Defence Research and Development Canada | Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

A Mobile Ad Hoc Networking Test Bed

Cem Sen, Mazda Salmanian and Matthew Kellett

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2005-158
August 2005

A Mobile Ad Hoc Networking Test Bed

Cem Sen
Turkish Army

Mazda Salmanian
Matthew Kellett
Defence R&D Canada – Ottawa

Defence R&D Canada – Ottawa

Technical Memorandum
DRDC Ottawa TM 2005 -158
August 2005

Abstract

Wireless computer networks are becoming increasingly important to the military and the use of inexpensive, light hardware based on the IEEE 802.11 wireless networking standards has given these networks unprecedented mobility. The advent of self-organizing, peer-to-peer mobile ad hoc networks (MANETs) based on these devices challenges traditional network conceptions of routing and security. Research into these and other aspects of MANETs requires extensive field testing or specialized test facilities. In this technical memorandum, we give an overview of the special properties of MANETs and how routing protocols such as Optimized Link State Routing (OLSR) allow them to function. We discuss the limitations of the Windows platform for use in our research. Finally, we detail the set up of MANET test bed in Linux using tools from the United States' Naval Research Laboratory (NRL). The tools allow for the emulation of MANETs, including simulating the effects of node movement and terrain on the network. The test bed will allow us to do our initial research in a lab environment and to demonstrate our results in a graphical, non-technical manner.

Résumé

Les réseaux informatiques sans fil prennent de plus en plus d'importance pour les militaires et le recours au matériel léger et peu coûteux basé sur les normes de réseaux sans fil IEEE 802.11 assure à ces réseaux une mobilité jamais encore atteinte. La mise en place de réseaux mobiles ad hoc d'égal à égal auto-organisateurs (MANET) basés sur ces appareils vient remettre en question les conceptions traditionnelles touchant le routage et la sécurité des réseaux. Les travaux de recherche sur ces aspects des MANET nécessitent de nombreux essais sur le terrain ou l'utilisation d'installations de test spécialisées. Dans ce document technique, nous présentons un aperçu des propriétés particulières des MANET et expliquons comment les protocoles de routage comme Optimized Link State Routing (OLSR) leur permettent de fonctionner. Nous traitons également des limitations de la plate-forme Windows pour nos travaux de recherche. Enfin, nous détaillons l'installation du banc d'essai MANET sous Linux au moyen d'outils du Naval Research Laboratory (NRL) des États-Unis. Ces outils permettent d'émuler les MANET, et comprennent la simulation des effets du terrain et des déplacements des noeuds sur le réseau. Ce banc d'essai nous permet d'effectuer les travaux initiaux de recherche dans un environnement de laboratoire et de présenter nos résultats de façon graphique et non technique.

This page intentionally left blank.

Executive summary

Mobile ad hoc networks (MANETs) are self organizing, peer-to-peer wireless networks that break the traditional paradigms associated with computer networks. Due to their nature, MANETs pose new problems in routing and security. The use of hardware based on the IEEE 802.11 wireless networking standards has made the use of MANETs by the military possible and attractive.

In this document, we look into the properties of mobile ad hoc networks and how they differ from traditional wired and infrastructure-based wireless networks. We discuss how MANET routing works by looking at the Optimized Link State Routing (OLSR) protocol. The limitations of using the Windows platform for research are shown to be, for example, lack of access to the source code of the operating system for tapping into the modules that control the routing algorithm. Finally, the detailed set up of a MANET test bed is provided. The test bed is a series of Linux tools from the United States' Naval Research Laboratory that provide the capability to emulate a MANET. The tools are used to simulate the motion of nodes and the effects of range and terrain on connectivity. They also allow for the display of network topology in a graphical, non-technical manner. The emulation and display features are made possible through a central computer that is wired to the MANET for collection and processing of routing information and signal strength. The central computer is also a wireless node in the MANET. This wired backbone relieves the wireless channels of the MANET from traffic that is used for displaying the situational awareness. This test bed gives us the capability of doing our initial research on the security of mobile ad hoc networks in a lab environment before moving to field testing.

Sen, C., Salmanian, M., Kellett M. 2005. A Mobile Ad Hoc Networking Test Bed.
DRDC Ottawa TM 2005-158. Defence R&D Canada – Ottawa.

Sommaire

Les réseaux mobiles ad hoc (MANET) sont des réseaux informatiques sans fil d'égal à égal auto-organisateurs qui rompent avec les modèles traditionnels de réseaux informatiques. De par leur nature, les MANET posent de nouveaux problèmes sur le plan du routage et de la sécurité. Le recours au matériel basé sur les normes de réseaux sans fil IEEE 802.11 rend l'usage des MANET par les militaires à la fois possible et intéressant.

Dans le présent document, nous nous penchons sur les propriétés des réseaux mobiles ad hoc et sur les caractéristiques qui les distinguent des réseaux câblés traditionnels et des réseaux sans fil basés sur une infrastructure. Nous examinons le fonctionnement du routage par MANET en étudiant le protocole Optimized Link State Routing (OLSR). Nous traitons également des limitations de la plate-forme Windows pour nos travaux de recherche qui ont demontré en autre le manque d'accèssibilité au code source du systeme d'operation afin de pouvoir avoir accès aux modules qui controlent l'algorithme de routage. Enfin, nous détaillons la configuration du banc d'essai pour MANET. Ce banc d'essai est constitué d'un jeu d'outils Linux du Naval Research Laboratory (NRL) des États-Unis qui permettent d'émuler les MANET. Ils servent à simuler le déplacement des nœuds ainsi que l'effet des distances et de la configuration du terrain sur la connectivité. Ils permettent également d'afficher la topologie du réseau de façon graphique et non technique. Les dispositifs d'émulation et d'affichage sont rendus possibles par un ordinateur central qui est câblé au MANET pour la collection et le traitement de l'information de routage ainsi que de la puissance du signal. L'ordinateur central est également un noeud sans fil dans le MANET. Cette épine dorsale de câble soulage les canaux sans fil du MANET du trafic qui est employé pour montrer la conscience situationnelle en réseau. Ce banc d'éssai nous permet d'effectuer nos travaux initiaux de recherche sur la securité des réseaux mobiles ad hoc en laboratoire avant de passer aux essais sur le terrain

Sen, C., Salmanian, M., Kellett M. 2005. A Mobile Ad Hoc Networking Test Bed.
DRDC Ottawa TM 2005-158. R & D pour la défense Canada – Ottawa.

Table of contents

List of figures

Acknowledgements

We would like to thank Vahid Aftahi for his support in setting up the test bed. We would like to thank Dr. Peter Mason who was instrumental to start our interaction with CRC. We appreciate Dr. Louise Lamont (CRC) and her team for assisting with the test bed setup. We would also like to thank Donald Montreuil for translating the abstract and executive summary of this document.

This page intentionally left blank.

1. Introduction

Wireless networks are becoming an indispensable part of modern military operations. They allow the military to be mobile while remaining well connected. Historically, wireless voice and data networks have relied on heavy platforms that limited mobility or range. These networks were also time consuming to set up and take down. The advent of mobile ad hoc networks (MANETs) using inexpensive hardware based on the IEEE 802.11 standard has provided the convenience of wireless connectivity without the dependence on infrastructure-based platforms. MANETs provide peer-to-peer networking that allows information to be routed through other nodes in the network. The network's typology is dynamic and self-healing when users enter or leave the network.

MANETs challenge traditional conceptions of routing and security due to their self-organizing, peer-to-peer nature and require specialized test facilities to minimize the need for testing in the field. The Secure Mobile Networking group at Defence R&D Canada has set up a test bed to study the security of these networks. The test bed allows researchers not only to emulate and test new authentication and intrusion detection algorithms (to name just a few applications) but also to demonstrate the results of the research. MANET routing algorithms added to the test bed allow for multi-hop connectivity between the nodes on top of the simple mesh connectivity provided by most standard operating systems.

This document is an overview of the properties of mobile ad hoc networks (MANETs) and how those properties can be emulated in a test bed in order to research and demonstrate security. The document discusses how mobile ad hoc networks function and how MANET routing algorithms such as Optimized Link State Routing (OLSR) can be used to create multi-hop mobile networks. The limitations of using Windows as a platform for MANET research are discussed. The set up of the MANET test bed in Linux using tools from the United States' Naval Research Laboratory (NRL) is detailed. These tools allow for the realistic emulation of MANETs in a lab environment and the graphical display of these networks for demonstration purposes.

Following this introduction, an overview of mobile ad hoc networking and its applications are presented in Section 2. Section 3 details the setup of a MANET in a Windows 2000 environment with Optimized Link State Routing protocol (OLSR) followed by streaming wireless video testing. The details of setting up a mobile ad hoc test bed in Linux are presented in Section 4 and a summary and suggestions for future work are given in Section 5.

2. Ad Hoc Networking

Wireless local area networks (WLANs) in infrastructure mode require the use of one or more access points (APs). With this configuration, the AP provides a central interface to a network of nodes. As an optional feature, the 802.11 standards specify an "ad hoc" mode. It may be defined as a self-organizing wireless network in which mobile nodes are responsible for discovery of each other and subsequent cooperation to establish communication links [1]. Some product vendors are beginning to base their solutions on ad hoc mode. As an example, Motorola Mesh Networks offers a wireless broadband network system based on 802.11b/g ad hoc mode and a patented peer-to-peer routing technology [2]. This mode in the specification results in a wireless mesh topology where mobile devices provide the routing mechanisms in order to extend the range of the network. For example, a user on one side of a building can send a packet destined to another user on the far side of the facility, well beyond the point-to-point range of 802.11b/g radio, by having the signal hop from client device to client device until it gets to its destination. This can extend the range of the wireless LANs from hundreds of feet to kilometres, depending on the density of wireless users.

