USING A HELIO BASED PROTOCOL IN A BATTLEFIELD SENSOR NETWORK WITH DIRECTIONAL ANTENNAS AND ENHANCED SECURITY

Except where reference is made to the work of others, the work described in this dissertation is my own or was done in collaboration with my advisory committee. This dissertation does not include proprietary or classified information.

Fred L. Strickland

Certificate of Approval:

Lloyd Stephen Riggs Professor Electrical and Computer Engineering	Yu Wang, Chair Assistant Professor Computer Science and Software Engineering
Min-Te Sun Assistant Professor Computer Science and Software Engineering	Chwan-Hwa ”John” Wu Professor Electrical and Computer Engineering

George T. Flowers
Interim Dean
Graduate School

USING A HELIO BASED PROTOCOL IN A BATTLEFIELD SENSOR NETWORK WITH DIRECTIONAL ANTENNAS AND ENHANCED SECURITY

Fred L. Strickland

A Dissertation

Submitted to

the Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

Auburn, Alabama
August 9, 2008

USING A HELIO BASED PROTOCOL IN A BATTLEFIELD SENSOR NETWORK WITH DIRECTIONAL ANTENNAS AND ENHANCED SECURITY

Fred L. Strickland

Signature of Author

Date of Graduation

VITA

Fred Lon Strickland, son of Alonzo Abe and Myrtle Lorene (Fields) Strickland, was born on April 23, 1952 in Gilroy, California. He graduated with a Bachelor of Arts degree in Religion from Stetson University in 1974. Afterwards, he joined the United States Air Force. During his 21-year military career, Fred completed a Masters of Arts Management and Supervision: Administration (MBA) degree from Central Michigan University in 1977, an Associates of Science degree in Communications Technology from the Community College of the Air Force in 1984, and a Bachelor of Science degree in Computer Science from University of Maryland in 1987. While working on these degrees, he worked in various Air Force communications positions. After retiring from the Air Force, he completed the Masters of Computer Information Science from Troy State University Montgomery in 2001 and was inducted into Gamma Beta Phi Honor Society. Since receiving the MBA, Fred has taught at numerous colleges and universities. He entered the doctoral program in Computer Science and Software Engineering at Auburn University in 2002. After completing the required course work, Fred was inducted into the now defunct Alpha Theta Chi [Regional] Honor Society, into the Delta Epsilon Iota Academic Honor Society, into Golden Key International Honour Society, and into Upsilon Pi Epsilon (International Honor Society for the Computing and Informaton Disciplines). Fred was nominated and accepted to the 2007-2008 Preparing Future Faculty (PFF) program. Fred married Sharyn Lynn Fischer, born to John Robert and Lois Jeanne (Wesley) Metzen and later became the daughter of Donald and Lois Jeanne (Wesley) Fischer, on December 23, 1974 and has a son, James Allen Strickland, born on December 31, 1984. Fred's research interests lie in bridging the gap between wireless computing and communications technology.

DISSERTATION ABSTRACT

USING A HELIO BASED PROTOCOL IN A BATTLEFIELD SENSOR NETWORK WITH DIRECTIONAL ANTENNAS AND ENHANCED SECURITY

Fred L. Strickland

Doctor of Philosophy, August 9, 2008
(M.S., Troy University Montgomery, 2001)
(B.S., Univeristy of Maryland–University College, 1987)
(A.S., Community College of the Air Force, 1984)
(M.A., Central Michigan University, 1977)
(B.A., Stetson University, 1974)
(A.A., Florida Junior College at Jacksonville, 1972)

111 Typed Pages

Directed by Yu Wang

The problem is that current battlefield sensors are deployed close to each other, are draining batteries at a fast pace, are using protocols that result in late and coarse grain information, and put the human operator at risk. In labs and in graduate research, the problem solving approach is to address a small segment of an area. The other issues are assumed to be solved or are left to someone else to address. As a result, when someone attempts to pull together the various solutions, mismatches and conflicts arise.

This dissertation project used an integrated approach of addressing at the same time some of the software, hardware, and security issues for supporting a wireless environment. For example, the public safety world needs the ability to locate a person or an asset with a minimal amount of infrastructure and overhead. Current technology does a poor job of pinpointing the exact location and tends to provide information in two-dimensions. (Closely related to this is the issue of locating users that are using access points.) Another example is a sensor network whereby most solutions result in energy-demanding approaches.

The narrow focus of this dissertation project has been the battlefield sensor network. In additional to the normal challenges of establishing and maintaining the network, there are the requirements to operate undetected. The current approach is to use minimal transmitter power, which requires

the close spacing of the sensors. But this approach has some drawbacks. For example, when there are many sensors in an area, the likelihood of a chance discovery increases. Closely related to this drawback are two other problems: Greater network congestion and greater likelihood of signal interception.

Our novel concept could solve many problems and have enhanced security. Our proposed approach makes the following assumptions:

1. The base station or the net control station (NCS) has the following capabilities:
    (a) Able to communicate with many nodes at the same time on several channels.
    (b) Very robust with high speed processing for handling large volume of information.
    (c) Unlimited power. (No batteries used.)
    (d) Directional antenna with active sectors.
2. The nodes have the following capabilities:
    (a) Function as a sensor.
    (b) Transmit straight to the NCS.
    (c) Able to change frequencies and channels.
    (d) Receive control messages.

Simulation and real world experience show that these and other problems could be solved in a simple energy-saving way.

“All truth passes through three stages. First, it is ridiculed, second it is violently opposed, and third, it is accepted as self-evident.” – German philosopher Arthur Schopenhauer (1788-1860)[1]

ACKNOWLEDGMENTS

I would like to express my deep gratitude to Dr. Alvin S. Lim, who helped put me on this journey. I wish to express my very deep gratitude to my advisor, Dr. Yu Wang for her encouragement, insight, and support. She has helped to keep me on track. Thanks are also due to all members of my advisory committee–I received hardware insights from the Department of Electrical and Computer Engineering representatives and I received software insights from the Department of Computer Science and Software Engineering representatives. Special thanks are due to members of the Department of Computer Science and Software Engineering for all the useful advice, encouragement, prayers, and support I have received throughout my career as an Auburn graduate student. Finally, I wish to express my deepest thanks to my wife, Sharyn F. Strickland, for her help and her encouragement and to my son, James A. Strickland for being proud of his father.

Style manual or journal used The plainnat option of the NatBib package that is part of the LaTeX2e package. Citation usage and bibliography follows the IEEE style with some adjustments based on the Graduate School guidance and on van Leunen's *A Handbook for Scholars.*

Computer software used The document preparation package LaTeX2e using the book document class with selected options.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

When the purpose or function of any wireless network is reduced to the key points, then we are looking at (1) locating resources and (2) collecting information. The wireless network attempts to locate people, resources, other computers, or access points. And the wireless network attempts to collect data or sensor information and route it to the requestor.

1.1 Location Examples

For some concrete examples of the first key point, consider public safety individuals, airborne search and rescue, and locating users on an access point. Each of these are attempting to do resource location with minimal overhead or no infrastructure.

Individuals working in the public safety world have enough challenges without having to deal with the problem of imprecise location information. A glaring and tragic example from recent history is "9-11." On 11 September 2001, the buried firefighters' air tanks made "man-down" chirping sounds. However, the rescuers could not determine exactly where the person was located and how deep in the rumble. The haunting sounds continued until the batteries expired.

The United States Department of Homeland Security (DHS) used its SAFECOM Program to explore this problem area and other related issues. In March 2004, DHS published *Statement of Requirements for Public Safety Wireless Communications and Interoperability* [7]. The DHS envisioned that future firefighters would wear a vest that would measure each firefighter's "pulse rate, breathing rate, body temperature, outside temperature, and three-axis gyro and accelerometer data" plus measure the available air supply in the personal oxygen tank [7]. In addition, the vests would transmit geo-location, sensor data, and the firefighter identification (ID). Today such a vest does not exist and there are no reliable means to precisely locate a firefighter or other public safety person inside a structure.

The foregoing is from the viewpoint of supporting public safety workers, but miners have lost their lives from coal mining explosion and from cave-ins. It is tragic when the miners survive a cave-in, but die when the rescuers have no idea where to look to find them. A recent tragic example in this century was the Crandall Canyon mine near Huntington, Utah. In August 2007, 6 miners died from most likely from a lack of air and 3 rescue workers died from attempting to dig a rescue tunnel. (The rescue approach is to drill tunnels until one of these breaks through to the correct spot.) After this cave-in, the rescue tunnel drilling was called off. If the 6 trapped miners were still alive, then in time they would die from the lack of food, water, and air. Wayne Rash, the Senior Analyst for *eWEEK Labs* wrote an article asking whether RFID could have helped to locate the miners[8].

The Air Force Auxiliary/Civil Air Patrol (AFAUX/CAP) "flies 95 percent of all federal inland [search and rescue] missions" [9]. Flying a gird search pattern and keeping track of the airborne resources are major challenges. This could result in two worst case situations. The first is that an area is notcovered and the victim is missed. The second is that the aircraft could fly into each other and drop out of the sky.

Locating a person who is moving from access point to access point is another challenge. How does the environment perform tracking when the only device the person is carrying is a portable computer?

1.2 Collection Examples

For an example of the second key point, consider civil (non-military) wireless sensor networks and battlefield sensor networks. Both collect information where it is not possible to run landlines. Or the location is not safe for a person to be. Another usage might be when the object is moving as in the case of wildlife or of a military target.

These tend to be in industrial, scientific and medical (ISM) radio bands with a number operating in the 902-928 MHz ISM sub band. To avoid using high power and shortening the battery life, the sensors tend to be place very close to each other. But this approach has several drawbacks.

First, more nodes are needed in order to relay messages from other nodes. Second, overlapping data collection coverage may result. Compounding the last drawback is that some routing protocols do not scale up very well with a large number of nodes. One protocol attempts to solve this drawback by having certain nodes preprocess or aggregate the data and these make contact with other nodes for relaying messages. The result of this approach is that these special nodes must be carefully deployed to be in the correct spot or every node is given this ability and a scheme must be provided that will determine which nodes will be "special" and which nodes will be "regular." The solution thus becomes more complex.

1.3 Battlefield Sensor Networks

Battlefield sensor networks have additional challenges. Whereas civil sensors could be placed with great precision and special units could be added to the sensor field, battlefield sensors might need to be air dropped and this would make placement very general. Hence, every unit must have the same ability. Civil sensors may not be bothered by wildlife or by a person exploring the wilderness. With battlefield sensors, the enemy is looking for anything that is not natural to the area. If close spacing is used, then the chances are increased that a battlefield sensor might be noticed. Will the enemy hear the transmissions? Depending upon the location, civil users might be able to swap out batteries. For battlefield sensors, this might not be an option. Some civil sensors could be configured to sample the general environment and route this information to the base station[1]. For a rapidly changing combat environment, the information needs to be current and sent immediately to the home base. Will the battlefield sensors be able to transmit the information to home base in a timely manner? Civil sensors do not have a threat from a "foreign power" trying to take over the network. For battlefield sensors, this is a very real threat. Civil sensors relay for each other. For battlefield sensors, the extra transmissions could make it easier for the enemy to discover the network and to map it.

There is another drawback that is frequently lost in the discussions on battlefield sensor networks. The information must be passed to the command center. How is this done? Extrapolating the

[1] It is customary in formal writing to use a shorter form for an expression that appears numerous times. Unfortunately, the shortened form of "base station" is "BS," which is also an American English expletive ("bad language"). So I will use the complete spelling in order to avoid invoking this meaning in the reader's mind.

discussion, it would seem that the commander center must be a sensor node hop away or there must be a "bread crumb" line of something (sensors or generic nodes) providing an "Information Highway" to the commander center. The first approach sets up the command center to be attacked by a missile or to be overrun by a swarm of foot soldiers. The second approach provides a series of single point failures or an easy way for the enemy to find the command center. Having duplicate "bread crumb" routes does not solve the problem, because these provide more means for locating the command center.

1.4 White Hats vs. Black Hats

The rapid and "break-neck" pace in the development of wireless technology has created new capabilities and opportunities. On one side, the "white hat" computer community tries to exploit these for the benefit of mankind. But on the other side, the "black hats" try to find new ways to make life difficult for everyone by such acts as denial of service attacks, blocking messages, and changing messages.

Since there is no "gatekeeper" or inspector to make sure the players are legitimate and that everyone plays by the rules, it would seem to be a wiser course of action to incorporate safety and security features during the development stage. But safety and security are rarely considered during the "drawing board" stage. As a result, many fixes and patches are needed to address weaknesses in a deployed system.

1.4.1 Small Parts

In labs and in graduate research, the normal problem solving approach is to address a small segment of an area. The other issues are assumed to be solved or are left to someone else to address. As a result, when someone attempts to pull together the various solutions, mismatches and conflicts arise.

1.4.2 Focus

With the limitations of time and of resources, the dissertation problem area was narrowed to address the unique challenges of battlefield sensors. Rather than attempt to build a harden sensor, the focus was on devloping a workable protocol.

Previous efforts took a “table top” study approach to identify the needed features for such a protocol. The proposed protocol has three parts:

- Directional antennas
- Software to determine range and direction
- Security

1.5 The Helio Family

The approach is a heliocentric (“helio” is the shorten form) protocol suite. For over the past year or more, the concepts and issues have been explored. At this writing, there are four helio-based protocols.

HERBSUDAI[2] (**HE**liocentric **R**obust **B**ase **S**tation **U**sing **D**irectional **A**ntennas and **I**nferences) could be used for tracking people or resources.[3]

HAP (**H**eliocentric **A**P **P**rotocol) and **HAPDA** (**H**elicoentric **A**P **P**rotocol using **D**irectional **A**ntennas) could be used for routing traffic in a network.

HEAPINGS (**HE**liocentric **A**d hoc **P**rotocol using **I**nferences and **N**ominal resources to provide a **G**lobal view with **S**ecurity) could be used in a combat or battlefield sensor environment.[4][5]

[2] Pronounced as “Herbs You Doll.”

[3] The IEEE 7th BIBE (BIBE07) accepted 65 papers out of 500-plus submissions for inclusion in a printed proceedings. Noteworthy papers that could not be included were rendered as poster session papers and these were to be published on the conference website. In checking before, during and after the conference dates of 14 through 17 October 2007, none of the poster session papers were placed on the conference website.

[4] Until 25 June 2007, this was an unpublished and unpresented concept. On that day, I presented a paper at the 2007 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP ’07)[10]. The proceedings were published in the Fall.

[5] A second paper was presented at WORLDCOMP ’08[11].

Chapter 2

LITERATURE REVIEW

To provide a background of the helip protocols, the work of others will be reviewed.

The literature review is divided along three lines. The first part is from the viewpoint of engineers–in a single word “hardware.” The second part is from the viewpoint of computer sciencists–in a single word “software.” The third part covers security and privacy issues.

The interest in hardware (especially radios and antennas) has been present since the dawn of radio communications, but the computer scientists’ interest has only been since the 1980s. And of course, the interest in security has grown as the result of many bad experiences with viruses and other problems.

Commercial interests and topics are covered as extra material in Appendix B.

2.1 Hardware Viewpoint

Many papers have been written on radio communications and on antennas. Most of the papers included in this literature review are from personal communications conferences and symposiums such as the International Conferences on Personal Wireless Communications (better known as PWC yy) and the Institute of Electrical and Electronics Engineers (IEEE) International Symposium on Personal, Indoor and Mobile Radio Communications (better known as PIMRC yyyy). Other papers are from sources that address antenna applications and theory. There are three general areas:

- Efforts to Improve Signal Strength
- Smart Antenna Systems
- Obtaining Information from Antennas

Some papers could be placed into two areas and the decision is based on which topic is covered in greater depth.

Software Defined Radios (SDRs)[12] are the newest frontier in communications hardware work. A working premise of this PhD effort is that the nodes will have the ability to generate any wavelength (a radio frequency). By assuming the usage of SDRs, this enables using a totally different approach. Instead of using software to overcome the limitations of the hardware, the advanced hardware will enable a simpler protocol to be used.

2.1.1 Efforts to Improve Signal Strength

One approach is to use transmit diversity, which involves using several antennas. A good example of this concept is the defunct northern tier (the unpopulated areas of northern Canada) Distant Early Warning communications sites (better known as "DEW line" sites) that used large troposphere scatter ("troposcatter") communications systems. These sites used two large antennas in order to improve the chances of the distant stations receiving a complete signal. Northern Lights disrupt HF communications by interfering with the skip or bounce behavior in the upper layers of the atmosphere. The troposphere level in the lower atmosphere does not seem to be bothered as much. See Figure 2.1 to view a diagram of a troposcatter network (courtsey of US Army.[1]).

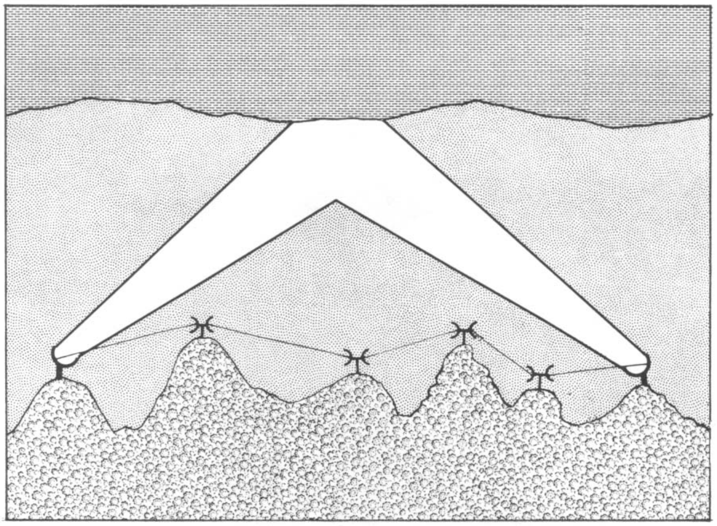


Figure 2.1: Drawing of Troposcatter Network

[1] Source is from the Army's history website. http://www.history.army.mil/books/Vietnam/Comm-El/Photos/pg08.jpg

Vishwakarma and Shanmugan took this concept and applied it to a base station with the intent to see if this could “improve the forward link transmission performance (throughput, range, capacity and quality) without increasing the complexity of the mobile station [13].” They only did analysis with a simulator of two diversity schemes, but the results did look promising. Elsewhere Chheda explored this concept by analyzing three different diversity schemes [14].

Another concept is to use different polarization. It is common knowledge that both ends of the communications link should use the same polarization. Jeppesen et al. used this approach in order to reduce interference and improve performance [15].

2.1.2 Smart Antenna Systems

Smart antennas are antennas that can develop beams in one or more desired directions. Much work has been done with these systems. These have resulted in a number of benefits.

Traditional antennas work well with narrow signals, but do not work well with spread spectrum techniques. Adaptive arrays (“Smart Antenna Systems”) are used to “maintain orthogonal signal constellation in code division multiple-access signaling (DS-CDMA)” by means of tracking the desired signal and generating null patterns toward unwanted signals [16]. Currently, researchers are attempting to solve challenges such as when a signal bandwidth goes beyond a threshold, then the performance falls off [16].

Smart antennas can improve the capacity of a cellular tower while performing load balancing. Feuerstein et al. discovered through simulations and field trials that a “bolted on” smart antenna resulted in greater than 50 percent improvement; flexible sectorization resulted in improvements up to 75 percent; and integrated as a subsystem resulted in improvements ranging from 100 percent to 200 percent [2]. Figure 2.2 (courtesy to Feuerstein et al.) shows a block diagram of how the smart antenna might be integrated into a radio.

Rambabu and Rajagopal explored using a “pilot beam” with a smart antenna system [3]. The result is that each cellular phone user would be dead center of a directional beam as illustrated by Figure 2.3 (courtesy to K. Rambabu and R. Rajagopal). The idea of using smart antennas in a cellular phone network has been explored for some time by many researchers. Rambabu and Rajagopal’s approach is to use a “pilot beam” to augment sectors that have a “spike” of heavy

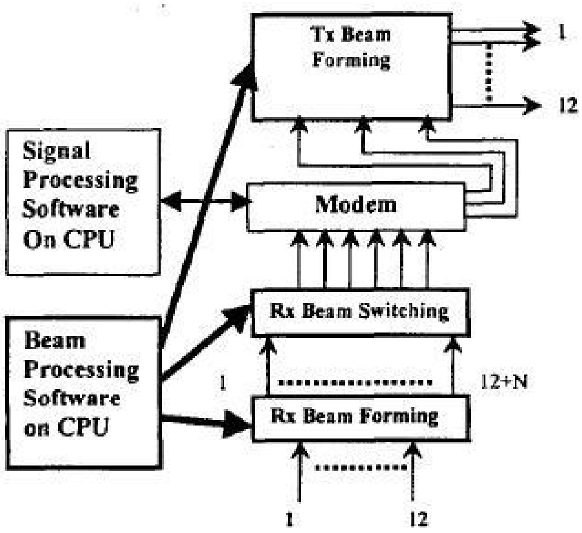

Tx Beam Forming
1
12
Signal Processing Software On CPU
Modem
Rx Beam Switching
Beam Processing Software on CPU
1
12+N
Rx Beam Forming
1
12

Figure 2.2: Smart antenna equippped channel element [2]

traffic.

Smart antennas could be used on both ends of the communications link. Czylwik explored using smart antennas in space division multiple access (SDMA), time division duplex (TDD), and frequency division duplex (FDD) [17]. He found that frequency reuse is improved, co-channel interference is reduced, and less power is needed by the mobiles. Czylwik's focus was not on these benefits, but rather he spent the rest of his paper on how to reduce the effects of fast fading.

2.1.3 Obtaining Information from Antennas

2.1.3.1 Direction of Arrival

Engineers are aware that signals reach an antenna from different directions. For example, Dandekar et al. used the direction of arrival (DOA) as one tool for analyzing their smart antenna data [18]. AlMidfa et al. used polarization diversity to improve the estimation of the DOA [19].

DOA could be used with field strength to determine the distance to or from a station. This is called propagation modeling and one could do this for an area. Hoppe et al. found a novel way to reduce the processing workload by preprocessing some of the data ahead of time [4]. They took a

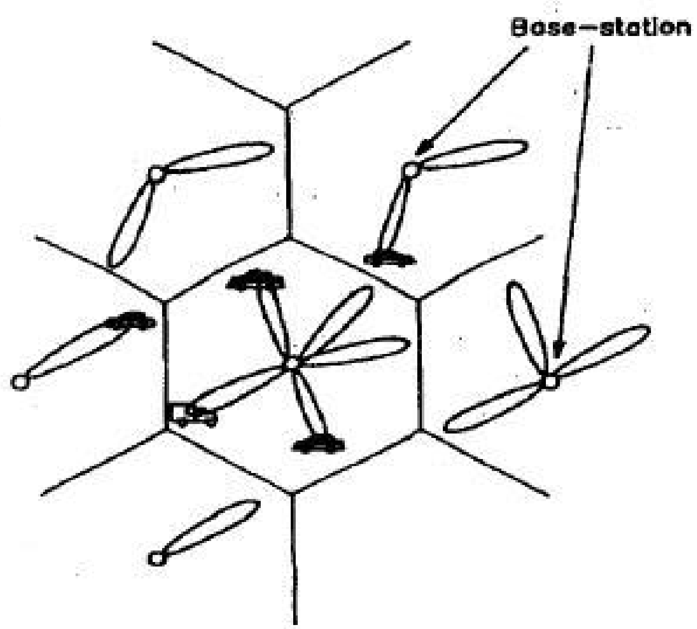


Figure 2.3: Tracking of mobiles wit multiple beams[3]

building (see Figure 2.4 (courtesy to Hoppe et al.).) and create a database based on the planes, corners, and its material. Then they preprocessed the data so that they could know ahead of time how a signal would travel through the building and the amount of degradation that would be experienced.

The preprocessing assumes that every signal that comes into the building at a certain point would take the same path through the building. Figure 2.5 (courtesy to Hoppe et al.) illustrates this idea.

