which is a scalable simulation environment for wireless network systems using the parallel discrete-event simulation. Their parameters of interest are control overhead, data throughput, and end-to-end packet propagation delay. Table 7 describes their simulation results (R is the average number of active nodes, and N is the total number of nodes in the network):

In routing protocols that use the shortest hop or delay as a route selection metric, some nodes need to support many routes. These nodes continuously consume energy, which will eventually be exhausted, resulting in node failures. Route selection considerations also include energy reserves. ABR uses route-relaying load as one of its metrics and prevents node failures of this kind. However this is not the case for DSR.

PROTOCOLS	DBF	DSR	ABR
Control Message Overhead	Bad	Good	Better
Data Throughput	Poor	Good	Better
End-to-End Delay	Bad	Good	Better
Table Storage Overhead	3N	$R\sqrt{N} + 4R$	5R+1
Low Detection/Interception Probability	Bad	Better	Bad
Low Power Operation	Bad	Better	Bad

Table 7. Simulation Results of DBF, DSR, and ABR Routing Protocols.

The authors point out that ABR is a strong candidate for the multihop mobile wireless environment along with DSR. Both of these protocols place an emphasis on-demand routing scheme, taking into account other considerations in addition to the measures obtained via simulation.

17. Racherla, G., Chilakalapudi, S., "SatSim – A Simulator for Mobile Satellite Networks," paper appears in IEEE in 1999

In this article, the authors present a modular simulation environment for mobile satellite networks.

Satellite systems, especially LEO (Low Earth Orbiting) Satellites are being used to increase the global coverage of communications to a wider customer base. These systems can support both terrestrial wired and wireless networks and have a great advantage in that they can be used to provide services to regions of the globe where building a terrestrial infrastructure is not possible because of economic or demographic reasons (e.g. areas of low-density population).

An important aspect of the wireless satellite communications is the handovers. Since a satellite is moving continuously, its coverage area also keeps changing. In order to maintain continuous connectivity between a source and a destination, satellites need to perform "handovers" among one another so that continuity of service is maintained. The routing and re-routing algorithms for satellite networks draw inspiration from the routing and re-routing algorithms for terrestrial wireless systems. Among the proposed re-routing algorithms for satellite networks is the Footprint Handover Re-route Protocol (FHRP).

The authors point out the unavailability of a dedicated satellite network simulation tool. Therefore, they propose and have implemented a modular simulation environment for mobile satellite networks. This work follows their simulator, MadSim, for wireless ad hoc networks.

The article concludes that most of the simulation environments used currently are too general, cumbersome, and inadequate for designers who want to either prototype or validate mobile satellite networks. Since current simulation languages/tools are too general for mobile satellite networks, they are slow when compared with specialized tools such as SatSim.

18. Ettus, M., "System Capacity, Latency, and Power Consumption in Multihop-routed SS-CDMA Wireless Networks," article appears in IEEE in 1998

In addition to high error rates and constantly varying channels, mobile communication imposes new constraints, including limiting energy supplies, and the need for portability. In this article, the authors present a system for wireless networking that utilizes code division multiple access (CDMA), in conjunction with spread spectrum (SS)

modulation. Moreover, a new routing method, minimum consumed energy routing (MCER) is evaluated.

Providing high throughput and low latency, efficiently using the shared spectrum, and conserving power are difficult to achieve goals in ad hoc wireless networks. Scaling of these networks often leads to poor responsiveness, collision, and even congestion collapse.

The new system differs from traditional SS-CDMA systems in both its routing and channel access mechanisms. When CDMA is used, stations are able to transmit at the same time, and thus no coordination across the network is necessary. The near-far problem is solved by local coordination. By using automatic power control in conjunction with spread spectrum modulation, an energy efficient, as well as spectrum efficient, system can be created which is capable of simultaneously providing high-bandwidth and low-latency communications.

In a multihop wireless network, congestion and latency may rise dramatically with increasing network size, due to the increased number of stations traversed by packets en route to their destination. A new method, minimum consumed energy (MCE) routing, was developed to solve these problems as well as save energy in mobile units. In stead of routing based on minimizing the total energy transmitted along a packet's path (as in minimum transmitted energy routing), total energy consumption is used as the metric.

In order to validate the suggested system a simulator, SSNetSim, was developed. SSNetSim allows an entire network of stations, each with its own traffic, to be accurately simulated. MCE routing causes packets to take fewer hops through the network. Fewer

transmissions are necessary, thus reducing congestion. Also, there are fewer heavily loaded stations, and the load is spread much more evenly, helping to reduce congestion and latency. MCE routing was shown to reduce total network power consumption by about 15%, reduce latency by 75%, and reduce congestion by 75%, over the standard minimum energy routing.

The article concludes that the use of minimum consumed energy routing optimizes mobile unit battery life, as well as providing a good compromise for latency and bandwidth, to provide for high throughput.

REF. NO	App.		ACCESS								ROUTING													
	Military	Civilian	TDMA	FDMA	CSMA	ODMA	CDMA	SS-	W-	DBTMA	DSR	OSPF	ZRP	FSR	HSR	GSR	ABR	MTE	MCE	Simulation /Model	SECURITY	INTERNET MOBILE	POWER CONS.	QoS
1	X					X																		
2	X	X																			X			
3	X				X							X										X		
4		X	X				X		X													X	X	X
5			X				X													X				
6			X				X																	
7	X																			X		X		X
8	X				X															X		X		
9																					X	X		
10		X																		X				
11											X									X				
12					X		X			X			X							X			X	X
13		X									X									X	X	X		
14											X									X		X		
15											X			X	X	X				X				X
15											X						X			X		X		X
17		X																		X				
18							X	X										X	X	X				

Table 8. Overview of Literature Review.

APPENDIX B. DIRECT ACTION SCENARIO

Two special operations (SF) teams will conduct a direct action (DA) mission against the enemy air control radar (Target A) and the air defense unit (Target B). The two targets are 1800 meters apart from each other. The assault will be conducted concurrently, in coordination with Operations Center (OC), where the battalion commander is also located. After the targets are consolidated, the engineer NCOs will locate demolition charges, and will fuse with the order of detachment commanders.

At the beginning of the scenario, they have already traversed several hundred meters. They will now execute one additional movement drill, which will place them in the last covered and concealed position prior to the objectives. Once in the assault position, the second buddy group led by EO will lay down suppressive fires, while the two flank buddy groups will attack the respective flanks of the targets.

The final assault carries high risk of injury. We have built into the scenario a serious wound, which will require medical attention and subsequent actions for evacuation.

During most of the movement drills, the special operators will be alternately running forward and then taking up a prone position. In the final assault phase, the second buddy group will be primarily lying prone, while the others will be upright and running forward.

Notes:

1. Transmissions would normally include call signs, but we have not included any of that normal traffic here in the interest of space.

2. Organization of a typical SF team is as follow:

   Detachment Commander

   Executive officer (EO)

   Operations Sergeant (OS)

   Operations & Intelligence NCO (IS)

   Weapons NCO (W)

   Assistant Weapons NCO (AW)

Assistant Weapons NCO (AW)

Engineer NCO (E)

Assistant Engineer NCO (AE)

Medical NCO (M)

Assistant Medical NCO (AM)

Communications NCO (C)

Assistant Communications NCO (AC)

3. During the assault, there would normally not be many radio transmissions – there would be a conscious attempt to use radio listening silence, or, at a minimum, use arm and hand signals as much as possible. But for this exercise, with a focus on communication capabilities, some radio transmissions have been scripted which might normally not occur.

4. A and B stands for the Team A and the Team B, the two different operating teams.

WHO SPEAKS TO WHOM		MESSAGE	SIZE (BYTES)	BEGINNING TIME
OC	A	MOVE	100	5S
OC	B	MOVE	100	5010MS
A	EO-A	MOVE	100	8S
B	EO-B	MOVE	100	9S
EO-A	A	SET	100	25S
EO-B	B	SET	100	27S
A	IS-A	MOVE	100	27S
A	OS-A	MOVE	100	27S
B	IS-B	MOVE	100	30S
B	OS-B	MOVE	100	30S
OS-A	A	SET	100	46S
IS-A	A	SET	100	53S
OS-B	B	SET	100	53S
IS-B	B	SET	100	54S
A	OC	SET	100	55S
B	OC	SET	100	55S
OC	IS-A	LAST CONDITION OF THE TARGET AREA	100	58S
OC	IS-B	LAST CONDITION OF THE TARGET AREA	100	59S
IS-A	OC	PICTURE	100K	1M
IS-B	OC	PICTURE	100K	3M

OC	A	BEGIN	100	4M
OC	B	BEGIN	100	4M
A	EO-A	LAY DOWN SUPRESSIVE FIRE	200	190S
B	EO-B	LAY DOWN SUPRESSIVE FIRE	200	200S
A	IS-A	CONDUCT ASSAULT ON LEFT FLANK	200	201S
A	OS-A	CONDUCT ASSAULT ON RIGHT FLANK	200	207S
IS-A	A	WILCO	100	208S
OS-A	A	WILCO	100	209S
B	IS-B	CONDUCT ASSAULT ON LEFT FLANK	200	210S
B	OS-B	CONDUCT ASSAULT ON RIGHT FLANK	200	215S
IS-B	B	WILCO	100	218S
OS-B	B	WILCO	100	220S
A	IS-A	GO, NOW!	100	245S
A	OS-A	GO, NOW!	100	245S
B	IS-B	GO, NOW!	100	245S
B	OS-A	GO, NOW!	100	245S
AE-A	M-A	NEED MEDIC FOR W	200	250S
M-A	AE-A	ROGER. ON THE WAY!	200	252S
IS-A	EO-A/A/OC	WE'RE AT THE TARGET.	200	260S
IS-B	EO-B/B/OC	WE'RE AT THE TARGET.	200	263S
EO-A	C-A	MOVE FORWARD TO THE TARGET AREA	200	265S
EO-B	C-B	MOVE FORWARD TO THE TARGET AREA	200	265S
W-B	M-B	NEED MEDIC FOR E.	200	270S
M-B	W-B	COMING RIGHT NOW!	200	272S
EO-A	IS-A/OS-A	MOVE 250 M. NORTH/SOUTH FOR OP.	600	295S
EO-B	IS-B/OS-B	MOVE 250 M. NORTH/SOUTH FOR OP.	600	297S
EO-A	A	MOVING TO THE TARGET AREA	200	340S
EO-B	B	MOVING TO THE TARGET AREA	200	340S
OS-A	EO-A	OP READY.	100	360S
IS-A	EO-A	OP READY.	100	360S
OS-B	EO-B	OP READY.	100	363S
IS-B	EO-B	OP READY.	100	363S
EO-A	A	HAVE SEIZED THE OBJECTIVE	200	410S
EO-B	B	HAVE SEIZED THE OBJECTIVE	200	415S
M-B	OC	E-B HAS SEVERE CHEST WOUND AND MUST BE EVACUATED	400	425S
OC	M-B	APPROVED. HELO IS COMING	300	430S
EO-A	OC	KILLED FIVE ENEMY SOLDIERS. ESTIMATE THREE ENEMY SOLDIERS WITHDREW TO THE SOUTH. RELATED PERSONNAL PREPARING THE DEMOLITION CHARGES. HAS 2 OP AT 200 M.	1K	600S
EO-B	OC	KILLED FIVE ENEMY SOLDIERS. ESTIMATE THREE ENEMY SOLDIERS WITHDREW TO THE SOUTH. RELATED PERSONNAL PREPARING THE DEMOLITION CHARGES. HAS 2 OP AT 250 M.	1K	620S
C-A	OC	ENCRYPTED FILE TRANSFER	5 ITEMS	625S
C-B	OC	ENCRYPTED FILE TRANSFER	5 ITEMS	630S