Ad hoc networking is a multi-layer problem. The physical layer must adapt to rapid changes in the wireless channel characteristics. The media access control (MAC) layer needs to minimize collisions, allow fair access, and reliably transport data over the shared wireless links in the presence of rapid network changes. The network layer needs to distribute the information by calculating efficient paths while mobile links dynamically change and bandwidth is at a premium. It also needs to integrate smoothly with traditional, non-ad hoc-aware networks and perform networking functions such as auto-configuration in this changing environment. The transport layer must be able to handle delay and packet loss statistics that are very different from those of wired networks. Finally, applications need to be designed to handle frequent disconnection and reconnection with their peers as well as variable delays and packet loss [3]. These multi-layer issues are well explained in a previous SMN study [4] from a security point of view.

2.1 Current and future applications

The applications of ad hoc networks can be categorized as follows:

1. Military Applications: Ad hoc networks are particularly suited to battlefield scenarios where soldiers or unattended vehicles (UxV) require mobile and instantaneous communication links operating in a hostile environment.

2. Commercial Applications: The current application of ad hoc networking is local (LAN) or personal area networking (PAN) depending on the radio range of the system. In a PAN, users’ devices - such as laptops, mobile phones, and Personal Digital Assistants (PDAs) - collaborate amongst each other to set up an ad hoc network and exchange data.

3. Emergency and Rescue Applications: Ad hoc networks could be deployed in emergency and rescue situations where the fixed infrastructure may have been destroyed due to a disaster.

4. Sensor Networks: Collection of environmental data is a typical application of such networks.

This report considers building a mobile ad hoc networking test bed for military tactical applications, such as the one described in [4].

2.2 Aspects of ad hoc networking

The features that constitute a network as ad hoc are the following: node discovery, routing, node identity, security, multicasting along with network management, and quality of service (QoS). A brief explanation is provided below to expand on them.

1. Node Discovery in Ad Hoc Networks: This feature is used to determine the addresses of directly reachable nodes, known as neighbors. Each node maintains neighborhood information, which effectively is a list of addresses of the nodes that are one hop away. The node that is one hop away can contact another node directly over the radio link. A generic method of neighbor discovery is through broadcasting “HELLO” packets on the radio links [5]. However, this mechanism depends on the routing protocol. Routing and discovery of neighboring nodes in ad hoc networks is considered a data-link layer task and the techniques are not yet specified in the standards (IEEE 802.11 or Bluetooth). Discovery of, and communication with, non-neighboring nodes in ad hoc networks are features of some routing protocols proposed to the Internet Engineering Task Force (IETF) [6].

2. Routing in Ad Hoc Networks: Communication between non-neighboring nodes in an ad hoc network requires the use of routing protocols so that multi-hop paths may be discovered and utilized. Ad hoc routing protocols have additional features as listed below:

a. Support for dynamic network topologies including the ability of path set up for nodes that move randomly and rapidly.

b. Support for bandwidth and channel constraints including path loss, interference, noise, and fading.

c. Support for power constraints including optimization for power conservation for calculation of paths and processing routing information. Since the nodes are mobile, operation is typically battery dependent and hence the available power is exhaustible.

d. Support for security including secure exchange of routing information with trusted neighbours. A wireless network is prone to security threats due to the ease of eavesdropping and spoofing, because an intruder does not require physical attachment to the network. Routing protocols must exchange information only with trusted nodes.

The challenge that these four constraints pose, coupled with the fundamental importance associated with routing protocols for communication between non-neighboring nodes, has resulted in a situation whereby routing is the single most active area of ad hoc networking research in academia [1].

3. Node Identity in Ad Hoc Networks: This aspect is concerned with the identification of any entity within the network, in a way that distinguishes it from all other entities. MAC and IP addresses have been the primary IDs for nodes but vulnerabilities associated with MAC addresses and challenges of IP address assignment to nodes outside of a subnet have made this aspect another area of research. A difficult constraint in military applications calls for radio silence and nodal anonymity in ad hoc networks for non-disclosure of a user identity.

4. Security in Ad Hoc Networks: This aspect encompasses a number of goals - authentication, data integrity, confidentiality, non-repudiation, and availability. Researching these areas is the primary focus of the Secure Mobile Networking Group in Defence R&D Canada. The test bed documented in this report is for testing and demonstrating the research results from this group.

5. Multicasting in Ad Hoc Networks: Multicasting may be defined as the transmission of data to a group of receivers identified by a single destination address and hence, is intended for group oriented messaging.

6. Network Management in Ad Hoc Networks: Network management can be divided into monitoring and control. Monitoring is the collection of information about the usage of network resources, while control is the policing aspect of network resource usage. There is also much ongoing research in these areas specific to ad hoc networks.

7. QoS in Ad Hoc Networks: QoS may be defined as a set of application requirements that need to be met by the network while transporting a stream of packets from source to destination. Real-time applications, such as audio and video conferencing, in particular, pose strict requirements in terms of bandwidth, delay, and bit error rate (BER) on the network.

In the test bed, the first three aspects were of most importance for establishing the connectivity of the network: discovery, routing, and identity. The final three aspects presented above are subjects for further research on the test bed as they relate to security, especially authentication and intrusion detection techniques.

2.3 Peer-to-peer (P2P) networking

A P2P network may be defined as an application layer overlay (network) in which all entities are equal and all contribute some of their resources, so that each entity (peer) is both a content requestor and a content provider [1]. This definition makes some participating nodes both a router and a server. The word “peer” means the nodes are equal. In essence, P2P means “an equal communicating with another equal”. The importance of the definition lies in the word “equal”, as it implies that no distinction theoretically exists between the entities that make up the network. Each peer is therefore analogous to both a client and a server, which we define as a node for the purposes of this document.

In this test bed, a Linux application displays P2P ad hoc networking on a central node for demonstration purposes. However prior to Linux, we examined the limitations of our mobile ad hoc networking in a Windows 2000 environment.

3. Setup in a Windows 2000 Enviroment

A basic ad hoc P2P network setup is shown in Figure 1, by using commercial wireless cards in a Windows 2000 environment. As new nodes join the network outside the range of the peer, it needs additional features for multi-hop capability. This section provides the details of the added features required for a mobile ad hoc test bed.

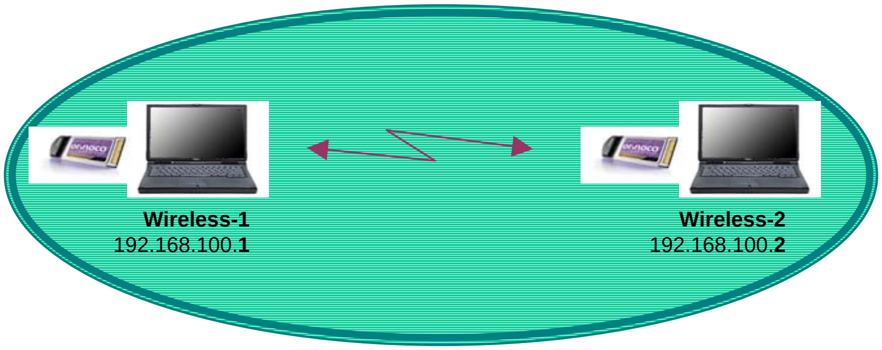


Figure 1: A basic P2P ad hoc network

To set up an ad hoc network with multi-hop connectivity as shown in Figure 2, one needs to install an ad hoc routing protocol on all three laptops. We used the Optimized Link State Routing (OLSR) protocol which can be downloaded from "http://www.olsr.org"- "Windows binary with installer (OLSR-0.4.7-setup. exe)". With an ad hoc routing protocol, the Wireless-3, for example, can route packets to Wireless-2 through Wireless-1 when it goes out of range of the Wireless-2.

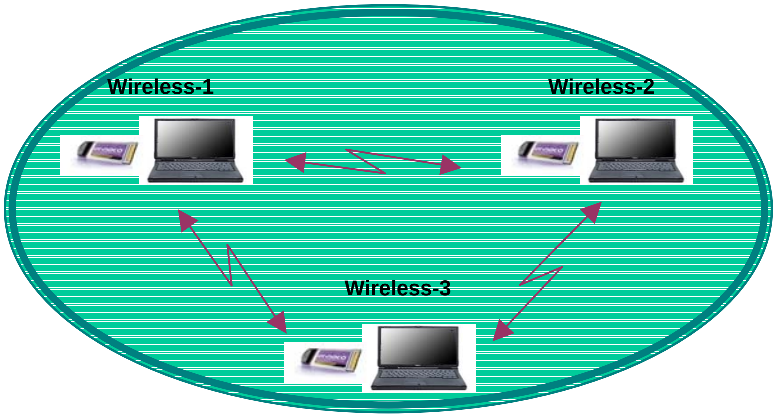


Figure 2: An ad hoc network with mesh connectivity

In a mesh network there are no fixed "points of failure". Ad hoc networks' self-healing properties appear when users join, leave, or move, making the network topology dynamic. Much of the ad hoc networking properties are attributed to the routing protocol. For this reason, a short explanation of OLSR is provided below.