Although preprocessing does speed up the raw work, the approach has some draw backs. First, creating the database for one building takes time. Second, deploying the database of more than one building would be a problem since laptops do not have unlimited storage. Third, buildings experience change over time–aging and structure changes such as a room addition or a major renovation. Fourth, the model does not address things in a room–adding or removing items would change the

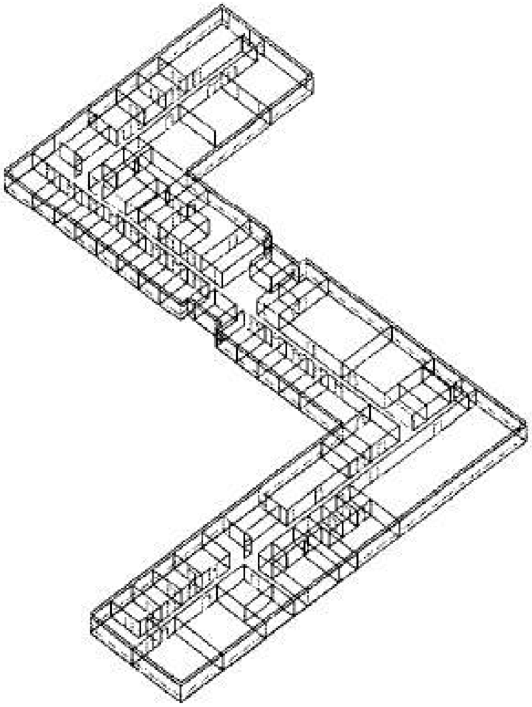


Figure 2.4: Example for an indoor database [4]

signal path and behavior. Fifth, collecting changes and publishing to the users would take time and it would be hard to keep current. Sixth, should temporary structures be documented or not? In short, attempting to provide a fire department or public service agency with this information for a whole city would be impossible. Keeping the information on a major fixed system (such as a super computer) means that the user needs to link-up and stay connected while traveling to a service call. Cellular towers are not yet providing full coverage to every spot in a city. Creating a new network of cells independent of the public cellular system would be very expensive and may not be possible due to legal and other reasons.

Instead of using ray tracing, with or without data preprocessing, other researchers are looking at models that create a smaller database or that make assumptions about the environment. Tingley and Phlavan used a statistical model of the space-time radio propagation to estimate behaviors [20]. Their early results indicated that this tracks nicely and the system could be used to determine

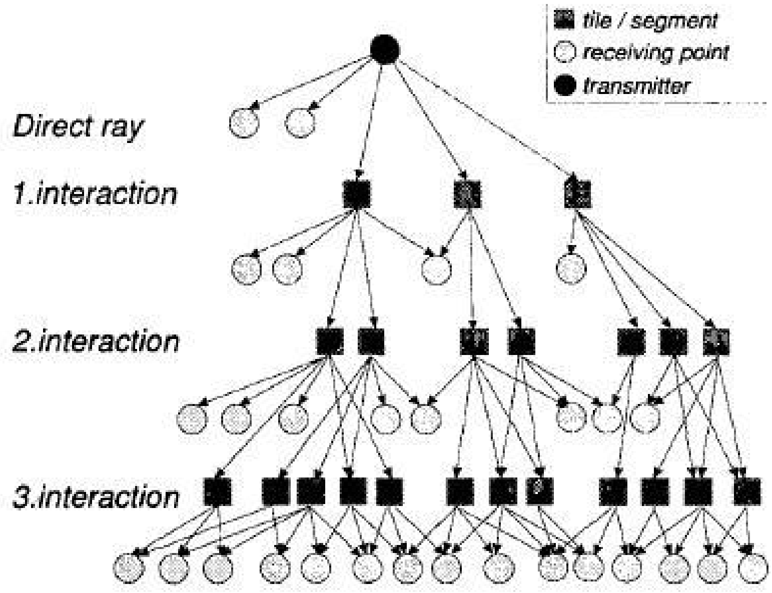


Figure 2.5: Tree structure of the visibility relations [4]

geo-location.

Curry et al. found that the angles of arrival (AOA) would vary greatly and this could give rise to the belief that the source could be located anywhere. But when one looks for clusters where the AOA varies slightly from each other, then these would have the shortest route to the transmitter. With this insight, Curry et al. attempted to develop algorithms that could quickly determine the correct route between the transmitter and the receiver. See Figure 2.6 (courtesy to Curry et al.).

2.1.3.2 Wired for Geo-location

Both the IEEE 802.11 standard and the European Telecommunications Standards Institute (ETSI) HIgh PERformance Radio Local Area Networks (HIPERLAN) standards addressed geo-location requirements in future wireless Local Area Networks (LAN). Xinrong et al. explained that the HIPERLAN/2 “geo-location system architectures can be roughly grouped into two categories, mobile-based and network-based” and that both approaches need “more than three geo-location Base Stations (GBS) ... [in order] ... to geometrically locate [a mobile terminal] using multiple [Time of Arrival

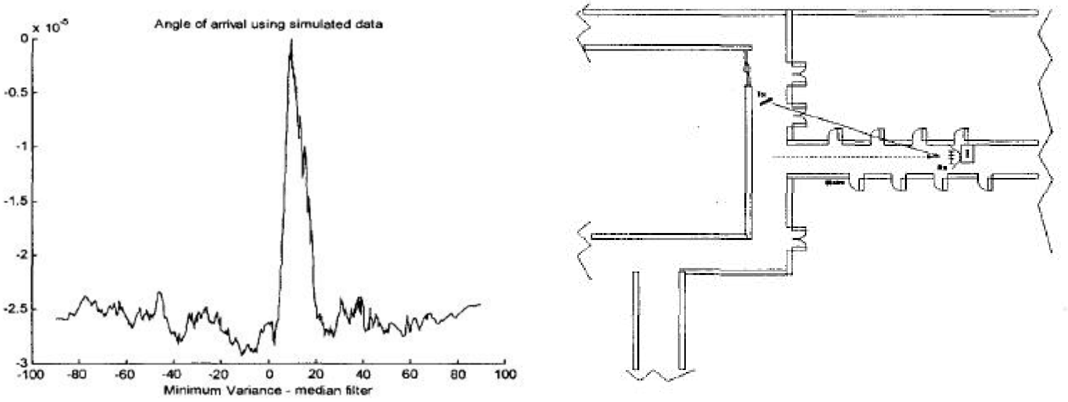


Figure 2.6: Discovering and mapping the best routes through a building

and Time Difference of Arrival] measurements [5]. (This is a different approach from the commercial examples that are mentioned in Appendix B.)

Although this approach is independent of the Global Positioning System (GPS) and is able to extract location information from the signal, it falls short for firefighters, AFAUX/CAP, and battlefield deployed sensors. The HIPERLAN/2 network operates in 5 GHz band with 30 meters range typical for an indoor environment and 150 meters possible inside a large room (such as a gymnasium). The information is extracted from access points in the room. See Figure 2.7 (courtesy to Xinrong et al.) for how the HIPERLAN/2 network is configured. In the normal mode (Centralized Mode), access points manage all transmissions, including mobile to mobile transmissions. If power is lost to the access points, then geo-location information cannot be obtained. Also the mobile user must be accepted as a valid participant in the network.

2.1.3.3 Radars

Radio Detection and Ranging (RADAR or radar) is a concept that dates back to at least the 1940s. Although research is still being done, the concept has matured to the point that commercial and non-commercial systems have been deployed. The concept is that information can be extracted from the signal to determine a target's range and position. A strong narrow, beam is sent out. When it hits an object, part of the energy is bounced back to the source where a sensitive receiver processes

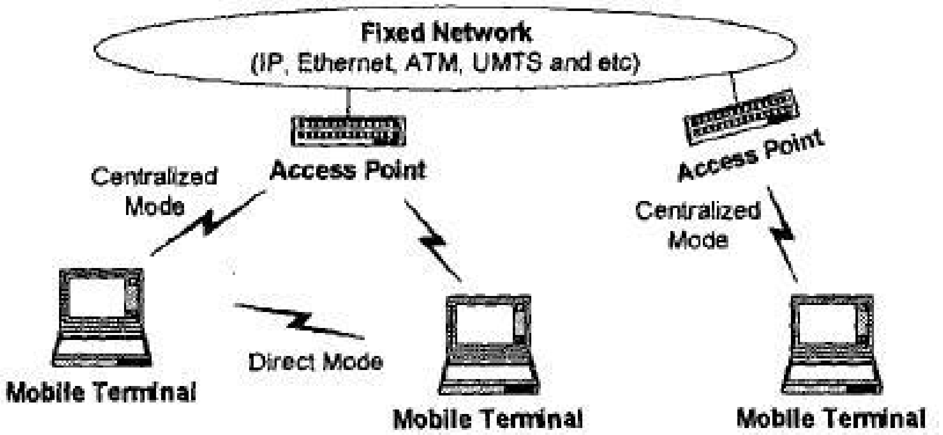


Figure 2.7: the HIPERLAN/2 network [5]

the signal[21].

There are different types used. A slow pulse rate radar can reach out to a great distance. A fast pulse rate radar can track close-in targets. A Doppler radar can track a large number of small objects, such as rain drops. Fast clocks and equations are used to obtain distance and direction. See Figure 2.8 (courtsey of Air University, Air Force) for an illustration.

One example of ongoing research is V. A. Kryachko's 2003 paper concerning a better equation for determining the direction finding characteristic of a pencil-beam antenna [22]. Another example is Bagdasaryan et al. 2003 conference paper concerning a better way to correct for background interferences when an adaptive antenna array is used to determine the direction of a signal [23]. A third example is Kukobko et al. 2003 conference paper about calculations for reducing the impact that an aircraft radome (the cover or shield that protects the radar while in flight) has on the direction-finding function [24].

There is a class of radars known as subsurface radiolocation. These are portable and can penetrate the ground in order to find objects. The approach takes four stages in order to generate useful information. This is still a new area and papers are being published. For example, Grinev et al. explored a different solution to the inverse problem set [25].

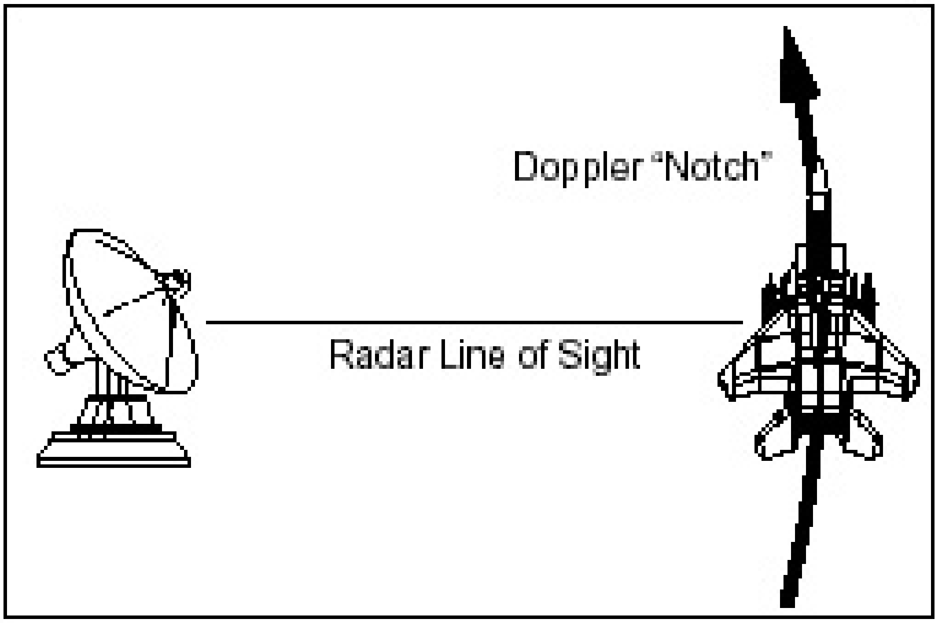


Figure 2.8: Ground radar tracking an aircraft

Radars do not require a "wired" environment. Radars can function in a stand-alone configuration and do not need support from GPS. But there are drawbacks:

- The site needs to support a high power transmitter.
- The receivers are very sensitive.
- The antennas are huge (large, high gain parabolic antennas).
- The target must be useful. (Can reflect the signal back.)
- A network would require close placement[2].

Hence radars would not be very helpful for supporting resource locating or for supporting battlefield sensors.

[2] For example, Doppler weather radars are placed 100 or more miles apart. Great details are gathered about the tops of storm systems, but not about the lower levels. DrK̇elvin Droegemeier of the Center for Analysis and Prediction of Storms, Sarkeys Energy Center, University of Oklahoma, Norman OK 73019, would like to see Doppler dishes placed about 20 miles apart [26]. In such a Doppler radar rich world, more information could be provided about weather systems and tornado formation should be easier to track.

2.1.3.4 Pulse Signal Propagation

Much work is being done with pulse signal propagation. Pazynin and Sirenko explored pulse signal propagation in the urban environment by using the finite-difference method [27]. Their main interest is with pulsed emissions and they saw that these lessons could be applied to communications systems such as a cellular telephone network. They determined that their approach would use a small database. This is in opposition to Hoppe et al. approach, which uses a huge database.

2.1.3.5 Distances in Free Space (Real World, not in a Lab)

Rosengren et al. offered a different approach for measuring antenna radiation efficiency [6]. The traditional measurement method involves using free space or special chambers with the result that the multi-path component is eliminated. Rosengren et al. see this approach as being expensive, labor-intensive, and time consuming with questionable results. Their premise is that measurements need to be performed in a test environment that is similar to the real world. Figure 2.9 (courtesy to Rosengren et al.) shows how the test environment is configured with the transmit antenna in one corner and the receiving antenna is in the middle near the far side. Any object added to the room would cause the transmitted signal to take multiple paths to the receiver. In the case of the cylinder, it is filled with material that is similar to the density and material that exists inside the human skull.

They found that the measurements are "... almost the same in the whole ... chamber ... if the receiving antenna is [half a wavelength distance] away from the wall." Rosengren et al. generated results for three distances on two different occasions with the result that the measured values ranged from 89 to 98 percent of the free space values. Although Rosengren et al. main purpose was to show a cheaper, faster way for determining radiation efficiencies, they did work with distances.

Davis et al. took measurements in several hospital corridors and found that within one meter, the field strength fell off as expected, but beyond that radius, the decline *was slower than expected*[3] [28]. They wrote that the separation requirements may need to be increased between the various medical devices that use the radio spectrum. Trueman et al. worked with one hospital corridor and used

[3] Italics are mine.

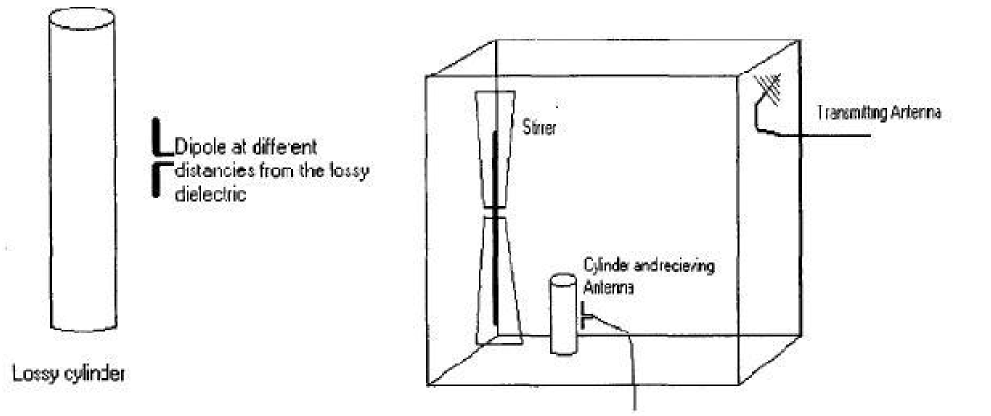


Figure 2.9: Model for FDTD calculations (left) and a sketch of measurement setup in the reverberation chamber [6]

geometrical optics. They noticed that walls of various construction material had different reflection values with plaster and wire construction having the greatest reflection values [29].

2.2 Software Viewpoint

2.2.1 Efforts in Using Directional Antennas without any Protocols

For the longest time, only engineers worked with antennas. But that began to change in the 1980s when the Association for Computing Machinery (ACM) published a paper [30] on multi-beam antennas for satellites. This paper listed two benefits of directional antennas: "Available power can be concentrated in areas actually in use at a given time" and nulls could be created as a block against interference. The rest of the paper addressed dish antennas and the special issues of satellite communications. There was no efforts to explore these identified benefits.

The ACM Special Interest Group (SIG) on Office Information Systems existed from 1983 to 1988. In the final year before it became part of the Information Systems SIG, an interesting paper was published. Pahlava wrote about radio frequency systems and infrared systems for offices [31]. He noted that two or more cells could be connected with "a high-power, *narrow-beam*[4], optical signal."

[4] Italics are mine.

The author did not explore this idea. Instead, he explored improving signals with different diversity techniques.

In the late 1980s and early 1990s, cellular networks were the “hot new technology.” *IEEE Transactions on Vehicular Technology* explored using directional antennas whereas ACM looked at power management schemes. Rosberg was typical of the ACM writers of the period when he acknowledged that “more efficient spatial reuse techniques employ[ing] directional and smart antennas [would] enable better frequency sharing” [32]. But no work was done in this area.

In the same issue that the Rosberg’s article appeared, van Rooyen wrote about a different approach in which a model was created to show that directional antennas, Maximum Ratio Combining (MRC) diversity, and a combination of these two resulted in a great improvement over omni-directional antennas in DS-CDMA traffic [33]. However, there was no attempt to address any protocols.

In the only 1998 ACM paper that addressed any directional aspects, Gabber and Wool only looked at using GPS [34]. This was to determine the location of the customer’s rented broadcasting satellite receiver unit. Although this was not a true directional antenna usage, what is noteworthy is the attempt to present an algorithm for how this might be done.

2.2.2 Efforts in Using Directional Antennas in Support of Protocol Based Communications

In 1989, Pronios wrote about using directional receive antennas as a means to improve the slotted ALOHA access protocol [35]. This simple change enabled transmitters to have greater successes in delivering messages and to begin to have a regional approach to traffic handling. Simulation studies indicated that “the throughput improvement was substantial for heavy traffic conditions, and the gains were further amplified if the number of available receivers ... [were] increased.”

In 1992, there was more interest in improving the performance of the slotted ALOHA packet system. Ward’s and Compton’s first paper was about using an adaptive array antenna [36]. The only change that was made to the protocol was to add a preamble, which gave the adaptive antenna enough time to notice the signal and generate an antenna pattern toward the sending station. In their second paper, they expanded the project from a single beam to a multi-beam system [37]. Again, the ALOHA protocol was not changed. The acquisition of signal stage was changed. The

ALOHA receive slots were made a bit wider. If the first packet is completely received, then a second packet from a different station could be received. If this second packet came in too quick, then collision would result and both packets would be rejected.

Sugihara et al. explored how an adaptive array could improve the performance of slotted non-persistent carrier sense multiple access (CSMA). The results suggested that this "... attains higher throughput and lower values for average number of transmissions and schedulings than the conventional slotted nonperistent CSMA mode" [38]. The authors acknowledged that their approach creates (actually, worsens) the hidden terminal or station problem, but they believed that this is something that the network could live with. Also the authors only considered the situation of the base station using the adaptive array; there was no consideration of having both ends using adaptive array antennas.

Shad et al. explored using a smart antenna on an indoor base station [39]. Their main interest was in the use of static space division multiple access (SDMA) and time division multiple access (TDMA) capacity of an indoor system and to explore performing dynamic slot assignments. The smart antenna was the means for obtaining the high quality communications. After five years of work, they provided more information about Dynamic Slot Allocation (DSA) [40]. This paper confirmed that DSA could result in better system capacity. There was no attempt to design a protocol or to improve a current protocol.

Sass provided information about the "tactical Internet" [41]. The US Army's Mobile Subscriber Equipment (MSE) provides circuit switched voice telephone and facsimile, and packet formatted computer data. The MSE uses Internet Protocol (IP) routers and interfaces with other IP networks. Directional antennas are top-mounted on 15- to 30-meter tall masts and are manually aimed. The non-MSE fixed stations in the net may use directional antennas too. The mobile platforms use omni-directional antennas. Directional antennas are used to improve the signal strength (9 dBi gain at 225 to 400 MHz, 20 dBi gain at 1350 to 1850 MHz, and 37 dBi gain at 15 GHz). There are some changes in the protocols, but these were designed to improve the Quality of Service (QoS) and the speed of delivery in a combat environment. These changes did not factor in the benefit of using directional antennas.

One of the results of the military's need for flexible communications is the software defined radio architecture. Razavilar et al. explored how this architecture with smart antennas could solve some communications problems [42]. Currently, the base station requires the mobiles to reduce power in order to combat co-channel interference (CCI) and the far-near problem. By directing a beam[5] to the user or a group of users in the same general area, nulls are "deployed" to block any possible interference. The base station could support more users. The side-benefit is that this increases the received signal strength and thus the user may use a less potent receiver antenna and a lower transmit power setting. Their algorithms only dealt with beam forming.

Gomes et al. looked at Greedy Randomized Adaptive Search Procedure (GRASP) as a means to solve frequency assignment problems within a cellular system [43]. GRASP looks at the most loaded antenna and tries to add more users. If that is not possible, then it looks at the antenna with the next large amount of users. This reduces CCI and adjacent channel interference. It depends upon distance to solve co-site, co-cell, and far-site interference. The authors did not consider directional antennas in their work.

Kobayashi and Nakagaw took a different tact by using a sectored approach instead of using a CSMA/CA approach for all directions [44]. In a computer simulation, an eight-sector arrangement enabled a base station to enjoy a threefold improvement over the omni-directional CSMA/CA and transmission delays were reduced.

Yi et al. looked at capacity improvements with directional antennas [45]. There was no effort to put forth a new protocol or to revise an existing protocol. Instead they looked at antenna patterns. They pointed out that benefits can be achieved by narrowing the antenna beam, but a point is reached when no further narrowing would produce any more benefits.

Cheng et al. wrote about how an electronically steerable parasitic array radiator antenna could be used in both omni-directional and directional mode in order to support ad hoc networks [46]. This antenna is able to develop high gain in both modes.

At MobiHOC 2001, Ramanathan presented some answers to nagging questions such as how to use directional antennas and what are the implications upon ad hoc networking [47]. In a mili-

[5] This is the main energy or signal coming from the antenna. Directional antennas can be positioned to point in a selected direction. The other directions receive very little energy. The receiving behavior is similar; only the directional part receives a strong signal and the other directions would receive very little. The word "null" is some times used to describe these weak or non-received signals.

tary environment, directional antennas mounted on vehicles resulted in better immunity to signal jamming and interceptions. On the other hand, directional antennas may not be possible with laptops, personal digital assistant (PDAs) and other small devices. Instead of creating a new protocol or changing a current protocol, the author merely used current protocols such as CSMA/CA (in two versions: aggressive and conservative), Hello, and link-state routing. He replaced the omni-directional antennas with directional antennas and ran some network simulations. He concluded that performance improvements could be realized: More throughput, less power used, and better neighbor discovery. He did not attempt to solve any problems, but pointed out some areas where future work could be done. (Korakis et al. attempted to expand on Ramanathan's work and they noticed that this protocol must limit the range of the directional antenna, otherwise there is a coverage mismatch [48].)

Takai et al. proposed replacing both the physical layer carrier sensing and the medium access control sub layer (MAC) virtual carrier sensing with Directional Virtual Carrier Sensing (DVCS) [49]. This works with the current protocols by supporting "both directional transmission and reception based on the radio reciprocity, which allows directional transmissions of all frames without incurring unnecessary collisions." The MAC protocols do not need to be modified to work with directional antennas when DVCS is used. In brief, DVCS "...allows the MAC protocol to determine direction-specific channel availability." The authors concluded that DVCS could improve MAC protocols by using directional antennas to work with a subset of nodes while letting the other nodes continue to function in an omni-directional configuration.

2.2.3 Efforts in Using Location Awareness in Support of Protocol Based Communications

Ko and Vaidya noted that wireless networks are burdened with extra message traffic in order to determine valid routes [50]. Their approach, called Location-Aided Routing (LAR), would use GPS location information for route discovery. If the sender does not know the location of the desired station, then it floods out a route request message. On the other hand, if the sender knows the general zone or area, then the route request message is flooded just to that area. If the sender knows that the desired node is in a certain direction, then the route request message is flooded to every node on that "compass heading." Since this protocol does not use directional antennas, every node within range of the transmitting node would hear the route request message. LAR would begin to have some benefits when the nodes are some distance apart and if the deployment area is sizeable. Otherwise, LAR would have the same behavior as a regular ad-hoc network.

Instead of using GPS, Nasipuri and Li proposed a scheme whereby certain sensor nodes would function as a local "GPS" for the other sensor nodes in the network [51]. A node listens to three or more beacon stations in order to determine its position in relation to these stations. The proposal is interesting in that the approach is similar to the space based GPS system. The drawback is that the beacons seem to be transmitting frequently, which would enhance the enemy's ability to detected the sensor network plus drain these beacon nodes' batteries quickly.

