A Preliminary Study of Routing Protocols in a Tactical Data Link Ad Hoc Network in Colombian Maritime Scenario

Estudio Preliminar de Protocolos de Enrutamiento en una Red Ad-Hoc de Enlace de Datos Tácticos en un Escenario Marítimo Colombiano

DOI: https://doi.org/10.25043/19098642.207

Arturo Arenas Castro [1]
Geovanny D. Sánchez Marín [2]
Guefry L. Agredo Méndez [3]
Camilo E. Segovia Forero [4]

Abstract

Tactical Data Link (TDL) systems are a kind of Mobile Ad Hoc NETwork (MANET) used in diverse maritime operational environments such as natural disasters, surveillance, maritime search, and rescue. A TDL network is usually composed of nodes or units representing surface ships, submarines, and aircrafts able to participate in maritime operations. A routing protocol is required to establish communication between nodes, which guarantees the route from the source node to the destination node. A TDL has been developed in the Colombian Caribbean Sea (CTDL). However, no efficient routing protocol has been implemented. This works to perform a preliminary study to implement an appropriate routing protocol for the CTDL.
Local environment constraints, in addition to the chosen protocols' performance analysis, will provide preliminary alternatives for a routing protocol with acceptable efficiency. This article provides a background of ad-hoc networks routing protocols, a description of the Colombian Caribbean maritime operational environment, a comparative analysis of routing protocols, and a discussion of conclusions and future developments regarding CTDL.

Key words: Routing, MANET, Table Driven, tactical data link.

Resumen

El sistema de enlaces tácticos de datos (Tactical Data Link, TDL) es una especie de red móvil Ad-hoc (Mobile Ad-Hoc Network, MANET) utilizada en diversos entornos operativos marítimos como desastres naturales, vigilancia, búsqueda y rescate en el mar, entre otros. Por lo general, una red TDL se compone de nodos o unidades que representan buques de superficie, submarinos y aeronaves capaces de participar en operaciones marítimas. Los protocolos de enrutamiento son necesarios para establecer la comunicación entre los nodos que garantiza el establecimiento de la ruta desde el nodo de origen al nodo de destino. Se ha desarrollado un TDL en el mar Caribe Colombiano (CTDL); sin embargo, no se ha implementado ningún protocolo de enrutamiento eficiente. Por lo tanto, el objetivo de este trabajo es realizar un estudio preliminar para implementar un protocolo de ruteo apropiado al CTDL.
Las restricciones de entorno local, además del análisis de rendimiento de los protocolos elegidos, proporcionarán candidatos preliminares para un protocolo de enrutamiento con una eficiencia aceptable. El artículo proporciona antecedentes de protocolos de enrutamiento en redes Ad-Hoc, una descripción del entorno operativo marítimo del caribe Colombiano, un análisis comparativo de los protocolos de enrutamiento y unas conclusiones y desarrollos futuros con respecto a CTDL.

Palabras claves: Protocolos de Enrutamiento, MANET, Enlace de datos tácticos.

Date Received: June 7th 2020 - *Fecha de recepción: Junio 7 de 2020*
Date Accepted: July 5th 2020 - *Fecha de aceptación: Julio 5 de 2020*

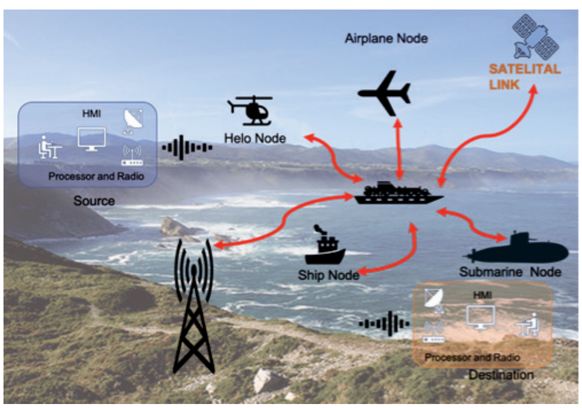
[1] Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad del Cauca. Popayán, Colombia. Email: arturoarenas@unicauca.edu.co
[2] Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad del Cauca. Popayán, Colombia. Email: geosanmarin@gmail.com
[3] Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad del Cauca. Popayán, Colombia. Email: gagredo@unicauca.edu.co
[4] Facultad de Ingenieria Naval. Escuela Naval Almirante Padilla. Cartagena, Colombia. Email: camilo.segovia@armada.mil.co

Introduction

A TDL is an ad-hoc [1] network with a specific task, characterized for having two or more units (nodes) equipped with wireless communications with network integration ability establishing a direct or indirect (through relay nodes) contact. TDL features are self-organized and adaptative. Even when data is underway, the path from the source to the destination node requires no administration system. Ad-hoc networks could have different forms, such as mobile, standalone, or network of any other system.