IS-B	B	IMAGERY REPORTS FROM OP.	10240	640S
OS-B	B	IMAGERY REPORTS FROM OP.	10240	660S
IS-A	A	IMAGERY REPORTS FROM OP.	10240	665S
OS-A	A	IMAGERY REPORTS FROM OP.	10240	685S
E-A	A	CHARGES ARE READY	100	686S
E-B	B	CHARGES ARE READY	100	700S
A	OC	TEAM IS READY FOR DEMOLITION	100	701S
B	OC	TEAM IS READY FOR DEMOLITION	100	705S
A	E-A	FIRE AND OBSERVE 100M BEHIND	100	710S
B	E-B	FIRE AND OBSERVE 100M BEHIND	100	710S
EO-A	A/OC	MISSION IS ACCOMPLISHED	100	730S
EO-B	B/OC	MISSION IS ACCOMPLISHED	100	731S
A	EO/IS/OS	WITHDRAWAL.	200	735S
B	EO/IS/OS	WITHDRAWAL.	200	735S

APPENDIX C. GLOMOSIM FILE FORMATS

CONFIG.IN

```
# Glomosim is COPYRIGHTED software.  It is freely available without fee for
# education, or research, or to non-profit agencies. No cost evaluation
# licenses are available for commercial users. By obtaining copies of this
# and other files that comprise GloMoSim, you, the Licensee, agree to abide
# by the following conditions and understandings with respect to the
# copyrighted software:
#
# 1.Permission to use, copy, and modify this software and its documentation
#   for education, research, and non-profit purposes is hereby granted to
#   Licensee, provided that the copyright notice, the original author's names
#   and unit identification, and this permission notice appear on all such
#   copies, and that no charge be made for such copies. Any entity desiring
#   permission to incorporate this software into commercial products or to use
#   it for commercial purposes should contact:
#
#   Professor Rajive Bagrodia
#   University of California, Los Angeles
#   Department of Computer Science
#   Box 951596
#   3532 Boelter Hall
#   Los Angeles, CA 90095-1596
#   rajive@cs.ucla.edu
#
# 2.NO REPRESENTATIONS ARE MADE ABOUT THE SUITABILITY OF THE SOFTWARE FOR ANY
#   PURPOSE. IT IS PROVIDED "AS IS" WITHOUT EXPRESS OR IMPLIED WARRANTY.
#
# 3.Neither the software developers, the Parallel Computing Lab, UCLA, or any
#   affiliate of the UC system shall be liable for any damages suffered by
#   Licensee from the use of this software.
#
# $Id: CONFIG.IN,v 1.28 1999/10/16 01:14:59 hxy Exp $
#
# Anything following a "#" is treated as a comment.
#
#
#The following two parameters stand for the physical terrain in which the nodes
#are being simulated. For example, the following represents an area of size 100
#meters by 100 meters. All range parameters are in terms of meters.
#
# Terrain Area we are simulating.
TERRAIN-RANGE-X     1000
TERRAIN-RANGE-Y     600
#
#The following parameter represents the power range of wireless nodes in the
#simulation. For example, a node can reach any other node within 50 meters of
#its position.  The user must specify either a power range value as shown
#below or the transmission power value.  If the user specifies a power
#range other than 250 meters, a new transmission power will be calculated
#using the free space propagation model and the new power range.
#
POWER-RANGE         250
#
#The following parameter represents the transmission power of the wireless
```

```
#nodes in the simulation.  For example, a node transmits with a power of
#12 dBm as stated below.  This specific value was calculated using a 250m
#power range.  Changing this value will cause the recalculation of the power
#range using the free space propagation model and the new transmission power.
#
#RADIO-TX-POWER       12
#
#
#The following represents the number of partitions (or entities) used to
#represent the terrain in which the simulation is being simulated. Generally,
#the higher the number of partitions in your simulation the faster your
#simulation will run. Of course, this is only true upto a certain limit. For
#example, if you have a 100 by 100 region and try to run your simulation with
#(100 * 100) partitions your simulation will run slowly. As a rough estimate
#try to set the length and width of each partition such that it is greater than
#the power range of a radio.
#
#NOTE: THIS IS NOT CURRENTLY SUPPORTED IN THE DISTRIBUTED VERSION
#
# Number of partitions in x and y range.
PARTITION-NUM-X     1
PARTITION-NUM-Y     1
#
#
#The following is a random number seed used to initialize  part of the seed of
#various randomly generated numbers in the simulation. This can be used to vary
#the seed of the simulation to see the consistency of the results of the
#simulation.
#
SEED                1
#
#The folowing parameter represents the maximum simulation time. The numberd
#portion can be followed by optional letters to modify the simulation time.
#For example:
#        100NS   - 100 nano-seconds
#        100MS   - 100 milli-seconds
#        100S    - 100 seconds
#        100     - 100 seconds (default case)
#        100M    - 100 minutes
#        100H    - 100 hours
#        100D    - 100 days
#
SIMULATION-TIME     1600S
#
#
#The following parameter represents the number of nodes being simulated.
#The BBN uses 9 nodes. Reference Point model uses 12
#
NUMBER-OF-NODES     25
#
#
#The following parameter represents the node placement strategy.
#- RANDOM: Nodes are placed randomly within the physical terrain.
#- UNIFORM: Based on the number of nodes in the simulation, the physical
#  terrain is divided into a number of cells. Within each cell, a node is
#  placed randomly.
#- GRID: Node placement starts at (0, 0) and are placed in grid format with
#  each node GRID-UNIT away from its neighbors. The number of nodes has to be
#  square of an integer.
#- FILE: Position of nodes is read from NODE-PLACEMENT-FILE. On each line of
#  the file, the x and y position of a single node is separated by a space.
#
```

```
#NODE-PLACEMENT       GROUP_RANDOM
#NODE-PLACEMENT       RANDOM
#NODE-PLACEMENT       UNIFORM
#NODE-PLACEMENT       GRID
#GRID-UNIT            30
NODE-PLACEMENT       FILE
NODE-PLACEMENT-FILE ../bin/nodes.input
#
#
#The propagation models used for determining if a node is reachable:
#- Free Space: Predicts received signal strength when the transmnitter and
#  receiver have a clear, unobstructed line-of-sight path between them.
#  Received power decays as a function of the T-R separation distance.
#- Rayleigh Fading Distribution: The Rayleigh Fading Distribution is used to
#  describe the statistical time varying nature of the received envelope of a
#  flat fading signal, or the envelope of an individual multipath component.
#- Ricean Fading Distribution: When there is a dominant stationary (nonfading)
#  signal component present, such as a line-of-sight propagation path, the
#  small-scale fading envelope distribution is Ricean. In such a situation,
#  random multipath components arriving at different angles are superimposed on
#  a stationary dominant signal. At the output of an envelope detector, this
#  has the effect of adding a dc component to the random multipath. The effect
#  of a dominant signal arriving with many weaker multipath signals gives rise
#  to the Ricean distribution. As the dominant signal becomes weaker, the
#  composite signal resembles a noise signal which has an envelope that is
#  Rayleigh. Thus the Ricean distribution degenerates to a Rayleigh
#  distribution when the dominant component fades away.
#  The Ricean distribution is often described in terms of a parameter K which
#  is defined as the ratio between the deterministic signal power and the
#  variance of the multipath. It is given by:
#  K = (A^2) / (2*sigma^2) or, in terms of dB:
#  K(dB) = 10log((A^2)/(2*sigma^2)) (dB)
#  The paramter K is known as the Ricean factor and completely specifies the
#  Ricean distribution. As A->0, K->-infinity dB, and as the dominant path
#  decreases in amplitude, the Ricean distribution degenerates to a Rayleigh
#  distribution.
#  The formulas for computing these 3 propagation models were taken from:
#  "Wireless Communication", Chapters 3 & 4, by Theodore S. Rappaport.
#  You can look there for more detailed information about these models.
#
PROPAGATION-FUNC     FREE-SPACE
#PROPAGATION-FUNC     RAYLEIGH
#
#PROPAGATION-FUNC     RAYLEIGHMOBILITY
# RAYLEIGH_FADE_MARGIN only used for PROPAGATION-FUNC RAYLEIGHMOBILITY
# Range: 5.0, 10.0 15.0 20.0 25.0 dB
#RAYLEIGH_FADE_MARGIN 25.0
#
#
#PROPAGATION-FUNC     RICEAN
## RICEAN-K-FACTOR only used for PROPAGATION-FUNC RICEAN
#   Ratio between deterministic signal power and the variance of the multipath.
#   (range: -5.0dB to 20.0dB)
#RICEAN-K-FACTOR      6.0
#
#
#The following parameter represents the bandwidth (in bits per second) at which
#nodes will transmit messages.
#
BANDWIDTH            500000
#
#
```

```
#For some layers of the simulation, there are multiple protocols built into the
#simulation. You can specify the protocol that you are interested in by
#commenting out the protocols that you are not interested in. For example for
#the radio layer, we have radio with and without capture ability. For the MAC
#layer we have protocols for CSMA, MACA, and IEEE802.11. For the routing
#protocol we have Bellmanford and OSPF.
#
RADIO-TYPE           RADIO-NO-CAPTURE
#RADIO-TYPE           RADIO-CAPTURE
#
#MAC-PROTOCOL         CSMA
MAC-PROTOCOL         802.11
#
PROMISCUOUS-NODE       YES
NETWORK-PROTOCOL     IP
#
ROUTING-PROTOCOL     DSR
#ROUTING-PROTOCOL     BELLMANFORD
#ROUTING-PROTOCOL     WRP
#ROUTING-PROTOCOL     FISHEYE
#FISHEYE-FILE         FISHEYEConfig
#
#For the transport layer there are various protocols which can be used
#individually or concurrently. If you are only interested in simulating a
#particular protocol, you can place a "NO" for other protocols you are no
#interested in. This will probably make your simulation a little faster.
#
TRANSPORT-PROTOCOL-TCP  YES
TRANSPORT-PROTOCOL-UDP  YES
#
#
#The following is used to setup applications such as FTP and Telnet.
#The file will need to contain parameters that will be use to
#determine connections and other characteristics of the particular
#application.
APP-CONFIG-FILE      ../bin/app.conf
#
#
#The following parameters determine if you are interested in the statistics of
#a a single or multiple layer. By specifying the following parameters as YES,
#the simulation will provide you with statistics for that particular layer. All
#the statistics are compiled together into a file called "GLOMO.STAT" that is
#produced at the end of the simulation. If you need the statistics for a
#particular node or particular protocol, it is easy to do the filtering. Every
#single line in the file is of the following format:
#Node:      9, Layer:  RadioNoCapture, Total number of collisions is 0
#
APPLICATION-STATISTICS          YES
TCP-STATISTICS                  NO
UDP-STATISTICS                  NO
ROUTING-STATISTICS              YES
NETWORK-LAYER-STATISTICS        NO
MAC-LAYER-STATISTICS            YES
RADIO-LAYER-STATISTICS          NO
CHANNEL-LAYER-STATISTICS        NO
MOBILITY-STATISTICS             NO
#
#
#The following represent parameters for mobility. If MOBILITY is set to NO,
#than there is no movement of nodes in the model. For the other models, if a
#node is currently at position (x, y), it can possibly move to (x-1, y),
#(x+1, y), (x, y-1), and (x, y+1); as long as the new position is within the
```

```
#physical terrain. For random waypoint, a node randomly selects a destination
#from the physical terrain. It moves in the direction of the destination,
#moving one meter every MOBILITY-INTERVAL time period. After it reaches its
#destination, the node stays there for MOBILITY-PAUSE time period.
#For random drunken, a node randomly moves to one of its neighboring positions
#every MOBILITY-INTERVAL time period. The MOBILITY-PAUSE value does not affect
#the random drunken model.
#The MOBILITY-INTERVAL and MOBILITY-PAUSE values are represented in the same
#format as SIMULATION-TIME values.
#Currently the mobility models work only when there is a single partition in
#the simulation.
#
#MOBILITY  YES
#MOBILITY RANDOM-DRUNKEN
#MOBILITY RANDOM-WAYPOINT
# The following parameters are necessary for all the mobility models
MOBILITY-INTERVAL 1S
MOBILITY-D-UPDATE  1
#
# The following parameters are for Random_waypoint model
#MOBILITY-WP-PAUSE       100MS
#MOBILITY-WP-MIN-SPEED   0
#MOBILITY-WP-MAX-SPEED   6
MOBILITY TRACE
MOBILITY-TRACE-FILE        ../bin/mobility.in
#
#
# Propagation Function SIRCIM
# NOTE: THIS IS NOT CURRENTLY SUPPORTED IN THE DISTRIBUTED VERSION
#PROPAGATION-FUNC    SIRCIM
#
# TOPOGRAPHY only used for PROPAGATION-FUNC SIRCIM
#   OBSTRUCTED: Obstacles between source and destination
#   LINE-OF-SIGHT: Direct path between source and destination
#TOPOGRAPHY         OBSTRUCTED
#TOPOGRAPHY         LINE-OF-SIGHT
#
#
# BUILDING-TYPE only used for PROPAGATION-FUNC SIRCIM
#   OPEN-PLAN: Buildings such as factories and indoor sports arenas which have
#              mostly large open areas with a few large obstructions at various
#              locations within the building.
#   HARD-PARTITIONED: Typical multi-story office building with many internal
#                     partitions constructed of reinforced concrete or drywall.
#                     Corridors are typically six to ten feet wide. Walls which
#                     partition the offices from corricdors are constructed
#                     from the floor to the ceiling.
#   SOFT-PARTITIONED: Typical multi-story office building with large open areas
#                     that are partitioned into office cubicles by 5-foot-high
#                     movable cloth covered plastic dividers.
#BUILDING-TYPE      OPEN-PLAN
#BUILDING-TYPE      HARD-PARTITIONED
#BUILDING-TYPE      SOFT-PARTITIONED
#
#
#GUI-OPTION: YES allows GloMoSim to communicate with the Java Gui Vis Tool
#            NO does not
GUI-OPTION   YES
GUI-RADIO    YES
GUI-ROUTING  YES
```