2.2.4 Efforts in Developing Protocols to Use Directional Antennas in Ad Hoc Environments

2.2.4.1 Simple Tone Sense (STS)

In 1992, Yum and Hung proposed a simple tone sense (STS) protocol for a multi-hop packet radio networks with multiple directional antennas [52]. This protocol called for the traffic exchanging stations to transmit tones on the unneeded antennas. The intent is that other stations would hear and would know to keep silent. This tries to manage the hidden station problem and to reduce conflicts. They envision that the directional antennas are able to provide 360-degree coverage.

There are some problems with their approach. One of the stated assumptions is that the network consists of all fixed stations; so it would not work with moving users. Another problem is that it takes energy to transmit tones. So a node that is doing this would deplete its batteries in a short amount of time. And still another problem is that those nodes that are aligned in a parallel fashion to the two exchanging nodes would hear the tones on their own directional antennas (perpendicular to this pair's signals), but would not attempt to exchange traffic despite the fact that all of these pairs are using directional antennas and thus would not harm each other's efforts.

is that this approach prevents exchanges that would not conflict from taking place. Hence, the over all throughput is reduced. In short, in order to gain a conflict-free environment, the traffic volume is reduced.

2.2.4.2 Modified Dynamic slot Assignment (DSA) MAC Protocol

In 1996, Horneffer and Plassmann explored using directed (adaptive) antennas in an European wireless cellular network with a modified dynamic slot assignment (DSA) MAC protocol [53]. The regular version of DSA uses one physical channel with several traffic channels multiplexed to that channel. Reservation information and ACKs are sent from the base station to the clients via piggyback messages. With the modified DSA, the base station could handle several clients if they are within the coverage area of the directional antenna beam. If this is not the case, then the modified DSA has a provision For handling this situation. It would use several transmissions in order to service all the clients in the different sectors. The modified DSA does not use a broadcast approach and does not piggyback acknowledgments. Instead a special signaling burst is used. The authors admit that there are some efficiency issues that require more work. What is noteworthy is that this appears to be the first documented attempt to develop a protocol for a mobile environment that uses directional antennas. This is an evolutionary step toward having a protocol to handle an ad hoc mobile network.

In 1997 Sakr and Todd wrote about “reverse link throughput and capacity” [54]. They used the same environment as described by Sugihara [38]. That is, the ALOHA base station uses a beamforming antenna and the clients do not. What is noteworthy about this paper is that the authors devoted some space to a modified carrier-sense protocol. This proposed protocol is able to use smart antennas to reduce CCI and thereby has a more aggressive frequency re-use plan. The protocol uses time division duplexing (TDD) and the Request to Send/Clear to Send (RTS/CTS) reservation mechanism. The protocol has the ability to handle busy periods: “...when the channel becomes busy, this transition defines the start of an uncertainty interval of duration Tr seconds ...[during which] any station generating a packet is free to commence transmitting.” The base station works through the received packets to resolve them and creates starting times for the clients to use. Other clients not involved are carrier-sensed inhibited from transmitting. Then the base station manages the network. When a number of packets have been received, the base station switches from a directional antenna to an omni-antenna in order to broadcast an ACK message. This protocol has provisions for handling NAK packets and for handling the hidden station problem.

There is one weak area. When the nodes are just in communications range through the usage of directional antennas, but are not within omni-directional antenna range, some messages will be missed. Hence, the omni-directional antenna ACK broadcasts will not be heard. One means to over come this weakness is to use high power–this could be a problem if the station is on batteries.

2.2.4.3 Directional MAC (D-MAC)

Ko et al. appear to be the first ones to look at designing a protocol for using directional antennas within an ad hoc network [55]. The proposed Directional MAC (D-MAC) comes in two versions. Both versions use omni-directional antennas for exchanging data and both use a directional antenna for transmitting ACKs. The other nodes not involved in the current exchange may use a different directional antenna for communications in another direction. This sets the stage for having two or more exchanges occurring at the same time.

Scheme-1 has the requesting stations using directional antennas for transmitting RTS messages and the sink stations using omni-directional antennas for sending out CTS messages. This message is modified to provide information about the locations of the two stations, so that other stations can determine whether it is safe to transmit in another direction. Directional antennas are used for the actual exchange of data.

Scheme-2 uses omni-directional antennas for transmitting the RTS messages. But as more links are established, the RTS messages are transmitted on directional antennas. This version has the benefit of avoiding conflicts from stations that are not aware of a far station transmitting.

The authors used the ns-2 simulator and discovered that both versions performed better than a regular omni-directional antenna network. The biggest problem with the regular MAC approach is that a single transmission "locks up" a large area. The proposed D-MAC protocol does not have this weakness. (Choudhury et al. attempted to go further with this work. They noticed that the authors did not consider the extra gain that directional antennas provide [56]. Korakis et al. saw this weakness from a different viewpoint; that is, this protocol must limit the range of the directional antenna, otherwise there is a mismatch in coverage [48]. None of these critics offered the suggestion of increasing the power level when an omni-directional antenna is being used.)

Nitin Vaidya's approach[57] (written as DMAC instead of D-MAC) has all nodes listening on omni-directional antennas. When a station wishes to send traffic, it will use a directional antenna to transmit a RTS message. The receiving station would reply with a CTS on a directional antenna. This approach has the weakness that stations not within the directional antenna coverage will not know what is about to transpire.

2.2.4.4 Nasipuri et al. MAC Protocol

Nasipuri et al. perceived that the previous approach has some weaknesses in the matters of location and tracking [58]. Their MAC protocol uses RTS/CTS messages with directional antennas. Instead of 90-degree coverage per antenna, the nodes have six or more antennas with conical radiation pattern. All the nodes are always oriented to the north. Against this backdrop, the MAC protocol is modified to obtain the direction of any node based upon clues provided by the transmission from the distant node. Since all the nodes are always in motion, direction (not distance) is the only useful piece of information. The narrow beam pattern reduces the likelihood of conflicts. Simulation studies revealed that the average throughput was two to three times better than the regular or omni-directional antenna approach.

In another paper, Nasipuri et al. considered creating routes with a directional On-Demand Routing scheme [59]. Working with the selected MAC protocol, flooding would be reduced. That is,"with directional antennas, [the authors] proposed that a new route discovery [message] is propagated from **S** in the direction of **D** with the help of directional transmissions of a query packet by a restricted set of nodes in the network." Others[6] noticed that Nasipuri et al. overlooked the gain or greater range that directional antennas bring to a network. Another problem area is the need to find north. All the nodes must be working off of the same grid scheme or coordinate system. So is north from GPS or from certain nodes? What enhancements do the nodes need to have in order to use this information?

[6] Choudhury et al. pointed out that the authors failed to consider the extra gain that directional antennas provide [56]. Korakis et al. saw this weakness from a different viewpoint; that is, this protocol must limit the range of the directional antenna, otherwise there is a coverage mismatch [48].

2.2.4.5 Bandyopadhyay et al. MAC Protocol

Bandyopadhyay et al. looked at using electronically steerable passive array radiator antennas as a means to support a MAC protocol [60]. This antenna would only transmit to cover a 60-degree slice and the antenna would develop null patterns against unwanted signals. There is no need to find north. The MAC protocol uses omni-directional RTS packets. Instead of noting that a direction is busy, the details of the session are stored at each neighbor node. The other station would transmit a CTS packet on an omni-directional antenna. Both messages would contain the duration. The two stations would switch to directional antennas. Other nodes would use the stored information plus the knowledge of where the two stations are located to determine if another proposed link could be established without destroying the current communications. Despite not having a fully fleshed out routing scheme, the authors had several simulation runs with very encouraging results.

At MobiHOC 2001, Bandyopadhyay et al. presented a short paper that provided more information about the adaptive MAC protocol and the directional routing scheme [61]. Each node tracks information such as the angle and the Signal to Interference and Noise Ratio (SINR) about its neighbors. Thus a node would have a snapshot of the directions of the various communications and this would help it to select the best possible direction when communicating with another node. The link-state routing protocol can capture most of the network health through monitoring and a minor amount of service message traffic. When the network is new, flooding is used to pass a RTS packet to a desired station. The CTS packet comes back in the same fashion. Directional antennas are used for the actual exchange. As the network matures (more knowledge is gained), more use will be made of directional antennas. Link-state updates are periodically exchanged between two nodes; this approach over time will provide new information to all nodes without the need for massive flooding. The aging scheme is similar to DSDV. Choudhury et al. thinks this protocol is a bit complex [56]. Even if it was not so complex, updates to the network would take some time to reach every node. A rapidly changing topography would have problems with updates.

2.2.4.6 Directional Antenna Based MAC Protocol with Power Control (DMACP)

The next natural development is to marry directional antennas with power control and create a new protocol. Nasipuri et al. did that and they named their protocol **D**irectional antenna based **MAC** protocol with **P**ower control (DMACP) [62]. They modified the regular MAC protocol so that it would obtain directional information on the involved nodes and that it would determine what is the least amount of transmitter power for contacting a certain node. The authors proposed that RTS packets and CTS packets are sent on the full power setting and that during the exchanges the nodes would determine what power level should be used for the actual data transmissions. They concluded that DMACP could improve power conservation and traffic throughput.

2.2.4.7 Multi-Hop RTS MAC (MMAC)

Choudhury et al. compared two directional MAC protocols [56]. The basic **D**irectional **MAC** (DMAC) is based on elements from Ko et al. [55] and Takai et al. [49]. The second one is called **M**ulti-Hop RTS **MAC** (MMAC). The authors viewed DMAC as being weak in addressing the hidden terminal problem plus being deaf to other stations. On the other hand, MMAC attempted to use the greater transmission range with better frequency reuse than DMAC. The DMACs two problems are present here too, but the authors believe that their approach could compensate for these weaknesses. The MMAC defines neighbors either as Direction-Omni (DO) or Direction-Direction (DD). The multi-hop RTS packet is used to tell two distant nodes to direct their antenna beams toward each other. The rest of the MMAC protocol uses neighbor discovery, link characterization, proactive routing, and a position information module. Channel reservation is the key to the success of MMAC. The authors conclusions are mixed. On one hand, they stated that MMAC has better results than regular MAC and DMAC. But on the other hand, they stated that "the performance ... clearly depends on the topology and flow pattern in the network [with] more aligned topologies degrading the performance...." They admitted that more work is needed.

2.2.4.8 Receiver-Oriented Multiple Access (ROMA)

Bao and Luna-Aceves have a different approach that uses a distributed receiver-oriented multiple access (ROMA) channel access scheduling protocol [63]. This can support multiple beams and multiple sessions. Instead of using on-demand schemes or signal scanning in order to resolve communication targets, ROMA "determines a number of links for activation in every time slot using only two-hop topology information." Using a neighbor-aware contention resolution (NCR) algorithm and directional antennas, ROMA offers four major benefits. First, both transmitting and receiving can be done with directional antennas. Second, storing local two-hop information requires less memory than storing global topology. Third, ROMA divides the nodes into equal groups of transmitters and receivers for each time slot. (ROMA has a tool for pairing stations for the best network throughput.) Fourth, ROMA can generate antenna use schedules. ROMA is better than other scheduling approaches, but this has considerable overhead.

2.2.4.9 Roy et al. MAC Protocol

At MobiHoc 2003, Roy et al. presented a MAC protocol that would strive for load balancing via "maximally zone disjoint routes" [64]. That is, the routes would be selected that would have the smallest impact on other stations. In order to do this, each node must keep track of the nearby nodes and what exchanges are occurring. This information is shared with other nodes. Each intermediate node determines what is the best route from its location. Despite this overhead, the simulations indicated that this approach is far better than reactive routing with regular MAC protocols. They do not know if this would work during periods of high mobility or with a large network.

2.2.4.10 Korakis et al. MAC Protocol

Korakis et al. attempted to address all the shortcomings of the current directional MAC protocols by using only directional antennas [48]. To establish contact, a RTS packet is transmitted on one "compass" heading; then it moves to the next "compass" heading and repeat the same RTS packet. This continues until all "compass" headings are covered. Any station not addressed by the message would update its local table and not transmit in the direction of the RTS requesting station. The addressed station would reply at the end of the last RTS transmission, but its reply would be only in one direction. At the end of the RTS and CTS exchange, every node within range knows what is about to take place. The information is stored in a table and this is used to make decisions about transmitting or not transmitting and in which direction. Using directional antennas instead of omni-directional antennas should reduce the hidden station problem due to the greater coverage.

2.3 Sensor Protocols

The main difference between ad hoc networks and sensors networks is in the matter of movement. Ad hoc networks tend to have movement whereas sensor networks tend not to have any movement. This is not a hard requirement since an ad hoc network could be stationary. In section 2.2.2 above, there was a mention of Nasipuri and Li work on a location scheme for sensor networks.[51] Another trait of sensor networks is the need to stretch out the lifetime of batteries.

For this discussion, we assume that sensor nodes are fixed, must use low power, and must survive for a long time. Within these limitations, researches have explored various issues.

Some researchers have explored using sleep procedures whereas some nodes are inactive and thus extending battery life. Some researchers have considered using a schedule for waking up nodes. The various efforts do achieve the goal of extending the sensor network life time, but the drawback is that messages may be missed or delayed. Sampling changes in air temperature is one thing, but detecting a column of tanks is another matter.

Some offered solutions are interesting, but carry a huge overhead. Simple can be better. There is no need to add control behaviors to the nodes and thus avoid the issues that Sinopoli et al. explored[65] in a Defense Advanced Research Projects Agency (DARPA) funded research project.

Simple can still be better. As Chong and Kumar pointed out, a centralized network has potentially the best performance[66] and avoids the difficulties of trying to design a workable decentralized algorithm for a self-organizing sensor network or other “smart nodes” scheme.

Some think that SPIN (Sensor Protocols for Information via Negotiation) in some form could save energy and make the sensor network better[67]. Still others think that directed diffusion protocol is the way to go[68], [69]. But the nodes have to be aware of the tasking applications. This involves some broadcasting and this means extra messages being exchanged between nodes. The nodes need to be smart enough to select the best path, have enough memory to store the data, and be able to do some pre-processing of the received data.

This is a "hot" topic since research indicates that as a data-centric protocol, directed diffusion would use less energy than other standard routing protocols such as flooding[7] and multicast. There are other protocols or approaches that depend upon the nodes having knowledge of their environment, their data requirements, and of their neighbors. Such requirements adds additional overhead. Alvarez et al. offered a middleware solution in order to have reliable communications, but that involves more work to achieve this[70]. They do acknowledge that directional antennas have some advantages such as less energy consumption, less fading area, and less channel interference. However, they never used this information in the balance of their paper. Weslsh and Mainland suggested abstract regions or interfaces as a means of making it easier to build sensor network applications[71].

2.4 Security Viewpoint

Security has become an important issue. Whether it is a person having "fun" reading private communications or a determined adversary that wants to do great damage, defenses are needed. Microsoft spends considerable effort deploying security patches for their operating systems and for their software packages. Anti-virus companies are releasing updates that attempt to combat the latest "bug." In April 2005, the House Homeland Security Committee's Economic Security, Infrastructure Protection and Cybersecurity Subcommittee approved H.R. 285, the DHS Cybersecurity Enhancement Act of 2005, which "create[d] a new cybersecurity czar [72]." For the past few years, Auburn University has offered an Information Assurance Option for graduate computer science students to add to their transcript.[73] George Washington University has courses in information security management[74].

Tanenbaum divides security problems into four areas: secrecy, authentication, nonrepudiation, and integrity control [75]. The following paragraphs briefly explain these areas:

- Encrypting a message is an example of ensuring secrecy for a message. Using the Advanced

[7] This is one node passing a message to all nearby nodes. Each of those nodes would repeat the message to all its nearby neighbors. The message is not transmitted to the node that gave it the message. In a wired network, the nodes upstream would not repeat the message to nodes upstream of it. However, downstream nodes in a topography that has multiple links would receive the same message several times.

Encryption Standard (AES) would provide a long period of protection for any message.

- Authentication relates to the problem of determining that the sender is who we think it is.
- Nonrepudiation relates to the problem of a sender claiming that a sent message is false–he/she did not send out the message.
- Integrity control relates to sent messages–Did a message really come from a certain sender?

Best practices point to using security tools from start to finish and be inside a closed system. Mobile users can gain some measure of the ideal by deploying with an encryption key. The challenge for both fixed users and mobile users is supplying the next encryption key. A currier service on a regular route can handle the fixed user, but this may not be possible for a mobile user deep behind enemy lines.

Another issue is that encryption schemes require more central processor unit (CPU) work–This is another drain on the batteries. If a node or a user is compromised, then things become "interesting."

Closely related to security is the matter of survival. Sensor nodes need to avoid detection. If a node is destroyed, then the network needs to be robust enough to continue.

Sensors networks need to deal with bogus nodes that are trying to take over the network or are trying to be members of the network. Is there a way to use these bogus nodes to help out the sensor network?

2.4.1 Wireless Security

Wired communications can only be exploited by physically taping into a cable. Hence, physical security results in communications security. This is not the case with wireless communications; anyone with a receiver can capture and record the transmission. One might expect that encryption would improve the situation.

Some security approaches have been rendered useless. Wired Equivalent Privacy (WEP) is a case in point. It has a small key space. A number of keys are used frequently. Given a reasonable amount of time, the key and the plaintext message can be obtained. With this information, false messages could be generated. The security task is made more difficult when some devices have a default setting with security disabled.

David B. Johnson looked at the problems and the current solutions[76]. Fixed stations are fairly easy to handle. Slowly moving stations are possible to support, but the matter of large numbers of fast moving stations is very challenging to handle. A location registry is one possible approach, but registration authentication is needed in order to prevent evil nodes from creating problems for the network.

2.4.2 Some Hardware Solutions

Ultra-Wideband (UWB) systems have the promise of high data rates, robustness to interference, and low power usage. Racherla et al. wrote that UWB systems have “high transmission security low prime power requirements” and that the UWB technology is able “to perform precision geo-location which can aid in ad-hoc or mesh networking where the operations of the mobile hosts benefit by knowing the location of the other hosts”[77]. Devices are able to function at the background noise level and are able to exist without causing problems to other systems. Transmissions are very brief and take place at widely space intervals. The UWB technology supports distributed sensor networks, ad-hoc networks, and geo-location.

Chapter 3

THE HEAPINGS CONCEPT

Of the helio protocols listed in the first chapter, **HEAPINGS** is the most mature. Analysis points to a number of benefits:

- Could pass information in near real time
- Could hid the nodes locations
- Could avoid network congestion
- Could extend the life time of all nodes' batteries
- Could avoid close spacing of nodes
- Could avoid the need for a "bread crump" trail to the base station
- Could avoid having bogus nodes impact the network
- Would let the nodes operate with low power
- Would use the base station's greater power and abilities to obtain the big picture
- Would avoid using message flooding
- Would avoid using aggregation with its reduced precision and timeliness
- Would provide geo-location information without using GPS

A conference paper appeared in the WORLDCOMP '07 proceedings[10]. The high points of the paper follows[1].

[1] In spots, I have expanded the topic and I have removed all citations. WORLDCOMP '07 had a seven-page limitation and so some information had to be cut out.

3.1 HEAPINGS High Points

We found that nearly every scheme or protocol used the same three approaches:

1. Nodes are independent and robust.

2. Flooding is during part of the network's life.

3. Use only one frequency.

These three approaches may actually create problems. We argue that there should be centralized control with nominal nodes, no flooding, and use the best frequency band. Not all researchers are using the previously mentioned approaches. For example, the work on tiered architecture breaks with the first approach. (In some ways, our work is an extension of this area. Although our concept was created prior to discovering papers in this area.)

Tiered networks do not use robust, full-featured nodes. Researchers in this area use different terms and different assumptions, but there are some common elements. The micronodes (the sensors), macronodes (the gateways), and preprocessing of data are used. One research group calls the upper tier the "coordination units" and they assumed these to be "not energy constrained." The Tenet Architecture[2] has the same assumptions, but calls the upper tier nodes "masters." Another research group suggested having multi-tiers and multi-modal networks.

Again, those nodes at the lowest levels have less ability. These collect information and forward to the next level. The next level contains nodes that are more robust. Above these nodes might be connections to the Internet. Just like the other networks, flooding is used and only one frequency is used.

This is a good start, but we think more could be done. Our approach does not require the low level nodes to have knowledge of their neighbors[3].

[2] See http://enl.usc.edu/projects/tenet for more information.

[3] There are real world systems deployed to monitor wildlife. One research group is exploring how to determine a location, but so far their efforts requires the low level nodes to develop a list of nearby nodes.

3.2 HEAPINGS: A Description

Our novel concept could solve many problems and have enhanced security. Our proposed approach makes the following assumptions:

1. The base station or the net control station (NCS)[4] has the following capabilities:
   (a) Able to communicate with many nodes at the same time on several channels.[5]
   (b) Very robust with high speed processing for handling large volume of information.
   (c) Unlimited power. (No batteries used.)
   (d) Directional antenna with active sectors.
2. The nodes have the following capabilities:
   (a) Function as a sensor.
   (b) Transmit straight to the NCS.
   (c) Able to change frequencies and channels.
   (d) Receive control messages.

The network center ("*HE*liocentric") is the NCS and each node is subordinate to it. There is no node-to-node communication. (This is known as a star topography or as a directed net. The ALOHA net is an early example.)

The NCS and the nodes form the network through an *A*d hoc means. That is, the nodes have enough information to contact the NCS. After a quick roll call, the network is formed and the NCS has a table of all active nodes. (The nodes do not have a pre-deployment list nor do they maintain a routing table–Both actions are not needed.)

[4] Normally writers use the "BS" expression for "base station." I followed that custom when I submitted my conference papers. I was not comfortable doing this. In the quoting of my conference paper within this document, I will use "NCS" instead of "BS." Again, I wish to avoid invoking the wrong image in the reader's mind.

[5] The terms "channel" and "frequency" are normally synonymous. For this writing, the word "frequency" will refer to big jumps like from 915 MHz to 40 MHz and the word "channel" will refer to small frequency changes like from 915 MHz to 915.025 MHz.

Table 3.1: Example NCS Table Entries

NodeID	Distance	Direction
001	10 units	000
002	15 units	010
003	20 units	330
....	...	...

This *P*rotocol would use clues or *I*nferences to determine additional information. The NCS would use signal strength to determine the distance to a node and would use the directional antenna to determine the direction of the node in reference to itself and thus avoid the need for GPS. This information is stored in a table. As a result of the roll call and these clues, this table contains the node ID plus the distance and the direction from the NCS. See Table 3.1 for example entries.

The nodes have *N*ominal ability. The nodes collect data and use the radio to contact the NCS. The nodes have the software and the hardware pieces for these two activities. The nodes do not need the ability to determine its location or to manage a routing table or complex algorithms for handling lost contact. Furthermore, the nodes do not need to process or aggregate the data of other nodes. In short, the nodes collect data, transmit straight to the NCS, and comply with any NCS' instructions.

The NCS would use the transmitted data plus the clues from the nodes' transmissions to determine a *G*lobal view of the environment. For example, several nodes might transmit a short message (moving object). The NCS would process these messages by including the nodes' locations and the time of receipt to determine additional insights such as the speed and compass heading of the object.

*S*ecurity is achieved, because the NCS has a list of valid nodes. This prevents bogus nodes from joining the network. Security is enhanced by selecting frequencies that will propagate out to the nodes and no further. This would make it difficult for the enemy to intercept communications. If the nodes have the ability to use directional antennas, then this would go further to reduce the chance of interceptions. If a node is discovered, the enemy cannot determine where the next node is located.

Consider Fig. 3.1. The NCS (the black dot) transmits to the nodes (the three rings). Nodes on the outer most ring would hear the message, although the signal is a bit weaker. Beyond this, the

Table 3.2: Selected United States ISM Frequencies

Frequency	Distance
40.68 MHz	111 km/69 miles
915.00 MHz	5 km/3 miles
2450.00 MHz	2 km/1 miles
5800.00 MHz	0.78 km/0.49 miles (2565.7 ft)

signal is too weak. So the enemy (the small circles) would not hear anything.