3.1 Optimized Link State Routing (OLSR)

The Optimized Link State Routing protocol communicates with the immediate neighboring nodes of a peer in the network and adds them to a routing table it creates. These neighbors, also assumed to have OLSR, can be multipoint relays (MPRs) who perform a forwarding operation for the peer. An MPR forwards packets to either the next MPR or to the destination node. When an MPR is no longer a neighbor, it is either further away than one hop or out of the network entirely. Although it is not necessary for a peer to have more than one MPR, it can be useful to have more than one, especially when an MPR is out of reach. An entire network broadcast of a message is more efficient when a peer has more than one MPR.

Under this protocol, nodes use two processes to maintain the routing information: neighbor sensing and topology discovery. The neighbor sensing process consists of a peer using “HELLO” messages to indicate to its neighbors that it has arrived or when the node is turned on. The neighbors use this information to determine whether to be an MPR for the sender or not. The “HELLO” message includes and updates the state of each neighboring link on the table. In the topology discovery process, the peer broadcasts the link state to all its neighbors, who then forward it to all their MPRs. Therefore, the peer is capable of generating the current picture of the entire network topology [1]. A peer also maintains information about the neighbors that have selected it as an MPR. This set is called the Multipoint Relay Selector (MS) set of a node. A peer informs other nodes about its preference to be an MPR by stating a number in the range from 0 (never) to 7 (always) in its “HELLO” messages. A property of a well-connected (mesh) ad hoc network is that all nodes can reach each other through a series of available MPRs, and that no network partitioning is established. An MPR flooding method is used for distributing link state information - the status of the links in the network. The route from the source to the destination is calculated such that it is a sequence of hops through the MPRs. Nodes that are not in the MS set of a particular peer do not forward traffic through the peer.

3.2 Multi-hop communications

The OLSR protocol enables multi-hop communications in the test bed; a peer can communicate to a remote node via the forwarding capability of other nodes, as depicted in Figure 3.

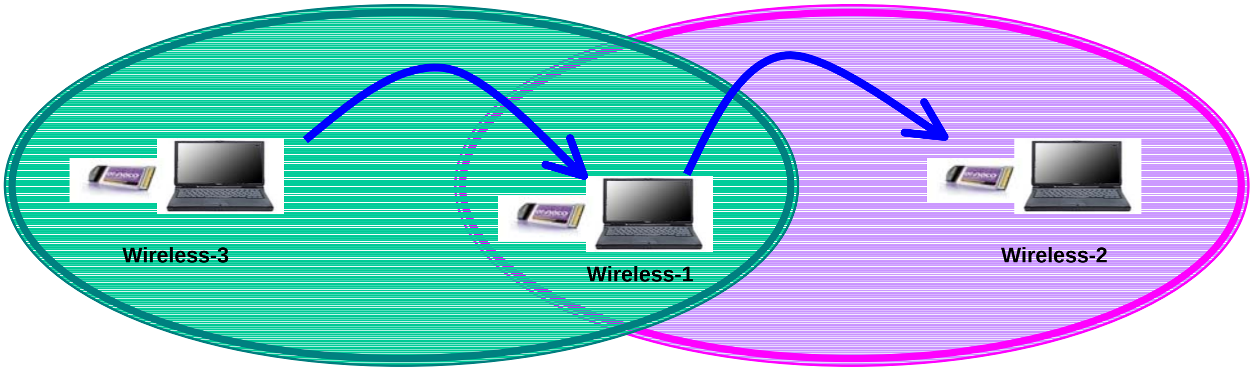


Figure 3: A multi hop ad hoc network

Each node in an ad hoc network, making use of OLSR, periodically broadcasts a “HELLO” message to its neighbors. A peer learns about its network reach (nodes that are one-hop or more away) from its immediate neighbors' "HELLO" messages. Within a "HELLO" packet, the sender lists the IP addresses of all the one-hop nodes with which it has a bidirectional link. In addition, it lists the IP addresses of the one-hop nodes from which it received a "HELLO" packet, but has not yet validated whether the link is bidirectional. The neighbors must return an acknowledgement (ACK) upon receiving of a "HELLO" packet. Unacknowledged packets are retransmitted "n" times. After "n" retransmissions, the neighbor is declared unreachable. As a result of this procedure a node, finding its own IP address within a received "HELLO" packet, may consider the link with the sender as bidirectional. With the reception of "HELLO" packets, a peer also learns of the nodes that are two or more hops away.

When Wireless-1 and Wireless-2 are within Wireless-3's communication range, as shown in Figure 2, the neighbor list of Wireless-3 is as follows[1]:

The Neighbor List of Wireless-3 (192.168.100.3) : ………..consists of Wireless-1 (192.168.100.1) and Wireless-2(192.168.100.2)

Neighbor list (18 : 42 : 17.625000) **:…………..………..Neighbor list (Hour : Minute : Seconds)**

192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]. **…………………………..……………… (Wireless-1)**

Link state

The list of 2-hop neighbors

Willingness to communicate / forward for 2-hop neighbors

Message interval

192.168.100.2: l = 1 : m = 0 : w = 6 [2hlist:]. **…………………………..…..……...… (Wireless-2)**

When Wireless-2 moves out of Wireless-3's communication range, as shown in Figure 3, Wireless-3 loses the direct link to Wireless-2, and it begins to use Wireless-1 as a relay to access and share files with Wireless-2. The ad hoc, multi-hop routing for connectivity comes at a cost.

Experimental results collected at Wireless-3 show that there is a significant delay between losing contact with Wireless-2 and re-establishing contact through Wireless-1. In the experiment the "HELLO" time interval was set to 2 seconds, and "HELLO" timeout was set to 6 seconds - default values. As shown below, after 2 "HELLO" timeouts (12 seconds) the link was set to pending; but it took an additional 3 timeouts (18 seconds) to switch over to routing through Wireless-1 totalling 30 seconds, as outlined below.

The Neighbor List of Wireless-3 :

Neighbor list (18:42:17.625000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 1 : m = 0 : w = 6 [2hlist:]

HYST [192.168.100.2] *HELLO timeout* 0.406 **………………… First HELLO timeout, and the link quality is decreasing**

[1] The OLSR ReadMe file has the following command in order to view the log files in the command window: c:\Program files\ olsr.org> olsrd -i if04

Hysteresis-link sensing mechanism	**6 seconds**	**Link quality constant (between 0 and 1, representing poor to high quality) [6].**

```
Neighbor list (18:42:19.327000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 1 : m = 0 : w = 6 [2hlist:]

HYST[192.168.100.2]HELLO timeout 0.203 ..................... Second HELLO timeout, and the
                                                             link quality is still decreasing

HYST [192.168.100.2] link set to pending! ..................... Declaring the link as set to pending
Deleting IPv4 route to 192.168.100.2 / 255.255.255.255 via 192.168.100.2.
Neighbor list (18:42:20.929000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 0 : m = 0 : w = 6 [2hlist:] ....... Wireless- 3 loses the direct link to Wireless- 2

HYST[192.168.100.2]HELLO timeout  0.102 ..................... Third HELLO timeout, and the link
                                                              quality is still decreasing
Neighbor list (18:42:22.832000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 0 : m = 0 : w = 6 [2hlist:]
Neighbor list (18:42:24.635000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 0 : m = 0 : w = 6 [2hlist:]

HYST[192.168.100.2]HELLO timeout  0.051 ..................... Fourth HELLO timeout, and the link
                                                              quality is still decreasing
Neighbor list (18:42:26.638000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 0 : m = 0 : w = 6 [2hlist:]
HYST[192.168.100.2]HELLO timeout  0.025 ..................... Fifth HELLO timeout, and the link
                                                              quality is still decreasing
```

Since the link quality is almost zero, Wireless-3 begins to use Wireless-1 as a relay to access Wireless-2; it is reported as follows:

```
Neighbor list (18:42:28.540000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
Setting 192.168.100.1 as MPR (Multipoint Relay)
Adding IPv4 route to 192.168.100.2 / 255.255.255.255 via 192.168.100.1.
Neighbor list (18:42:30.143000):
192.168.100.1: l = 1 : m = 0 : w = 3 [2hlist:]
192.168.100.2: l = 1 : m = 0 : w = 6 [2hlist: 192.168.100.1:]
                                                  ..................... Wireless- 3 begins to
                                                  use Wireless- 1 as a relay to access and
                                                  share files with Wireless- 2
Topology Declaration: adding entry 192.168.100.1
```

For experimental OLSR protocol, please see ref. [7] where delay calculation is discussed in detail. The reference verifies our finding of a large delay.

3.3 Remarks

In this section an overview of the setup in Windows 2000 was presented. Using wireless 802.11 cards in Windows 2000, in ad hoc mode, is limited to mesh connectivity. However, routing protocols like OLSR resolve this limitation and enable multi-hop connectivity. But the dynamics of this connectivity and self-healing are slow and connection re-established through a peer can take up to 30 seconds per connection. In the next section, we look at the throughput delay of the connection itself via real-time video transmission.

3.4 Streaming Wireless Video

Enabling live video transport over an ad hoc network is a challenging task. The wireless links in an ad hoc network are highly error-prone and can fade frequently because of node mobility, interference, and the lack of line of sight. Live video transport typically requires strict bandwidth and delay guarantees. It is very hard to maintain a stable end-to-end route with enough bandwidth to sustain live video transmission. Furthermore, compressed video itself is susceptible to transmission errors [8]. The aim of this experiment is to measure the processing delay through the wireless ad hoc connection.