NODES.IN

```
# INITIAL LOCATIONS OF 25 NODES
500 300
700 300
720 300
710 310
710 290
710 300
700 290
700 310
710 320
712 330
720 320
680 300
680 320
300 300
320 280
300 280
280 280
280 300
270 280
290 280
280 320
300 320
290 310
310 290
330 290
```

MOBILITY.IN

```
#
# mobility trace format:
# simclock node-address destination(x and y coordinates) speed[m/s]
# lines must be sorted in time increasing order
#
9S 5 760.0 300.0 10.0
9S 6 760.0 290.0 10.0
9S 7 760.0 310.0 10.0
12S 17 200.0 300.0 9.0
12S 18 200.0 290.0 9.0
12S 19 200.0 310.0 9.0
#MS 0 500.0 250.0 7.5
20S 11 740.0 290.0 8.0
20S 12 740.0 310.0 8.0
21S 23 220.0 290.0 8.0
```

```
21S 24 220.0 310.0 8.0
29S 2 820.0 140.0 10.0
29S 3 840.0 160.0 10.0
29S 4 860.0 120.0 10.0
29S 8 820.0 400.0 9.0
29S 9 860.0 390.0 9.0
29S 10 840.0 410.0 9.0
30S 14 160.0 160.0 9.0
30S 15 180.0 140.0 9.0
30S 16 120.0 180.0 9.0
30S 20 140.0 410.0 9.0
30S 21 160.0 420.0 9.0
30S 22 180.0 400.0 9.0
245S 2 960.0 300.0 11.0
245S 3 970.0 310.0 11.0
245S 4 980.0 250.0 11.0
245S 8 960.0 320.0 11.0
245S 9 950.0 310.0 11.0
245S 10 980.0 300.0 11.0
245S 14 20.0 290.0 10.0
245S 15 10.0 300.0 10.0
245S 16 90.0 210.0 10.0
245S 20 20.0 320.0 10.0
245S 21 25.0 320.0 10.0
245S 22 30.0 310.0 10.0
253S 18 90.0 215.0 16.0
265S 11 960.0 290.0 14.0
265S 12 960.0 290.0 14.0
265S 23 20.0 290.0 14.0
265S 24 20.0 310.0 14.0
273S 7 980.0 250.0 16.0
300S 2 960.0 20.0 12.0
300S 3 950.0 30.0 12.0
300S 8 960.0 570.0 12.0
300S 9 950.0 580.0 12.0
300S 10 970.0 580.0 12.0
310S 14 30.0 20.0 12.0
310S 15 20.0 30.0 12.0
310S 20 30.0 570.0 12.0
310S 21 20.0 580.0 12.0
310S 22 40.0 580.0 12.0
340S 5 955.0 290.0 10.0
340S 6 955.0 300.0 10.0
#340S 7 955.0 310.0 10.0
340S 17 40.0 290.0 10.0
340S 19 40.0 310.0 10.0
#341S 18 40.0 300.0 11.0
#OBSERVE
710S 17 140.0 290.0 12.0
710S 19 140.0 310.0 12.0
710S 23 120.0 290.0 12.0
710S 24 120.0 310.0 12.0
710S 5 855.0 290.0 12.0
710S 6 855.0 300.0 12.0
710S 11 860.0 290.0 12.0
```

```
710S 12 860.0 290.0 12.0
710S 7 880.0 250.0 14.0
710S 4 880.0 250.0 14.0
#WITHDRAW
736S 2 720.0 300.0 12.0
736S 3 710.0 310.0 12.0
736S 4 710.0 290.0 12.0
736S 5 710.0 300.0 12.0
736S 6 700.0 290.0 12.0
736S 7 700.0 310.0 12.0
736S 8 710.0 320.0 12.0
736S 9 712.0 330.0 12.0
736S 10 720.0 320.0 12.0
736S 11 680.0 300.0 12.0
736S 12 680.0 320.0 12.0
737S 14 320.0 280.0 12.0
737S 15 300.0 280.0 12.0
737S 16 280.0 280.0 12.0
737S 17 280.0 300.0 12.0
737S 18 270.0 280.0 12.0
737S 19 290.0 280.0 12.0
737S 20 280.0 320.0 12.0
737S 21 300.0 320.0 12.0
737S 22 290.0 310.0 12.0
737S 23 310.0 290.0 13.0
737S 24 340.0 300.0 12.0
#END
```

APP.CONF

```
CBR 0 1 2 250 100MS  5S 0S
CBR 0 13 2 250 100MS  5S 0S
CBR 1 5 2 250 100MS  8S 0S
CBR 13 17 2 250 100MS  9S 0S
CBR 5 1 2 250 100MS  25S 0S
CBR 17 13 2 250 100MS  27S 0S
CBR 1 2 2 250 100MS  27S 0S
CBR 1 8 2 250 100MS  27S 0S
CBR 13 14 2 250 100MS  30S 0S
CBR 13 20 2 250 100MS  30S 0S
CBR 8 1 2 250 100MS  46S 0S
CBR 2 1 2 250 100MS  53S 0S
CBR 20 13 2 250 100MS  53S 0S
CBR 14 13 2 250 100MS  54S 0S
CBR 1 0 2 250 100MS  55 0S
CBR 13 0 2 250 100MS  55S 0S
CBR 0 2 2 250 100MS 58S 0S
CBR 0 14 2 250 100MS 58S 0S
CBR 2 0 10 500 10MS 1M 0S
CBR 2 1 10 500 10MS 1M 0S
CBR 14 0 10 500 10MS 69S 0S
CBR 14 13 10 500 10MS 69S 0S
CBR 0 1 1 500 100MS 4M 0S
CBR 0 13 1 500 100MS 4M 0S
#lay down
```

```
CBR 1 5 4 250 100MS 190S 0S
CBR 13 17 4 250 100MS 200S 0S
#conduct left/right flank
CBR 1 2 2 500 100MS 201S 0S
CBR 1 8 2 500 100MS 207S 0S
CBR 2 1 2 250 100MS 208S 0S
CBR 8 1 2 250 100MS 209S 0S
CBR 13 14 2 500 100MS 210S 0S
CBR 13 20 2 500 100MS 215S 0S
CBR 14 13 2 250 100MS 218S 0S
CBR 20 13 2 250 100MS 220S 0S
CBR 1 2 2 500 100MS 245S 0S
CBR 1 8 2 500 100MS 245S 0S
CBR 13 14 2 500 100MS 245S 0S
CBR 13 20 2 500 100MS 245S 0S
#NEED MEDIC
CBR 15 18 2 500 100MS 250S 0S
CBR 18 15 2 500 100MS 252S 0S
#WE'RE AT THE TARGET
CBR 2 5 2 500 100MS 260S 0S
CBR 2 1 2 500 100MS 260S 0S
CBR 2 0 2 500 100MS 260S 0S
CBR 14 17 2 500 100MS 263S 0S
CBR 14 13 2 500 100MS 263S 0S
CBR 14 0 2 500 100MS 2633 0S
#MOVE FORWARD 11-12-23-24
CBR 5 11 2 500 100MS 265 0S
CBR 17 23 2 500 100MS 265 0S
#NEED MEDIC
CBR 3 7 2 500 100MS 270S 0S
CBR 7 3 2 500 100MS 272S 0S
#NORTH/SOUTH OPs
CBR 5 2 2 1500 100MS 295S 0S
CBR 5 8 2 1500 100MS 295S 0S
CBR 17 14 2 1500 100MS 297S 0S
CBR 17 20 2 1500 100MS 297S 0S
#EXECUTIVES MOVE FORWARD
CBR 5 1 2 500 100MS 340 0S
CBR 17 13 2 500 100MS 340 0S
#OPs SET
CBR 2 5 2 250 100MS 360S 0S
CBR 8 5 2 250 100MS 360S 0S
CBR 14 17 2 250 100MS 363S 0S
CBR 20 17 2 250 100MS 363S 0S
#SEIZED THE OBJ
CBR 5 0 2 500 100MS 410S 0S
CBR 17 0 2 500 100MS 415 0S
#MED EVAC
CBR 18 0 2 1000 100MS 425 0S
CBR 0 18 3 500 100MS 430 0S
#REPORT
CBR 5 0 2 2000 100MS 600S 0S
CBR 17 0 2 2000 100MS 620 0S
#FTP ENCRYPTION FILES TO OC
FTP 14 0 10 625S
```

```
FTP 23 0 10 630S
#VISUAL REPORTS FROM OPs TO TEAMS
CBR 14 13 20 1024 100MS 640 0S
CBR 20 13 20 1024 100MS 660 0S
CBR 2 1 20 1024 100MS 665S 0S
CBR 8 1 10 1024 100MS 685S 0S
#DEMOLITION CHARGES ARE READY
CBR 24 13 1 500 100MS 686 0S
CBR 12 1 1 500 100MS 700S 0S
#TEAM>>OC READY
CBR 1 0 1 500 100MS 701S 0S
CBR 13 0 1 500 100MS 705S 0S
#FIRE & OBSERVE 100M BEHIND
CBR 1 11 1 500 100MS 710S 0S
CBR 13 23 1 500 100MS 710S 0S
#SUCCESSFUL
CBR 5 1 2 500 100MS 730 0S
CBR 5 0 2 500 100MS 730 0S
CBR 17 13 2 500 100MS 731 0S
CBR 17 0 2 500 100MS 731 0S
#WITHDRAW
CBR 1 5 2 500 100MS 735S 0S
CBR 1 2 2 500 100MS 735S 0S
CBR 1 8 2 500 100MS 735S 0S
CBR 13 17 2 500 100MS 735S 0S
CBR 13 14 2 500 100MS 735S 0S
CBR 13 20 2 500 100MS 735S 0S
#CBR 13 17 10 2000 100MS 500S 0S
#END
```