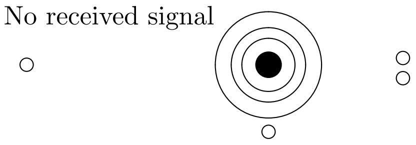


Figure 3.1: Communications Rings

With the Friis equations, one can determine where the signal is too weak. If the cutoff point is -86 dBm and the power is 20 dBm, then Table 3.2 would show where the signal is too weak.[6]

The fourth frequency is used for many wireless devices. Notice the distance is barely 3/4 of a kilometer. The third frequency was used by older wireless devices. Notice the distance is doubled to a bit over 2 kilometers. The second frequency is used by some sensors and is very close to the cellular telephone frequencies. Notice the distance is 5 kilometers. Eons ago, the first frequency was used for cordless telephones, but now the third and fourth frequencies are used. In practice, distances are less since whip and internal antennas are poor radiating devices.

Expanding the idea of the HEAPINGS base station having a list of valid nodes, if a new node tries to enter the network or a known node appears to be in a different location, then the base station can tag or mark the node as questionable and will watch the node closely.

Encoding the transmissions for increased security is an option. Of course, this will add to the energy drain and be an additional overhead. There may be situations where these trade-offs are needed. Otherwise the security that comes from being far apart and using a frequency that goes

[6] These figures assume no line losses, zero antenna gain, and a flat earth. -86 dBm threshold and 20 dBm output power are typical of 802.11 devices.

only so far may be good enough for the mission.

3.3 Flooding and Service Messages

Protocols may be proactive (nodes keep their own and other's tables current) or reactive (sender uses a route discovery message prior to sending data), control messages are flooded out. In static networks, these messages would reduce since caching would "replay" a previously used route. In dynamic networks, control messages are numerous and could reach the point where every message is a control message. Many protocols ignore the fact that many nodes are within radio range of the sender. For example, a third ring node (see Fig. 3.1) hears a message at least three times (the sender, the nearest first ring node, and the nearest second ring node). If other nodes are within range, then more "repeats" are heard.

No current protocol differentiates among the various line-of-sight (LOS) frequencies; all frequencies are regarded as the same with manufacturers preferring the higher ISM frequencies (5.8 GHz as "better" than 2.4 GHz). So large numbers of nodes must be used along with either a network protocol or a multi-hop scheme.

All nodes are draining energy at nearly the same pace. To keep the network alive longer, energy saving tricks are used (like sleeping and reduced power). When used, some nodes will have a longer life, but the trade-off is delayed or missed messages.

3.4 No Flooding: Only Node-to-NCS and NCS-to-Nodes Communications

In contrast, the HEAPINGS NCS has the routing table and not the nodes. Flooding and relaying are not used. All nodes are one hop away. Only nodes with data would transmit and the whole network would live longer. Changing frequencies is the tool for keeping all the nodes in direct contact with the NCS. The area could be a large room (then could use 5.8 GHz), or several floors (then could use 2.4 GHz), or several city blocks (then could use 915 MHz), or the size of a city (then could use 40 MHz). This is possible, because the NCS is using directional antennas and these radio bands have these behaviors. Changing the transmit power level is not necessary.

The nodes transmit only to the NCS and the NCS transmits directly to each node. There is no need to have any nodes relaying for another node. This simple change avoids flooding and its tendency to have a “blizzard” of messages.

When a node has data, it requests permission to send (RTS). This avoids conflicts, corrupted messages, and congestion.

When two or more nodes have data, they RTS and the NCS would only acknowledge (ACK) the node with the highest ID. This node transmits its data while the others would move to the next open channel. On the second channel, the highest ID would receive the ACK. This is repeated until each node receives an open channel. With a powerful NCS, many messages could be received at nearly the same time. The only delay is when the nodes change channels. The worst case would be when a node tries every channel and none are open. The node would start from the first channel and would repeat the RTS with a note that this is a second attempt. The NCS would ACK and accept its data. This likelihood is very remote and we will explain later on.

After the data is passed, the nodes would return to channel 1.[7] This scheme has an efficiency of 100% channel usage and almost no delay.[8]

Some may see this as a broadcasting approach, which is true. However, all wireless schemes are broadcasting to some degree. Any supporter that thinks his/her scheme is not broadcasting is ignoring the nature of the wireless environment.

3.5 Large Message Volume

All protocols use a first-come-first-served approach until there are conflicts. The Slotted Aloha protocol[75] and others solved this with assigned, but limited slots. Other protocols use contention schemes[75], but there are conflicts and some nodes would wait before retrying. So more nodes are handled and traffic leveling is done. The problems are delayed data and possible unserviced nodes.

HEAPINGS messages are received fairly quickly. The channel number provides insights to the age of the data and this is included in the processing. Since there is almost always an open channel,

[7] If experience reveals that the data follow a “machine gun” pattern where the data comes several times, then the protocol could be modified whereby the nodes would delay for a period of time before returning to channel 1.

[8] Tanebaum[75] discussed the Binary Countdown Collision-Free Protocol. He noted that the nodes would wait until the first node was finished, then the base station would accept traffic from the node with the next highest ID. He pointed out that this would have an efficiency of 100 %. Our approach has the same efficiency, but with greater throughput.

there is no problem of new data overwriting old data.

Would the NCS be overloaded? Reality would mitigate the message volume. For example, the largest army may have about 14,000 tanks. It is doubtful that all 14,000 tanks would be in the same theater. If a typical tank is 3.4 meters wide and if the sensors are in a valley with a 40-meter wide opening, then only 10 or 11 tanks could travel abreast. This would reduce the amount of data collected and transmitted during any time period. If all 14,000 tanks passed through this valley, there would be from 1,272 to 1,400 messages, but transmitted at staggered times.

Since HEAPINGS rarely uses control messages, most transmissions are data messages. Real messages are not being held up by control or services messages. In short, with fast processors, with short messages, and with irregular and real time transmissions, the NCS could handle many nodes.

3.6 Frequency Selection

All the nodes would use "Frequency A" until the NCS directs a change to "Frequency B." The NCS would select a frequency that would ensure all nodes are in direct contact with itself. This avoids the need for relays. Also, using the highest working frequency would bring in an element of security since the signal would be too weak for anyone to use beyond a certain distance. (A different approach might be to assign each node a dedicated channel. But the problem is that this would not scale up very well. So having all the nodes on the same channel would be better. The nearby channels would be needed during heavy traffic periods.)

To make this clearer, consider again Fig. 3.1. The black dot is the transmitter. Stations on the three rings would hear the same message at the same time.[9] Stations on the outer most ring would hear the message, although the signal is a bit weaker. Beyond this ring, the signal is too weak to be useful. So the enemy (the small circles) would not be aware of a transmitter in the center, because the weak signal would be covered up by background noise.

To make the point stronger, look at Table 3.3. This is listing of all United States approved LOS ISM frequencies. Recall that we can determine how far a signal travels before it becomes too weak

[9] Light travels about 300,000,000 meters (about 186,000 miles) per second. The equatorial radius of the earth is about 6,000 kilometers (about 4,000 miles) and the circumference is about 40,000 kilometers (about 25,000 miles). Since we are dealing with distances much less than the earth's circumference–such as 1 degree or about 111 kilometers (about 69 miles)–We can regard a message as arriving at all spots at the same time.

Table 3.3: US ISM Frequencies (-86 dBm sensitivity and 20 dBm output)

Frequency (MHz)	Distance (kilometers/miles)	Expressed in feet when below a mile
40.68	111 / 69	
915.00	5 / 3	
2450.00	2 / 1	
5800.00	0.78 / 0.49	2565.7
24125.00	0.19 / 0.12	616.8316
61250.00	0.07 / 0.05	242.9561
122500.00	0.037 / 0.023	121.4781
245000.00	0.0185 / 0.0115	60.73903

by using the Friis[10] suite of equations. If -86 dBm is used as the cutoff point, then our Table 3.3 shows the rough spot where the signal is too weak to be useful for a 20 dBm transmitter.[11]

The NCS selects a frequency that would ensure communications with all of the nodes. With stationary sensors, the selected frequency would work for the duration of the network. If the nodes are mobile as in the case of the military's flying sensor platforms, then a frequency change plan would be used. For example, the NCS might detect that the nodes are moving away when the signal level begins to drop. When a decision point is reached, the NCS would direct all nodes to change to the new frequency. (The frequency list is pre-loaded in all of the nodes. The NCS would direct the nodes to change to the next frequency in the list.)

HEAPINGS is not a frequency hopper. HEAPINGS does not need high power nor need power control; all the nodes may use the same low power setting. The NCS uses a directional antenna for receiving weak signals. Some amateur HF stations use five watts or less, high gain directional antennas, and small radios to talk around the world.[12]

[10] Sometimes this is misspelled as "Friss." For more information on Harld T. Friis, see the IEEE website biography section.

[11] These figures assume no line losses, zero antenna gain, and a flat earth. -86 dBm threshold and 20 dBm output power are typical of IEEE 802.11 standard devices. Also, there was no consideration whether or not any radios exist that could transmit on any of these frequencies.

[12] http://www.wb8nut.com/qrp.html has information about a 500-milliwatt radio and a 12-volt powered 750-milliwatt radio.

3.7 How HEAPINGS Functions

3.7.1 Establishing the Network

Sensors are deployed in an area with random[13] spacing. This could be anywhere from 5 kilometers (3 miles) to the horizon. These could be placed far apart. The NCS could be on a mountain ridge. The nodes are set to use 915 MHz as the starting frequency. The NCS transmits a roll call message. It only hears from those nodes that are at the maximum distance of about 6 kilometers (4 miles) away or less.[14] The number of nodes, N, is known. Reaching a small number tells the NCS that a frequency change is needed. The NCS commands these nodes to use a lower frequency such as 40 MHz.

At the same time, those nodes that did not hear the NCS would wait a bit, and then switch to the lower frequency. When the NCS is on the new frequency, it would send out a new roll call message. Both the previously found nodes and the previously "missing" nodes would reply. The NCS would acknowledge each node and add an entry in its table–the node ID, distance (based on signal strength), and bearing (based from the base station's directional antenna).

3.7.2 Sensors Working–An Example

A northeastern sensor detects a tank. It transmits a simple message, "Tank" and its node ID. The NCS records that a tank was sighted at a certain time.[15] From the information about the node's direction and distance, the NCS can provide addition data about this tank sighting. If nodes west of this node start transmitting messages on this tank, then the NCS can look at the time-of-receipt and these nodes' locations to determine how fast the tank is moving and its direction of travel. If several tanks are present, then these would generate several messages. Thus the NCS could determine that more than one tank is moving through the area.

[13] A random placement is more likely than a precise placement. This makes for an interesting academic study, but not very useful for the real world.

[14] Based on 20 dBm output and 3 dBi antenna gain.

[15] The time is based on the NCS's internal clock. The nodes do not use a clock.

3.8 Comparing Other Protocols with HEAPINGS

The following paragraphs provide more insights on HEAPINGS by comparing and contrasting with other protocols.

3.8.1 Flooding and Service Messages

Many protocols expect the nodes to be very robust (that is, having many abilities). Some protocols are proactive and the nodes keep their own and other's routing tables current. Other protocols are reactive and will send out a route discovery message prior to sending out data. Either way, control messages are used and these are flooded out. In a static environment, these messages would become fewer since caching techniques would "replay" a previously used route. In a dynamic environment, control messages would be numerous and could reach the point where all the messages are control messages. To solve this problem, the solution might be to slow things down or to reduce the network membership.

As mentioned earlier, nearly all current protocols do not take advantage of the fact that many nodes are within direct communications range of a sending node. Again, a node that is located on the third ring (see Fig. 3.1) from the sending node would hear a message at least three times (the sender, the nearest node on the first ring, and the nearest node on the second ring node). And again if there are other nodes on the first and second rings that are within radio range of this example third ring node, then four or more repeats of the sender's message could be heard—a total of at least seven transmissions. If the outer most nodes do not realize that there are no more nodes, then this message would be repeated several more times. Until the message has worked its way to the network edge, no new message could be introduced. Some protocols attempt to reduce the amount of flooding, but none can completely eliminate it.

In contrast, HEAPINGS has the routing table at the NCS. It does not send out table update messages. Flooding is not needed, because each node is able to hear the NCS. Changing frequencies is the tool to ensure that all nodes are able to stay in direct contact with the NCS and thus avoid using relays.

In other protocols, all LOS frequencies are regarded as the same with manufacturers preferring

ISM frequencies and they perceive 5.8 GHz as the best one to use. There is no frequency management, or selection guidance. To handle communications beyond direct node contact, either a network protocol is used or a multi-hop approach is used. This adds additional overhead.

There is a continum from one end that uses simple hardware and complex protocols to the other end that uses complex hardware and simple protocols. As radio technology continues to advance, the wiser decision may be to rethink the protocols and use those that best take advantage of the latest hardware.

Sensor networks tend to be stable, but this is not a requirement for HEAPINGS since a LOS frequency is able to cover an area. So a dynamic environment is not a problem. The area could be the size of a large room (would use 5.8 GHz), or could be several floors (would use 2.4 GHz), or could be several city blocks (would use 915 MHz), or could be the size of a "city-state" (would use 40 MHz). If some nodes started to move beyond the coverage area, then the NCS would command all nodes to change to a lower frequency. Since these are all LOS frequencies without a sky wave component, then all nodes would still stay in direct contact. Rapid movement within the area is not a problem as direct communications is always possible.

In other protocols, energy saving schemes are used in order to keep nodes alive for a longer period of time. Sleep schemes, reduced power, and other novel ideas are used. With flooding being a part of these protocols, all the nodes are draining energy at nearly the same pace. When these schemes are used, some nodes will have a longer life, but there are trade-offs; messages are either delayed or lost.

HEAPINGS nodes do not relay messages. Only those nodes with data would transmit. The result is that the entire network would live longer than the life time of a typical node. So a sleep scheme is not needed and is not desirable. To express this point in different terms, in the traditional network, any event happening at the farthest distance would require every node from this distance to the base station to be involved in relaying the message. In time, if every event happen at the farthest edge, then all the nodes would die together. In the HEAPINGS network, only the outer nodes are involved. When this outer ring of nodes die, then the next ring of nodes would step in. These may preceive the events in a weak fashion, but at least there are nodes alive that can collect data and send to the base station. That cannot be said of the traditional network, which at this point in time the entire network would be dead.

3.8.2 Handling Large Volume of Messages

Another difference is how high traffic volume would be handled. All protocols would use first-come-first-served approach until there are conflicts. The Slotted Aloha protocol[75] and others would solve the conflicts with assigned slots. There is a limit on the number of available slots. Have more users than slots and there are problems. Other protocols might use a contention scheme[75]. There are still conflicts, but some of the nodes would wait for a period of time before retrying. The benefit is that more nodes may be handled and traffic leveling is done. The problem is that traffic is delayed and it is possible for a node to never receive service.

HEAPINGS has a different approach. When a node has data, it performances an RTS. The NCS will ACK and the node would transmit. If the node does not receive an ACK and it does hear the NCS, then it would change to a different channel. This repeats until an ACK is received. However, if the node is on an open channel and it does not hear from the NCS, then the node has a transmitter problem and it would stop attempting to make contact.

This approach has a number of benefits. Messages are received fairly quickly. The order of trying new channels provides insights to the age of the information. If the node is on the fifth channel, then the message has about four or five units of time delay (aging). The NCS would take that into account when processing the information. Since there is almost always an open channel to the NCS, the issue of new data overwriting old data is not a problem.

3.9 Answering Critics

In seeking feedback on this concept, a number of issues were raised. These are valid and need to be addressed. Only the negative comments are covered. The positive ones were omitted.

3.9.1 This is Not a Frequency Hopper Scheme

A frequency hopper scheme is an attempt to keep the other side from eaves dropping on communications. The dwell time and the list of frequencies are only known to the net members. The other side would have to guess the dwell time and the list of frequencies. HEAPINGS uses one frequency until it is time to change to another frequency. It does not hop around.

However, that does not prevent the user from adding a hop scheme that uses nearby frequencies. Of course, any such enhancements would involve overhead and higher energy draining.

3.9.2 High Power and Power Control is Not Needed

All the nodes are assumed to be in the same configuration and using the same power level. The power level is set at a low level. By using the proper frequency and the proper antenna, weak signals can be received and processed by the NCS. If need be, the NCS could increase the power level. But this should not be necessary.

Closely related to this is the matter of power control. The deployed nodes use the lowest power and the NCS selects a reasonable power level. Since the lowest setting is used, this should enhance the battary life of the nodes. The NCS has access to unlimited power.

Some amateur HF stations use five watts or less to talk around the world. They achieve this by using high gain directional antennas and small radios.[16]

3.9.3 Bit Rate Issue

The higher frequencies are favored, because of the belief that these support greater bandwidth (more information) in a unit of time. Combat environment sensors would be sending short messages with a small amount of information.

3.9.4 Idle Listening vs. Sleeping

There seems to be at least two understandings of the term “sleeping.” Some see this as complete shut down while others see only certain functions are shut down. One reviewer from the first group wrote that idle listening uses more energy than sleeping. Putting nodes to sleep could be done, but the premise is that the sensors need to be awake in order to collect information. Being asleep goes against this requirement.

[16] http://www.wb8nut.com/qrp.html has information about a radio that has a standard output of 500 milliwatts. Another version puts out 750 milliwatts and uses a 12-volt battery.

If the second group preceives the transmitter as draining energy even when not transmitting, then putting the transmitter to "sleep" would let the node continue to collect data while saving energy from a sleeping transmitter. It is not clear what are the assumptions for turning the transmitter back on again.

In a sense, this is a question that is more influenced by hardware than by software. If the circuit is designed where no energy is consumed when the transmitter is not being keyed, then this becomes a non-issue for the second group and HEAPINGs. This becomes a discussion between the first group and the "all others."

3.9.5 Why Single Hop is Better than Multihop

One reviewer wanted it spelled out clearly why single hop is better than multihop. Multihop involves many nodes in order to relay one message. Single hop involves just one node. So if the nodes in the single hop network and in the multiho network are using the same amount of energy, than a message sent in a multihop network would costs more energy than in a single hop network.

3.9.6 Software Defined Radios

One reviewer was concerned about the size of the sensor node. Today, companies are making and selling radios that can operate from 30 MHz to 512 MHz and these are no bigger than a "brick."[17] Size does not matter as things are becoming smaller all the time.

3.9.7 Border and Pipeline

One reviewer suggested reviewing computer networking issues such as border and pipeline. This is a sensor network, not the upper level Internet router.

3.9.8 Old Concept

Three reviewers reacted to the submitted conference paper being a concept paper. All protocols started off as a concept. The writers may nor may not include any simulation work. Then they or others will take the concept one step further by running experiments and tests.

[17] See Harris Radio website: www.rfcomm.harris.com/products/tactical-radio-communications/RF-5800m-hh.pdf

One reviewer wrote that this is “similar to the traditional wireless LAN communication case.” Furthermore, the reviewer saw the HEAPINGS concept as “neither new nor challenging.” Also the reviewer thought that “granting too much powers to a single NCS seems not a good idea, because the compromise of NCS [would] paralyze the whole network.” A second reviewer did not believe that a centralized protocol is feasible! The first reviewer did agree that “the idea of frequency selection is more reasonable” but “this small fix could not change the fact that the architecture is not ideal in a combat environment.”

The above mentioned second reviewer did not like the selection of the cited work that had been done by others and did not like the level of coverage. Since all sensors networks must route information from point to point, the focus was on protocols that have a routing component. It would be ideal to attempt to correct this imbalance, but conferences have page limits. As a result not everything could be included.

What is interesting is that HEAPINGS and tier sensor networks share a number of common traits. These three reviewers objected to certain HEAPINGS features that also exist in tier sensor networks. Progress comes by marrying old ideas with new approaches. Also some of the old ideas like ALOHA were of a centralized nature.

As HEAPINGS matures, consideration might be given to handling the loss of a NCS. Maybe the way things are done with gateway routers could be considered. Today combat sensors route information to a central location. HEAPINGS would do the same thing, but without flooding and relays.

3.9.9 Antenna Design

One person wrote ”widely varying frequencies put considerable burden on the antenna designer.” This is a valid hardware concern. HF radios could be used with an antenna tuner in order to operate on any frequency between 2 and 30 MHz. The Harris company makes the FALCON III AN/PRC-152 handheld radio that operates on any frequency between 30 and 512 with the same antenna[78]. This radio normally uses 5 watts and 10 watts to hit a satellite.

Another concern was about the feasiblity of a directional antenna being able to cover a large part of the radio spectrum. As an example, When the AN/PRC-152 is mounted in a vehicle rack, it is called the VRC-110. It can use the following directional antennas:

- RF-387-AT001 (30108 MHz) Dipole Whip (3.3 m)
- RF-387-AT002 (30108 MHz) Dipole Whip w/GPS Antenna (3.3 m)
- RF-398-03 (30108 MHz) — Dipole Whip (0.3 m)
- RF-9070 (100-400 MHz) Biconical (6.1 m) Mast
- RF-3080-AT001 UHF STACOM (240-400 MHz) Manpack or Base Station Antenna Set

Today, the directional antennas do not cover the same range as the whip antenna. Tomorrow, that could change.

So the march of technology has made the matter of having a radio cover a large part of the radio spectrum a non-issue. Today it is 30 to 512 MHz, tomorrow it will be even more. And the same thing is true for antennas; 300 MHz of radio spectrum can be covered by one directional antenna. Tomorrow, it will be even more.

3.10 Analysis From a Mathematical Viewpoint

Since the popular simulation packages have weaknesses[79, 80, 81] and may not correctly simulate HEAPINGS, we decided to use some mathematical approaches before attempting to create any simulations.

3.10.1 Roll Call

In a regular sensor environment, the NCS would transmit the roll call message. The nearby nodes would receive and relay the message to the next "ring" of nodes. These nodes in turn would repeat the message. This would continue until the extreme edge is reached. Then the nodes would transmit their answers. The effort of relaying from node to node would continue until the requesting node is reached.

On the other hand, the HEAPING NCS would transmit the request. All of the nodes would hear this message. Then the nodes would transmit their answers straight to the NCS.

Table 3.4: Comparing Regular and HEAPINGS

Roll Call Actions	Regular	HEAPINGS
Nodes Relaying	462	0
All Nodes Replying	5,566	484
Total	6,028	484

If the nodes are deployed in m rings with n nodes on each ring, then the total is mn. Assume that each node will only relay for two nodes (a node on an inner ring and a node on an outer ring) and transmitting uses one energy unit.

In a regular network, n nodes on $m-1$ rings would transmit the message for a total of $n(m-1)$ times. Then each node replies and after relays, the total is $nm(m+1)/2$ (ring m's messages used mn energy units to reach the NCS; ring $m-1$'s messages used $(m-1)n$ units to do the same, and so on). The grand total is $(n(m-1)+nm(m+1)/2)$ energy units, which is $O(nm^2)$.

HEAPING nodes do not repeat messages so no energy units are used. In replying, each node transmits back for a cost of mn units, which is $O(nm)$, one order of magnitude lower than using flooding. In an example of 22 rings with 22 nodes on each ring (see Table 3.4), the improvement is about 92%.

In the matter of network life time, the regular network would require the nodes to relay. The ring closest to the NCS would have the greatest energy drain. Every time the NCS transmits, these nodes would be transmitting. Every time a distant node replies, these would be involved. If the outer most ring was involved in every exchange, then the entire network would die together. There are other schemes that attempt to reduce the amount of flooding. For those that really can achieve this, the network would last a bit longer. However, none of these schemes can avoid using flooding during some stage of the network's existence. The network's life time is fairly close to the average life time of a node. If nodes are put to sleep, then the network would last longer, but at the expense of timely message delivery. The trade-off is long network life time and slow message delivery versus short network life time and quick message delivery.

In the HEAPINGS approach, the nodes' life time would be variable. If the outer most ring was transmitting frequently, then these would die first. The next ring of nodes would become the new

Table 3.5: Comparing Aggregation and HEAPINGS

	Regular	Aggregation	HEAPINGS
Nodes used	10240	2303	1024
Savings	–	7937	9216
Time used	10	10	1

first line of data collection. The rest of the nodes would still have energy available. The issue of trade-offs does not exist, because other nodes are not needed to relay messages.

3.10.2 Aggregation Or Not

Aggregation's intent is to "substantially reduces the communication overhead." Consider a m-ring network with 2^m nodes on each ring. Assume two nodes feed to one node (this would be halved each time as in 2^m, $2^{(m-1)}$, $2^{(m-2)}$, ..., 2, 1). The total is $2^{(m+1)} - 1$ nodes. The saving is $(m-2)2^m + 1$ nodes $((m2^m - (2^{(m+1)} - 1))$. Accounting for processing time, let's assume 1 time unit is used. Then 10 time units are used.