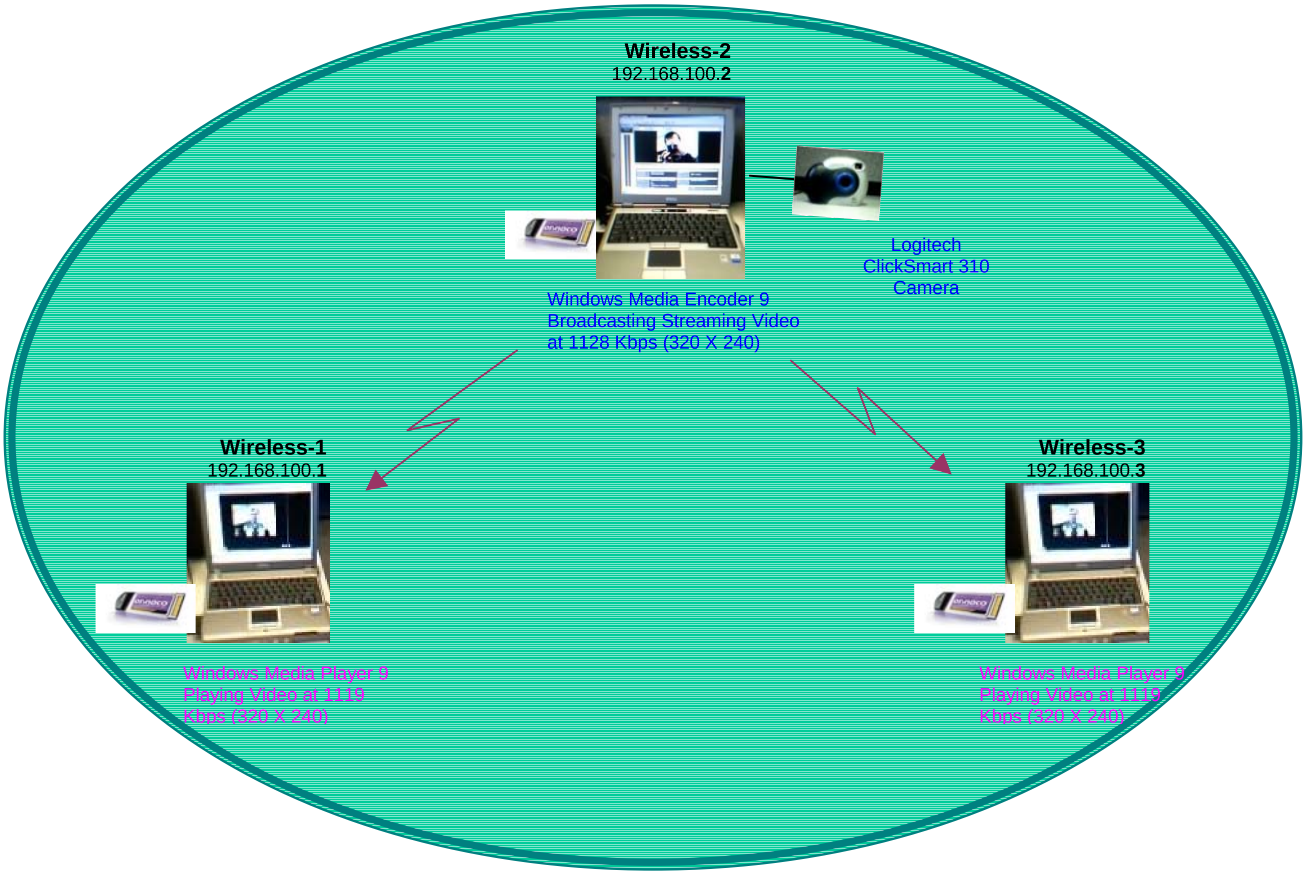
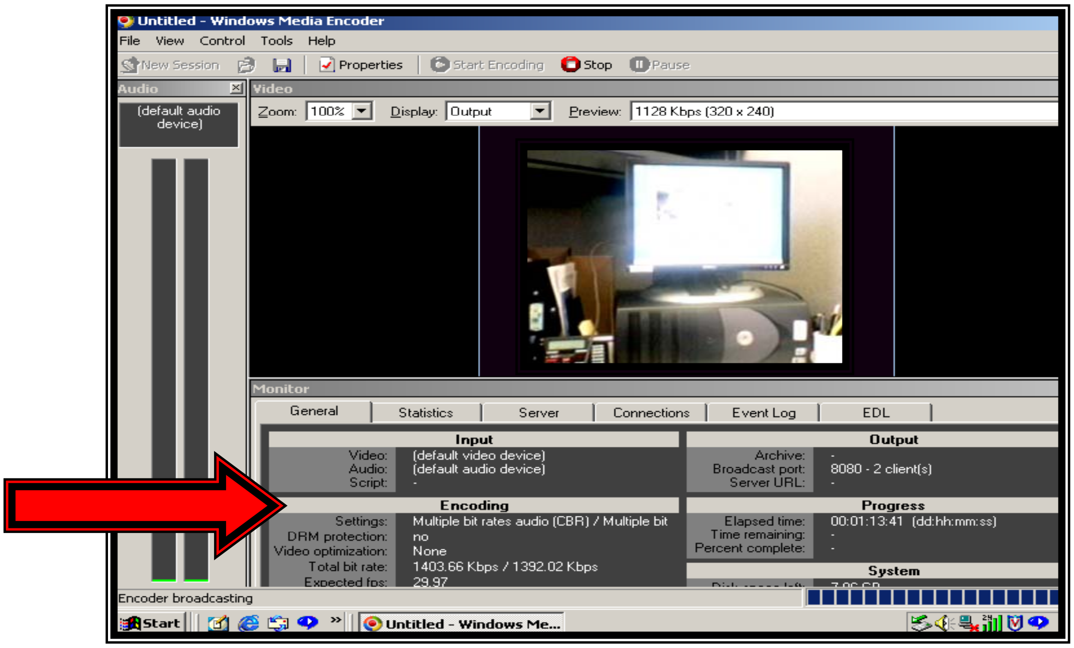

Wireless-2
192.168.100.2
Logitech ClickSmart 310 Camera
Windows Media Encoder 9 Broadcasting Streaming Video at 1128 Kbps (320 X 240)
Wireless-1
192.168.100.1
Wireless-3
192.168.100.3
Windows Media Player 9 Playing Video at 1119 Kbps (320 X 240)
Windows Media Player 9 Playing Video at 1119 Kbps (320 X 240)

Figure 4: Streaming wireless video on an ad hoc network

To enable live video transport over an ad hoc network, one can set up the network as shown in Figure 4. In this setup “Windows Media Encoder” and “Windows Media Player” applications on a Windows 2000 Operating System were used.

Windows Media Encoder comes with preset profiles that have been optimized to provide good quality video and audio for various situations, maximizing bandwidth utilization and data storage size. In these Microsoft applications two factors must be considered: frame rate and frame size. Both parameters dramatically affect the raw data rate and the quality of the video. If such systems are to be used in a battlefield, the available bandwidth must not be exhausted for the inevitable packet re-transmissions.

After the desired picture quality was achieved, the values used in the setup were 20 frames per second, at 320 x 240 pixels (frame size) in Kbits, which resulted in an average 1128 Kbps raw data rate. This is roughly one quarter of the throughput of WiFi systems. The Windows Media Encoder application allows for monitoring the input source and the resulting output - both as depicted in Figure 5.



(default audio device)

Zoom: 100%
Display: Output
Preview: 1128 Kbps (320 x 240)

Input
Video: (default video device)
Audio: (default audio device)
Script: -

Output
Archive: -
Broadcast port: 8080 - 2 client(s)
Server URL: -

Encoding
Settings: Multiple bit rates audio (CBR) / Multiple bit
DRM protection: no
Video optimization: None
Total bit rate: 1403.66 Kbps / 1392.02 Kbps
Expected fps: 29.97

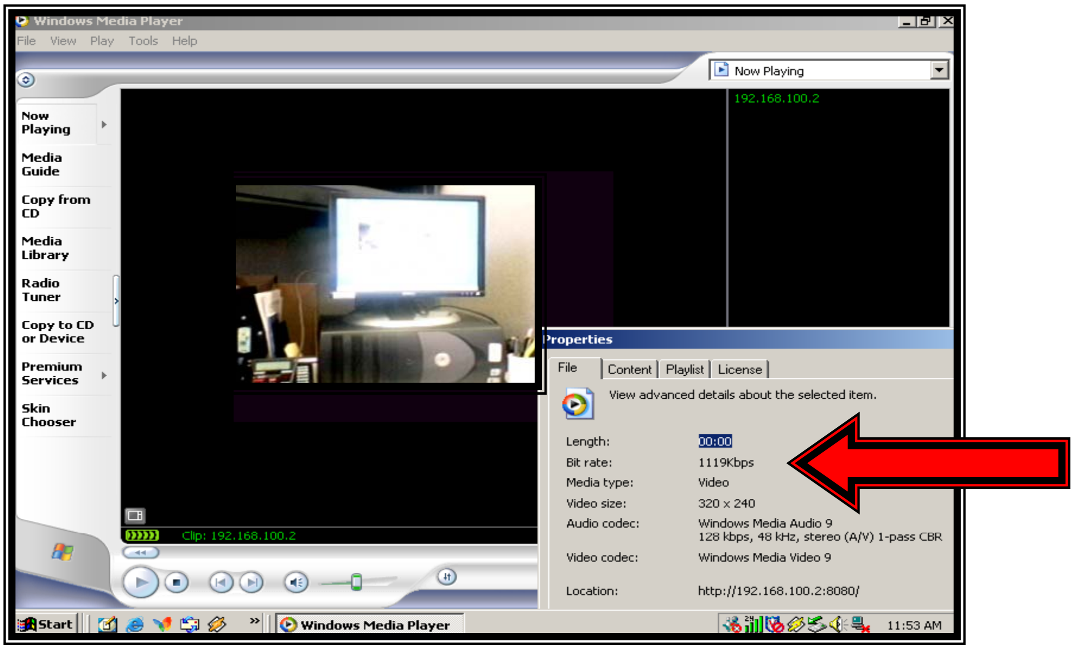
Progress
Elapsed time: 00:01:13:41 (dd:hh:mm:ss)
Time remaining: -
Percent complete: -

System

Encoder broadcasting

Figure 5: Windows Media Encoder monitoring screen

The encoder on the IP address 192.168.100.2 was setup to broadcast the signal to the Windows Media Players at the receiving ends, Wireless-1 (192.168.100.1) and Wireless-3 (192.168.100.3). Captured data as seen by the Windows Media Player screen is shown in the Figure 6.