Fig. 1 describes the functional elements of a TDL, which include a source node/unit willing to establish communication with another node called destination, directly or through relay nodes. Note that nodes have a Human Machine Interface (HMI), a processor module, and a transmission module that allows for information broadcasting.

Fig. 1. Tactical Data Link.



Most TDLs are developed either by the North Atlantic Treaty Organization (NATO) or by private commercial companies. These developments are not open source, generic, or for general use. The customizing network is not available to the end-user, and the original equipment manufacturer is not allowed to release the network or system security parameters.

For the Caribbean Sea scenario, the mentioned TDLs do not fit all information requirements such as weather conditions, units positions, sea state, or the performance of the participating teams, among others.

Although there has only been one TDL implementation in Colombia [2], no evidence of routing protocols has been found in its systems. Therefore, introducing routing protocols is necessary to contribute to the efficient development of the Colombian Tactical Data Link (CTDL).

In the early 1970s, the first ad-hoc networks, packet radio systems, were implemented [3]. They used routing protocols for mobile networks and faced restrictions such as:

1. High power consumption
2. Bandwidth restrictions
3. High Bit Error Rate (BER)

Currently, routing protocols have successfully overcome those constraints and have reached maturity to fulfill end user's needs.

This article provides an overview to recommend the appropriate TDL routing protocols to work in a specific maritime environment. To achieve these objectives, this paper provides a background on ad-hoc networks, followed by a description of the maritime operational environment in the Colombian Caribbean Sea and a discussion regarding routing protocols, including a comparative analysis among them and, finally, states the conclusions and expectations for future developments of the CTDL.

Background

Ad-hoc networks [4], [5] are wireless means to set up communications in different kinds of unexpected maritime environments, jungles, and deserts, where no established communications systems are available. Each node should detect other nodes or units present in the operational scenario to perform a handshake to guarantee an active link, communication, data, and network services, among them. Concerning these issues, ad-hoc networks do not solely need to detect other nodes, but they must also identify the types of neighboring node devices and their features. The intrinsic characteristics of the ad-hoc-network include its infrastructure-less configuration without a predetermined topology or centralized control. There is no fixed base radio station, router, wires, or fixed routes, whereby routed information will change as per network node mobility changes, which will be reflected in the link connectivity. Ad-hoc networks face many other constraints, such as different hardware brands (computers, mobile phones, communication equipment, etc.), and power consumption becomes critical due to the relay of information packets between nodes, which requires hardware to work permanently.

Some of the challenges and difficulties [1] that ad-hoc mobile networks face are:

1. The use of the radio spectrum is regulated by the government of each country. While performing tests, the ISM (Industrial, Scientific, and Medical) band, whose frequencies are clustered around 2.4 GHz, could be used. Nevertheless, end-users must verify the availability of the spectrum for each specific case.
2. Media Access is a significant challenge [1]. Unlike wire networks, Ad-hoc network control is not centralized, and there is no synchronization time. Therefore, *Time Division Media Access (TDMA)* or *Frequency Division Media Access (FDMA)* schemes are not feasible, and most of the *Media Access Control (MAC)* protocols do not manage mobile nodes; hence the *Quality of Service (QoS)* is weak. Media access must be distributed fashion mobile nodes allow MAC protocols to maintain access in the same channel, whereas at the same time, avoiding collisions with neighboring nodes.
3. *Transmission Control Protocol (TCP)* performance [1] is vital, considering that it provides network flow and congestion control. TCP is a connection-oriented protocol; thus, a connection is required before the data transmission. TCP calculates RTT (Round-trip time) and the packet loss rate between the source and the destination nodes. TCP assumes all network nodes are static; therefore, it is not able to detect if the node relay mobility affects RTT or packet loss, which, in turn, becomes another Ad-hoc network challenge.
4. In terms of security ad-hoc networks are intranets [1]. Such communications are already isolated but not warded from attackers. Neighbor authentication is used to classify friend or hostile relay nodes, requiring encrypted and protected communications due to multiple node involvement. Packet origin and ID flow or label authentication are mandatory.
5. Last but not least, routing [1]. When used, mobile nodes link and break in an indeterministic way. Bellman-Ford route algorithm was used in early ad-hoc networks to perform and update routing information due to the random movement of the nodes and the network's topology continuous changes. Conventional wireless routing protocol performance proved to be insufficient for Ad-hoc networks, hence the need to improve protocols and adapt them to new topologies. State of the art provides various routing algorithms.