Left out of the foregoing is the matter of irregular timing of events. This is aggregation major weakness. How long should the nodes on the next inner rings wait? How will these determine that something is one actor (a tank moving) in different places or a single event in various places (people walking)? If a delay is added for collecting the information, then this increases the delivery time. When would the data become too stale to be useful?

In contrast, HEAPINGS used 2^m nodes and 1 time unit. Although aggregation would save energy over a regular sensor network, it cannot surpass HEAPINGS' speed and savings.

As a concrete example (see Table 3.5, consider a ten-ring sensor network with 1,024 nodes on each ring. Assume that two nodes feed information to one node. So the flow would be 1,024 to 512, then to 256, then to 128, then to 64 nodes, then to 32 nodes, then to 16 nodes, then to 8 nodes, then to 4 nodes, then to 2 nodes, and finally to 1 node. This is a total of 2,303 nodes. This is a savings of 7937 nodes (10,240 - 2,303) or 77.5% (1 - 2303/10240).

However, we need to account for processing time. To make the math easy, we will assume that one time unit is used. So in the ten-ring example, 10 time units are used.

In contrast, HEAPINGS would only use 1,024 nodes and less than 1 unit of processing. Although aggregation would save energy and time over a traditional sensor network, it cannot surpass the savings obtained by the HEAPINGS approach. HEAPINGS saving is 90% (1 - 1024/10240).

Again, repeating the problems with aggregation. How long should the nodes on the next inner rings wait? How will these determine that something is one actor (a tank moving) in different places or a single event in various places (people walking)? If a delay is added in order to collect this information, then that would increase the delivery time. At what point would the report become too stale to be useful?

Once an event is detected, HEAPINGS nodes would transmit small messages straight to the NCS. By processing the pieces, the NCS could provide a Global view or "the big picture" without aggregation "coarse" reporting and its built-in delays.

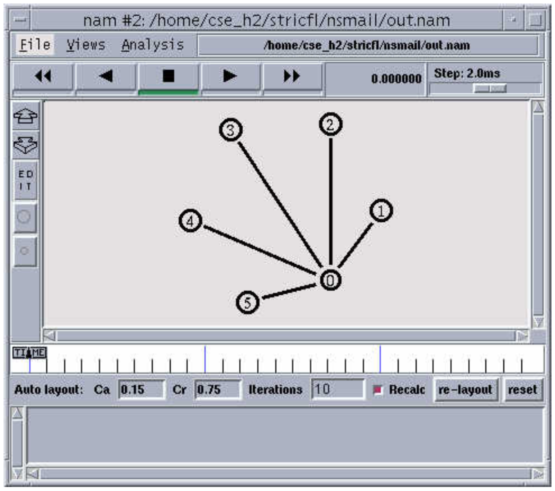
Chapter 4

SIMULATION WORK

The following describes in some detail the simulation work that was done on HEAPINGS and appears in the WorldComp '08 proceedings[11].

4.1 Ns2 Simulation

Using the example values from the Marc Greis' Tutorial[82] on the ns2 simulation program as a starting point, the first simulation effort was created with four nodes plus a sink node. The packet size was set as 500 bytes, the interval was set as 0.005, and the capacity was set as 1 Mb. This works out to 200 packets per second per link and the used bandwidth is 0.8 megabits per second per link. Together the four links have a total of 3.2 Mb per second. The base station has a capacity that is equal to the total capacity of all of the nodes. See Fig. 4.1 for the net configuration. The link from node 0 to node 5 is used as a sink or receiving station.



nam #2: /home/cse_h2/stricfl/nsmail/out.nam

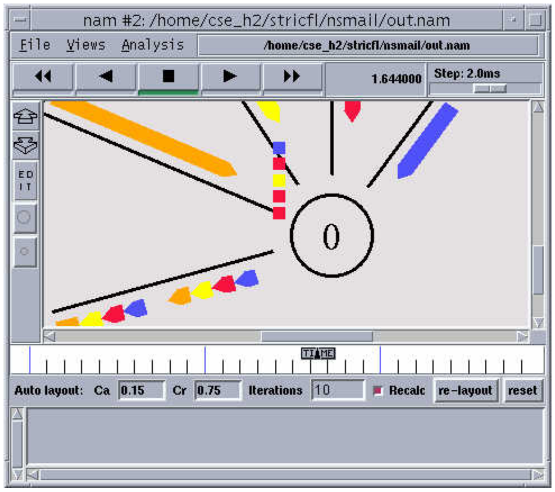
/home/cse_h2/stricfl/nsmail/out.nam

0.000000 Step: 2.0ms

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc

Figure 4.1: NS2 Prior to Executing Simulation

Using droptail handling for the nodes and a stochastic queuing approach for the base station, some packets are dropped. How much? A minor amount. Visually, the worst case might be five packets with maybe three packets from one source. The lost packets could be quickly retransmitted. See Fig. 4.2.



nam #2: /home/cse_h2/stricfl/nsmail/out.nam

/home/cse_h2/stricfl/nsmail/out.nam

1.644000

Step: 2.0ms

Auto layout: Ca 0.15 Cr 0.75 Iterations 10

Figure 4.2: Screen Shot of NS2 at the Maximum Load

The next simulation effort was to make the base station's capacity considerably greater than that of the total of all of the nodes. One would think that increasing the base station's capacity would provide the situation of no dropped packets. But ns2 simulator does not agree. Experimenting with capacity up to 100 Mb revealed that a few packets still would be dropped.

The third simulation effort varied the base station's delay from 10 ms to 5 ms and keep the capacity equal to the total of all of the nodes. This approached resulted in better behavior. The worst case packet drop situation improved visually from 5 to 3. Increasing the capacity from 4 Mb to 10 Mb did not result in any noticeable improvement. The ns2 simulation did not reflect any noticeable improvement with the base station's delay being improved to 2.5 ms or to 1 ms.

Of course, the ns2 simulation assumed packets are being generated every 0.005 units and that the packets are 500 bytes in size. This is not the case for a combat sensor network. Packet generation would be irregular and the message size would tend to be small. Also the nodes would not always be continuously transmitting at the same time to the base station.

(We tried to create a network with more nodes, but ns2 has a file size limit between 4,049 and 4,496 bytes. That is, whatever instructions that one might create with the tcl programming language, must be less than 5 kilobytes. Otherwise, the simulation software cannot run. As a result the simulation runs were limited to working with four feeding nodes. Again, the link between 0 and 5 is used for the sink or destination of the packets.)

4.2 OPNET Simulation

OPNET's Modeler software[83] is a commercial product that has the ability to do more than ns2. It covers the common protocols and vendor devices. The Modeler uses several editors:

1. the Project Editor
2. the Node Editor (Used to create node models that describe the internal flow of data within a network object.)
3. the Process Model Editor (Used to create process models that describe the behavioral logic of a module in a node model.)
4. the Link Model Editor
5. the Demand Editor
6. the Path Editor
7. the Packet Format Editor
8. the Antenna Pattern Editor (for use with the wireless module)
9. the ICI Editor
10. the Modulation Curve Editor (for use with the wireless module)
11. the Probability Density Function Editor
12. the Probe Editor
13. the Simulation Sequence Editor

14. the Filter Editor

In addition to the foregoing editors, there is the Analysis Tool.

There is a set of tutorials to help the new user to master each of the foregoing plus other features of OPNET's Modeler software. The provided tutorials could take 20 or more hours in order to complete and not every feature is covered.

OPNET's Modeler software can explore networks that range in size from an office to a campus to an enterprise to the world. The network could be configured as a bus, full mesh, randomized mesh, ring, star, tree, or as an unconnected net.

One can select actual vendor products. For example, one could select to use a stack of two 3Com® SuperStack® II 1100 and two SuperStack® II 3300 (See `http://www.3com.com/products/en_US/detail.jsp?tab=support&pathtype=support&sku=3C16982-US`)[1] chassis with four slots, 52 auto-sensing Ethernet ports, 48 Ethernet ports, and 3 Gigabit Ethernet ports. The OPNET's Modeler is able to handle more nodes; the first tutorial uses a network that has 30 nodes. Modeler is able to collect statistics for individual nodes or for the entire network. One key statistic is server load and another one is Ethernet Delay. The wireless simulations can collect environmentally unique statistics.

4.2.1 Details on the Created Wireless Simulation

Instead of creating the entire HEAPINGS sensor network, we looked at the base station, one transmitting sensor node, and a moving jammer station. We narrowed our focus to exploring the difference between an omni-directional antenna and a directional antenna. We ran two different scenarios; the first one had the jammer moving behind the two stations (See Fig. 4.3 for route.) and the other had the jammer going between the two stations (See Fig. 4.4 for route.). Within each scenario, we used an omni-directional antenna and a directional antenna. The transmitting node only has an omni-directional antenna whereas the base station has the option of using either antenna. It does not matter what kind of antenna that the jammer is using, but we opted to use an omni-directional antenna.

[1] Both products have been discontinued for the SuperStack® III series.

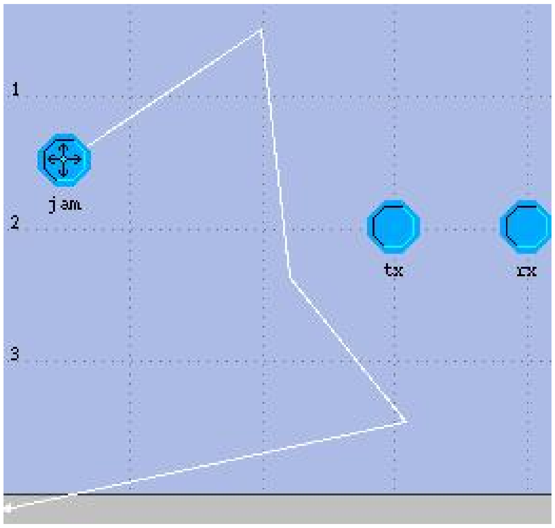


Figure 4.3: Jammer Trajectory Behind the Nodes

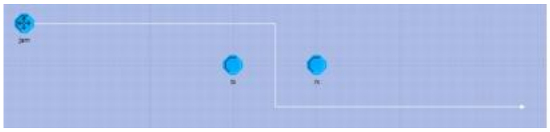


Figure 4.4: Jammer Trajectory Between the Nodes

Packets would be transmitted at 1024 bits per second while using 100 percent of the channel bandwidth. Or to express in different terms, the packet generator generates 1024-bit packets that arrived at the mean rate of 1.0 packets per second with a constant interarrival time. (These are the default values for OPNET wireless simulations.) We looked at the interference impact on receiving complete packets. If the signal-to-noise ratio (SNR) is too low, then the packets would be corrupted and must be rejected. We collected statistics on the bit error rate (BER) and on the throughput in packets per second. We used 0.0 errors per bit as the cut-off point. That is, only totally error-free packets were accepted; we did not considered using any error recovery protocol. (OPNET has the ability to limit collection of statistics to successful exchanges between two nodes. We did not use this option, because it would not show the amount of lost packets.)

To keep things simple, we did not vary the transmitter power, the frequency band, the modulation type, nor the distances. The jammer is given more power (20 versus 1 for the sensor node) and its signal modulation is changed–in order to create more impact on the receiver. The resulting signal

Table 4.1: The Four Scenarios

	Omni and Behind	Directional and Behind	Omni and Between	Directional and Between
Packets Created	1420	1420	1420	1420
–From Node	710	710	710	710
–From Jammer	710	710	710	710
Packets Destroyed	1296	724	1418	700
Packets Received	122	694	1418	718

would be perceived as noise. To have a more pronounced graphic for the second scenario, we followed the suggestion of the tutorial and changed the antenna gain from 20 dB to 200 dB. True, this is not a reasonable situation since in the real world antennas do not have that huge amount of antenna gain; this was done merely to illustrate a point.

4.2.2 Running the Wireless Simulation

Table 4.1 presents the four scenarios in a tabular form. The figures for the packets is the total amount generated during the simulation run.

The Packets Destroyed and the Packets Received do not equal the Packets Created figure, because the simulation ended just before the last packet from the jammer and from the node reached the base station. Otherwise, these would have been processed and included in the total.

4.2.2.1 Packet Reception Statistics

With the jammer being beyond both the sensor node and the base station, the impact was reduced. So 122 packets were successfully received with the omni-directional antenna. When the directional antenna is used, the amount of received packets improved to 694 or almost a six fold increase.

With the jammer traveling between the sensor node and the base station, the amount of good packets was zero. The directional antenna enabled almost half of the packets to be received.

It appears that the second effort was better than the first effort. That is not necessary true. The two tracks were different. There was no attempt to draw the two tracks to prove the same exposure time of the jammer to the base station. The Fig. 4.3 track was quickly created while as the Fig. 4.4

track was drawn to be equal distance for the north south leg and parallel to the directional antenna's main beam. The other point is that an antenna with very high gain tends to have a very narrow footprint–that is, a good balance between no gain and very high gain would enable the base station to monitor more of the environment.

4.2.2.2 Bit Error Rate and Packet Throughput Results

In the first scenario (See Fig. 4.5), the BER starts off low and begins to increase. This follows the rough arc path[2] of the jammer. And of course, the packet throughput started off high and fell to nil.

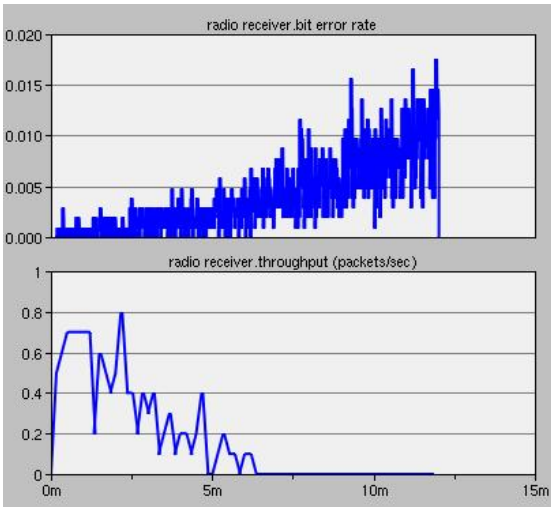


Figure 4.5: Jammer Trajectory Between the Nodes

When the first scenario is run with the high gain directional antenna, the BER is high, because the jammer is inside the antenna's cone (See Fig. 4.6.). When the jammer exits the antenna's cone, then the BER drops and the packet throughput goes up. Most of the time is jammer-free.

In the second scenario (See Fig. 4.7), the omni-directional antenna reviewed showed that the BER gradually increased as the distance between the jammer came close to the base station. The BER reached a maximum of about 0.32 errors per bit when the jammer is at the closest distance.

[2] The drawing reflects half of the curve, because the simulation was set to run as long as it took for the second scenario. The second scenario did not require as much time as the first.

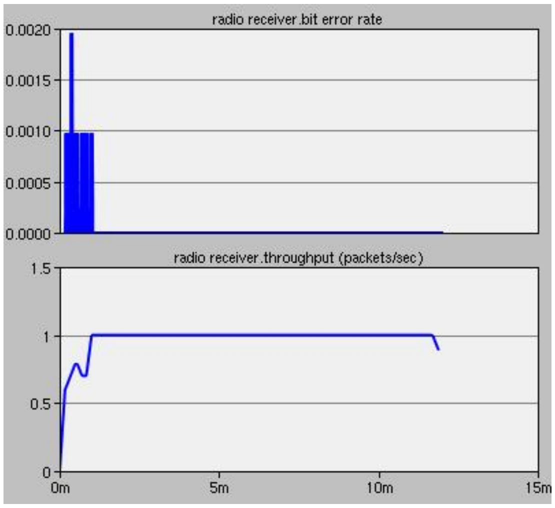


Figure 4.6: Jammer Trajectory Between the Nodes

There was no point when the environment appeared to be "free" of the jammer's transmissions. The two humps reflect the two points where the closest distance is the same.

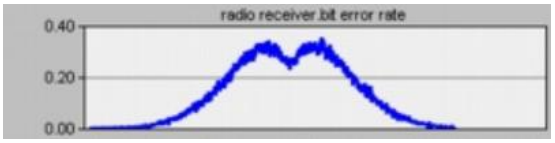


Figure 4.7: Jammer Trajectory Between the Nodes

When the second scenario is run with the high gain directional antenna, the BER is the same as the background noise and it appears that the jammer does not exist. When the jammer aligns with the transmitter and the base station (comes into the antenna's cone, the result is a total loss of packets. Fig. 4.8 shows a pronounced spike for the period of the alignment.

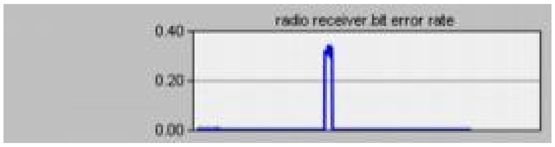


Figure 4.8: Jammer Trajectory Between the Nodes

4.3 Analysis

In [10], we used mathematical analysis to show that HEAPINGS is able to generate more useful work with almost no overhead.

HEAPINGS takes such a different approach from other protocols that it is hard to design a simulation that does a good job of showing off HEAPINGS features. So we took a small part of the protocol and designed a simulation to show one feature or benefit of HEAPINGS. That is, we had made the point that a HEAPINGS node could transmit straight to the base station and the base station's directional antenna would provide a narrow beam, greater reach, and insights to the location of the various nodes. The ns2 simulations showed that HEAPINGS is able to handle a large traffic volume with very little lost information. Again this comes from changing the operating assumptions. HEAPINGS has the benefit of using less resources to provide more information.

Furthermove, we stated that the nodes do not need to relay to other nodes. In other sensor networks, the nodes and the base station all use omni-directional antenna and relaying is used. So if a jammer was passing through the sensor field, communications within the network would be harmed, even destroyed. The OPNET simulation with omni-directional antennas supported this belief.

On the other hand, the jammer would only be effective if can come between a node and the base station–being in the general area will not give it the benefit of harming the communications. The OPNET simulation with directional antennas supported this belief.

So the OPNET's Modeler simulations showed the antenna behaviors and provided some useful insights. It is clear that a directional antenna with a reasonable amount of gain can cover an area and be able to receive a large amount of packets.

Now, the envisioned real world sensor network would have nodes that do not generate traffic continuously. So overloading the base station is not likely to be an issue. Also the other side may be more interested in shutting down the network than jamming it.

Chapter 5

EXPERIMENTAL WORK

The natural development or the next step would involve conducting some real world experiments. Due to unrepairable test equipment, limited flexiblity in the current test equipment and radios, and limited funds, it was not possible to conduct any proof-of-concept tests. This would need to be done by others or done at Auburn when funding is provided.

One way that others could confirm that the concepts are valid is to conduct some simple measurements. The following is an extract from a draft journal submission.

5.1 Introduction to the Draft Journal Submission

There is a symbiotic relationship between the military and science. What the military perceives as its need, science will rise to the occasion and produce the solution. The United States military began about in the early 1980s to shut down or greatly reduce their HF radio nets in favor of using the satellites (clear channel and dialing ease), cellular telephones (not tied down to a desk and dialing ease), and now the Internet (with access to much information). As a result, the current generation of computer scientists and computer engineers tend not to have the radio communications background and understanding that the older generations have had. They tend not to be interested in radio communications as a hobby nor to become amateur radio operators. They may not understand why there are problems with CrownCom's lofty goals of "using dynamic spectrum access".[84]

When hardware kits are ordered for various purposes, there does not seem to be much understanding about the radio section. Many wireless devices tend to operate in the 2 and 5 GHz sub bands. But sensor kits operate in much lower radio bands. A few universities are working with CubeSats and these operate in the 420 to 450 MHz sub band. For a number of the users and students, there is no thought about why the devices operate in these various sub bands. They may not understand that the lower frequencies propagate better than the higher frequencies. They may not understand antennas.

For example, the Auburn University Student Space Program has a document[85] that reports on the program progress. In the section that reported on how the students determined the range of the radios, this appeared on page 70:

> ... take the antenna and transceiver about a mile from the ground station to see if we could hear a signal to and from the antenna.

If communications is achieved, then it would be a minor miracle, because the distance between the satellite and the ground station would be closer to 700 kilometers, not the mile of the foregoing experiment. This documentation is very detailed, but there is no information about how to calculate the answer. Knowing the answer could determine if the right antenna is being used or if the proper transmit power setting is being used. Space makes for an expensive place to conduct trial and error experiments.

5.2 Working Background

So what do today's computer scientists and computer engineers have as a working background?

They and others know that laptop computers can use Wi-Fi locations to access the Internet. They may or may not understand why the range is so short for some locations and even shorter elsewhere. They may notice that their cellular telephones may require more recharging when they are away from large population centers, but they may not understand why. They have figured out that coverage around a spot is like a circle, but they may not realize the coverage is spherical.

What should computer scientists and computer engineers understand about the foregoing? They should understand that radio signals are traveling in an expanding front in all directions at about the speed of light or roughly 300,000,000 meters per second.[86] And they should understand that at this speed a radio wave could circle the globe in about 1/7 of a second.[86]

As a radio signal travels, it loses some of its energy. This comes more from the spreading or expanding wave front than from anything else. The strength drops in an inverse fashion. For

Table 5.1: Definitions of Terms in the Distance Equation

Term	Definition
H_{Tx}	Height of the transmit antenna.
H_{Rx}	Height of the receiver antenna.

example, if the wave strength or field strength[1] at 1 mile is 100 millivolts per meter[2], then at 2 miles it will degrade to 50 millivolts, at 3 miles it will degrade to 25 millivolts, and so on. Computer scientists and computer engineers should understand why lower frequencies survive the "trip" better than higher frequencies.

The proposed solution might be to use directional antennas. So how does a high gain antenna prevents this from happening? Computer scientists and computer engineers may not understand that directional antennas do not prevent this from happening. Instead it controls the amount of spread by reshaping the spreading pattern so that more energy or radio signal is traveling in the same direction.

5.3 What Should Be Understood?

Dealing with line-of-sight (LOS) frequencies (above 30 MHz), one learns that the curving earth will result in the signal traveling off into space. But LOS communications goes a bet beyond the expected distance to the horizon. So the question becomes: "How far is line-of-sight?" Equation 5.1 answers that question. Equation 5.1 assumes a smooth or flat earth and the receive antenna is on the ground. If the receive antenna has some height, then 5.2 would be better to use. Table 5.1 provides the definitions of the terms.

$$Distance(kilometers) = 4.124\sqrt{H_{Tx}(meters)} \tag{5.1}$$

$$Distance(km) = 4.124\left(\sqrt{H_{Tx}(m)} + \sqrt{H_{Rx}(m)}\right) \tag{5.2}$$

[1] This is the more common expression.

[2] The common way of expressing this.

The complete picture involves gain that is added to a signal and path losses that take from a signal. There are seven factors that contribute to the signal gain:

- Receiver sensitivity
- Receive antenna gain
- Receive antenna height
- Transmitter power
- Transmit antenna gain
- Transmit antenna height
- Required signal-to-noise ratio

These will be briefly explained in the following paragraphs.

5.3.1 Receiver sensitivity

Receiver sensitivity is the difference between hearing noise and hearing a weak signal. Table 5.2 has some rough values.[3] The last two columns of Table 5.2 reflects the rough receiver sensitivity for two signal widths[4] as provided by [86].[5] That is, the narrower the signal width, the better the values.

5.3.2 Antenna Gain

Antenna gain can range from 0 dBi for a whip antenna to 3 or so dBi for a dipole to 5 dBi or higher for a yagi antenna. If an antenna is embedded in a device, it could actually have a negative gain.

5.3.3 Antenna Height

The height of an antenna can add gain, but only when the antenna is at least 30 feet above the ground. An antenna mounted 50 foot above the ground sees about 4 dB gain improvement for a

[3] Those marked with an asterisk are provided values from [86]. The other values are interpolated by adding 3 dB and tripling the frequency.

[4] Communications people call this "bandwidths." To avoid confusion with the computer usage of this word, the normal communications term of "bandwidth" will not be used.

[5] [86] does not have an entry for the last column of the last row.