.STAT

The following ".stat" file is one of the statistical files that we get at the end of each simulation run. Due to the homogenous structure of the GloMoSim and some of its limitations, we get the statistics about all nodes and derive necessary information from the entire file.

```
Node:      0, Layer:          802.11, pkts from network: 167
Node:      0, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      0, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      0, Layer:          802.11, BCAST pkts sent to chanl: 8
Node:      0, Layer:          802.11, UCAST pkts rcvd clearly: 369
Node:      0, Layer:          802.11, BCAST pkts rcvd clearly: 14
Node:      0, Layer:          802.11, retx pkts due to CTS timeout: 66
Node:      0, Layer:          802.11, retx pkts due to ACK timeout: 16
Node:      0, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      0, Layer:          802.11, pkt drops due to retx limit: 0
Node:      0, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      0, Layer:      RoutingDsr, Number of Requests Txed = 8
Node:      0, Layer:      RoutingDsr, Number of Replies Txed = 3
Node:      0, Layer:      RoutingDsr, Number of Errors Txed = 0
```

```
Node:       0, Layer:       RoutingDsr, Number of CTRL Packets Txed = 11
Node:       0, Layer:       RoutingDsr, Number of Data Txed = 156
Node:       0, Layer:       RoutingDsr, Number of Data Originated = 156
Node:       0, Layer:       RoutingDsr, Number of Data Received = 359
Node:       0, Layer:    AppCbrServer, from 5 to 0 (id = 8), start = 730033593627 ns, end
= 730133793627 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 33692627 ns, throughput = 79840 bps
Node:       0, Layer:    AppCbrServer, from 5 to 0 (id = 6), start = 717393716936 ns, end
= 717464046602 ns (closed) ns, bytes recv = 4000 B, pkts recv = 2, avg. end-to-end delay
= 117378881769 ns, throughput = 455000 bps
Node:       0, Layer:    AppCbrServer, from 13 to 0 (id = 9), start = 705010516001 ns, end
= 705010516001 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end delay =
10516001 ns, throughput = 0 bps
Node:       0, Layer:    AppFtpServer, from 23 to 0 (cid = 3), start = 630177253932, end =
1203115757006 ns (closed) bytes sent = 296 B, bytes recv = 154267 B, throughput = 2154
bps
Node:       0, Layer:    AppCbrServer, from 17 to 0 (id = 6), start = 620105285229 ns, end
= 620216781529 ns (closed) ns, bytes recv = 4000 B, pkts recv = 2, avg. end-to-end delay
= 111033379 ns, throughput = 287005 bps
Node:       0, Layer:    AppCbrServer, from 18 to 0 (id = 1), start = 425096150403 ns, end
= 425137867266 ns (closed) ns, bytes recv = 2000 B, pkts recv = 2, avg. end-to-end delay
= 67008834 ns, throughput = 383537 bps
Node:       0, Layer:    AppCbrServer, from 17 to 0 (id = 5), start = 415097596251 ns, end
= 415133085229 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 65340740 ns, throughput = 225422 bps
Node:       0, Layer:    AppCbrServer, from 2 to 0 (id = 6), start = 260044642685 ns, end
= 260144961707 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 44800196 ns, throughput = 79745 bps
Node:       0, Layer:    AppCbrServer, from 14 to 0 (id = 1), start = 69051352581 ns, end
= 69343378835 ns (closed) ns, bytes recv = 5000 B, pkts recv = 10, avg. end-to-end delay
= 166766476 ns, throughput = 136973 bps
Node:       0, Layer:    AppCbrServer, from 2 to 0 (id = 1), start = 60064844773 ns, end =
60344082864 ns (closed) ns, bytes recv = 4500 B, pkts recv = 9, avg. end-to-end delay =
156375813 ns, throughput = 128922 bps
Node:       0, Layer:    AppCbrServer, from 13 to 0 (id = 3), start = 56045101415 ns, end
= 56052388083 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
998744749 ns, throughput = 548947 bps
Node:       0, Layer:    AppCbrServer, from 1 to 0 (id = 3), start = 55075945587 ns, end =
55113945814 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
44945700 ns, throughput = 105262 bps
Node:       0, Layer:    AppCbrClient, from 0 to 18 (id = 6), start = 430000000000 ns, end
= 430200000000 ns (closed) ns, bytes sent = 1500 B, pkts sent = 3, throughput = 60000 bps
Node:       0, Layer:    AppCbrClient, from 0 to 13 (id = 5), start = 240000000000 ns, end
= 240000001000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 4000000000
bps
Node:       0, Layer:    AppCbrClient, from 0 to 1 (id = 4), start = 240000000000 ns, end
= 240000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:       0, Layer:    AppCbrClient, from 0 to 14 (id = 3), start = 58000000000 ns, end
= 58100001000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 39999 bps
Node:       0, Layer:    AppCbrClient, from 0 to 2 (id = 2), start = 58000000000 ns, end =
58100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:       0, Layer:    AppCbrClient, from 0 to 13 (id = 1), start = 5000000000 ns, end =
5100001000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 39999 bps
Node:       0, Layer:    AppCbrClient, from 0 to 1 (id = 0), start = 5000000000 ns, end =
5100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:       1, Layer:          802.11, pkts from network: 50
Node:       1, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:       1, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:       1, Layer:          802.11, BCAST pkts sent to chanl: 12
Node:       1, Layer:          802.11, UCAST pkts rcvd clearly: 63
Node:       1, Layer:          802.11, BCAST pkts rcvd clearly: 30
Node:       1, Layer:          802.11, retx pkts due to CTS timeout: 17
Node:       1, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:       1, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:       1, Layer:          802.11, pkt drops due to retx limit: 2
Node:       1, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:       1, Layer:       RoutingDsr, Number of Requests Txed = 12
Node:       1, Layer:       RoutingDsr, Number of Replies Txed = 12
Node:       1, Layer:       RoutingDsr, Number of Errors Txed = 0
```

```
Node:      1, Layer:      RoutingDsr, Number of CTRL Packets Txed = 24
Node:      1, Layer:      RoutingDsr, Number of Data Txed = 26
Node:      1, Layer:      RoutingDsr, Number of Data Originated = 20
Node:      1, Layer:      RoutingDsr, Number of Data Received = 48
Node:      1, Layer:    AppCbrServer, from 5 to 1 (id = 7), start = 730010516554 ns, end
= 730110516554 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 10516554 ns, throughput = 80000 bps
Node:      1, Layer:    AppCbrServer, from 2 to 1 (id = 8), start = 718578125759 ns, end
= 718619680355 ns (closed) ns, bytes recv = 2048 B, pkts recv = 2, avg. end-to-end delay
= 52548903057 ns, throughput = 394276 bps
Node:      1, Layer:    AppCbrServer, from 12 to 1 (id = 0), start = 715139874858 ns, end
= 715139874858 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end delay =
15139874858 ns, throughput = 0 bps
Node:      1, Layer:    AppCbrServer, from 5 to 1 (id = 4), start = 340010514600 ns, end
= 340110514609 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 10514604 ns, throughput = 79999 bps
Node:      1, Layer:    AppCbrServer, from 2 to 1 (id = 5), start = 260021784609 ns, end
= 260122063623 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 21923116 ns, throughput = 79777 bps
Node:      1, Layer:    AppCbrServer, from 0 to 1 (id = 4), start = 240010517001 ns, end
= 240010517001 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end delay =
10517001 ns, throughput = 0 bps
Node:      1, Layer:    AppCbrServer, from 8 to 1 (id = 1), start = 209006515563 ns, end
= 209106515563 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
6515563 ns, throughput = 40000 bps
Node:      1, Layer:    AppCbrServer, from 2 to 1 (id = 3), start = 208006516001 ns, end
= 208106516001 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
6516001 ns, throughput = 40000 bps
Node:      1, Layer:    AppCbrServer, from 2 to 1 (id = 2), start = 60012653001 ns, end =
60332992224 ns (closed) ns, bytes recv = 5000 B, pkts recv = 10, avg. end-to-end delay =
127933273 ns, throughput = 124867 bps
Node:      1, Layer:    AppCbrServer, from 2 to 1 (id = 0), start = 53027962122 ns, end =
53106516001 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
17239061 ns, throughput = 50920 bps
Node:      1, Layer:    AppCbrServer, from 8 to 1 (id = 0), start = 46021073354 ns, end =
46106515563 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
13794458 ns, throughput = 46815 bps
Node:      1, Layer:    AppCbrServer, from 5 to 1 (id = 0), start = 25015747343 ns, end =
25106514600 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
11130971 ns, throughput = 44068 bps
Node:      1, Layer:    AppCbrServer, from 0 to 1 (id = 0), start = 5016144823 ns, end =
5106517001 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
11330912 ns, throughput = 44261 bps
Node:      1, Layer:    AppCbrClient, from 1 to 8 (id = 13), start = 735000000000 ns, end
= 735100002000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79998 bps
Node:      1, Layer:    AppCbrClient, from 1 to 2 (id = 12), start = 735000000000 ns, end
= 735100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999 bps
Node:      1, Layer:    AppCbrClient, from 1 to 5 (id = 11), start = 735000000000 ns, end
= 735100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      1, Layer:    AppCbrClient, from 1 to 11 (id = 10), start = 710000000000 ns,
end = 710000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:      1, Layer:    AppCbrClient, from 1 to 0 (id = 9), start = 701000000000 ns, end
= 701000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:      1, Layer:    AppCbrClient, from 1 to 8 (id = 8), start = 245000000000 ns, end
= 245100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999 bps
Node:      1, Layer:    AppCbrClient, from 1 to 2 (id = 7), start = 245000000000 ns, end
= 245100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      1, Layer:    AppCbrClient, from 1 to 8 (id = 6), start = 207000000000 ns, end
= 207100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      1, Layer:    AppCbrClient, from 1 to 2 (id = 5), start = 201000000000 ns, end
= 201100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      1, Layer:    AppCbrClient, from 1 to 5 (id = 4), start = 190000000000 ns, end
= 190300000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 4, throughput = 26666 bps
Node:      1, Layer:    AppCbrClient, from 1 to 0 (id = 3), start = 55000000000 ns, end =
55100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      1, Layer:    AppCbrClient, from 1 to 8 (id = 2), start = 27000000000 ns, end =
27100001000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 39999 bps
Node:      1, Layer:    AppCbrClient, from 1 to 2 (id = 1), start = 27000000000 ns, end =
27100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
```

```
Node:      1, Layer:    AppCbrClient, from 1 to 5 (id = 0), start = 8000000000 ns, end =
8100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      2, Layer:          802.11, pkts from network: 3245
Node:      2, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      2, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      2, Layer:          802.11, BCAST pkts sent to chanl: 3183
Node:      2, Layer:          802.11, UCAST pkts rcvd clearly: 28
Node:      2, Layer:          802.11, BCAST pkts rcvd clearly: 9473
Node:      2, Layer:          802.11, retx pkts due to CTS timeout: 80
Node:      2, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      2, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      2, Layer:          802.11, pkt drops due to retx limit: 6
Node:      2, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      2, Layer:      RoutingDsr, Number of Requests Txed = 3183
Node:      2, Layer:      RoutingDsr, Number of Replies Txed = 3
Node:      2, Layer:      RoutingDsr, Number of Errors Txed = 1
Node:      2, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3187
Node:      2, Layer:      RoutingDsr, Number of Data Txed = 58
Node:      2, Layer:      RoutingDsr, Number of Data Originated = 52
Node:      2, Layer:      RoutingDsr, Number of Data Received = 11
Node:      2, Layer:    AppCbrServer, from 1 to 2 (id = 12), start = 735219787033 ns, end
= 735219787033 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end delay =
119786033 ns, throughput = 0 bps
Node:      2, Layer:    AppCbrServer, from 5 to 2 (id = 2), start = 295028913001 ns, end
= 295126517001 ns (closed) ns, bytes recv = 3000 B, pkts recv = 2, avg. end-to-end delay
= 27715001 ns, throughput = 245891 bps
Node:      2, Layer:    AppCbrServer, from 1 to 2 (id = 7), start = 245010517001 ns, end
= 245110516998 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 10516999 ns, throughput = 80000 bps
Node:      2, Layer:    AppCbrServer, from 1 to 2 (id = 5), start = 201010516001 ns, end
= 201110516001 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 10516001 ns, throughput = 80000 bps
Node:      2, Layer:    AppCbrServer, from 0 to 2 (id = 2), start = 58023309251 ns, end =
58113948002 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
18628626 ns, throughput = 44131 bps
Node:      2, Layer:    AppCbrServer, from 1 to 2 (id = 1), start = 27014514384 ns, end =
27106515201 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
10514792 ns, throughput = 43477 bps
Node:      2, Layer:    AppCbrClient, from 2 to 1 (id = 8), start = 665000000000 ns, end
= 666900000000 ns (closed) ns, bytes sent = 20480 B, pkts sent = 20, throughput = 86231
bps
Node:      2, Layer:    AppCbrClient, from 2 to 5 (id = 7), start = 360000000000 ns, end
= 360100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      2, Layer:    AppCbrClient, from 2 to 0 (id = 6), start = 260000000000 ns, end
= 260100002000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79998 bps
Node:      2, Layer:    AppCbrClient, from 2 to 1 (id = 5), start = 260000000000 ns, end
= 260100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999 bps
Node:      2, Layer:    AppCbrClient, from 2 to 5 (id = 4), start = 260000000000 ns, end
= 260100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      2, Layer:    AppCbrClient, from 2 to 1 (id = 3), start = 208000000000 ns, end