For this study, the important constrain is item #5. As mentioned in the introduction, the CTDL lacks a routing protocol. Hence, the initial requirement is to know the operational environmental conditions where the CTDL will perform to determine the routing protocol. This will allow the designer to determine the CTDL features such as network size, node quantity, node mobility features, as well as environmental conditions such as oceanic status, wind, etc.

Maritime Operational Environment

The CTDL project [6] describes the Colombian Caribbean Sea environmental characteristics addressing end-user needs. Its scope is to enhance the operational direction performance, sensor integration, and information exchange in case of natural disasters, maritime domain awareness, and contributing to decision-making processes.

Usually, maritime operations are carried out in groups of units (nodes for ad-hoc networks), which can be surface vessels, aircraft, or submarines, according to each specific situation. Transmission of tactical information among them is fundamental to have a real-time scenario that enables operations coordination. The system must be secure and end user friendly, regarding the appropriate bandwidth use, and all the required software and hardware tools to visualize standard operation picture and information exchange among participant units.

The CTDL scenario composition is four vessels, one submarine, and two aircraft (one helicopter and one airplane). The analysis is performed considering each unit as a node having specific behaviors such as speed and altitude sensors and variables affecting the network like the line of sight and distance between nodes.

Weather conditions can influence a TDL design and its routing protocol. Therefore, factors such as humidity, air salinity, high temperatures, rainy and dry seasons, and all typical tropical conditions must be considered.

Now, certain features need to be considered for routing protocols to be able to perform in the maritime environment CTDL.

A. End-User Needs.

Need detaches from the essential CTDL requirement:

- Allowance of any node to join the network automatically and freely at any time.
- Automatic network management.
- Automatic packet relay to guarantee communications between source, intermediate, and destination nodes.
- The node array capacity must share messages automatically to accomplish the assigned mission.
- Implemented routing protocols should be aware of processes involving node capability, mobility, and bandwidth consumption.

B Functions and management.

- Tactical information, including all exchangeable situation awareness messages to obtain a common scenario among participant nodes, upgrade information, configuration reports, change reports, position and contact reports, daily reports, and all kinds of correlation information.
- The network must contemplate media access criteria and requirements, QoS, to control and organize the Ad-hoc network, specifically the management of routing protocols.
- Standard messaging system to control and share information to and from the actuators and sensors.

C. System.

- It should operate in the range of HF, VHF, and UHF bands.
- Allow any node to join the network automatically at any time.
- Change network topology upon request.
- CTDL should maintain source-destination links even if the relay node fails.
- Automatic network management.

D. Integration capacity.

- To Surface vessels. Nowadays, the system is incorporated into the command and control system, and it requires integration with other ships, helicopters, or submarines in the operations area.
- To Submarines, when a submarine navigates at the surface, CTDL requires sharing actuators or sensors information with other units or nodes' and must allow command and control message exchange.
- To Helicopters, its role is essential in search and rescue, during tsunami disasters, etc. Like other units, helicopters are required to share tactical information with other nodes.
- To airplanes, Colombian Maritime Patrol Aircrafts (MPA) have no CTDL Capability yet, which is mandatory for search and rescue (SAR), shipwreck search and assistance, and

disaster assistance, among other operations. Likewise, airplanes require TDL capability to share tactical information of processes involving the Safety of Life at Sea.