Table 5.2: Working Receive Noise Figures

Example Frequencies	Value in dB	Comments	3 kHz	100 kHz
50 MHz	3	Amateur*	167 dBW	150 dBW
144 MHz	5	Amateur*	164 dBW	149 dBW
150 MHz	5	Interpolating	164 dBW	149 dBW
222 MHz	5	Amateur*	164 dBW	149 dBW
432 MHz	8	Amateur*	161 dBW	146 dBW
450 MHz	8	Interpolating	161 dBW	146 dBW
915 MHz	9	ISM Interpolating	160 dBW	145 dBW
1296 MHz	10	Amateur*	159 dBW	144 dBW
1350 MHz	11	Interpolating	159 dBW	143 dBW
2450 MHz	12	ISM Interpolating	157 dBW	142 dBW
4050 MHz	14	Interpolating	155 dBW	139 dBW
5800 MHz	15	ISM Interpolating	154 dBW	??? dBW

50-mile leg and about 2 dB for a 100-mile leg. The best value is a 100-foot mounted antenna for a 50-mile leg where the added gain is 8 dB.

5.3.4 Transmitter Power

The more power pushing a signal, the longer it will last. To express the transmitter power in the same units as antenna, then one would take the log of the power and multiple the result by 10. For an example, a 500-watt station has 26.9897 dB above 1 watt.

$$26.9897 = 10log(500) \tag{5.3}$$

5.3.5 The Result

One would add the values to obtain the station gain. Then the matter of path loss must be considered. The first 100 miles, the path loss figures increase quickly. After the 100-mile point, the rate of increase tapers off.

For example, a station on 144 MHz is attempting to communicate with a station that is 300 miles away. The path loss of 214 dB. So combining the station gain, the signal is improved. Is the distant station able to work with the resulting signal? That is, if the network needs to have better

Table 5.3: Definitions of Terms in Friis Equation

Term	Definition
P_r	Power as perceived by the receiver.
P_t	Transmitter power.
G_t	Gain (dBi) as added by the transmitter antenna.
G_r	Gain (dBi) as added by the receiver antenna.
λ	The radio frequency in wavelengths.
R	The distance in the same measurement unit as wavelength.

dB values, then changes would be needed. Either reduce the distance or increase the antenna gain or raise the antenna higher or narrow the signal's bandwidth in order to gain improvements.

This is not the complete picture. A slight adjustment is needed for fading. Although fading is more common on frequencies below 30 MHz, VHF does experience some of this. Another small adjustment is needed to reflect line loss. In "quick-and-dirty" discussions, these two adjustments may be ignored and not be reflected in the calculations. One such equation is the Friis equation.

5.3.6 Friis Equation or Formula

The (Harald T.) Friis Transmission Equation may be used to determine the gain of the link (the "power" of the signal). There are different forms. The more simple form is the transmission equation 5.4.

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi R})^2 \tag{5.4}$$

Equation 5.4 is some times written from the viewpoint of the receiver as in equation 5.5.

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi R})^2 \tag{5.5}$$

Table 5.3 provides the definitions of the terms. Note that the antenna gains are expressed in dBi instead of other ratios and that the wavelength and the distance must be in the same units of measurement.

There are more complex forms of this equation. Some of these are attempts to capture the

Table 5.4: Definitions of Terms in Hata Equations

Term	Definition
L_U	For Urban areas. Answer in dB.
f	Frequency expressed in MHz.
h_B	Height in meters of the base station transmitter antenna.
C_H	One of these sub equations: Small to medium city: $0.8 + (1.1logf - 0.7)h_M - 1.56logf$ Large city ($150 \leq f \leq 200$): $8.29(log(1.54h_M))^2 - 1.1$ Large city ($200 < f \leq 1500$): $3.2(lo(1.75H_M))^2 - 4.97$
d	The distance expressed in kilometers.

impacts of impedance mismatches, directional antennas not pointing straight at each other, and different antenna polarizations. One form that is a slight modification of the basic Friis two-antennas-in-free-space equation adjusts the exponent "2" to be different values between "3" and "5" for urban settings. Although these adjustments reflect the urban environment, if at least one of antennas is at least 30 feet above the ground, then the measured gain will improve. This improvement is known as "station" gain.

5.3.7 Hata Equation or Formula

Another predication equation is the Hata suite. These various forms predicate the degradation of the signal. The equations attempt to capture what was found by real experiments in Tokoyo during the 1960s. The basic form of the Hata equation 5.6 follows:

$$L_U = 69.55 + 26.16logf - 13.82logh_B - C_H + [44.9 - 6.55logh_B]logd \tag{5.6}$$

Table 5.4 provides the definitions of the terms.

The Hata model for suburban areas uses equation 5.6, but improves the loss by two adjustments:

$$L_{SU} = L_U - 2(log\frac{f}{28})^2 - 5.4 \tag{5.7}$$

The Hata model for open areas uses equation 5.6, but improves the loss by three adjustments:

Work Sheet for Each Frequency	
Frequency	
Antenna Gain	
Transmitter Power	
Distance	
Antenna Height	
Signal Width	

Result of changing	Friis Calculated Values	Measured Values
Frequency		
Antenna Gain		
Transmitter Power		
Distance		
Antenna Height		
Signal Width		

Figure 5.1: Sample Form

$$L_O = L_U - -4.78(logf)^2 + 18.33logf - 40.97 \tag{5.8}$$

With the complex math steps, it is easy to forget that small values are better (less signal loss). Whereas, in the Friis family of equations large values are better (received signal strength or power).

The Hata equation is not perfect. There is work to correct errors or to improve it. See Medeissis and Kajackas[87] as an example.

5.4 The Approach

Previous generations of computer scientists and computer engineers gained an understanding of the foregoing from interactions with the physical world. Current and future generations tend to interact with a virtual world that may parallel the real world. Textbook study helps, but not completely. Our approach would help the new computer scientists and the new computer engineers to gain a feel for line-of-sight radio behaviors. The students would use a worksheet similar to Figure 5.1. These are the fields of the Friis equation plus the two fields that are not included.

Then the student notes a baseline value. Varies each parameter and notices the changes.

Modified Work Sheet			
Frequency	Mxxx.xxxx		
Antenna Gain	nn dBi		
Transmitter Power	nn watts		
Distance			
Antenna Height			
Signal Width		AFSK	FSK
Result of changing	Friis Calculated Values	Measured Values	
Distance			
Antenna Height			
Signal Width			

Figure 5.2: Modified Sample Form

5.4.1 Auburn University As An Example

Not all locations have fully stocked electrical/electrons lab. Auburn University is no different from the other universities. Yet these insights can be taught with the less than ideal equipment.

5.4.1.1 What is Available at Auburn University

At Auburn University, we only had a fixed frequency transmitter with a dipole antenna and with a fixed output power. So a student could vary the distance, the antenna heights, and the signal width. Figure 5.2 reflects the changes to the form.

Using AFSK or Audio Frequency-Shift Keying is useful, because it has a wider signal than FSK or Frequency-Shift Keying. AFSK varies audio tones whereas FSK varies or moves between two nearby frequencies. Changing the height of one end and changing the distance are options that are possible at any college or university. After the student has obtained a good spread of distances values and of antenna heights for each emission, then the results could be collected into a table like Figure 5.3. The Friis equation would be executed for each row.

The student should be able to notice some patterns and some “surprises.”

Distance	Height	AFSK	FSK	FRIIS
A	X	*	*	
A	Y	*	*	
A	Z	*	*	
B	X	*	*	
B	Y	*	*	
B	Z	*	*	
C	X	*	*	
C	Y	*	*	
C	Z	*	*	

Figure 5.3: Results

5.5 Conclusion

Once a student has done a number of measurements, he or she will begin to understand the nature of radio behavior. Also he or she will understand that real world does not always align with the results of an equation. This discovery will enable the student to take equation results with a "grain of salt."

Perhaps seeing that a narrower signal width has better results may encourage better hardware designs. For example, Single Side Band (SSB) is used instead of amplitude modulation (AM) on the HF bands, because SSB uses half the signal width of AM. The benefit is less power is needed and a clearer signal. Both federal and non-federal radio nets are converting from 16 kHz wide FM signals to 11 kHz or less. The benefit is a closer spacing of nets and a doubling of available radio channels. Television stations are beginning to convert from 6 MHz-plus wide signals to much narrower digital signals. The benefit is better sound and video while freeing up more radio spectrum for other services to use. Today too many wireless designs do not seem to consider the need for a small spectrum footprint. Maybe this teaching approach could help the students to think in terms of radio spectrum.

Future work would be to use this approach in a networking course to validate that this helped the students to understand more about wireless networking.

Chapter 6

CONCLUSIONS: ANTICIPATED BENEFITS

6.1 General Comments

I anticipate that the work on the helio protocol suite could result in the ability to track firefighters traveling through a burning building. The success of this effort would mean no wired environment, no need to carry a beacon, no need to have “fake” GPS or direction finding stations deployed around the burning building. The firefighters would not need to carry another device or radio. Instead all of the workload would be on the base station computer that could be on or in the fire chief’s vehicle. Heaven forbid that a repeat of 9-11 should take place. But if it does, then it should be easier to zero in on the exact locations of the trapped firefighters and other safety workers.

Likewise, the helio protocol suite could track a person moving through a building. From access point to access point, the person would be tracked. With directional antennas, the deployment of access points could be done better without the wasteful overlapping coverage.

Aircraft flying a grid pattern could have one aircraft functioning as a command-and-control element. Without the need for a heavy duty radar system, the locations of each involved “player” could be determined. The resources could be managed better. Aircraft would not bump into each other and no search area is missed.

6.2 Security Comments

I anticipate that the helio protocol suite could enhance the security of a sensor network on several levels.

6.2.1 Physcial Security

Physical security could be enhanced, because the base station does not need to be near any of the sensor nodes. The command element and the base station could be placed at some distance to the rear of the battlefield.

6.2.2 Mission Security

Mission security could be enhanced, because the nodes could be spread out for better coverage of an area. Each node transmitting back to the base station would provide a piece of the big picture. The base station could construct the big picture in real time and with greater precision. To achieve the same coverage with traditional sensors networks would require a greater number of nodes–and such an approach would require the network to deal with routing congestion and the great likelihood of a chance discovery.

Again, by having the nodes far a part, this would make it harder for someone to make a chance discovery. This is an always a present problem for the traditional sensor network.

Another part of mission security is the matter of lifetime. A network that dies quickly is a network that is not collecting and forwarding information. Anything that can enhance the lifetime of the network should be used. HEAPINGS achieves a longer lifetime by reducing service traffic and cutting out flooding messages. Also by using directional antennas, the nodes do not need to use high power to reach the base station.

6.2.3 Communications Security

Communications security is a balance between speed and costs. Taking advantage of the radio propagation behaviors and directional antennas would result in a low cost approach to communications security. That is, by selecting the right frequency in order to reach the nodes and not go any further, this would result in the other side not being able to intercept the radio signal.

Adding a bit of overhead, then the HEAPINGS base station could validate a node. That is, it has a list of valid nodes. After a roll call, it will know what nodes are present and where they are located. If a new node tries to enter the network or a known node appears to be in a different location from where it checked in, then the base station can tag or mark the node as questionable and will watch the node closely.

Encryption security is a question. Could the nodes' transmissions be encoded? This is not listed as one of the central features for HEAPINGS, because such effort would require extra overhead and a greater drain on the batteries. However, it is possible that the mission may be such that the commander would accept the reduced lifetime in order to have this feature. Thus, all decisions have trade-offs.

Future researchers might find an solution that would reduce the impact and thus give the commander greater flexibility.

Another way to have enhanced communications security is by reducing the amount of message traffic. HEAPINGS is able to greatly cut down the amount of message traffic by cutting out flooding and reducing service messages. Thus there are no transmission, the other side cannot guess where the transmitter is located.

6.3 The Future

HEAPINGS is a concept. It is still immature, but it does suggest a new direction for research. The Internet and the routing protocols are based on the cold war envirnoment where a nuclear bomb could take out a large part of the network. These "cold war" approaches have been applied to ad hoc networks and to sensor networks. That may not be the best approach for networks that are not trying for coast-to-coast coverage.

I did not know about triered networks when I first began my ponderings, but I was pleased to noticed that these researchers are beginning to break with the "cold war" mind set–for example, the nodes are not robust and do not have numerous abilities.

In short , my approach should result in better safety, better solutions to the geo-location problem, saved lives, and better collection of information.

BIBLIOGRAPHY

[1] Answers.com. Biography: Arthur schopenhauer, Year unknown; accessed 2008. URL http://www.answers.com/topic/arthur-schopenhauer?cat=entertainment.

[2] Martin J. Feuerstein, Michael A. Zhao, Yonghai Gu, and Scot D. Gordon. the future of smart antennas: Evolution to 3G and IP networks. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 1, pages 48–54, London, United Kingdom, September 18–21, 2000.

[3] K. Rambabu and R. Rajagopal. Smart base station antenna. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*, pages 303–306, Hyderabad, India, December 17–20, 2000.

[4] R. Hoppe, P. Wertz, G. Wolfle, and F. M. Landstorfer. Wideband propagation modelling for indoor environments and for radio transmission into buildings. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 1, pages 282–286, London, United Kingdom, September 18–21, 2000.

[5] Li Xinrong Li, Kaveh Pahlavan, Matti Latva-Aho, and Mika Ylianttila. Indoor geo-location using OFDM signals in HIPERLAN/2 wireless LANs. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 2, pages 1449–1453, London, United Kingdom, September 18–21, 2000.

[6] Kent Rosengren, Per-Simon, Kildal, Jan Carlsson, and Olof Lunden. A new method to measure radiation efficiency of terminal antennas. In *Proc. 2000 IEEE-APS Conference on Antennas and Propagation for Wireless Communications*, pages 5–8, Waltham, Massachusetts, November 6–8, 2000.

[7] Science and Technology Division. *Statement of Requirements for Public Safety Wireless Communications and Interoperability.* United States Department of Homeland Security, 1.0 edition, March 10, 2004. URL http://www.safecomprogram.gov/NR/rdonlyres/3FFFBFBA-DC53-440E-B2EF-ABD391F13075/0/SAFECOM_Statement_of_Requirements_v1.pdf.

[8] Wayne Rash. Mining for answers: Would RFID have helped in the utah mine tragedy? *eWeek*, page 60, September 10, 2007. URL http://www.eweek-digital.com/eweek/20070910_stnd/?pg=61.

[9] CAP Operations. Supporting our communities in times of need, Year unknown; accessed 2008. URL http://www.cap.gov/about/PROGRAMS/OPS.html.

[10] Fred L. Strickland, Yu Wang, and Alvin S. Lim. HEAPINGS: A secure counterintuitive sensor network protocol. In Hamid R. Arabnia, Victor A. Clincy, and Laurence T. Wang, editors, *Proc. 2007 International Conference on Wireless Netwoks (ICWN '07)*, pages 474–480, Las Vegas, Nevada, June 25–28, 2007. World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP '07).

[11] Fred L. Strickland and Yu Wang. HEAPINGS: From concept to simulations. In Hamid R. Arabnia and Victor A. Clincy, editors, *Proc. 2008 International Conference on Wireless Netwoks (ICWN '08)*, pages 590–596, Las Vegas, Nevada, July 14–17, 2008. World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP '08).

[12] Satish Jamadagni and M. N. Umesh. A PUSH download architecture for software defined radios. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*,

pages 404–407, Hyderabad, India, December 17–20, 2000.

[13] R. Vishwakarma and K. S. Shanmugan. Performance analysis of transmit antenna diversity in 3G WCDMA system. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*, pages 1–4, Hyderabad, India, December 17–20, 2000.

[14] Ashvin Chheda. On the forward link capacity of a wide band DS-CDMA system with transmit diversity. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*, pages 417–421, Hyderabad, India, December 17–20, 2000.

[15] Morten Jeppesen, Soren Holdt Jensen, and Gert Frolund Pedersen. Prediction based multi-antenna single-receiver mobile terminal. In *Proc. 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2001)*, pages A120–A124, San Diego, California, September 30, /October 3, 2001.

[16] Mostafa Hefnawi and Giles Y. Delisle. Impact of wideband CDMA signals on smart antenna systems. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*, pages 5–8, Hyderabad, India, December 17–20, 2000.

[17] Andreas Czylwik. Downlink beamforming for mobile radio systems with frequency division duplex. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 1, pages 72–76, London, United Kingdom, September 18–21, 2000.

[18] Kapil R. Dandekar, Hao Ling, and Guangham Xu. Smart antenna array calibration procedure including amplitude and phase mismatch and mutual coupling effects. In *Proc. 2000 IEEE International Conference on Personal Wireless Communications*, pages 293–297, Hyderabad, India, December 17–20, 2000.

[19] Khalid AlMidfa, Eustace Tameh, and Andrew Nix. Improved DOA estimation using polarisation diversity: Simulations using a wideband propagation model. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 1, pages 539–543, London, United Kingdom, September 18–21, 2000.

[20] R. Tingley and K. Pahlavan. A statistical model of space-time radio propagation in indoor environments. In *Proc. 2000 IEEE-APS Conference on Antennas and Propagation for Wireless Communications*, pages 61–64, Waltham, Massachusetts, November 6–8, 2000.

[21] Marshall D. Brain. How radar works, Year unknown; accessed 2008. URL `http://www.howstuffworks.com/radar2.htm`.

[22] V. A. Kryachko. The variant of equation of direction finding characteristic of the amplitude sum-difference direction finder. In *Proc. IVth International Conference on Antenna Theory and Techniques*, volume I, pages 376–377, Sevastopol, Ukraine, September 9–12, 2003. IEEE.

[23] S. T. Bagdasaryan, V. A. Tarshin, and V. A.Vasilyev. Measurements of reception direction of deterministic signal against spatially-correlated interferences with the use of the adaptive antenna array. In *Proc. IVth International Conference on Antenna Theory and Techniques*, volume I, pages 381–383, Sevastopol, Ukraine, September 9–12, 2003. IEEE.

[24] S. V. Kukobko, A. Z. Sazonov, and O. I. Sukharevsky. Calculation of nose dielectric radome effect on direction-finding characteristics of an antenna system. In *Proc. IVth International Conference on Antenna Theory and Techniques*, volume II, pages 657–660, Sevastopol, Ukraine, September 9–12, 2003. IEEE.

[25] A. Yu. Grinev, I. A. Chebakov, and A. I. Gigolo. Solution of the inverse problems of subsurface radiolocation. In *Proc. IVth International Conference on Antenna Theory and Techniques*, volume II, pages 523–526, Sevastopol, Ukraine, September 9–12, 2003. IEEE.

[26] PBS-TV. Hunt for the super twister, March 30, 2005. URL `http://www.pbs.org/wgbh/nova/transcript/3107_tornado.html`. This was a broadcast. Transcript is at web address.

[27] Vadim L. Pazynin and Yuriy K. Sirenko. Study of pulse signal propagation in urban envi-

ronment by the finite-difference method. In *Proc. IVth International Conference on Antenna Theory and Techniques*, volume II, pages 705–707, Sevastopol, Ukraine, September 9–12, 2003. IEEE.

[28] D. Davis, B. Segal, C. W. Trueman, R. Calzadilla, and T. Pavlasck. Measurement of indoor propagation at 850 MHz and 1.9 GHz in hospital corridors. In *Proc. 2000 IEEE-APS Conference on Antennas and Propagation for Wireless Communications*, pages 77–70, Waltham, Massachusetts, November 6–8, 2000.

[29] C. W. Trueman, D. Davis, and B. Segal. Ray optical simulation of indoor corridor propagation at 850 and 1900 MHz. In *Proc. 2000 IEEE-APS Conference on Antennas and Propagation for Wireless Communications*, pages 81–86, Waltham, Massachusetts, November 6–8, 2000.

[30] R. W. Matthews, W. G. Scott, and C. C. Han. Multibeam antennas for data communications satellites. In *Proc. 5th Symposium on Data Communications*, volume 2, pages 20–29, Snowbird, Utah, September 27–29, 1977. ACM.

[31] K. Pahlava. Practice and experience: Wireless intraoffice networks. *ACM Transactions on Office Information Systems*, 6(3):277–302, July 1988.

[32] Z. Rosberg and J. Zande. Toward a framework for power control in cellular systems. *Wireless Networks*, 4(3):215–222, March 1998.

[33] P. van Rooyen, R. Kohno, and I. Oppermann. DS-CDMA performance with maximum ratio combining and antenna arrays. *Wireless Networks*, 4(6):479–488, November 1998.

[34] Evan Gabber and Avishai Wool. How to prove where you are: Tracking the location of customer equipment. In *Proc. 5th ACM Conference on Computer and Communications Security*, pages 142–149, San Francisco, California, November 3–5, 1998.

[35] N. B. Pronios. Performance considerations for slotted spread-spectrum random-access networks with directional antennas. In *Proc. IEEE GLOBECOM'89*, volume 3, pages 1613–1617, Dallas, Texas, November 27–30, 1989.

[36] J. Ward and Jr R. T. Compton. Improving the performance of a slotted ALOHA packet radio network with an adaptive array. *IEEE Transactions on Communications*, 40(2):292–300, February 1992.

[37] J. Ward and Jr R. T. Compton. High throughput slotted ALOHA packet radio network with an adaptive array. *IEEE Transactions on Communications*, 41(3):460–470, March 1993.

[38] A. Sugihara, K. Enomoto, and I. Sasase. Throughput performance of a slotted nonpersistent CSMA with an adaptive array. In *Proc. 6th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '95)*, volume 2, pages 75–80, Toronto, Canada, September 27–29, 1995.

[39] F. Shad, T. D. Todd, V. Kezys, and J. Litva. Indoor SDMA capacity using a smart antenna basestation. In *Proc. 6th International Conference on Universal Personal Communications (ICUPC 97)*, pages 868–872, San Diego, California, October 12–16, 1997. IEEE.

[40] F. Shad, T. D. Todd, V. Kezys, and J. Litva. Dynamic slot allocation (DSA) in indoor SDMA/TDMA using a smart antenna basestation. *IEEE/ACM Transactions on Networking*, 9(1):69–81, February 2001.

[41] R. Sass. Communications networks for the Force XXI digitized battlefield. *Mobile Networks and Applications*, 4(3):139–155, October 1999.

[42] J. Razavilar, F. Rashid-Farrokhi, and K. J. R. Liu. Software radio architecture with smart antennas: A tutorial on algorithms and complexity. *IEEE Journal on Selected Areas in Communications*, 17(4):662–676, April 1999.

[43] Fernando C. Gomes, Panos Pardalos, Carlos. S. Oliverira, and Mauricio G. C. Resende. Reactive GRASP with path relinking for channel assignment in mobile phone networks. In *Proc. 5th International Workshop on Discrete Algorithms and Methods for Mobile Computing and*

Communications, pages 60–67, Rome, Italy, July 21, 2001. ACM.

[44] K. Kobayashi and M. Nakagaw. Spatially divided channel scheme using sectored antennas for CSMA/CA - 'Directional CSMA/CA'. In *Proc. 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, volume 1, pages 227–231, London, United Kingdom, September 18–21, 2000.

[45] S. Yi, Y. Pei, and S. Kalyanaraman. On the capacity improvement of ad hoc wireless networks using directional antennas. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pages 108–116, Annapolis, Maryland, June 1–3, 2003.

[46] J. Cheng, M. Hashiguchi, K. Ligusa, and T. Ohira. Electronically steerable parasitic array radiator antenna for omni- and sector pattern forming applications to wireless ad hoc networks. *IEE Proceedings Microwaves, Antennas and Propagation*, CL(4):203–208, August 2003. Has become *IET Microwaves, Antennas & Propagation.*

[47] R. Ramanathan. On the performance of ad hoc networks with beamforming antennas. In *Proc. 2nd International ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2001)*, pages 95–105, Long Beach, California, October 4–5, 2001.

[48] T. Korakis, G. Jakllari, and L. Tassiulas. A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pages 98–107, Annapolis, Maryland, June 1–3, 2003.

[49] M. Takai, J. Martin, A. Ren, and R. Bogrodia. Directional virtual carrier sensing for directional antennas in mobile ad hoc networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '02)*, pages 183–193, Lausanne, Switzerland, June 9–11, 2002.

[50] Y-B. Ko and N H. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. *Wireless Networks*, 6(4):307–321, 2000.

[51] A. Nasipuri and K. Li. A directionality based location discovery scheme for wireless sensor networks. In *Proc. Eighth Annual International Conference on Mobile Computing and Networking (MOBICOM '02)*, pages 105–111, Atlanta, Georgia, September 23–28, 2002. ACM.

[52] T-S. Yum and K-W. Hung. Design algorithms for multihop packet radio networks with multiple directional antennas stations. *IEEE Transactions on Communications*, 40(11):1716–1724, November 1992.