= 208100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      2, Layer:    AppCbrClient, from 2 to 1 (id = 2), start = 60000000000 ns, end =
60090001000 ns (closed) ns, bytes sent = 5000 B, pkts sent = 10, throughput = 444439 bps
Node:      2, Layer:    AppCbrClient, from 2 to 0 (id = 1), start = 60000000000 ns, end =
60090000000 ns (closed) ns, bytes sent = 5000 B, pkts sent = 10, throughput = 444444 bps
Node:      2, Layer:    AppCbrClient, from 2 to 1 (id = 0), start = 53000000000 ns, end =
53100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      3, Layer:          802.11, pkts from network: 3173
Node:      3, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      3, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      3, Layer:          802.11, BCAST pkts sent to chanl: 3170
Node:      3, Layer:          802.11, UCAST pkts rcvd clearly: 3
Node:      3, Layer:          802.11, BCAST pkts rcvd clearly: 9481
Node:      3, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:      3, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      3, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      3, Layer:          802.11, pkt drops due to retx limit: 0
Node:      3, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      3, Layer:      RoutingDsr, Number of Requests Txed = 3170
```

```
Node:      3, Layer:      RoutingDsr, Number of Replies Txed = 1
Node:      3, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:      3, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3171
Node:      3, Layer:      RoutingDsr, Number of Data Txed = 2
Node:      3, Layer:      RoutingDsr, Number of Data Originated = 2
Node:      3, Layer:      RoutingDsr, Number of Data Received = 2
Node:      3, Layer:    AppCbrServer, from 7 to 3 (id = 0), start = 272025840598 ns, end
= 272110516100 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 18178349 ns, throughput = 94478 bps
Node:      3, Layer:    AppCbrClient, from 3 to 7 (id = 0), start = 270000000000 ns, end
= 270100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      4, Layer:          802.11, pkts from network: 3220
Node:      4, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      4, Layer:          802.11, UCAST (non-frag) pkts sent to chan1: 0
Node:      4, Layer:          802.11, BCAST pkts sent to chan1: 3189
Node:      4, Layer:          802.11, UCAST pkts rcvd clearly: 33
Node:      4, Layer:          802.11, BCAST pkts rcvd clearly: 16720
Node:      4, Layer:          802.11, retx pkts due to CTS timeout: 3
Node:      4, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      4, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      4, Layer:          802.11, pkt drops due to retx limit: 0
Node:      4, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      4, Layer:      RoutingDsr, Number of Requests Txed = 3186
Node:      4, Layer:      RoutingDsr, Number of Replies Txed = 11
Node:      4, Layer:      RoutingDsr, Number of Errors Txed = 3
Node:      4, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3200
Node:      4, Layer:      RoutingDsr, Number of Data Txed = 20
Node:      4, Layer:      RoutingDsr, Number of Data Originated = 0
Node:      4, Layer:      RoutingDsr, Number of Data Received = 0
Node:      5, Layer:          802.11, pkts from network: 6396
Node:      5, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      5, Layer:          802.11, UCAST (non-frag) pkts sent to chan1: 0
Node:      5, Layer:          802.11, BCAST pkts sent to chan1: 6356
Node:      5, Layer:          802.11, UCAST pkts rcvd clearly: 27
Node:      5, Layer:          802.11, BCAST pkts rcvd clearly: 15643
Node:      5, Layer:          802.11, retx pkts due to CTS timeout: 33
Node:      5, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      5, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      5, Layer:          802.11, pkt drops due to retx limit: 3
Node:      5, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      5, Layer:      RoutingDsr, Number of Requests Txed = 6356
Node:      5, Layer:      RoutingDsr, Number of Replies Txed = 13
Node:      5, Layer:      RoutingDsr, Number of Errors Txed = 3
Node:      5, Layer:      RoutingDsr, Number of CTRL Packets Txed = 6372
Node:      5, Layer:      RoutingDsr, Number of Data Txed = 24
Node:      5, Layer:      RoutingDsr, Number of Data Originated = 18
Node:      5, Layer:      RoutingDsr, Number of Data Received = 12
Node:      5, Layer:    AppCbrServer, from 8 to 5 (id = 2), start = 743939505567 ns, end
= 743939505567 ns (closed) ns, bytes recv = 250 B, pkts recv = 1, avg. end-to-end delay =
383839505567 ns, throughput = 0 bps
Node:      5, Layer:    AppCbrServer, from 1 to 5 (id = 11), start = 735010517554 ns, end
= 735112552554 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 11535054 ns, throughput = 78404 bps
Node:      5, Layer:    AppCbrServer, from 2 to 5 (id = 7), start = 360180897665 ns, end
= 360180897665 ns (closed) ns, bytes recv = 250 B, pkts recv = 1, avg. end-to-end delay =
80897665 ns, throughput = 0 bps
Node:      5, Layer:    AppCbrServer, from 2 to 5 (id = 4), start = 260010517722 ns, end
= 260110516728 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 10517225 ns, throughput = 80000 bps
Node:      5, Layer:    AppCbrServer, from 1 to 5 (id = 4), start = 190006514600 ns, end
= 190306514600 ns (closed) ns, bytes recv = 1000 B, pkts recv = 4, avg. end-to-end delay
= 6514600 ns, throughput = 26666 bps
Node:      5, Layer:    AppCbrServer, from 1 to 5 (id = 0), start = 8017071875 ns, end =
8106514099 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
11792987 ns, throughput = 44721 bps
Node:      5, Layer:    AppCbrClient, from 5 to 0 (id = 8), start = 730000000000 ns, end
= 730100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999 bps
Node:      5, Layer:    AppCbrClient, from 5 to 1 (id = 7), start = 730000000000 ns, end
= 730100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
```

```
Node:      5, Layer:    AppCbrClient, from 5 to 0 (id = 6), start = 600000000000 ns, end
= 600100000000 ns (closed) ns, bytes sent = 4000 B, pkts sent = 2, throughput = 320000
bps
Node:      5, Layer:    AppCbrClient, from 5 to 0 (id = 5), start = 410000000000 ns, end
= 410100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      5, Layer:    AppCbrClient, from 5 to 1 (id = 4), start = 340000000000 ns, end
= 340100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      5, Layer:    AppCbrClient, from 5 to 8 (id = 3), start = 295000000000 ns, end
= 295100001000 ns (closed) ns, bytes sent = 3000 B, pkts sent = 2, throughput = 239997
bps
Node:      5, Layer:    AppCbrClient, from 5 to 2 (id = 2), start = 295000000000 ns, end
= 295100000000 ns (closed) ns, bytes sent = 3000 B, pkts sent = 2, throughput = 240000
bps
Node:      5, Layer:    AppCbrClient, from 5 to 11 (id = 1), start = 265000000000 ns, end
= 265100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      5, Layer:    AppCbrClient, from 5 to 1 (id = 0), start = 25000000000 ns, end =
25100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      6, Layer:          802.11, pkts from network: 3191
Node:      6, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      6, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      6, Layer:          802.11, BCAST pkts sent to chanl: 3187
Node:      6, Layer:          802.11, UCAST pkts rcvd clearly: 3
Node:      6, Layer:          802.11, BCAST pkts rcvd clearly: 18868
Node:      6, Layer:          802.11, retx pkts due to CTS timeout: 5
Node:      6, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      6, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      6, Layer:          802.11, pkt drops due to retx limit: 0
Node:      6, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      6, Layer:      RoutingDsr, Number of Requests Txed = 3187
Node:      6, Layer:      RoutingDsr, Number of Replies Txed = 3
Node:      6, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:      6, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3190
Node:      6, Layer:      RoutingDsr, Number of Data Txed = 1
Node:      6, Layer:      RoutingDsr, Number of Data Originated = 0
Node:      6, Layer:      RoutingDsr, Number of Data Received = 0
Node:      7, Layer:          802.11, pkts from network: 3196
Node:      7, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      7, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      7, Layer:          802.11, BCAST pkts sent to chanl: 3187
Node:      7, Layer:          802.11, UCAST pkts rcvd clearly: 8
Node:      7, Layer:          802.11, BCAST pkts rcvd clearly: 16733
Node:      7, Layer:          802.11, retx pkts due to CTS timeout: 2
Node:      7, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      7, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      7, Layer:          802.11, pkt drops due to retx limit: 0
Node:      7, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      7, Layer:      RoutingDsr, Number of Requests Txed = 3187
Node:      7, Layer:      RoutingDsr, Number of Replies Txed = 4
Node:      7, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:      7, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3191
Node:      7, Layer:      RoutingDsr, Number of Data Txed = 5
Node:      7, Layer:      RoutingDsr, Number of Data Originated = 2
Node:      7, Layer:      RoutingDsr, Number of Data Received = 2
Node:      7, Layer:    AppCbrServer, from 3 to 7 (id = 0), start = 270020549724 ns, end
= 270110516100 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 15532912 ns, throughput = 88922 bps
Node:      7, Layer:    AppCbrClient, from 7 to 3 (id = 0), start = 272000000000 ns, end
= 272100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:      8, Layer:          802.11, pkts from network: 66
Node:      8, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      8, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      8, Layer:          802.11, BCAST pkts sent to chanl: 57
Node:      8, Layer:          802.11, UCAST pkts rcvd clearly: 9
Node:      8, Layer:          802.11, BCAST pkts rcvd clearly: 68
Node:      8, Layer:          802.11, retx pkts due to CTS timeout: 18
Node:      8, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      8, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      8, Layer:          802.11, pkt drops due to retx limit: 2
Node:      8, Layer:          802.11, frgmnt drops due to retx limit: 0
```

```
Node:      8, Layer:      RoutingDsr, Number of Requests Txed = 57
Node:      8, Layer:      RoutingDsr, Number of Replies Txed = 2
Node:      8, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:      8, Layer:      RoutingDsr, Number of CTRL Packets Txed = 59
Node:      8, Layer:      RoutingDsr, Number of Data Txed = 7
Node:      8, Layer:      RoutingDsr, Number of Data Originated = 7
Node:      8, Layer:      RoutingDsr, Number of Data Received = 2
Node:      8, Layer:    AppCbrServer, from 5 to 8 (id = 3), start = 295061954188 ns, end
= 295153963678 ns (closed) ns, bytes recv = 3000 B, pkts recv = 2, avg. end-to-end delay
= 57957933 ns, throughput = 260842 bps
Node:      8, Layer:    AppCbrClient, from 8 to 1 (id = 3), start = 685000000000 ns, end
= 685900000000 ns (closed) ns, bytes sent = 10240 B, pkts sent = 10, throughput = 91022
bps
Node:      8, Layer:    AppCbrClient, from 8 to 5 (id = 2), start = 360000000000 ns, end
= 360100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      8, Layer:    AppCbrClient, from 8 to 1 (id = 1), start = 209000000000 ns, end
= 209100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      8, Layer:    AppCbrClient, from 8 to 1 (id = 0), start = 46000000000 ns, end =
46100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:      9, Layer:          802.11, pkts from network: 29
Node:      9, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:      9, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:      9, Layer:          802.11, BCAST pkts sent to chanl: 29
Node:      9, Layer:          802.11, UCAST pkts rcvd clearly: 0
Node:      9, Layer:          802.11, BCAST pkts rcvd clearly: 97
Node:      9, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:      9, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:      9, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:      9, Layer:          802.11, pkt drops due to retx limit: 0
Node:      9, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:      9, Layer:      RoutingDsr, Number of Requests Txed = 29
Node:      9, Layer:      RoutingDsr, Number of Replies Txed = 0
Node:      9, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:      9, Layer:      RoutingDsr, Number of CTRL Packets Txed = 29
Node:      9, Layer:      RoutingDsr, Number of Data Txed = 0
Node:      9, Layer:      RoutingDsr, Number of Data Originated = 0
Node:      9, Layer:      RoutingDsr, Number of Data Received = 0
Node:     10, Layer:          802.11, pkts from network: 29
Node:     10, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     10, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     10, Layer:          802.11, BCAST pkts sent to chanl: 29
Node:     10, Layer:          802.11, UCAST pkts rcvd clearly: 0
Node:     10, Layer:          802.11, BCAST pkts rcvd clearly: 97
Node:     10, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:     10, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     10, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     10, Layer:          802.11, pkt drops due to retx limit: 0
Node:     10, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     10, Layer:      RoutingDsr, Number of Requests Txed = 29
Node:     10, Layer:      RoutingDsr, Number of Replies Txed = 0
Node:     10, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     10, Layer:      RoutingDsr, Number of CTRL Packets Txed = 29
Node:     10, Layer:      RoutingDsr, Number of Data Txed = 0
Node:     10, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     10, Layer:      RoutingDsr, Number of Data Received = 0
Node:     11, Layer:          802.11, pkts from network: 3210