These features determine the implementation design of the routing protocol. End-user-needs can show the network topology. Functions and management can rule the network's size and density. The system offers the electromagnetic spectrum and bandwidth usage. Finally, integration capability drives network node quantity.

A designed scenario is essential; the CTDL simulation model is composed of two surface vessel nodes, one submarine node, one helicopter node, and one airplane node, as described in Table 1. The design purpose is to establish a future simulated scenario capability. This model must have assumptions, *i.e.*, all nodes must be in the line of sight range, and nodes should establish communications in the same frequency even if there are different hardware brands.

From Table 1, and the CTDL features, it is possible to infer that:

1. Regarding network node mobility (items 1 and 8 in table 3), according to CTDL's configuration, it is considered a moderate and low-density network.

2. Regarding delays and latency (item 4 in table 3), they are mobile and have low speed compared to ground vehicles or aircraft [7] [8] [9], making latency, messaging delays, and route restoration manageable and tolerable. However, as nodes speed increases, these variables become critical due to faster changes in distances among distribution nodes.

3. Regarding Bandwidth usage (item 5 in Table 3), nodes have brand diversity of communications equipment, technologies, capabilities, and performances that would limit available bandwidth and communication channel use and consumption. These limitations impose additional tasks to control messages required for routing protocols operation.

4. Regarding the routing metric (item 6 in Table 3); As already mentioned, the CTDL network is not expected to be highly congested; therefore, the route selection criteria lead to choosing the shortest route, which is more reliable than the least busy.

5. Regarding size and node quantity (item 7 in Table 3), CTDL is a small network compared to standard TDL systems generated by NATO, where the networks can have from two to a range between 100 and 200 nodes or users (e.g., Link-22 [10], corresponding to the state of the art of naval TDLs, which can handle up to 130 stations). CTDL has 25 nodes, expandable up to 100 in the network. Due to network size and the light messaging load per-node, information traffic is not expected to be as high, facilitating broadband use.

6. Regarding Multicast capability (item 9 in Table 3), the directed transmission is not allowed due to the use of omnidirectional antennas. However, the system can broadcast, multicast, or unicast any communication as required. Nevertheless, the casting method is an optimization issue in

Table 1. CTDL Scenario Composition.

Node #	Type of Unit	Speed	Speed rate	Height	Bandwidth	LOS	LOS rate
0	Vessel 1	15 N	1	0 ms	Vhf/Uhf	20 Miles	1
1	Vessel 2	15 N	1	0 ms	Vhf/Uhf	20 Miles	1
2	Submarine	5 N	0,33	-2 ms	Vhf/Uhf	10 Miles	0,5
3	Helicopter	100 N	5	500 ms	Vhf/Uhf	60 Miles	3
4	Airplane	130 N	6,2	1500 ms	Vhf/Uhf	60 Miles	3

the sense that the load on messages changes with the type of broadcast.

7. Regarding power (item 13 in Table 3), consumption management is not required as part of the study since participating nodes or units have constant and unrestricted power source availability.

8. Regarding node relay capability (item 14 in Table 3), Ad-Hoc and TDL network nodes must be able to serve simultaneously as source and relay. CTDL design has this capability.

9. Regarding the use of route cache/table expiration timers (item 15 in Table 3), CTDL uses GPS information in its messaging to determine node position among the established network, as well as a synchrony tool when using TDMA as a media access technique; that is, the use of GPS could leverage in algorithms that require synchrony in expiration timers.

Routing Protocols

There are different routing protocol classifications, though Setup is the best known one. Kuosmanen [11] proposes other rankings based on various technical characteristics:

- Communications model. It depends on the channel usage: single or multiple.
- Structure, the nodes are uniform when all nodes receive and transmit in the same way, this structure is flat, and there is no pecking order. Otherwise, if the nodes are not uniform, there is a hierarchy structure, and each node routing is given by its neighborhood status.
- Information status. It is based on the way information is obtained and how nodes interact with each other. These protocols are called topological. Another classification criterion by destination; nodes store only topological information of its neighborhood nodes.
- Setup. This classification is the best known. It is called 'proactive' when information is continuously sent (Table-Driven) and reactive when information is irregularly sent (On-Demand).
- Transmission mode may be unicast or multicast.