[53] Martin Horneffer and Dieter Plassmann. Directed antennas in the mobile broadband system. In *Proc. 15th Annual Joint Conference of the IEEE Computer Societies (IEEE INFOCOM '96)*, volume 2, pages 704–712, San Francisco, California, March 24–28, 1996.

[54] C. Sakr and T. D. Todd. Carrier-sense protocols for packet-switched smart antenna basestations. In *Proc. IEEE International Conference of Network Protocols*, pages 45–52, Atlanta, Georgia, October 28–31, 1997.

[55] Young-Bae Ko, Vinaychandra Shankarkumar, and Nitin H. Vaidya. Medium access control protocols using directional antennas in ad hoc networks. In *Proc. IEEE INFOCOM 2000*, volume 1, pages 13–21, Tel Aviv, Israel, March 26–30, 2000.

[56] Romit Roy Choudhury, Xue Yang, Ram Ramanathan, and Nitin H. Vaidya. Using directional antennas for medium access control in ad hoc networks. In *Proc. 8th Annual International Conference on Mobile Computing and Networking (MOBICOM '02)*, pages 59–70, Atlanta, Georgia, September 23–28, 2002. ACM.

[57] Nitin Vaidya, Year unknown; accessed 2008. URL `http://www.crhc.uiuc.edu/wireless/talks/purdue.ppt`. Versions of this talk presented at University of Pennsylvania (July 2002) and Purdue University (August 2002). Slides used for a presentation at the 2002 CCW work-

shop, Santa Fe (there are more slides here than included in the workshop proceedings).

[58] A. Nasipuri, J. You S. Ye, and R. E. Hironmoto. A MAC protocol for mobile ad hoc networks using directional antennas. In *Proc. IEEE WCNC 2000*, volume 3, pages 1214–1219, Chicago, Illinois, September 23–28, 2000.

[59] A. Nasipuri, J. Mandava, H. Manchala, and R. E. Hiromoto. On-demand routing using directional antennas in mobile ad hoc networks. In *Proc. 9th International Conference on Computer Communications and Networks*, pages 535–541, Las Vegas, Nevada, October 16–18, 2000. IEEE.

[60] S. Bandyopadhyay, K. Hasuike, S. Horisawa, and S. Tawara. An adaptive MAC protocol for wireless ad hoc community network (WACNet) using electronically steerable passive array radiator antenna. In *Proc. GLOBECOM 01: IEEE Global Telecommunications Conference (GLOBECOM 2001)*, volume V, pages 2896–2900, San Antonio, Texas, November 25–29, 2001.

[61] S. Bandyopadhyay, K. Hasuike, S. Horisawa, and S. Tawara. An adaptive MAC and directional routing protocol for ad hoc wireless network using ESPAR antenna. In *Proc. 2nd International ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2001)*, pages 243–246, Long Beach, California, October 4–5, 2001.

[62] A. Nasipuri, K. Li, and U. R. Sappidi. Power consumption and throughput in mobile ad hoc networks using directional antennas. In *Proc. 11th International Conference on Computer Communications and Networks*, pages 620–626, Miami, Florida, October 14–16, 2002. IEEE.

[63] Lichun Bao and J.J. Garcia-Luna-Aceves. Transmission scheduling in ad hoc networks with directional antennas. In *Proc. 8th Annual International Conference on Mobile Computing and Networking (MOBICOM '02)*, pages 48–58, Atlanta, Georgia, September 23–28, 2002. ACM.

[64] S. Roy, D. Saha, S. Bandyopadhyay, T. Ueda, and S. Tanaka. A network-aware MAC and routing protocol for effective load balancing in ad hoc wireless networks with directional antennas. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pages 88–97, Annapolis, Maryland, June 1–3, 2003.

[65] Bruno Sinopoli, Courtney Sharp, Luca Schenato Shawn Schaffert, and Shankar Sastry. Distributed control applications within sensor networks, August 2003. URL `http://robotics.eecs.berkeley.edu/~sinopoli/proceedings.pdf`.

[66] Chee-Yee Chong and Srikanta P. Kumar. Sensor networks: Evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, August 2003. URL `http://www.cs.utah.edu/classes/cs6935/papers/sensNet1.pdf`.

[67] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan. Adaptive protocols for information dissemination in wireless sensor networks. In *Proc. 5th annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 174–185, Seattle, Washington, August 15–19, 1999.

[68] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proc. 6th Annual International Conference on Mobile Computing and Networking*, pages 56–67, Boston, Massachusetts, August 6–11, 2000. ACM.

[69] Alvin Lim. Distributed services for information dissemination in self-organizing sensor networks, 2001. URL `http://www.eng.auburn.edu/users/lim/sensit/service.pdf`.

[70] Carme Àlvarez, Josep Diaz, Jordi Petit, José Rolim, and Maria Serna. Efficient and reliable high levelcommunications in randomly deployed wireless sensor networks. In *Proc. Second International Workshop on Mobility Management and Wireless Access Protocols (MobiWac '04)*, pages 106–110, Philadelphia, Pennsylvania, October 1, 2004. ACM. URL `http://www.ing.unipi.it/~o783499/research/docs/MSWiM04.pdf`.

[71] Matt Welsh and Geoff Mainland. Programming sensor networks using abstract regions. the

first USENIX/ACM symposium on networked systems design and implementation (NSDI '04), March 2004. URL http://www.usenix.org/events/nsdi04/tech/full_papers/welsh/welsh_html/nsdi.html.

[72] Michael Arnone. Cybersecurity bill gains steam. *Federal Computer Week*, XIX(12):12, April 2005.

[73] Department of Computer Science and Software Engineering. Graduate program handbook, general regulations, 2.6 graduate course requirements, Year unknown; accessed 2008. URL http://eng.auburn.edu/programs/csse/programs/grad/handbook/gen-reg.html.

[74] George Washington University. Studying infosec at gwu, Year unknown; accessed 2007. URL http://www.seas.gwu.edu/~infosec/.

[75] Andrew. S. Tanenbaum. *Computer Networks.* Prentice Hall PTR, fourth edition, 2003.

[76] David B. Johnson. Scalable support for transparent mobile host internetworking. *Wireless Networks*, 1:311–321, October 1999.

[77] G. Racherla, J. L. Ellis, D. S. Furuno, and S. C. Lin. Ultra-wideband systems for data communications. In *Proc. 2002 IEEE International Conference on Personal Wireless Communications*, pages 129–133, New Delhi, India, December 15–17, 2002.

[78] Harris. An/PRC-152 type-1 multiband multimisson handheld radio, 2008. URL http://www.rfcomm.harris.com/products/tactical-radio-communications/an-prc-152.pdf.

[79] Cengiz Alaettinoĝlu, Klaudia Dussa-Zierger, Ibrahim Matta, and A. Udaya Shankar. MaRS (maryland routing simulator) - version 1.0 user's manual. *University of Maryland College Park Technical Report*, 91(80):1–36, June 1991.

[80] Paul A. Fishwick. *Simulation Model Design and Execution: Building Digital Worlds.* Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1995.

[81] The network simulator -ns-2, 1995. URL http://www.isi.edu/nsnam/ns/.

[82] Marc Greis. Tutorial for the network simulator ns, Year unknown; accessed 2008. URL http://www.isi.edu/nsnam/ns/tutorial/.

[83] OPNET. OPNET modeler wireless suite, Year unknown; accessed 2008. URL http://www.opent.com/solutions/network_rd/modeler_wireless.html.

[84] CrownCom 2008. The third international conference on cognitive radio oriented wireless networks and communications, 2008. URL http://www.crowncom.org/index.shtml.

[85] Auburn University Student Space Program. AubieSAT-1: Auburn's first student-built satellite, April 2007. URL http://space.auburn.edu/page_attachments/0000/0046/Spring_2008.pdf.

[86] The American Radio Relay League. Radio wave propagation. In R. Dean Straw, editor, *The ARRL Antenna Book*, chapter 23, pages 1–35. The American Radio Relay League, Newington CT 06111, 1994.

[87] A. Medeisis and A. Kajackas. On the use of the universal Okumura-Hata propagation prediction model in rural areas. In *Proc. 51st Vehicular Technology Conference IEEE VTC 2000*, volume 3, pages 1815–1818, Tokyo, Japan, May 15–18, 2000.

[88] Scott Health and Safety. Pak-alert se questions and answers, Year unknown; accessed 2004. URL http://www.scotthealthsafety.com/PDFs/QA_pkalert_6097_702.pdf.

[89] Mine Safety Appliances Company. ICMTM 2000 and ICMTM 2000 plus integrated computer modules, Year unknown; accessed 2004. URL http://media.msanet.com/NA/UnitedStatesofAmerica/SAR/SelfContainedBreathingApparatus/SCBAPartsandAccessories/ICM2000andICM2000Plus/0119-27-ICM2000.pdf. Also explore the website for other documents such as 10018725.pdf.

[90] Jean MacDougall-Tattan. Firefighters safer thanks to new radios, March 24, 2003. URL http://www.eagletribune.com/news/stories/20030324/HA_002.htm.

[91] Communications-Applied Technology. Intrinsically safe wireless intercom system, Year unknown; accessed 2004 and 2008. URL http://www.c-at.com/ispages/is.html.

[92] On line Press Release. New kenwood trunking mobiles feature two-way paging fleetsync(tm) paging protocol extends capability of TK-980/981 mobiles, Year unknown; accessed 2004 and 2008. URL http://www.kenwood.net/indexKenwood.cfm?do=PRDetail&PRID=10.

[93] Sierra Wireless. MP 775 GPS rugged wireless modem for global EDGE, GPRS and GSM networks, Year unknown; accessed 2004.. URL http://www.sierrawireless.com/ProductsOrdering/mp775.asp.

[94] Peter H. Dana. Global positioning system overview, Year unknown; accessed 2004 and 2008. URL http://www.colorado.edu/geography/gcraft/notes//gps/gps_f.html.

[95] Oak Ridge National Laboratory. Sensor-based tagging and tracking system: Next-generation time, space, and position information system, Year unknown; accessed 2004. URL http://www.ornl.gov/sci/engineering_science_technology/sms/Hardy%20Fact%20Sheets/Sensor-Based%20Tagging.pdf.

[96] National Executive Committee for Space-Based PNT. U. s. space based positioning, navigation, and timing policy, December 15, 2004. URL http://pnt.gov/policy/.

[97] Rosum Corporation, Year unknown; accessed 2008. URL http://www.rosum.com/rosum_tv-gps_indoor_location_technology.html. Information is on several web pages. See other pages.

[98] Skyhook Wireless, Year unknown; accessed 2004.. URL http://www.skyhookwireless.com.

[99] Carmen Nobel. Skyhook rolls out wi-fi system. *eWeek*, 22(25):21, June 20, 2005.

[100] James Careless. First responder communications: Alternatives to CDPD. *Advanced Rescue Technology*, VII(4):71–78, August/September 2004.

[101] RFID Journal. Frequently asked questions, Year unknown; accessed 2004. URL http://www.rfidjournal.com/article/articleview/207#Anchor-What-363.

[102] News Scan. Target shares rfid plans. *InformationWeek*, page 14, August 16–23, 2004. There was a version on the Internet, but it is no longer available.

[103] Renee Boucher Ferguson. Rfid mandates spur industry action. *eWeek*, page 17, July 26, 2004.

[104] Laurie Sullivan. IBM shares RFID lessons. *InformationWeek*, page 64, October 25, 2004.

[105] Bob Brewin. No silver bullets: Initial DoD RFID hype gets tempered by reality. *Federal Computer Week*, XIX(13):39+, May 2005.

[106] Andy Ward, Paul Webster, and Peter Batty. Local positioning system – technology overview and applications, September 2003. URL http://web.archive.org/web/20051024070310/http:/ubisense.net/Product/files/Ubisense+LBS+overview+white+paper+September+2003.pdf.

[107] SWS Security. Sws security's tracknet networked radio direction finder system, Year unknown; accessed 2004. URL http://www.swssec.com/tracknet.html.

[108] United States Fire Administration. Firefighter fatality retrospective study, April 2002. URL http://www.usfa.fema.gov/downloads/pdf/publications/fa-220.pdf.

[109] NOAA. Emergency personal locator beacon system becomes operational nationwide, Year unknown; accessed 2004.. URL http://www.noaanews.noaa.gov/stories/s1168.htm.

[110] NOAA. Homepage, Year unknown; accessed 2004.. URL http://www.noaanews.noaa.gov.

[111] NOAA. Personal locator beacons–help from above, Year unknown; accessed 2004.. URL http://www.noaanews.noaa.gov/magazine/stories/mag96.htm.

[112] Princeton MN Automated Flight Service Station. Direction finding (DF) service, Year unknown; accessed 2005. URL http://www.pnmafss.faa.gov/pages/DF.asp.

[113] Federal Communications Commission. Enhanced 911, Year unknown; accessed 2008. URL http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html. Ac-

cessed 'Enhanced 911' on http://www.fcc.gov/911/enhanced/ on 11 October 2004. It has been replaced by 'Enhanced 911 - Wireless Services' on http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html, which was accessed on 15 May 2008.

[114] Kathryn Manzi. Rescue 21 update. *On Scene*, pages 7–8, Summer 2004.

[115] Skip Liepman. C2 constellation. *Military Information Technology*, 8(6):10–13, 2004.

[116] Clarence A. Robinson Jr. Sensors bolster army prowess, Year unknown; accessed 2008. URL `http://www.afcea.org/signal/articles/anmviewer.asp?a=30&z=10`.

[117] Robert S. Dudney. Where do UAVs go from here? *Air Force Magazine*, 88(7):2, July 2005. URL `http://www.afa.org/magazine/july2005/0705editorial.pdf`.

[118] California Institute for Telecommunications and Information Technology. ECE 156/MAE 149/SIO 238 sensor networks, Year unknown; accessed 2005. URL `http://www.calit2.net/technology/features/8-7-03_SensornetClass.htm`. Accessed 19 July 2005. Clayton Okino was an instructor for this course. See Student paper by Cheng-yu Sung, Chris Hiestand, and Shadi Ghandchi on Battlefield Sensors (1 August 2003. http://www.calit2.net/technology/features/sensorNetClass/ece156-battlefield.pdf).

[119] David Culler, Jason Hill, Mike Horton, Kris Pister, Robert Szewczyk, and Alec Wood. Mica: the commercialization of microsensor motes. *Sensor Technology and Design*, April 2002. URL `http://www.sensorsmag.com/articles/0402/40/main.shtml`.

[120] Sarah Yang. Researchers create wireless sensor chip the size of glitter, June 2003. URL `http://www.berkeley.edu/news/media/releases/2003/06/04_sensor.shtml`.

[121] G. Anastasi, A. Falchi, A. Passarella, M. Conti, and E. Gregori. Performance measurements of motes sensor networks. In *Proc. 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 174–181, Venice, Italy, October 4–6, 2004.

APPENDICES

Appendix A: A LISTING OF WRITTEN PAPERS

Five papers were created as result of this work. These are:

1. HEAPINGS

   - HEAPINGS: A Secure Counterintuitive Sensor Network Protocol
   - HEAPINGS: From Concept to Simulations

2. Accepted by never published by the conference:

   - HERBSUDAI: A Counterintuitive Resource Tracking Protocol

3. Paper submitted, but not accepted:

   - HAP and HAPDA: Two Geolocation Approaches

4. Journal submission:

   - Teaching Radio Propagation and Friis Equation by Using Real World Measurements

Appendix B: COMMERCIAL AND INFORMAL INFORMATION

.1 Introduction

This will explore what has been done in the past. Some things are still being done today. There are some peeks into the future. Much of this information has come from non-peer reviewed sources. Firefighters are used as a typical example of a first respondor. What applies to them, could be applied to other emergency service activities. Reconnaissance is another way of saying sensors.

.2 What has been done without radios?

.2.1 Firefighters without radios

Fire departments have used a tag system. A firefighter would give to the senior person on the scene a tag that had some information written on it. This would show that certain individuals were on the scene and in the fire, but did not show their exact location.

Later when air packs became standard firefighting equipment, alarms were added. These would sound when the person is not moving. The assumption is that a firefighter would always be moving and doing something. If the person is motionless, then the conclusion is that the person is in trouble.

One example is the Scott Health Safety Company's Pak-Alert SE distress alarm, which consists of a flashing red light emitting diodes (better known as "LEDs") and twin audible sounders [88]. See Figure 1 (courtsey of Mine Safety Appliances Company). Another example is the Mine Safety Appliances Company's offering. The product comes in two models: the ICM 2000 and the ICM 2000 Plus. Both models use two high-pitched tones followed by a buzz and a flashing red light [89]. See Figure 2 (courtsey of Mine Safety Appliances Company).

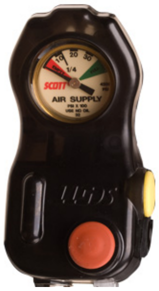


Figure 1: Scott Health and Safety's Pak-Alert SE

These products and others on the market go by various names such as "chirpers" or Personal Alert Safety System or PASS. The problem is that none of these are designed to transmit the exact location of a down firefighter.

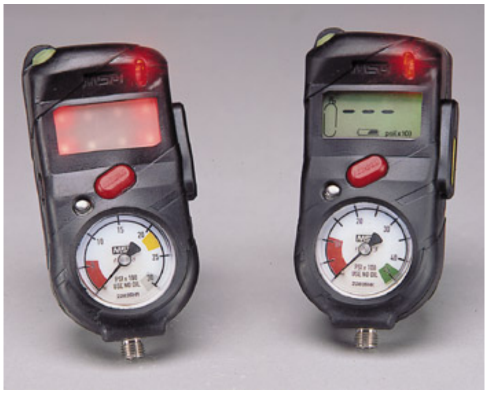


Figure 2: MSA's ICM 2000 and ICM 2000 Plus

.2.2 Reconnaissance without radios

When a nation needed information about the activities of the other side, spies were used. These might work inside a foreign government building. Or they might crawl on their stomachs to peer over the hilltop in order to see what the foreign military is doing.

Both activities are risky. Some individuals have been captured or killed.

.3 What has been done with radios?

.3.1 Firefighters with radios

Using simplex radios is an improvement over Personal Alert Safety System since two-way communications is possible. However, handheld units have limited power and limited range [90].

Using a duplex system or a repeater system overcame the limited power and the limited range problems [90]. Of course, the burning building needs to be in the coverage area of a nearby firefighter repeater. Communications-Applied Technology's (CAT) solution is to install a portable repeater (for example, the Intrinsically Safe Wireless Intercom System) on a large fire truck [91]. However, no position information is transmitted. Figure 3 (courtsey to Communications-Applied Technology) shows the company's Aircraft Wireless Intercom System repeater.

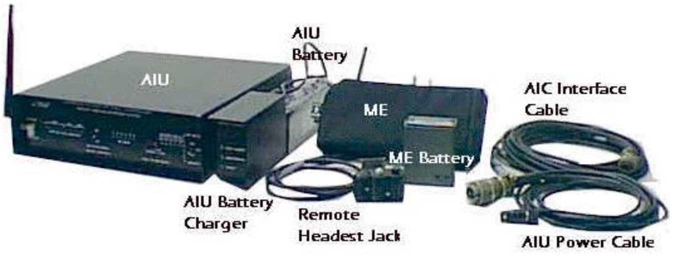


Figure 3: CAT's Aircraft Wireless Intercom System Repeater

.3.2 Reconnaissance with radios

When a nation needed information about the activities of the other side, technicians were used. They would plant electronic listening devices ("bugs") inside a foreign government building. Or agents might crawl on their stomachs to peer over the hilltop in order to see what the foreign military is doing and report back via radio.

Electronic devices and radio communications has improved the level of safety, but there is still some risk and some individuals have been captured or killed.

There is another part of electronic reconnaissance that does not involve planting listening devices. These are called sensors. This has become a major area of interest. This will be covered in greater detail at the end of this appendix.

.4 What has been done with the Global Positioning System?

The Global Positioning System (GPS) has been considered a simple solution for determining a location. There are various devices on the market that will provide location information. Some models will provide elevation too.

This ability has been combined with various communications systems. Some cellular telephone companies supply special services that use GPS.

Kenwood combined a radio with an automatic vehicle location (AVL) device, a GPS module, and a messaging system to create a fleet management product. FleetSync^{TM} is a proprietary product offering that can enhance the dispatching of vehicles [92]. The Kenwood website does not elaborate about the details of the position reporting feature.

Another example is the Sierra Wireless' MP 880 GPS or MP GP 881 (the MP 775 GPS is an older version) [93]. These products provide a ruggedized modem for data communications. If the network supports voice, then voice communication is available. The supporting functions are placed inside a black box and this is mounted elsewhere in the vehicle such as in the trunk. The user and the home station can read the GPS location information. The system operates in the sub bands between 869 MHz and 1990 MHz. See Figure 4 (courtsey of Sierra Wireless).

These systems and others that use GPS suffer from one serious weakness: If the devices' antennas cannot see four GPS satellites, then time and position information will not be available. Even with access to four GPS satellites, the accuracy is 100 meters horizontally and 156 meters vertically [94]. In layman's terms, that means a person or an object could be anywhere within a 50-meter (164-foot) radius of a spot and could be anywhere up or down 78 meters (256 feet). That is still a large search area.

Oak Ridge National Laboratory and the US Army are working to develop the next generation of devices whereby tracking is better and GPS information is used when available [95]. It goes by the name of Next-Generation Time, Space, and Position Information System (TSPI). It is still too early to know how this will be done and what will be the results.

In December 2004, President George W. Bush issued a Presidential Decision Directive that mentioned the need to develop "terrestrial augmentations" for position reporting [96].

Even before President Bush's directive, the Rosum Corporation was formed in 2000 in order to address the short comings of GPS. Their solution uses television signals for determining positions inside a building or beyond the view of GPS satellites [97]. The approach is that a Rosum device detects as many signals as possible (analog television signals, digital television signals, and/or satellite signals) and measures the time of arrivals. This data is sent to a Rosum location server. The location server calculates the device's location in two dimensions and passes this information back

Figure 4: Sierra Wireless MP 880W GPS and MP 881W GPS Black Box

to the device for display plus to any tracking application [97]. This can meet most of the time the FCC's E911 position requirements.

However, as wonderful as this technology may be, there are at least seven major drawbacks. First, high power (1,000 kilowatts or more) television stations tend to be located within 50 miles (80 kilometers) of major population centers and solid coverage goes out to about 200 miles. That is, if a person is in an area that has no television towers and no clear view of three GPs satellites, then the Rosum system will not work. Second, each television signal needs to have a synchronization code transmission. Third, there needs to be at least three television signals. In some markets, that may not be the case. Fourth, monitor units must be deployed at fixed locations to analyze the stability and timing of nearby television signals and provide the information to the location server. Fifth, communication links must exist between the monitor units and the location server. Sixth, the user must have a Rosum chip on their arm or embedded in a radio. Seventh, information is expressed in terms of two dimensions. To obtain a 3D position requires the deployment of "pseudo TV transmitters (PTTs)"around the target of interest [97].

With the Rosum's TV-GPS Plus system, the incident commander can pinpoint a firefighter's location to the "level of a room in the building." This is very good, but the website grosses over a few things. First, someone must deploy the PTTs and that takes time. Second, Knowing where to place the PTT is not address on the Rosum website. The previous illustration shows that three PTT units are used, but in another example of an amusement park four PTT units are used. If the spacing must be equal distance, then what happens if the distances are not equal? Third, the PTT units broadcast on unused TV channels and this means that Rosum or the user must obtain a radio license from the FCC [97]. If a new television station enters the market, then the PTT frequencies might need to be changed and the new frequency cannot legally be used until a new FCC radio license is obtained. Not mentioned on the Rosum's website is the fact that the United States over the next few years is realigning the television broadcast band. That means the PTT units might not be legal to use after the "sunset" of the old broadcast bands. Finally, the FCC license a television station to an area and if the PTT are licensed in a similar fashion, then would mean the PTT units cannot be used outside of the home area of the fire unit.

Skyhook Wireless uses the large number of Wi-Fi access points as a positioning system [98]. It works best in a dense urban area, but it is only accurate within 20 meters. The company's website is thin on details. In a general magazine, the reported noted that the system can determine a position within 30 meters, plus or minus 10 meters for 25 of the most populated United States cities [99].

.4.1 Firefighters with Global Positioning Systems

GPS devices are being combined with other systems in order to create products for firefighters. For example, the Aurora Colorado Fire Department uses General Packet Radio Service (GPRS) with a GPS wireless modem and Motorola's Advanced Vehicle Locating software in order to provide firefighting crews with changing maps that will guide them to the site and details about the burning structure [100].