Node:     11, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     11, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     11, Layer:          802.11, BCAST pkts sent to chanl: 3187
Node:     11, Layer:          802.11, UCAST pkts rcvd clearly: 20
Node:     11, Layer:          802.11, BCAST pkts rcvd clearly: 18880
Node:     11, Layer:          802.11, retx pkts due to CTS timeout: 10
Node:     11, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     11, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     11, Layer:          802.11, pkt drops due to retx limit: 1
Node:     11, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     11, Layer:      RoutingDsr, Number of Requests Txed = 3187
Node:     11, Layer:      RoutingDsr, Number of Replies Txed = 7
Node:     11, Layer:      RoutingDsr, Number of Errors Txed = 1
```

```
Node:     11, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3195
Node:     11, Layer:      RoutingDsr, Number of Data Txed = 15
Node:     11, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     11, Layer:      RoutingDsr, Number of Data Received = 3
Node:     11, Layer:    AppCbrServer, from 1 to 11 (id = 10), start = 711049535124 ns,
end = 711049535124 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end
delay = 1049535124 ns, throughput = 0 bps
Node:     11, Layer:    AppCbrServer, from 5 to 11 (id = 1), start = 265039093652 ns, end
= 265110514216 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end delay
= 24803934 ns, throughput = 112012 bps
Node:     12, Layer:          802.11, pkts from network: 3210
Node:     12, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     12, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     12, Layer:          802.11, BCAST pkts sent to chanl: 3191
Node:     12, Layer:          802.11, UCAST pkts rcvd clearly: 17
Node:     12, Layer:          802.11, BCAST pkts rcvd clearly: 18867
Node:     12, Layer:          802.11, retx pkts due to CTS timeout: 3
Node:     12, Layer:          802.11, retx pkts due to ACK timeout: 3
Node:     12, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     12, Layer:          802.11, pkt drops due to retx limit: 0
Node:     12, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     12, Layer:      RoutingDsr, Number of Requests Txed = 3191
Node:     12, Layer:      RoutingDsr, Number of Replies Txed = 3
Node:     12, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     12, Layer:      RoutingDsr, Number of CTRL Packets Txed = 3194
Node:     12, Layer:      RoutingDsr, Number of Data Txed = 16
Node:     12, Layer:      RoutingDsr, Number of Data Originated = 1
Node:     12, Layer:      RoutingDsr, Number of Data Received = 0
Node:     12, Layer:    AppCbrClient, from 12 to 1 (id = 0), start = 700000000000 ns, end
= 700000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:     13, Layer:          802.11, pkts from network: 540
Node:     13, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     13, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     13, Layer:          802.11, BCAST pkts sent to chanl: 11
Node:     13, Layer:          802.11, UCAST pkts rcvd clearly: 551
Node:     13, Layer:          802.11, BCAST pkts rcvd clearly: 33
Node:     13, Layer:          802.11, retx pkts due to CTS timeout: 182
Node:     13, Layer:          802.11, retx pkts due to ACK timeout: 4
Node:     13, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     13, Layer:          802.11, pkt drops due to retx limit: 4
Node:     13, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     13, Layer:      RoutingDsr, Number of Requests Txed = 11
Node:     13, Layer:      RoutingDsr, Number of Replies Txed = 16
Node:     13, Layer:      RoutingDsr, Number of Errors Txed = 3
Node:     13, Layer:      RoutingDsr, Number of CTRL Packets Txed = 30
Node:     13, Layer:      RoutingDsr, Number of Data Txed = 510
Node:     13, Layer:      RoutingDsr, Number of Data Originated = 18
Node:     13, Layer:      RoutingDsr, Number of Data Received = 44
Node:     13, Layer:    AppCbrServer, from 17 to 13 (id = 7), start = 731043936336 ns,
end = 731110516602 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 27226469 ns, throughput = 120155 bps
Node:     13, Layer:    AppCbrServer, from 24 to 13 (id = 0), start = 686038663515 ns,
end = 686038663515 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end
delay = 38663515 ns, throughput = 0 bps
Node:     13, Layer:    AppCbrServer, from 14 to 13 (id = 9), start = 640127553232 ns,
end = 648979579673 ns (closed) ns, bytes recv = 18432 B, pkts recv = 18, avg. end-to-end
delay = 876173127 ns, throughput = 16657 bps
Node:     13, Layer:    AppCbrServer, from 14 to 13 (id = 5), start = 263095700825 ns,
end = 263133173039 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 64435932 ns, throughput = 213491 bps
Node:     13, Layer:    AppCbrServer, from 20 to 13 (id = 1), start = 220006515941 ns,
end = 220106515941 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end
delay = 6515941 ns, throughput = 40000 bps
Node:     13, Layer:    AppCbrServer, from 14 to 13 (id = 3), start = 218006515980 ns,
end = 218106515980 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end
delay = 6515980 ns, throughput = 40000 bps
Node:     13, Layer:    AppCbrServer, from 14 to 13 (id = 2), start = 69013072980 ns, end
= 69309310498 ns (closed) ns, bytes recv = 5000 B, pkts recv = 10, avg. end-to-end delay
= 122284881 ns, throughput = 135026 bps
```

```
Node:     13, Layer:    AppCbrServer, from 14 to 13 (id = 0), start = 54031084919 ns, end
= 54106515980 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
18800449 ns, throughput = 53028 bps
Node:     13, Layer:    AppCbrServer, from 20 to 13 (id = 0), start = 53026356712 ns, end
= 53106515941 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
16436326 ns, throughput = 49900 bps
Node:     13, Layer:    AppCbrServer, from 17 to 13 (id = 0), start = 27020451610 ns, end
= 27106514999 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
13483304 ns, throughput = 46477 bps
Node:     13, Layer:    AppCbrClient, from 13 to 20 (id = 13), start = 735000000000 ns,
end = 735100002000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79998
bps
Node:     13, Layer:    AppCbrClient, from 13 to 14 (id = 12), start = 735000000000 ns,
end = 735100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999
bps
Node:     13, Layer:    AppCbrClient, from 13 to 17 (id = 11), start = 735000000000 ns,
end = 735100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     13, Layer:    AppCbrClient, from 13 to 23 (id = 10), start = 710000000000 ns,
end = 710000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:     13, Layer:    AppCbrClient, from 13 to 0 (id = 9), start = 705000000000 ns, end
= 705000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
Node:     13, Layer:    AppCbrClient, from 13 to 20 (id = 8), start = 245000000000 ns,
end = 245100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999
bps
Node:     13, Layer:    AppCbrClient, from 13 to 14 (id = 7), start = 245000000000 ns,
end = 245100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     13, Layer:    AppCbrClient, from 13 to 20 (id = 6), start = 215000000000 ns,
end = 215100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     13, Layer:    AppCbrClient, from 13 to 14 (id = 5), start = 210000000000 ns,
end = 210100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     13, Layer:    AppCbrClient, from 13 to 17 (id = 4), start = 200000000000 ns,
end = 200300000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 4, throughput = 26666
bps
Node:     13, Layer:    AppCbrClient, from 13 to 0 (id = 3), start = 55000000000 ns, end
= 55100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:     13, Layer:    AppCbrClient, from 13 to 20 (id = 2), start = 30000000000 ns, end
= 30100001000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 39999 bps
Node:     13, Layer:    AppCbrClient, from 13 to 14 (id = 1), start = 30000000000 ns, end
= 30100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:     13, Layer:    AppCbrClient, from 13 to 17 (id = 0), start = 9000000000 ns, end
= 9100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:     14, Layer:          802.11, pkts from network: 76
Node:     14, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     14, Layer:          802.11, UCAST (non-frag) pkts sent to chan1: 0
Node:     14, Layer:          802.11, BCAST pkts sent to chan1: 18
Node:     14, Layer:          802.11, UCAST pkts rcvd clearly: 16
Node:     14, Layer:          802.11, BCAST pkts rcvd clearly: 42
Node:     14, Layer:          802.11, retx pkts due to CTS timeout: 88
Node:     14, Layer:          802.11, retx pkts due to ACK timeout: 2
Node:     14, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     14, Layer:          802.11, pkt drops due to retx limit: 5
Node:     14, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     14, Layer:      RoutingDsr, Number of Requests Txed = 18
Node:     14, Layer:      RoutingDsr, Number of Replies Txed = 2
Node:     14, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     14, Layer:      RoutingDsr, Number of CTRL Packets Txed = 20
Node:     14, Layer:      RoutingDsr, Number of Data Txed = 56
Node:     14, Layer:      RoutingDsr, Number of Data Originated = 53
Node:     14, Layer:      RoutingDsr, Number of Data Received = 6
Node:     14, Layer:    AppCbrServer, from 13 to 14 (id = 7), start = 245010516980 ns,
end = 245110516980 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 10516980 ns, throughput = 80000 bps
Node:     14, Layer:    AppCbrServer, from 13 to 14 (id = 5), start = 210010515980 ns,
end = 210110515980 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 10515980 ns, throughput = 80000 bps
```

```
Node:     14, Layer:    AppCbrServer, from 13 to 14 (id = 1), start = 30019740314 ns, end
= 30106515282 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
13127798 ns, throughput = 46096 bps
Node:     14, Layer:    AppCbrClient, from 14 to 13 (id = 9), start = 640000000000 ns,
end = 641900000000 ns (closed) ns, bytes sent = 20480 B, pkts sent = 20, throughput =
86231 bps
Node:     14, Layer:    AppFtpClient, from 14 to 0 (cid = -1), start = 0, end =
1600000000000 ns (not closed), bytes sent = 0 B, bytes recv = 0 B, throughput = 0 bps
Node:     14, Layer:    AppCbrClient, from 14 to 17 (id = 7), start = 363000000000 ns,
end = 363100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000
bps
Node:     14, Layer:    AppCbrClient, from 14 to 0 (id = 6), start = 2633000000000 ns,
end = 1600000000000 ns (not closed) ns, bytes sent = 0 B, pkts sent = 0, throughput = 0
bps
Node:     14, Layer:    AppCbrClient, from 14 to 13 (id = 5), start = 263000000000 ns,
end = 263100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999
bps
Node:     14, Layer:    AppCbrClient, from 14 to 17 (id = 4), start = 263000000000 ns,
end = 263100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     14, Layer:    AppCbrClient, from 14 to 13 (id = 3), start = 218000000000 ns,
end = 218100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000
bps
Node:     14, Layer:    AppCbrClient, from 14 to 13 (id = 2), start = 69000000000 ns, end
= 69090001000 ns (closed) ns, bytes sent = 5000 B, pkts sent = 10, throughput = 444439
bps
Node:     14, Layer:    AppCbrClient, from 14 to 0 (id = 1), start = 69000000000 ns, end
= 69090000000 ns (closed) ns, bytes sent = 5000 B, pkts sent = 10, throughput = 444444
bps
Node:     14, Layer:    AppCbrClient, from 14 to 13 (id = 0), start = 54000000000 ns, end
= 54100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:     15, Layer:          802.11, pkts from network: 14
Node:     15, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     15, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     15, Layer:          802.11, BCAST pkts sent to chanl: 10
Node:     15, Layer:          802.11, UCAST pkts rcvd clearly: 3
Node:     15, Layer:          802.11, BCAST pkts rcvd clearly: 50
Node:     15, Layer:          802.11, retx pkts due to CTS timeout: 2
Node:     15, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     15, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     15, Layer:          802.11, pkt drops due to retx limit: 0
Node:     15, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     15, Layer:      RoutingDsr, Number of Requests Txed = 10
Node:     15, Layer:      RoutingDsr, Number of Replies Txed = 2
Node:     15, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     15, Layer:      RoutingDsr, Number of CTRL Packets Txed = 12
Node:     15, Layer:      RoutingDsr, Number of Data Txed = 2
Node:     15, Layer:      RoutingDsr, Number of Data Originated = 2
Node:     15, Layer:      RoutingDsr, Number of Data Received = 2
Node:     15, Layer:    AppCbrServer, from 18 to 15 (id = 0), start = 252018851359 ns,
end = 252110515242 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 14683300 ns, throughput = 87275 bps
Node:     15, Layer:    AppCbrClient, from 15 to 18 (id = 0), start = 250000000000 ns,
end = 250100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     16, Layer:          802.11, pkts from network: 289
Node:     16, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     16, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     16, Layer:          802.11, BCAST pkts sent to chanl: 8
Node:     16, Layer:          802.11, UCAST pkts rcvd clearly: 269
Node:     16, Layer:          802.11, BCAST pkts rcvd clearly: 53
Node:     16, Layer:          802.11, retx pkts due to CTS timeout: 43
Node:     16, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     16, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     16, Layer:          802.11, pkt drops due to retx limit: 0
Node:     16, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     16, Layer:      RoutingDsr, Number of Requests Txed = 7
Node:     16, Layer:      RoutingDsr, Number of Replies Txed = 21
Node:     16, Layer:      RoutingDsr, Number of Errors Txed = 1
```

```
Node:     16, Layer:      RoutingDsr, Number of CTRL Packets Txed = 29
Node:     16, Layer:      RoutingDsr, Number of Data Txed = 260