View advanced details about the selected item.

Length:	00:00
Bit rate:	1119Kbps
Media type:	Video
Video size:	320 x 240
Audio codec:	Windows Media Audio 9 128 kbps, 48 kHz, stereo (A/V) 1-pass CBR
Video codec:	Windows Media Video 9
Location:	http://192.168.100.2:8080/

Figure 6: Windows Media Player screen

In our experimental wireless network, the measured end-to-end delay (the delay from the source to the destination and back to the source) was 6 to 9 seconds. It was 6 seconds with 802.11b and 9 seconds with 802.11g, even though 802.11g's data rate is higher than that of 802.11b.

The same test was performed on an equivalent wired configuration of the network in Figure 4 in order to measure the difference and find the wireless contribution to the delays. The measured end-to-end delay was 7 to 8 seconds. Because this test was performed with non-identical laptops from the wireless experiment, no specific conclusion could be made on comparing the measurements. However, we found that the delay caused by Windows Media Player was 5 to 6 seconds.

The logical sources of delay are buffering during route discovery, queuing at the transmission queue, and retransmissions by TCP and 802.11. But the actual source of the delay is Windows Media Player. The delay problem is documented at the Microsoft Help and Support website (http://support.microsoft.com/?kbid=827560#kb4) as follows: "When one streams files from a Windows Media Services 9 Series server, he/ she may notice a delay of five or six seconds when you switch between files. This delay may be an undesirable user experience. This problem occurs because of the way that the Windows Media Player 9 Series server submits the client-rendering log to the Windows Media Services 9 Series server. When the server is set up to accept client rendering logs, an internal error may be incorrectly reported on the client when the client waits for a response from the server. If this behavior occurs, the client times out after a default period and then opens the next file. In this case, the server receives the correct log from the client."

The delays caused by the wireless components are due to buffering during route discovery, queuing at the transmission queue, and retransmissions by the MAC layer. The delays caused by the wired components are also due to buffering during route discovery, queuing at the transmission queue, and retransmissions by the MAC layer. Routing related queues are the same for both wired and wireless connections. However, transmission queues and delays due to MAC retransmissions are different for the two connections and depend on available bandwidth and channel conditions. For this experiment, we expect similar results from both wired and wireless connections given ample bandwidth on the radio channels, and identical equipment. This experiment has shown that the processing delay through the wireless ad hoc connection is not a bottleneck for the link.

A possible explanation for the higher delay through 802.11g may be specifically due to the transmission queue because the system is based on Orthogonal Frequency Division Multiplexing [9] (OFDM) as opposed to Direct Sequence Code Division multiplexing in 802.11b. The network cards with OFDM capability may require more signal processing to prepare the data frame for transmission. Real-time data can be very demanding and show processor delays more noticeably.

4. Setup in a Linux Environment

As mentioned before, the purpose of setting up a test bed is to have a stable platform to perform research and to test security solutions for mobile ad hoc networks. The network in the Windows environment was limited by the lack of access to the source code of the operating system, especially to the routing algorithms and the modules that control them. Thus, another test bed was set up in a Linux environment where we can analyze vulnerabilities of OLSR and verify authentication, intrusion detection, and prevention techniques [4] within MANETs.

This section provides the details of the mobile ad hoc test bed, which we set up using the Fedora Core 2 Linux distribution. This version is readily available from the Internet and was chosen because it was stable, recommended for the test bed tools and it included IPv6, the next generation version of the Internet Protocol.

To set up an ad hoc network with mesh connectivity with multi-hop capability in Linux, one needs to download and compile the OLSR routing protocol - just as we did in the Windows environment. We received the help of our colleagues from Communication Research Centre (CRC), who had some experience in this area and in research on OLSR. They recommended that we use a modified version of OLSR called "CRCOLSR6D (CRC-modified version of NOLSRD, IPv6 only, crcolsr6d_v11)", which can be found from http://www.crc.ca/en/html/manetsensor/home/software/software . The crcolsr6d modules should be installed on all the nodes in the network to establish mesh connectivity with multi-hop capability.

4.1 Application for network display

Another purpose for setting up a test bed is to have a stable platform to demonstrate the researched solutions for security of mobile ad hoc networks. The move to Linux was also required in order to have access to the open-source software for the display application. To display network situational awareness, one needs to download, compile, and install several tools from http://proteantools.pf.itd.nrl.navy.mil/mne-scripts.html. Based on our CRC colleagues' experience, we chose the Naval Research Laboratory's (NRL) display modules which include the following: Mobile Network Emulator (MNE), Multi-Generator (MGEN), C-based Mathematical Application Programming (CMAP) Environment, and Scripted Display Tool (SDT). All these tools are open source software from the NRL PROTocol Engineering Advanced Networking (PROTEAN) group. The functions of these modules are explained below with the aid of Figures 7 and 8.

Figure 7 shows the major functional components of the tools used in test bed. The OLSR module communicates over the wireless network (bearer traffic - shown in blue font) to perform its functions of neighbor sensing and topology discovery. The MNE module communicates over a wired network (display application traffic - shown in red font) in order to perform the tasks of extracting the network information from OLSR logs and displaying the current network situation. The test bed management applications communicate through a wired backbone, leaving the wireless network free of overhead. MNE generates (emulates) positions for the mobile ad hoc nodes, broadcasts those positions to the other nodes over the wired backbone, logs positions of all the nodes, and blocks those out-of-range nodes from communicating over the wireless link. The OLSR module logs routing information about all mobile ad hoc nodes in the network, and re-routes traffic when MNE blocks a specific link. Triggered by running a test, the current network situation with the movement of the nodes can be seen on a central display using the log files provided by MNE and OLSR through display tools CMAP and SDT.

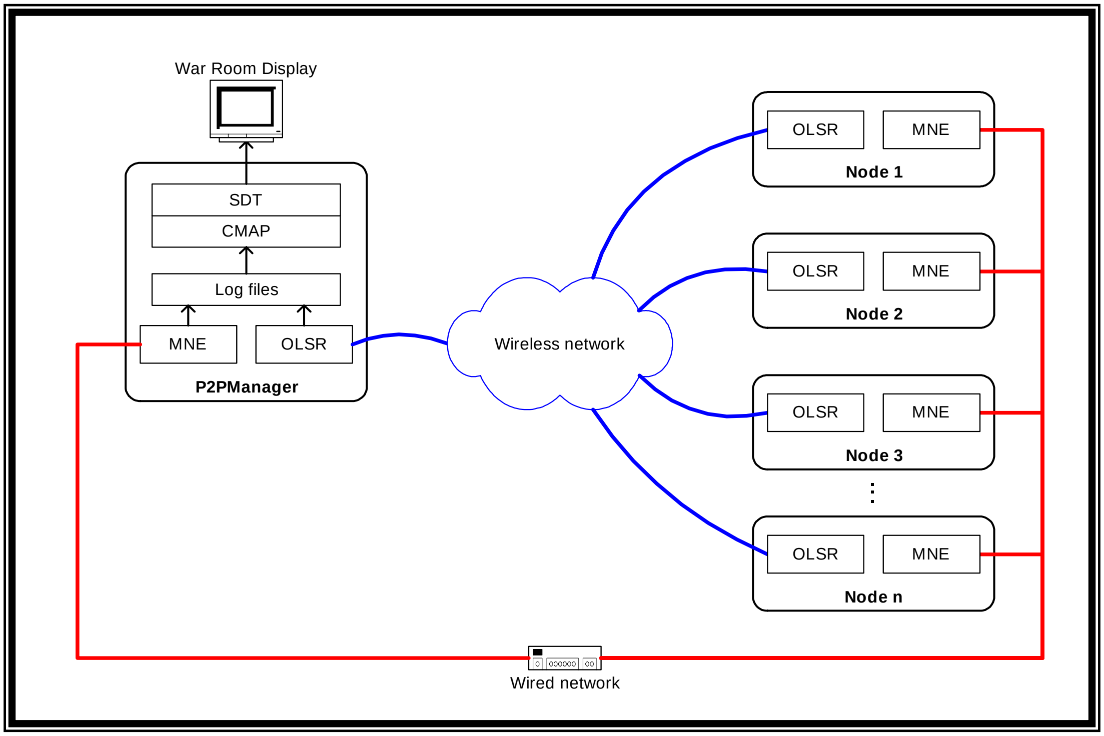


Figure 7: The functional components of the test bed

The relationship among the tool modules used in the test bed is visualized through a functional flow diagram as provided in Figure 8:

- The MNE and OLSR modules provide log files;
- CMAP provides lists of each node's IP and MAC addresses, and display image;
- SDT provides background images with bounds in longitude and latitude, graphical CMAP information with node icons, movements, and links;
- MGEN was not used in the test bed because the network display does not depend on it. Its function is to generate real-time UDP/IP (User Datagram and Internet Protocol) traffic patterns - of unicast and multicast types - and calculate (from its logs) performance statistics on throughput, packet loss and delay.