At least one fire department is using the previously mentioned Kenwood product. The Kenwood website quotes an unidentified fire department spokesperson. The person discussed how this system has improved communications. But there was no mention of the GPS positioning features [90].

Again firefighters go inside buildings and that takes them out of view of any GPS satellites. Hence, any GPS enabled devices would be useless.

.4.2 Reconnaissance with Global Positioning Systems

In the battlefield environment, the military has used pilotless devices to view the terrain. Some of these use GPS as part of the navigation systems.

.5 What has been done with the Radio Frequency Identification?

Radio Frequency Identification (RFID) uses radio frequencies and a passive device or tag. A transmitter sends out a signal that envelopes the tag and generates a field. The embedded microchip circuits are energized and a return message is sent. This message may contain information such as serial numbers, ownership, and shipping container data. Normally, the tag information does not change. The RFID tags will only react to a certain frequency from one of the RFID radio bands (125 kHz, 13.56 MHz, 850-900 MHz, or 2.45 GHz). The RFID bands have certain behaviors. Low frequencies are better at penetrating non-metallic materials and are cheaper to manufacture, but have low data transfer rates. Whereas UHF frequencies are better for distance and faster data transfers, but have poor abilities for penetrating materials and must have a line-of-sight view. Another drawback is the overall distance. At best, passive RFID tags have about a 20-foot range. If a battery powered RFID model is used, then the range is increased anywhere from 100 to 300 feet [101].

This technology has been around since the 1970s [101]. It is only recently that the cost-benefit equation has improved to the point that Target, Wal-Mart, the United States Department of Defense, and others are requiring vendors to use RFID on shipments to their warehouses [102] [103]. The tags are manufactured in different shapes such as buttons, "lip stick" shapes, credit card size, key rings, and so on. See Figure 5 (courtesy of Texas Instruments) for an example of a button shaped RFID tag.

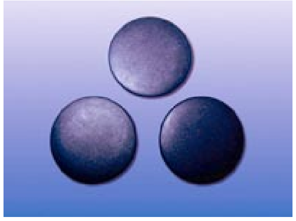


Figure 5: RFID Tag (Texas Instruments 13.56 MHz encapsulated Transponder)

However, these are not without problems. IBM Global Services discovered that RFID tags are not free from radio frequency interference (RFI). Forklifts, bug zappers, cellular telephone towers, walkie-talkies, and other handheld devices can create RFI [104]. In a recent real world test, the DoD discovered that RFID readers are able to read a pallet tag almost 100% of the time, but attempting to read stacked cases dropped the success level to 80% [105].

.5.1 Firefighters with the Radio Frequency Identification

Having a firefighter wear a RFID tag is not a workable solution. The read-only tag information does not change. In order to pass the information, there must be a transmitter nearby and on the correct frequency. Some buildings were constructed with metallic materials and in such an environment the building would function as a screen room–that is, signals cannot enter or leave. Other buildings have thick walls. Even with a battery powered RFID tag, the best distant is about 300 feet. That distance would be exceeded when the structure has several floors and has a large base. Another drawback is the storage size; it is about 2 kilobytes (kB). Tags can be read-write or read-only. Read-write tags can only be updated when a radio signal is received. A firefighter would not have a simple way of providing revised data while fighting a fire.

.5.2 Reconnaissance with the Radio Frequency Identification

RFID tags would not work for CAP since the aircraft fly patterns where the distances are greater than 300 feet.

RFID tags would not work in a sensor environment since data requirements are greater than 2 kB. Also the base station must be able to reach all of the RFID tags with a strong signal. That increases the chance of being detected by the other side. The flip side problem is that the RFID tags might not be able to generate a strong enough signal to reach the base station receive antenna. Also the nature of RFID tends to eliminate the option of relaying messages.

.6 What has been done with Local Positioning Systems?

Placing sensors around an area such as a prison or a controlled area is possible. These are called “Local Positioning Systems” (LPS) and these are independent of GPS[106]. Individuals wear a tag and the system can track their movements. See Figure 6 (courtsey to Sidney Fels, Changsong Shen, Baosheng Wang, and Steve Oldridge) for an example of the system that the Department of Electrical and Computer Engineering at the University of British Columbia is developing. This is fine for a regular environment, but there are some limitations.

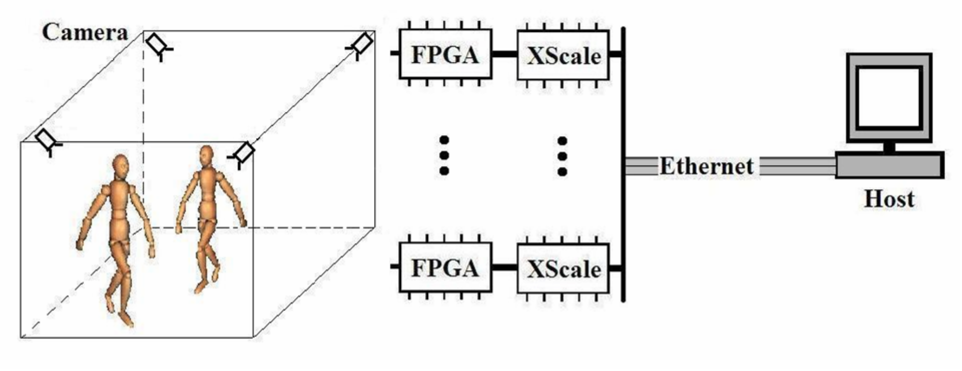


Figure 6: A Local Positioning System

One problem is that there are no standards. The result is that one company's tags may not be recognized by another company's system. Having a unique product tends to encourage repeat purchases and keeps a purchaser from trying to find a suitable replacement from another company. But it works against having the ability to have a person tracked from one environment to another environment. This market has not reached the point where the customers want to have a common standard.

Another form of LPS is a large geographical area that uses radio direction finding and tags. The SWS Security's TRACKnet Networked Radio Finder System is such an example [107]. This system requires a large infrastructure: computers, special software, a local GPS receiver, dedicated data lines between all the stations, and a local map. The "target" carries a simple beacon transmitter. This system takes the bearings from the stations to the target and plots these on a map. The intersection of the lines determines the location of the target. The information is in two dimensions. Even if a city was completely covered, the system would only be able to narrow the location down to a city block.

NexGen City (2002 start-up) attempted the same coverage by using an ad hoc networking approach. All the active laptops and various devices that are mounted on sides of buildings and on street lights are used to achieve city-wide coverage [100]. Each unit functions as a router and as a repeater. So far it appears that the only deployed, real world system is in Garland Texas.[1]

.6.1 Firefighters with Local Positioning Systems

The problem of no common standard means that a firefighter with a single LPS tag would not be tracked from one system to another system. If a firefighter wanted to be tracked, then that would mean carrying tags for each known LPS in the fire district.

There are three problems with the LPS approach.

The first problem is that a firefighter would have to take time to select the correct tag. And time is not the firefighter's friend. If the fire was huge and several buildings with difference systems were burning, then tracking would end upon entry into the other system's coverage.

The other problem is that firefighters carry many pounds (kilograms) of equipment with the result that overexertion has caused a number of deaths. Firefighters have a good reason for not

[1] In an effort to confirm information and obtain permissions to use images, it appears this company had some problems such as law suits and unhappy public. The website does not exist anymore.

wanting to carry another device. In the United States Fire Administration's report, *Firefighter Fatality Retrospective Study*, it was found that the leading cause of death on the job is heart attack at 44 percent with trauma a distanced second at 27 percent[108]. Firefighters may not be willing to add another bit of weight even if it is a few ounces (grams), because of the increased stress of carrying the extra weight.

Still another problem is that LPS requires external power and during a fire that may not be present. The fire may interrupt the power flow or the power company may turn it off.

Darrell McClanahan, Garland telecommunications manager, wants to be able to collect a firefighter's life signs via NexGen City system. But this is not likely to happen. The company admits that their equipment has a location error of plus or minus 10 meters. The firefighters would have to wear something that would collect the life signs data and transmit it to a nearby laptop computer. This will run headlong into the problem that firefighters are not near a laptop computer while fighting a fire. So the extra weight would be unwelcomed.

.6.2 Reconnaissance with Local Positioning Systems

It is unlikely that AFAUX/CAP aircraft or AFAUX/CAP ground teams or agents would be operating inside a "wired" environment.

.7 What has been done with Locator Transmitters and Beacons?

For years, aircraft have carried emergency locator transmitters (ELT) that operated on 121.5 MHz and on 243 MHz. See Figure 7 (courtesy of Artex Aircraft Supplies) for an example of a small ELT. When an ELT is transmitting, certain satellites will receive the signal and relay to the nearest rescue coordination center. In the United States, this is the Air Force Rescue Coordination Center on Langley Air Force Base, Virginia. The center calls HQ AFAUX/CAP National Operations Center (NOC) and in turn the NOC dispatches teams to the general search area. The teams use trackers that work when within line-of-sight distances (roughly 50 miles (80 kilometers) or less) of the target.

On 1 July 2003, the Personal Locator Beacon (PLB) System became operational [109]. A person would purchase a PLB and would register with the National Oceanic and Atmospheric Administration (NOAA) [110]. When the PLB is turned on, participating satellites[2] hear the signal and relay it to the nearest rescue coordination center. See Figure 8 (courtesy U.S. National Oceanic and Atmospheric Administration (NOAA)).

.7.1 Firefighters with Locator Transmitters and Beacons

Could this technology have helped to locate down firefighters in the rubble of 9-11? It is true that after the grounding of all aircraft in the United States, the first aircraft permitted back into the air were AFAUX/CAP aircraft[3]. Even if all the firefighters had ELTs, AFAUX/CAP still could not fix a precise position on down firefighters, because ELTs transmit a simple signal and do not provide location information.

PLBs have saved many outdoorsmen, but they cannot help firefighters. At best, the standard 406 MHz PLB can locate a person within a two-mile (3-kilometer) radius and the top-of-line PLBs

[2] Some satellites carry receivers for both the ELT and PLB. As the ELT receivers fail, there is no plan to repair or replace them. The day will come when all ELT tracking will be done by ground based stations and any chance air borne platforms.

[3] This is the source of the first images of the World Trade Center site.

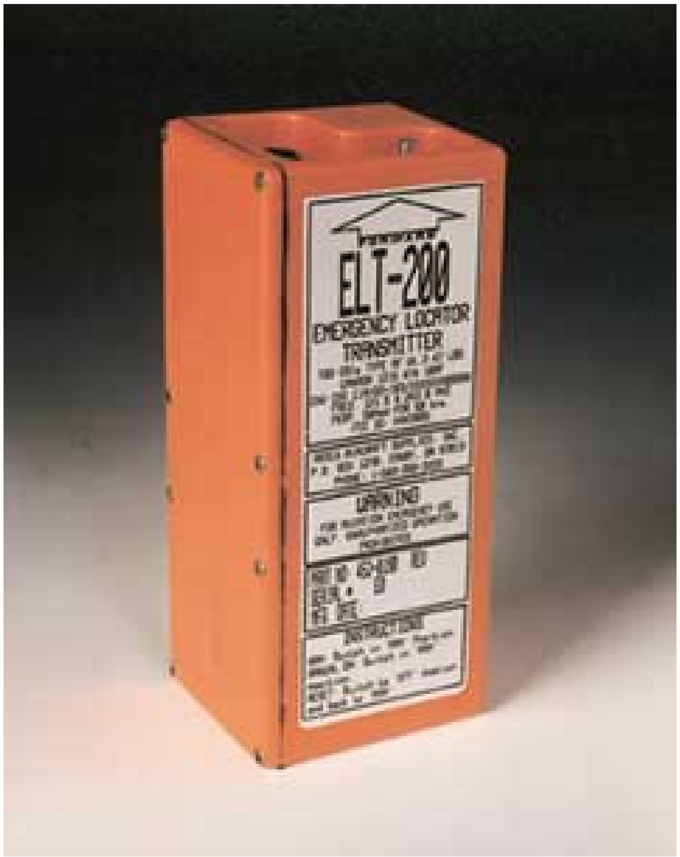


Figure 7: Artex ELT 200 operates on 121.5 and 243 MHz

have GPS receivers that can reduce the search radius to less than 400 feet (122 meters) [111]. Of course, if the satellites cannot hear the signal, then this enhancement is useless.

.7.2 Reconnaissance with Locator Transmitters and Beacons

It is unlikely that agents would be using these devices for collecting information. They wish to avoid detection. The purpose of ELTs and PLBs is the opposite.

.8 What has been done with Radar?

How are aircraft tracked? Air traffic controllers use radar with an identification friend or foe (better known as IFF or IFF/SIF) module. The radar locates the aircraft and the IFF transmits a query. The aircraft's IFF unit replies with a small data message. The sector air traffic controller will see displayed on the monitor the aircraft as a blip and a floating box. See Figure 9 (courtsey to NASA). Air traffic controllers follow the movement of the blip in order to follow the progress of the aircraft. A dialogue transpire between the air traffic controller and the pilot. Instructions are passed and the pilot reports passing certain landmarks or navigational aid system (NAVAIDS).

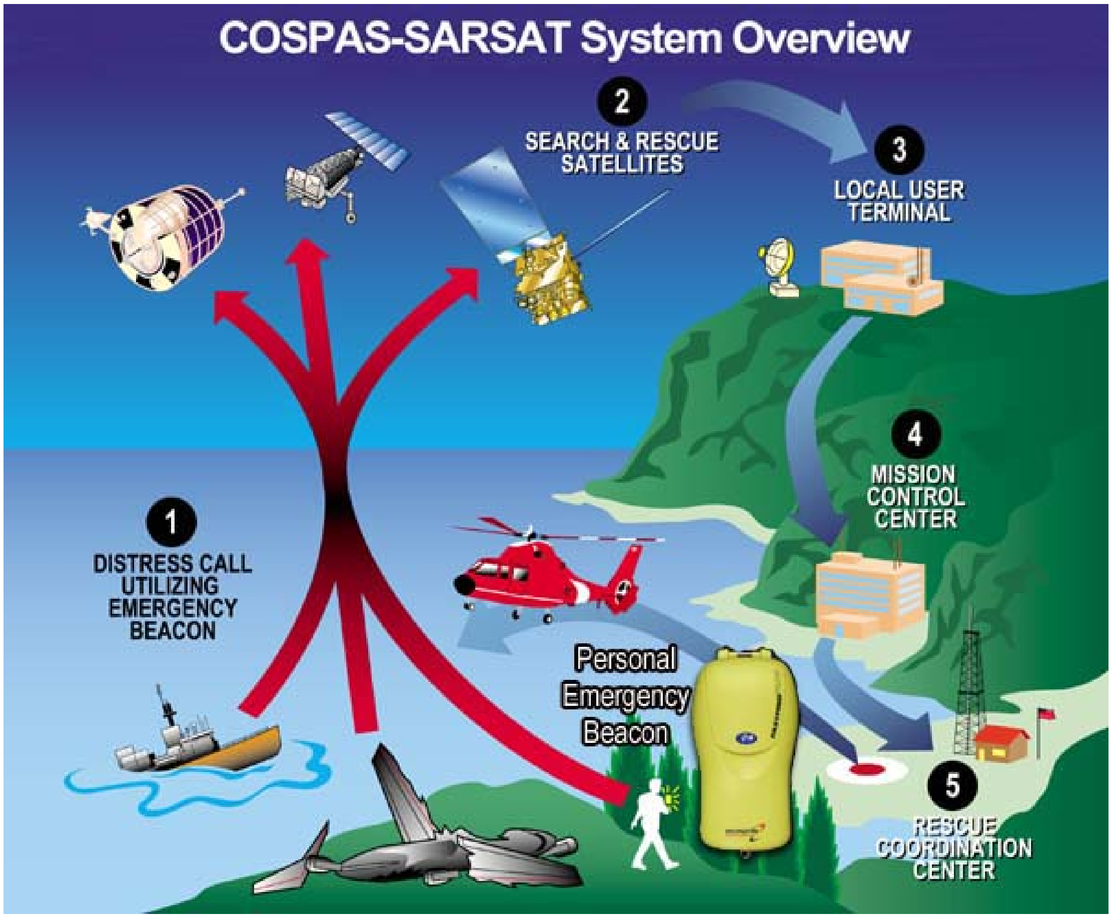

COSPAS-SARSAT System Overview
2
SEARCH & RESCUE SATELLITES
3
LOCAL USER TERMINAL
4
MISSION CONTROL CENTER
1
DISTRESS CALL UTILIZING EMERGENCY BEACON
Personal Emergency Beacon
5
RESCUE COORDINATION CENTER

Figure 8: COSPAS-SARSAT System Overview

In addition to the foregoing, a pilot uses NAVAIDS such as a VHF Omnidirectional Range (better known as a VOR) navigation system, Tactical Air Navigation System (better known as TACANS), and navigation beacons in order to stay on course. If a pilot is disoriented and if the air traffic controller cannot see the aircraft on the radar monitor, then the pilot can contact a nearby Automated Flight Service Station (AFSS) Radio and request Orientation Service. The Flight Service Controller would collect key pieces of information and uses the station's direction finding (DF) equipment to determine the bearing of the aircraft from the DF site. A secondary means is to use several devices (another DF site, a VOR, Automatic Direction Finder (better known as ADF) to triangulate the aircraft's position and provide a new heading to the pilot. This is not a priority service and may be not be available if the AFSS workload is too heavy [112].

.8.1 Firefighters with Radar

Radar requires large targets in order to obtain a position. Firefighters are smaller than an aircraft and would tend to be inside a burning structure.

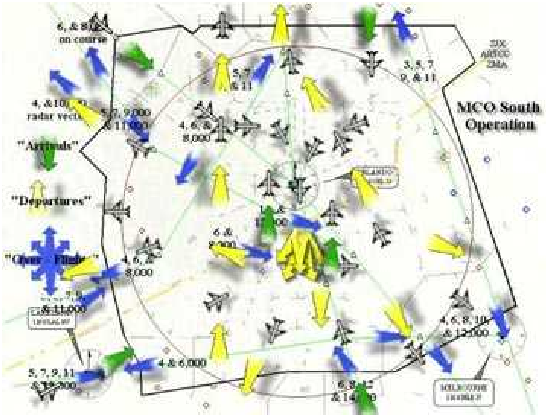


Figure 9: View of numerous aircraft on a radar scope.

.8.2 Reconnaissance with Radar

It is unlikely that agents would be using these devices for collecting information. Radars use high power transmitters and large receiving antennas.

.9 What has been done with Enhanced 911 Service?

What about the new Federal Communications Commission (FCC) requirement that cellular telephone providers must provide location information with 911 calls[4]? The Phase I requirement is to locate callers by cellular radio towers and Phase II requirement is to locate the caller within a 50-meter (164 feet) radius in the best case [113].

.9.1 Firefighters with Enhanced 911 Service

The location information is not precise enough and firefighters would not have time to use a cellular phone to report their position. There is another drawback. Cellular phone service may not be available. Land lines to the towers could be broken. All the circuits could be busy. Or as have happen during nature disasters, the cellular phone system could be off line. Finally, cellular phone service is non-existent or spotty in rural areas. If the fire was near the boundary of two or more telephone area codes and if a cellular telephone tower from a different area code was the closest, then any dialed telephone number would need to have the area code included.

.9.2 Reconnaissance with Enhanced 911 Service

It is unlikely that agents would be using cellular telephones for collecting information.

[4] Network-based technologies must be able to locate a cell phone unit within 100 meters 67% of the time and within 300 meters 95% of the time. Handset-based technologies must be able to locate a cell phone unit within 50 meters 67% of the time and within 150 meters 95% of the time.

.10 What has been done to support the uniformed services?

Rescue 21 (R21) is the United States Coast Guard's (USCG) program for upgrading its approach to saving lives. One of R21 core features is the ability to track platforms (ships and aircraft). In order to do this, it uses fixed sites and each platform carries a Rescue 21 transmitting package [114]. Figure 10 (courtsey to the United States Coast Guard) is the logo for this program[5]

Figure 10: US Coast Guard Rescue 21 Advanced Communications System (Logo)

The United States military has had an abiding interest in direction finding for years. It could be used to locate an offending enemy station. It could be used to help an aircraft to determine its location over the ocean. And of course, the great interest in finding and recovering downed pilots.

The military has various nets and systems that are devoted to communications, computing, and control. One example is the Command and Control Constellation, which is built on the ConstellationNet network. This consists of sensors, platforms, and command centers [115]. This supports the Air Force requirements for command and control, intelligence, surveillance, and reconnaissance. It is not intended to support civilian needs and it is designed for working with aircraft, not with individuals on the ground or in a building.

.10.1 Firefighters with support from uniformed services systems

USCG firefighting and rescues tend to be on watercraft and a number of these have small "real estate." Location information is not as big as a concern as it is for land based firefighters. Hence, the issues and the approaches are different from land based fires.

.10.2 Reconnaissance with support from uniformed services systems

It is unlikely that agents could use the USCG systems or the military nets for collecting information. Again, these systems are intended to work with aircraft, not with individuals on the ground or in a building.

[5] This was capture early in this research. When I contacted the USGS for permission, they could not find this image anymore. They have a blanket policy of granting permission for all images as long as credit is given.

.11 What has been done with the Sensors?

Sensors are popular, because these can be deployed without putting a person in danger. However, as wonderful and as successful current battlefield sensors are, there are still some problems. Edward T. Blair, the United States Army's program executive officer for intelligence, electronic warfare and sensors (PEO IEW&S) (Fort Monmouth, NJ)[116] stated that one major weakness is that the sensors cannot track much more than 10 targets at the same time. Taking a big picture view, Gen John P. Jumper, the Air Force Chief of Staff, pointed out that every military activity wants it own UAV system with the resulting problems in safety and radio frequency conflicts[117]. That is, sensors need to have a collision-free channel.

Some undergraduate students in a University of California San Diego course (ECE 156 Sensor Networks taught by Clayton Okino of the Jet Propulsion Laboratory) determined that sensor density is another problem area[118]. Chee-Yee Chong and Srikanta P. Kumar noted some more problems such as network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security[66].

Here is a list of these and other problem areas:

- Sensors cannot track a large number of targets at the same time.
- Energy shortfall.
- Availability of air platforms such as the OAVs and UAVs.
- UAVs loiter time over an area is limited.
- Returning data to home station is a problem. (UAVs are used sometimes.)
- UAVs cannot carry heavy sensors.
- Frequency coordination is not being done.
- UAVs can be detected by the other side.
- Sensor density is a problem.
- Network discovery.
- Control and routing.
- Collaborative signal and information processing.
- Tasking and querying.
- Security.

If the Crossbow's MICA product is a typical sensor device, then many MICA sensor nodes are designed to operate on 916 MHz[119]. That will result in congestion on this frequency and poor distance coverage.

Berkeley Motes are even smaller than Crossbow's MICA product and these Motes operate in the same radio band. For example, the 5-millimeter square "smart dust" chip (see Figure 11 (courtsey of Jason Hill and David E. Culler at University of California, Berkeley)) operates on 902 MHz[120]. Anastais et al. examined the MICA2 and the MICA2DOT Berkeley Motes and noticed that rain and fog will degrade the signal[121]. For Anastais et al., the factors that impact transmission range are transmitter power, receiver sensitivity, the antenna gain, and data transmission rate. They did not consider that the actual frequency used has the greatest impact. It is a known fact among radio engineers that weather has a great impact on short wave length (that is, microwave) emissions.

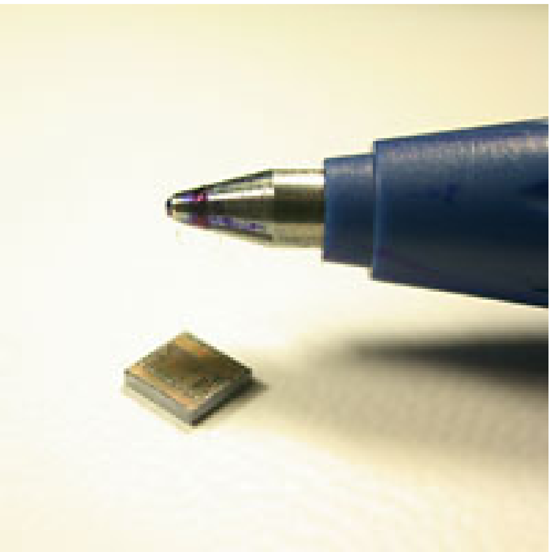


Figure 11: “Smart Dust” Chip