Node:     16, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     16, Layer:      RoutingDsr, Number of Data Received = 0
Node:     17, Layer:          802.11, pkts from network: 62
Node:     17, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     17, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     17, Layer:          802.11, BCAST pkts sent to chanl: 11
Node:     17, Layer:          802.11, UCAST pkts rcvd clearly: 48
Node:     17, Layer:          802.11, BCAST pkts rcvd clearly: 55
Node:     17, Layer:          802.11, retx pkts due to CTS timeout: 67
Node:     17, Layer:          802.11, retx pkts due to ACK timeout: 2
Node:     17, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     17, Layer:          802.11, pkt drops due to retx limit: 5
Node:     17, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     17, Layer:      RoutingDsr, Number of Requests Txed = 11
Node:     17, Layer:      RoutingDsr, Number of Replies Txed = 9
Node:     17, Layer:      RoutingDsr, Number of Errors Txed = 2
Node:     17, Layer:      RoutingDsr, Number of CTRL Packets Txed = 22
Node:     17, Layer:      RoutingDsr, Number of Data Txed = 40
Node:     17, Layer:      RoutingDsr, Number of Data Originated = 14
Node:     17, Layer:      RoutingDsr, Number of Data Received = 11
Node:     17, Layer:    AppCbrServer, from 20 to 17 (id = 2), start = 746940707171 ns,
end = 746940707171 ns (closed) ns, bytes recv = 250 B, pkts recv = 1, avg. end-to-end
delay = 383840707171 ns, throughput = 0 bps
Node:     17, Layer:    AppCbrServer, from 13 to 17 (id = 11), start = 735033737979 ns,
end = 735110516602 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 22127290 ns, throughput = 104195 bps
Node:     17, Layer:    AppCbrServer, from 14 to 17 (id = 4), start = 263010516722 ns,
end = 263110516728 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 10516725 ns, throughput = 79999 bps
Node:     17, Layer:    AppCbrServer, from 13 to 17 (id = 4), start = 200006514999 ns,
end = 200306514999 ns (closed) ns, bytes recv = 1000 B, pkts recv = 4, avg. end-to-end
delay = 6514999 ns, throughput = 26666 bps
Node:     17, Layer:    AppCbrServer, from 13 to 17 (id = 0), start = 9015511295 ns, end
= 9106514201 ns (closed) ns, bytes recv = 500 B, pkts recv = 2, avg. end-to-end delay =
11012748 ns, throughput = 43954 bps
Node:     17, Layer:    AppCbrClient, from 17 to 0 (id = 8), start = 731000000000 ns, end
= 731100001000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 79999 bps
Node:     17, Layer:    AppCbrClient, from 17 to 13 (id = 7), start = 731000000000 ns,
end = 731100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     17, Layer:    AppCbrClient, from 17 to 0 (id = 6), start = 620000000000 ns, end
= 620100000000 ns (closed) ns, bytes sent = 4000 B, pkts sent = 2, throughput = 320000
bps
Node:     17, Layer:    AppCbrClient, from 17 to 0 (id = 5), start = 415000000000 ns, end
= 415100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000 bps
Node:     17, Layer:    AppCbrClient, from 17 to 13 (id = 4), start = 340000000000 ns,
end = 340100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     17, Layer:    AppCbrClient, from 17 to 20 (id = 3), start = 297000000000 ns,
end = 297100001000 ns (closed) ns, bytes sent = 3000 B, pkts sent = 2, throughput =
239997 bps
Node:     17, Layer:    AppCbrClient, from 17 to 14 (id = 2), start = 297000000000 ns,
end = 297100000000 ns (closed) ns, bytes sent = 3000 B, pkts sent = 2, throughput =
240000 bps
Node:     17, Layer:    AppCbrClient, from 17 to 23 (id = 1), start = 265000000000 ns,
end = 265100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     17, Layer:    AppCbrClient, from 17 to 13 (id = 0), start = 27000000000 ns, end
= 27100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
Node:     18, Layer:          802.11, pkts from network: 266
Node:     18, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     18, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     18, Layer:          802.11, BCAST pkts sent to chanl: 8
Node:     18, Layer:          802.11, UCAST pkts rcvd clearly: 248
Node:     18, Layer:          802.11, BCAST pkts rcvd clearly: 55
Node:     18, Layer:          802.11, retx pkts due to CTS timeout: 37
Node:     18, Layer:          802.11, retx pkts due to ACK timeout: 0
```

```
Node:     18, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     18, Layer:          802.11, pkt drops due to retx limit: 0
Node:     18, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     18, Layer:      RoutingDsr, Number of Requests Txed = 8
Node:     18, Layer:      RoutingDsr, Number of Replies Txed = 16
Node:     18, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     18, Layer:      RoutingDsr, Number of CTRL Packets Txed = 24
Node:     18, Layer:      RoutingDsr, Number of Data Txed = 242
Node:     18, Layer:      RoutingDsr, Number of Data Originated = 4
Node:     18, Layer:      RoutingDsr, Number of Data Received = 5
Node:     18, Layer:    AppCbrServer, from 0 to 18 (id = 6), start = 430098346454 ns, end
= 430222147266 ns (closed) ns, bytes recv = 1500 B, pkts recv = 3, avg. end-to-end delay
= 52514395 ns, throughput = 96929 bps
Node:     18, Layer:    AppCbrServer, from 15 to 18 (id = 0), start = 250024551503 ns,
end = 250110515284 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 17533393 ns, throughput = 93062 bps
Node:     18, Layer:    AppCbrClient, from 18 to 0 (id = 1), start = 425000000000 ns, end
= 425100000000 ns (closed) ns, bytes sent = 2000 B, pkts sent = 2, throughput = 160000
bps
Node:     18, Layer:    AppCbrClient, from 18 to 15 (id = 0), start = 252000000000 ns,
end = 252100000000 ns (closed) ns, bytes sent = 1000 B, pkts sent = 2, throughput = 80000
bps
Node:     19, Layer:          802.11, pkts from network: 8
Node:     19, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     19, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     19, Layer:          802.11, BCAST pkts sent to chanl: 8
Node:     19, Layer:          802.11, UCAST pkts rcvd clearly: 0
Node:     19, Layer:          802.11, BCAST pkts rcvd clearly: 60
Node:     19, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:     19, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     19, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     19, Layer:          802.11, pkt drops due to retx limit: 0
Node:     19, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     19, Layer:      RoutingDsr, Number of Requests Txed = 8
Node:     19, Layer:      RoutingDsr, Number of Replies Txed = 0
Node:     19, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     19, Layer:      RoutingDsr, Number of CTRL Packets Txed = 8
Node:     19, Layer:      RoutingDsr, Number of Data Txed = 0
Node:     19, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     19, Layer:      RoutingDsr, Number of Data Received = 0
Node:     20, Layer:          802.11, pkts from network: 66
Node:     20, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     20, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     20, Layer:          802.11, BCAST pkts sent to chanl: 58
Node:     20, Layer:          802.11, UCAST pkts rcvd clearly: 6
Node:     20, Layer:          802.11, BCAST pkts rcvd clearly: 79
Node:     20, Layer:          802.11, retx pkts due to CTS timeout: 17
Node:     20, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     20, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     20, Layer:          802.11, pkt drops due to retx limit: 2
Node:     20, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     20, Layer:      RoutingDsr, Number of Requests Txed = 58
Node:     20, Layer:      RoutingDsr, Number of Replies Txed = 1
Node:     20, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     20, Layer:      RoutingDsr, Number of CTRL Packets Txed = 59
Node:     20, Layer:      RoutingDsr, Number of Data Txed = 7
Node:     20, Layer:      RoutingDsr, Number of Data Originated = 7
Node:     20, Layer:      RoutingDsr, Number of Data Received = 0
Node:     20, Layer:    AppCbrClient, from 20 to 13 (id = 3), start = 660000000000 ns,
end = 661900000000 ns (closed) ns, bytes sent = 20480 B, pkts sent = 20, throughput =
86231 bps
Node:     20, Layer:    AppCbrClient, from 20 to 17 (id = 2), start = 363000000000 ns,
end = 363100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000
bps
Node:     20, Layer:    AppCbrClient, from 20 to 13 (id = 1), start = 220000000000 ns,
end = 220100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000
bps
Node:     20, Layer:    AppCbrClient, from 20 to 13 (id = 0), start = 53000000000 ns, end
= 53100000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 2, throughput = 40000 bps
```

```
Node:     21, Layer:          802.11, pkts from network: 29
Node:     21, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     21, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     21, Layer:          802.11, BCAST pkts sent to chanl: 29
Node:     21, Layer:          802.11, UCAST pkts rcvd clearly: 0
Node:     21, Layer:          802.11, BCAST pkts rcvd clearly: 107
Node:     21, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:     21, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     21, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     21, Layer:          802.11, pkt drops due to retx limit: 0
Node:     21, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     21, Layer:      RoutingDsr, Number of Requests Txed = 29
Node:     21, Layer:      RoutingDsr, Number of Replies Txed = 0
Node:     21, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     21, Layer:      RoutingDsr, Number of CTRL Packets Txed = 29
Node:     21, Layer:      RoutingDsr, Number of Data Txed = 0
Node:     21, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     21, Layer:      RoutingDsr, Number of Data Received = 0
Node:     22, Layer:          802.11, pkts from network: 29
Node:     22, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     22, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     22, Layer:          802.11, BCAST pkts sent to chanl: 29
Node:     22, Layer:          802.11, UCAST pkts rcvd clearly: 0
Node:     22, Layer:          802.11, BCAST pkts rcvd clearly: 109
Node:     22, Layer:          802.11, retx pkts due to CTS timeout: 0
Node:     22, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     22, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     22, Layer:          802.11, pkt drops due to retx limit: 0
Node:     22, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     22, Layer:      RoutingDsr, Number of Requests Txed = 29
Node:     22, Layer:      RoutingDsr, Number of Replies Txed = 0
Node:     22, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     22, Layer:      RoutingDsr, Number of CTRL Packets Txed = 29
Node:     22, Layer:      RoutingDsr, Number of Data Txed = 0
Node:     22, Layer:      RoutingDsr, Number of Data Originated = 0
Node:     22, Layer:      RoutingDsr, Number of Data Received = 0
Node:     23, Layer:          802.11, pkts from network: 350
Node:     23, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     23, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     23, Layer:          802.11, BCAST pkts sent to chanl: 12
Node:     23, Layer:          802.11, UCAST pkts rcvd clearly: 164
Node:     23, Layer:          802.11, BCAST pkts rcvd clearly: 53
Node:     23, Layer:          802.11, retx pkts due to CTS timeout: 541
Node:     23, Layer:          802.11, retx pkts due to ACK timeout: 25
Node:     23, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     23, Layer:          802.11, pkt drops due to retx limit: 8
Node:     23, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     23, Layer:      RoutingDsr, Number of Requests Txed = 12
Node:     23, Layer:      RoutingDsr, Number of Replies Txed = 8
Node:     23, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     23, Layer:      RoutingDsr, Number of CTRL Packets Txed = 20
Node:     23, Layer:      RoutingDsr, Number of Data Txed = 330
Node:     23, Layer:      RoutingDsr, Number of Data Originated = 324
Node:     23, Layer:      RoutingDsr, Number of Data Received = 150
Node:     23, Layer:    AppCbrServer, from 13 to 23 (id = 10), start = 710035755953 ns,
end = 710035755953 ns (closed) ns, bytes recv = 500 B, pkts recv = 1, avg. end-to-end
delay = 35755953 ns, throughput = 0 bps
Node:     23, Layer:    AppCbrServer, from 17 to 23 (id = 1), start = 265017085089 ns,
end = 265110514216 ns (closed) ns, bytes recv = 1000 B, pkts recv = 2, avg. end-to-end
delay = 13799652 ns, throughput = 85626 bps
Node:     23, Layer:    AppFtpClient, from 23 to 0 (cid = 1), start = 630141937375, end =
645239410580 ns (closed), bytes sent = 154267 B, bytes recv = 267 B, throughput = 81744
bps
Node:     24, Layer:          802.11, pkts from network: 12
Node:     24, Layer:          802.11, pkts lost due to buffer overflow: 0
Node:     24, Layer:          802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:     24, Layer:          802.11, BCAST pkts sent to chanl: 9
Node:     24, Layer:          802.11, UCAST pkts rcvd clearly: 4
Node:     24, Layer:          802.11, BCAST pkts rcvd clearly: 56
```

```
Node:     24, Layer:          802.11, retx pkts due to CTS timeout: 2
Node:     24, Layer:          802.11, retx pkts due to ACK timeout: 0
Node:     24, Layer:          802.11, retx pkts due to FRAG ACK timeout: 0
Node:     24, Layer:          802.11, pkt drops due to retx limit: 0
Node:     24, Layer:          802.11, frgmnt drops due to retx limit: 0
Node:     24, Layer:      RoutingDsr, Number of Requests Txed = 9
Node:     24, Layer:      RoutingDsr, Number of Replies Txed = 2
Node:     24, Layer:      RoutingDsr, Number of Errors Txed = 0
Node:     24, Layer:      RoutingDsr, Number of CTRL Packets Txed = 11
Node:     24, Layer:      RoutingDsr, Number of Data Txed = 1
Node:     24, Layer:      RoutingDsr, Number of Data Originated = 1
Node:     24, Layer:      RoutingDsr, Number of Data Received = 0
Node:     24, Layer:    AppCbrClient, from 24 to 13 (id = 0), start = 686000000000 ns,
end = 686000000000 ns (closed) ns, bytes sent = 500 B, pkts sent = 1, throughput = 0 bps
```