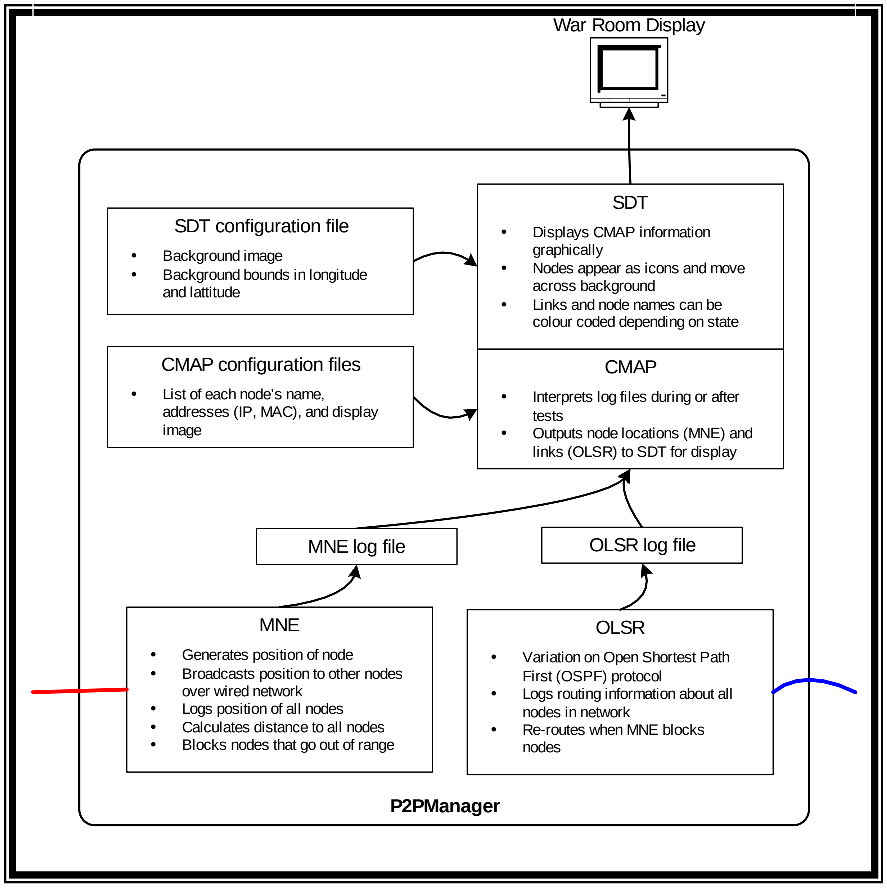

War Room Display
SDT
Displays CMAP information graphically
Nodes appear as icons and move across background
Links and node names can be colour coded depending on state
SDT configuration file
Background image
Background bounds in longitude and lattitude
CMAP configuration files
List of each node's name, addresses (IP, MAC), and display image
CMAP
Interprets log files during or after tests
Outputs node locations (MNE) and links (OLSR) to SDT for display
MNE log file
OLSR log file
MNE
Generates position of node
Broadcasts position to other nodes over wired network
Logs position of all nodes
Calculates distance to all nodes
Blocks nodes that go out of range
OLSR
Variation on Open Shortest Path First (OSPF) protocol
Logs routing information about all nodes in network
Re-routes when MNE blocks nodes
P2PManager

Figure 8: The relationship among the tools used in test bed

NRL-developed MNE is designed to run under Linux environments with IPTABLES network filtering capability installed. IPTABLES are building blocks of a framework inside the Linux 2.4.x and 2.6.x kernel which support firewall functions and filtering. The emulator includes a software process that writes location information to a shared memory.

The MNE scripts are a set of scripts for Linux that are used to automate IPv6 mobile ad hoc networking tests. These scripts are designed to emulate a MANET for each node in the network. Each node should have two interfaces: one hard-wired interface with static addresses for test application traffic, and one wireless interface for bearer traffic. These scripts are designed for a network where one special node, designated as "XCom", is set to be the desktop P2P Manager. XCom acts as a master control node for the MNE scripts. XCom is the machine that starts tests and gathers results. The MNE scripts are designed to be installed and run by the root. The scripts are also designed such that XCom must have automatic secure shell (SSH) access to each machine in the network (achieved using the HonorMe script provided with MNE). XCom can start tests and run commands through SSH [10].

MNE can also be used to generate motion patterns that can be communicated via the test application traffic channel using IP multicast to all nodes participating in the emulation. Emulated nodes can listen in on this test application channel to pick up the location information for other nodes. The emulation nodes can then compare this information with their own emulated location. By having location and other information available locally, nodes can determine with which nodes they can establish effective communication links. They can do this using a variety of wireless propagation models, the simplest of which is a basic range model. Using this model, when the calculated distance to a given node is beyond the specified range, a MAC address filter drops all incoming packets from that node on the emulated interface before being delivered to the appropriate application. To the network applications, this makes the local link between the two nodes appear unusable [11]. In theatre, without a centralized emulator, all nodes must broadcast their location to their neighbors and share it in order to build a limited situational awareness picture for every node based on its routing information. The emulator, however, provides the total network picture, ideal for “war room” demonstrations.

CMAP provides a means of translating output from log files for OLSR and MNE into an output which can be read by SDT. This mobility visualization tool keeps track of node movements, network links between nodes, and the status of data reception. The background image and corresponding coordinates are set via an sdtsetup.cfg file in standard SDT style input format. A parser (a computer program that breaks down text into recognized strings of characters for further analysis) reads in a cmap.cfg file that is used to assign names to nodes, and to provide a list of corresponding MAC addresses, and IP addresses to the nodes.

The SDT tool must be built with the wxWidgets library for graphical user interface applications. wxWidgets library is an open-source, cross-platform, C++ Graphical User Interface (GUI) toolkit freely available from http://www.wxwidgets.org.wxWidgets . wxWidgets gives a single, easy-to-use API (application program interface) for writing GUI applications on multiple platforms.

The SDT tool provides a simple visualization capability using standard image files for a background image and another set for overlaid images of nodes. Nodes are assigned iconic images for the display from standard format image file types (e.g. jpeg and gif). A custom coordinate system can be defined for the background while node positions can be dynamically updated to "move" their associated icons about the background. Displayed nodes can also be dynamically "linked" and "unlinked" with lines of user-specified color and thickness. This makes SDT well suited for one of its intended purposes, that is, to provide a real-time visualization of dynamic, mobile data communication networks.

MGEN provides the ability to perform IP network performance tests and measurements using UDP/IP traffic. The toolset generates real-time traffic patterns so that the network can be loaded in a variety of ways. These script files can be used to emulate the traffic patterns of unicast and multicast UDP/IP applications. The receive portion of this tool set can be scripted to dynamically join and leave IP multicast groups. MGEN log data can be used to calculate performance statistics on throughput, packet loss rates, and communication delay [10]. Since we generated our own test traffic such as FTP, we did not need to use MGEN.

4.2 A mobile ad hoc networking test bed

Following the installation of the modules described in the previous section in the Linux environment, we built a mobile ad hoc network with a topology shown in Figure 9. The wireless traffic is shown in blue font, representing a mesh of connections with multi-hop capability. The display application traffic is shown in red font, which performs out-of-band logging, addressing, and dynamic emulation of mobile nodes.