Regardless of how protocols are classified, the classification depends on their specific use, and they can be classified independently of the model. This article is based on the Setup model and breakdowns, as shown in Fig. 2 [1] of "Table-Driven" and "On-Demand" systems.

Fig. 2. Routing Protocols.

Setup models are described as follows:

A. Proactive or Table-Driven Protocols.

Coya Rey [12] explains MANET as the use of packets to discover nodes in a network and the path to reach them from or to a specific node. A given supposition is that all routes are already defined and, at some point in time, used. So, a table works to maintain updated route information; the main merit is that route information is permanently available, providing an easy way to establish the path from/to nodes. One of the drawbacks in MANETS is the existence of high amounts of data at each node, causing the network to slow down and the update process to be sluggish, especially when links are broken.

Venkat [13] states that route protocols are implemented in small networks with a high traffic density because of the constant packet information flow. Below is a description of the principal route protocols.

- DSDV, Destination Sequenced Distance Vector., Elizabeth M. Royer [14], defines it as a "Table Driven" protocol based on the classic Bellman-Ford distribution. This mechanism was improved by dodging routing loops within the network.
  Every network node keeps a table with routing information, including all possible destinations, as well as its possible relay nodes. Therefore, route information will always be available regardless of the existence of the

source node requirement of that information. Each entry is tagged with a sequential number assigned by the target node. This allows the relay nodes to distinguish between a worn path and a new one, thus avoiding routing loops. Tables are updated permanently and sent to the network to maintain consistency, causing high network traffic, which negatively impacts network resources usage. Full dump table update packets are used to improve this issue. This sort of packages carries all routing information and requires multiple Network Protocol Data Units (NPDUs, Relay Nodes). During the network's low traffic periods, packets are occasionally transmitted. Incremental small packets are used only for information that needs to be used by a relay node that has changed since the last full dump into the network.

- WRP, Wireless Routing Protocol. Murthy [15] [16] describes this protocol, which addresses the issue of reaching free or direct links. It is a "Table Driven" protocol that keeps complete information in all network nodes. This model is a typical Route Discovery Algorithm, which in this case, avoids the issue of counting to infinite [17], forcing each node to perform a consistency check with all its neighbors on predecessor node information. This process eliminates loops and provides a quick convergence for route searching when links are broken. Each node must keep four tables:

    1. The distance table shows the number of nodes between source and destination.
    2. The routing table indicates the next relay node.
    3. The cost-link table reflects delays associated with a specific link.
    4. Relay Message List (LMR) table contains a sequential update message number, a relay count, a flag-vector acknowledgment with one entry per neighbor node, and a list of updates sent in the update message.

LMR records the refresh message updates that need to be retransmitted and the neighbor nodes that need to confirm relay, and so on. The algorithm decongests the network's traffic channeling information flow to the appropriate route instead of across the entire system.

Each node sends an update after it has processed the receiving information from its neighbors or when changes are detected in neighbor links. In the case of a broken link between two nodes, each one sends a message to their respective neighbors. Neighbor nodes modify the distance table, and the possibility of new routes through other nodes is verified. The new route is relayed to the source node with information to update tables to re-establish the link.

Each node notices the existence of a neighbor when it receives "acknowledgment" (AKG), among other messages. Inactive nodes must send a "hello" message to ensure connectivity. Otherwise, the resultant link failure will be misinterpreted as a false alarm. When a node receives "hello" from a new node, it joins the routing table, and the routing table sends an update message with the information from the four tables to the new node.

- CGRS *(Cluster head Gateway Switch Routing)*, unlike previous protocols, this is a flat organization. CGRS is hierarchical and uses a multi-hop cluster mobile network with various heuristic schemes. Ciang [18] mentions that with a cluster-type node, a code separation system between clusters, and channel access, it can achieve proper routing and bandwidth distribution. A distributed selection algorithm within the cluster chooses the head node. One drawback is frequent cluster head changes affecting overall protocol performance caused by busy nodes executing the selection process and, therefore, unable to perform their relay node task. Thus, instead of invoking a re-selection method, each time cluster membership changes, the head in the "Least Cluster Change" (LCC) algorithm only changes when two cluster heads come into contact or when a node goes out of range from all other cluster heads.