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Cameron Station
   Alexandria, Virginia 22304-6145

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. Dr. James Bret Michael 1
   Computer Science Department, Code CS
   Naval Postgraduate School
   Monterey, California 93943-5101

4. Dr. John Arquilla 1
   Special Operations Academic Group, Code SO/AR
   Naval Postgraduate School
   Monterey, California 93943-5000

5. Kara Kuvvetleri Komutanligi (Turkish Army HQ) 1
   MEBS Dairesi Baskanligi
   Bakanliklar-ANKARA / TURKEY

6. Kara Harp Okulu Komutanligi (Turkish Army Mil. Academy) 1
   Bakanliklar-ANKARA / TURKEY

7. Ozel Kuvvetler Komutanligi (Turkish Special Forces Command) 1
   Bakanliklar-ANKARA / TURKEY

8. Cetin Ogut 2
   Osman Yilmaz Mah.
   Istasyon Cd. Ogutler Apt. No: 10/18
   Gebze-KOCAELI / TURKEY

9. Professor Gordon H. McCormick 1
   Chairman, Special Operations Academic Group
   (Code SO/Mc)
   Naval Postgraduate School
   Monterey, CA 93943-5000

10. The Honorable Edward Warner 1
Assistant Secretary of Defense for
Strategy and Threat Reduction
The Pentagon, RM 4E817
Washington DC, 20301

11. The Honorable Brian Sheridan 1
Assistant Secretary of Defense for
Special Operations and Low Intensity Conflict
The Pentagon, Rm. 2E258
Washington, DC 20301-2500

12. Dr. James Miller 1
Deputy Assistant Secretary of Defense for
Requirements, Plans, and Counterproliferation
Washington, DC 20301-2900

13. Dr. Chris Lamb 1
Director for Requirements and Plans
Office of the Deputy Assistant Secretary of Defense for
Requirements, Plans, and Counterproliferation
The Pentagon, Rm. 4B856
Washington, DC 20301-2900

14. Mr. R. Stephen Day 1
Office of the Assistant Secretary of Defense for
Nuclear, Chemical, and Biological Defense Programs
3050 Defense Pentagon, Rm. 3C125
Washington, DC 20301-3050

15. GEN Peter J. Schoomaker 1
Commander in Chief
US Special Operations Command
MacDill AFB, FL 33608-6001

16. LTG William Tagney 1
Commander
US Army Special Operations Command
Ft. Bragg, NC 28307-5000

17. RADM Eric T. Olson 1
Commander
Naval Special Warfare Command
NAB Coronado
San Diego, CA 92155

18. Lt. Gen. Maxwell C. Bailey 1
Commander
Air Force Special Operations Command
Hurlburt Field, FL 32544

19. MG Bryan D. Brown 1
Commander
Joint Special Operations Command
Ft. Bragg, NC 29307

20. CAPT John McTighe 1
Commander
Naval Special Warfare Development Group
1636 Regulus Ave.
Virginia Beach, VA 23461

21. Joint Staff 1
J3 Special Operations Division
Attn: LTC McNamara
The Pentagon, Rm. 2C840
Washington, DC 20318-3000

22. RADM Joseph Sestak 1
Office of the Chief of Naval Operations
Director, Strategy & Policy Division (N51)
2000 Navy Pentagon, Rm. 4E566
Washington, DC 20350-2000

23. United States Special Operations Command 2
SOOP-JE
7701 Tampa Point Blvd
MacDill AFB, FL 33621-5323

24. United States Special Operations Command 1
SOOP-CP
Attn: Lt. Col. Christian Kazmierczak
7701 Tampa Point Blvd.
MacDill AFB, FL 33621

25. United States Special Operations Command 1
Washington Office
Attn: LTC Peter Allor
The Pentagon, Rm. 2C840
Washington, DC 20301

26. United States Special Operations Command 1
SOJA
Attn: LCDR Kevin Brew
7701 Tampa Point Blvd.
MacDill AFB, FL 33621-5323

27. Jennifer Duncan 3
Special Operations Academic Group
Code (CC/Jd)
Naval Postgraduate School
Monterey, CA 93943-5000

28. Library 1
Army War College
Carlisle Barracks, PA 17013

29. Library 1
Naval War College
Newport, RI 02840

30. Strategic Studies Group (SSG) 1
Naval War College
Newport, RI 02840

31. Department of Military Strategy 1
National War College (NWMS)
Ft. Leslie J. McNair
Washington, DC 20319-6111

32. US Army Command and General Staff College 1
Attn: Library
Ft. Leavenworth, KS 66027-6900

33. Library 1
Air War College
Maxwell AFB, AL 36112-6428

34. US Military Academy 1
Attn: Library
West Point, NY 10996

35. US Naval Academy 1
Attn: Library
Annapolis, MD 21412

36. Maraquat Memorial Library 1
US Army John F. Kennedy Special Warfare Center
Rm. C287, Bldg 3915
Ft. Bragg, NC 28307-5000

37. Commander 1
Naval Special Warfare Group One
NAB Coronado
San Diego, CA 92155

38. Commander 1
Naval Special Warfare Group Two
NAB Little Creek, VA 23521

39. Commander 1
Naval Special Warfare Center
NAB Coronado
San Diego, CA 92155

40. US Special Operations Command 1
Attn: Command Historian
McDill AFB, FL 33608-6001

41. US Air Force Special Operations School 1
EDO, Alison Bldg, 357 Tully St.
Hurlburt Fld FL 32544-5800

42. Naval Special Warfare Development Group 1
Attn: LCDR Michael Scott
1636 Regulus Ave.
Virginia Beach, VA 23461

43. Naval Special Warfare Development Group 1
Attn: LT Chris French
1636 Regulus Ave.
Virginia Beach, VA 23461

44. Dr. Dan Boger 1
Computer Science Department, Code CS/Bo
Naval Postgraduate School
Monterey, California 93943-5101