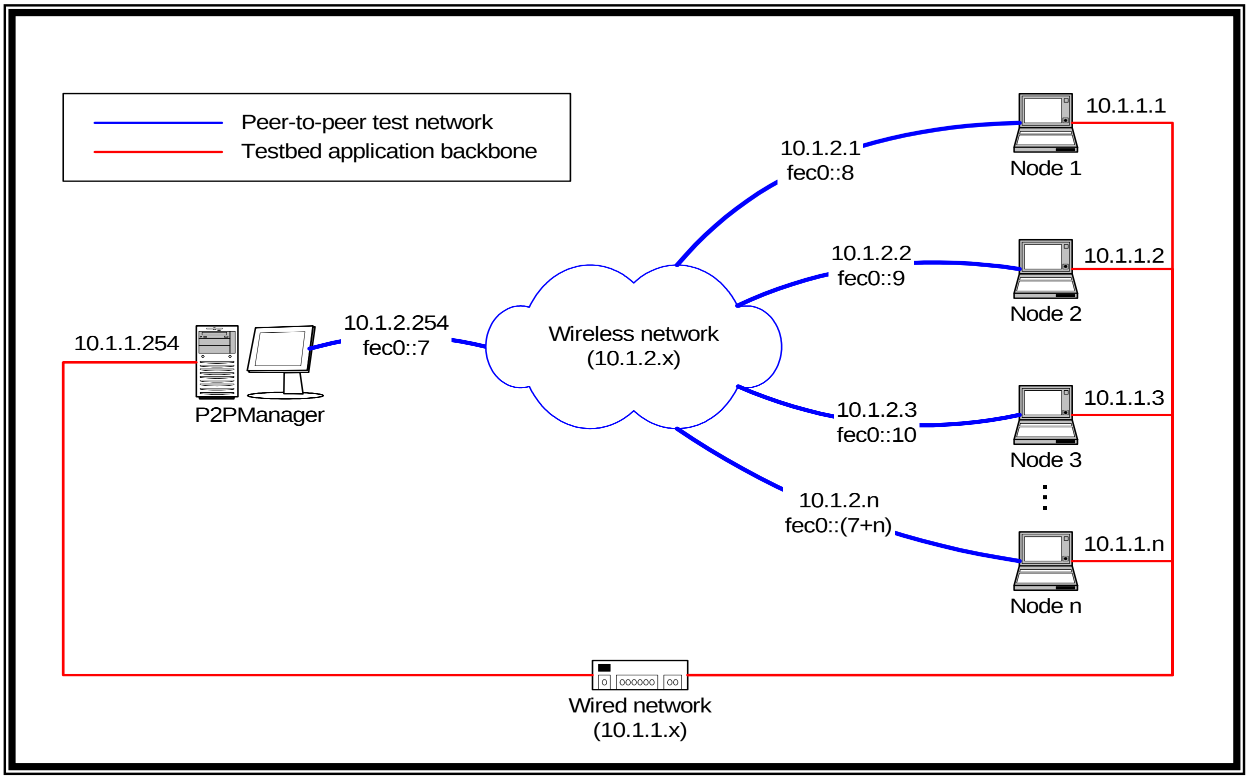


Figure 9: A mobile ad hoc networking test bed

We performed a similar test, as we did in the Windows environment, in order to measure the OLSR multi- hop link changeover delay when a node goes out of range. Experimental results collected at node3 show that there is a 2 second delay between losing contact with node2 and re-establishing contact through node1. In the experiment, the “HELLO” time interval was set to 2 seconds, and the “HELLO” timeout was set to 6 seconds – the default values. Compared to the measurements in the Windows environment, the dynamics of the self-healing capability is much faster in the Linux environment because it only takes up to only 2 seconds per connection (versus 30 seconds in Windows), as shown below:

```
CRCOLSR: CRC IPv6 HNA Version 1.0
                   OLSR6d Parameters are:
                   hello interval = 2.000000              ..................... Seconds
                   neighbor_hold_time =  6.000000         ..................... Seconds
                   topology_hold_time = 15.000000         ..................... Seconds
Node's WILLINGNESS is: 3      ..................... To be an MPR
A MANET NODE
----- interface name: eth1
debug level is: 0             ..................... A super view for logs (below), not too detailed
```

```
++++++++++++++++++ olsr calculate routing table! ++++++++++++++++++++
The source is always node3 (fec0::10) because the table was printed from node3.

ROUTING TABLE      18:02:01.274361 …..……… Time
DESTINATION        SOURCE       NEXT HOP     INTERFACE   METRIC

fec0::8            fec0::10     fec0::8      0           1
IPv6 addresses: node1 (fec0::8) establishes link to node 3 (fec0::10) via one hop (metric = 1).
For direct links (metric = 1) the next hop shows as the source itself.
fec0::9            fec0::10     fec0::9      0           1
IPv6 addresses: node2 (fec0::9) establishes link to node 3 (fec0::10) via one hop.


ROUTING TABLE      18:02:03.674663
DESTINATION        SOURCE       NEXT HOP     INTERFACE   METRIC
fec0::8            fec0::10     fec0::8      0           1
No information is available about the link between node2 and node3 (i.e. node2 loses the direct
link to node3)


ROUTING TABLE      18:02:03.419351
DESTINATION        SOURCE       NEXT HOP     INTERFACE   METRIC
fec0::8            fec0::10     fec0::8      0           1
Still no information is available about the link between node2 and node3.


ROUTING TABLE      18:02:04.999852
DESTINATION        SOURCE       NEXT HOP     INTERFACE   METRIC
fec0::8            fec0::10     fec0::8      0           1

fec0::9            fec0::10     fec0::8      0           2
Node3 begins to use node1 as a relay to access and share files with node2.
In this case metric = 2 hops.
```

We were not able to transmit live video through the network for comparative measurements because we could not find the Logitech ClickSmart 310 camera’s application software for Linux. However, as was shown in the Windows test, the main video transmission delay was due to buffering and processing by the Microsoft application.

A sample of a MNE log file is provided below[2], where communication range is set to 100 m from the P2P manager. When a node goes out of range from the central display node (P2P manager), the MNE blocks that node from communicating wirelessly.

A sample of an OLSR log file is also provided below[3], where routing tables of nodes are changed according to their position and distance.

Finally a screenshot of SDT in action is depicted in Figure 10.

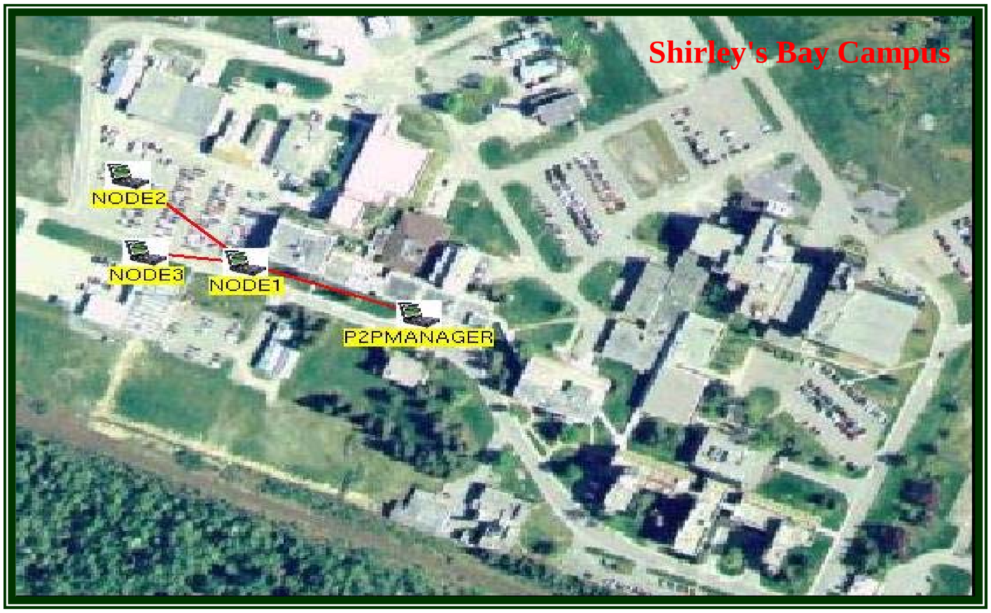


Figure 10: A screenshot of SDT in action

[2] The following command can be used in order to view the log files in terminal window: [root@p2pmanager data]# vi mne……log.

[3] The following command can be used in order to view the log files in terminal window: [root@p2pmanager data]# vi olsr……log.

SAMPLE MNE LOG FILE

```
Setting interface to eth0
New Range = 100.0m
        Src>0/Ad-hoc Mac>00:02:2D:1C:32:D0 Long>-75.887330 Lat>45.346675 TxTime>14:35:32
```

Node 0 (P2P manager) with MAC address, position, and time.

```
MNE: Src>1/Ad-hoc Mac>00:02:2D:1F:E2:88  Long>-75.887947 Lat>45.347198 TxTime>14:35:33
```

Node 1 with MAC address, position, and time within the pre-set distance range (distance is not shown).

```
MNE: Src>2/Ad-hoc Mac>00:02:2D:1C:32:CB Long>-75.890999 Lat>45.346451 TxTime>14:35:34
       IP 2 MAC=00:02:2D:1C:32:CB D=188.6m BLOCKED
```

Node 2 with MAC address, position, and time, out of distance range (distance is 188.6 m).

```
MNE: Src>3/Ad-hoc Mac>00:02:2D:1C:32:DE Long>-75.889198 Lat>45.346699 TxTime>14:35:36
       IP 3 MAC=00:02:2D:1C:32:DE D=146.4m BLOCKED
```

Node 3 with MAC address, position, and time, out of distance range (distance is 146.4 m).

```
MNE: Src>4/Ad-hoc Mac>00:02:2D:1C:32:A8 Long>-75.890999 Lat>45.347649 TxTime>14:35:38
        IP 4 MAC=00:02:2D:1C:32:A8 D=207.2m BLOCKED
```

Node 4 with MAC address, position, and time, out of distance range (distance is 207.2 m).

... while moving via the emulated scenario, the logs continue ...

```
        Src>0/Ad-hoc Mac>00:02:2D:1C:32:D0 Long>-75.887330 Lat>45.346675 TxTime>14:35:38
MNE: Src>1/Ad-hoc Mac>00:02:2D:1F:E2:88  Long>-75.887947 Lat>45.347198 TxTime>14:35:38
MNE: Src>3/Ad-hoc Mac>00:02:2D:1C:32:DE Long>-75.889111 Lat>45.346751 TxTime>14:35:38
MNE: Src>2/Ad-hoc Mac>00:02:2D:1C:32:CB Long>-75.890769 Lat>45.346450 TxTime>14:35:38
MNE: Src>4/Ad-hoc Mac>00:02:2D:1C:32:A8 Long>-75.890941 Lat>45.347649 TxTime>14:35:39
```

... nodes 2,3, and 4 are now within range ...

... while moving via the emulated scenario, the logs continue ...

```
        Src>0/Ad-hoc Mac>00:02:2D:1C:32:D0 Long>-75.887330 Lat>45.346675 TxTime>14:35:39
MNE: Src>2/Ad-hoc Mac>00:02:2D:1C:32:CB Long>-75.890712 Lat>45.346450 TxTime>14:35:39
MNE: Src>4/Ad-hoc Mac>00:02:2D:1C:32:A8 Long>-75.890884 Lat>45.347649 TxTime>14:35:40
MNE: Src>1/Ad-hoc Mac>00:02:2D:1F:E2:88  Long>-75.887947 Lat>45.347198 TxTime>14:35:40
MNE: Src>3/Ad-hoc Mac>00:02:2D:1C:32:DE Long>-75.889023 Lat>45.346804 TxTime>14:35:40
```

SAMPLE OLSR LOG FILE

```
CRCOLSR: CRC IPv6 HNA Version 1.0
            hello interval = 2.000000            ..................... Seconds
            neighbor_hold_time =  6.000000       ..................... Seconds
            topology_hold_time = 15.000000       ..................... Seconds
            Node's WILLINGNESS is: 3             ..................... To be an MPR
             ----- interface name: eth2
            debug level is: 0                    ....... A super view for logs (below), not too detailed

Routing-Links List: 14:35:34.392610              ..................... Time
fec0::7 -> fec0::8                  …………. IPv6 addresses: P2P manager establishes link to node 1
End of Routing-Links List.

Routing-Links List: 15:35:36.472458
fec0::7 -> fec0::8
fec0::8 -> fec0::9                  …………. IPv6 addresses: node 1 establishes link to node 2
End of Routing-Links List.

Routing-Links List: 14:35:38.552126
fec0::7 -> fec0::8
fec0::8 -> fec0::10                 …………. IPv6 addresses: node 1 establishes link to node 3
fec0::8 -> fec0::9
End of Routing-Links List.
```

New links are established through time as the nodes move within the network. Sample logs are provided below.

```
Routing-Links List: 14:35:39.916673
fec0::7 -> fec0::8
fec0::8 -> fec0::10
fec0::8 -> fec0::9
End of Routing-Links List.

Routing-Links List: 14:35:39.916673
fec0::8 -> fec0::11
fec0::7 -> fec0::8
fec0::8 -> fec0::10
fec0::8 -> fec0::9
End of Routing-Links List.

Routing-Links List: 14:35:40.657848
fec0::10 -> fec0::11
fec0::7 -> fec0::8
fec0::7 -> fec0::10
fec0::10 -> fec0::9
End of Routing-Links List.
```

```
Routing-Links List: 14:35:43.846981
fec0::10 -> fec0::11
fec0::7 -> fec0::8
fec0::7 -> fec0::10
fec0::10 -> fec0::9
End of Routing-Links List.

Routing-Links List: 14:35:49.929740
fec0::8 -> fec0::11
fec0::7 -> fec0::8
fec0::8 -> fec0::9
End of Routing-Links List.
```

4.3 Running tests

Tests can be run with a single command from the P2PManager (XCom) machine: “startAll”. This command is propagated to all the machines in the network with the same parameters. The syntax for the startAll command is:

```
startAll <motion_model> <scenario> [options]
```

The motion model can be one of several models implemented by NRL (waypoints - wp model, real motion model, fixed position - fixedpos model) or other tailored models. We used a model implemented for testing by DRDC’s Secure Mobile Networking Group of Network Information Operations Section (nio waypoints model).

- The “real” model plays back GPS data from a live test,
- The "fixedpos" model runs a scenario where all nodes have fixed GPS positions (no motion),
- The “nio” model is based on a predefined waypoints model that is designed to support node mobility where nodes travel to predetermined waypoints.

The scenario refers to the type of test (bearer) traffic produced. There are several models included with the scripts, most of which are "many-to-1" scenarios, where all nodes transmit data to the P2PManager, causing MNE and OLSR logs to be sent there as well.

The options are used, among other things, to control whether the test is an IPv4 or an IPv6 test. This is controlled with "-ipv4" and "-ipv6", or simply "-4" and "-6".

StartAll has many optional parameters to allow the user perform different tests. One parameter is the "-file <filename>" parameter, which can change the default motion model with the following options: wp, real, fixedpos, and nio motion models.

After the first step of a test has completed, one can use the "stopAll" script (from the P2PManager) to stop MNE and OLSR on all nodes. The next step is to display the results. One can use "cmap mne mne..…log   olsr olsr..….log | sdt" syntax to show the results on SDT.

5. Summary

As we have seen, there are various aspects of mobile ad hoc networks that can be emulated in a lab environment. We found that Windows was not a suitable platform for the test bed and that the Windows implementation of the OLSR MANET routing protocol had difficulties with re-routing when a node went out of range. We also found that due to limitations in the Windows Media platform, our tests using streaming video were inconclusive.

The test bed tools from the Naval Research Laboratory will be extremely useful in our future research into aspects of security in MANETs. The test bed allows us to test in the laboratory first before moving our tests into the field. It also allows us to display test results in a graphical, non-technical manner.

The OLSR implementation from our colleagues at the Communications Research Centre proved to be much quicker than the Windows implementation we used and also compatible with the test bed tools.

We believe the test bed will provide a useful tool in both doing our research and exhibiting the results. Future work will include investigations into authentication and intrusion detection in MANETs. Use of the test bed tools to create a network situational awareness application will also be investigated. This will involve removing the wired channel and removing some of the overhead in the test bed application communications. Finally, since streaming video is a demanding application and therefore an excellent benchmark for network performance, we will look to redo the wireless video tests in Windows and also to do them in Linux, in order to get a meaningful comparison of the platforms.

6. References

1. Borg, J., A Comparative Study of Ad hoc & Peer-to-Peer Networks, University College London, August 2003.

2. Geier, J., Understanding Ad hoc Mode, http://www.wi-fiplanet.com/tutorials/article.php/10724_%201451421_2 .

3. Ramanathan, R., Redi, J., A Brief Overview of Ad Hoc Networks: Challenges and Directions, BBN Technologies, 2001.

4. Genik, L., Salmanian, M., Mason, P., Schotanus, H.A., Verkoelen, C.A.A., Hansson, E., Mobile Ad Hoc Network Security from a Military Perspective, DRDC Ottawa TM 2004-252, Defence R&D Canada- Ottawa, December 2004.

5. Mason, P., Gorlatova, M., Security Overview of the 802.11 Wireless Networking Protocol, DRDC Ottawa TM 2004-155, Defence R&D Canada- Ottawa, November 2004.

6. Internet Engineering Task Force website www.ietf.org .

7. Clausen, T., Jacqet, P., Optimized Link State Routing Protocol (OLSR), http://rfc3626.x42.com/, October 2003.

8. Mao, S., Lin, S., Panwar, S., Wang, Y., and Celebi, E., Video Transport Over Ad hoc Networks: Multistream Coding With Multipath Transport, IEEE Journal on Selected Areas in Communications, Vol.21, No.10, PP.1721-1737, December 2003.

9. IEEE Technical Report, Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications. Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band - Corrigendum 1, 2003.

10. US Naval Research Laboratory, Mobile Ad Hoc Networking (MANet) Research Group website, http://proteantools.pf.itd.nrl.navy.mil/mne-scripts.html#install_tools .

11. Chao, W., Macker, J.P., Weston, J.W., NRL Mobile Network Emulator, NRL Information Technology Division, January 2003.

List of symbols/abbreviations/acronyms/initialisms

ACK	Acknowledgement
AP	Access Point
BER	Bit Error Rate
CMAP	C-based Mathematical Application Programming
COTS	Commercial Off-The-Shelf
CRC	Communications Research Center
DND	Department of National Defence
DRDC	Defence R&D Canada
HYST	Hysteresis-link Sensing Mechanism
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
LOS	Line of Sight
MAC	Media Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad hoc Networking
MGEN	Multi Generator
MNE	Mobile Network Emulator
MPR	Multipoint Relay
MS	Multipoint Relay Selector
NIO	Network Information Operations

NRL	Naval Research Laboratory
OLSR	Optimized Link State Routing
OSPF	Open Shortest Path First
PAN	Personal Area Network
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PROTEAN	Protocol Engineering Advanced Networking
QoS	Quality of Service
SDT	Scripted Display Tool
SMN	Secure Mobile Networking
SSH	Secure Shell
UDP	User Datagram Protocol
UxV	Unattended Vehicle
WAN	Wide Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

A Mobile Ad Hoc Networking Test Bed

4. AUTHORS (Last name, first name, middle initial)

Sen, C., Salmanian, M., Kellett M.

5. DATE OF PUBLICATION (month and year of publication of document)

August 2005

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

26

6b. NO. OF REFS (total cited in document)

11

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15BR01

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

N/A

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC Ottawa TM 2005-158

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

N/A

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unlimited

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Wireless computer networks are becoming increasingly important to the military and the use of inexpensive, light hardware based on the IEEE 802.11 wireless networking standards has given these networks unprecedented mobility. The advent of self-organizing, peer-to-peer mobile ad hoc networks (MANETs) based on these devices challenges traditional network conceptions of routing and security. Research into these and other aspects of MANETs requires extensive field testing or specialized test facilities. In this technical memorandum, we give an overview of the special properties of MANETs and how routing protocols such as Optimized Link State Routing (OLSR) allow them to function. We discuss the limitations of the Windows platform for use in our research. Finally, we detail the set up of MANET test bed in Linux using tools from the United States' Naval Research Laboratory (NRL). The tools allow for the emulation of MANETs, including simulating the effects of node movement and terrain on the network. The test bed will allow us to do our initial research in a lab environment and to demonstrate our results in a graphical, non-technical manner.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Mobile Ad Hoc Network, MANET, Test Bed, Optimized Link State Routing, OLSR, WLAN, 802.11