  CGSR is based on the DSDV protocol,

consequently with the same DSDV high traffic load. However, CGSR includes a modification with an approximation to a hierarchical routing from cluster head node to output gate node (output gate node is a cluster relay node, named by the author) in traffic from source to destination node. Output gate nodes are within the communication range between two or more cluster head nodes. The source node sends a packet to accomplish communication between the source and the destination node, and it is first routed to a cluster head node, which relays the packet to another cluster head node using the relay provided by the output gate node. The process continues until the packet reaches the destination node. When using CGSR, each node must have a cluster membership table where the network cluster head destination nodes store the information. These tables are periodically spread through the DSDV protocol; all nodes update the cluster membership table through the transmission from one of its neighbor nodes. In addition to the cluster membership table, each node must have a routing table to determine the next relay node to reach the destination node. When a packet is received, the node's cluster membership table and cluster routing table identify the closest cluster head node in route, then the routing table determines the next relay node to reach the specified closest cluster head node and transmits the packet to it.

B. Reactive or "On Demand" protocols.

Grady [4] defines this category as protocols that only create routes within the network when a source node demands it. Once a route is established, it is kept by a maintenance procedure until the destination becomes unreachable or the route is no longer needed. Coya Rey [12] mentions that On-Demand protocols fit best in small networks with low nodes and static traffic patterns in a highly mobile system.

Shobana [19] argues that such protocols compared to proactive ones have higher power consumption and a more significant message delay; flexibility in operations is accomplished by reducing route loads considering that no loops form in TDL networks.

- (AODV, Ad Hoc On-Demand Routing Protocol) Taneja [20] mentions that this is a variation of the previously described DSDV protocol. AODV minimizes the system requirement to broadcast the entire network up to the endpoints. Routes among network nodes are not permanent. The protocol searches for routes when required, which are kept active while being used. Taneja also points out the key steps to establish an AODV protocol are the following:

  1) Route creation verifies if there is an established route in the tables. If no path is available, the source node sends a ROUTE Request (RREQ) packet containing the IP address, current sequential number, destination IP address, destination node last sequential number, and emission ID. Sequential numbers control the message timeline. Once RREQ is broadcasted to all neighboring nodes, a time count to wait for response initiates. Upon RREQ reception, each relay node receives the request and prepares a route that is returned to the source node. Once the RREQ packet reaches its destination with the route creation information, it is returned with an RREP (Reply Route) message.
  2) *Search ring expansion technique*. The source node sends an RREQ packet to all neighboring nodes and relays, which successively do the same with their adjacent nodes. RREQ emission control is mandatory in vast networks. To perform this control, the source node uses a search ring expansion technique, which establishes a *time-to-live* (TTL) with an initial defined value. If there is no response during this search period RREQ packet is broadcasted again with an increased TTL value. TTL value will increase progressively until the default threshold is reached, ensuring the RREQ packet is posted to the entire network.
  3) Route Setting. When destination and relay nodes with the route receive an RREQ,

an RREP is created and broadcasted in a single direction towards the source node using the path back to the node from which RREQ information was received. When relay nodes receive an RREP, a new entry for the destination route is set in its route table. When the RREP message reaches the source node, the path from destination to source node is set; therefore, the source node can start transmitting.
4) Route Maintenance, the path between source and destination nodes is kept as long as the source node requires it. Considering that Ad Hoc network nodes are mobile and that source node moves during the active session, the route search process must be performed again to establish a new path between source and destination nodes. Conversely, if the destination node or relay nodes move, the link can be broken. The node where a broken link occurs initiates a string with the route error message (RERR, Route Error) to the affected neighbor node, which consequently propagates the RERR to its predecessor node. This process continues until the RERR message reaches the source node. Once it is received, the source node can stop broadcasting or restart the route search mechanism by sending a new RREQ message if the route is still required.

- DSR, Dynamic Source Routing. Coya Rey [12] defines it as a protocol that bases are routing on the source. Each node has a local cache to store information related to the desired route in the network. There are two possibilities for caching in each node. The first one is the path cache in which each node stores its path to the other node, and binding cache, in which each node adds a link to a graph that represents the node's perspective in the network topology. Links obtained from different routes could form new routes, so the binding cache handles more information than the path cache. Taneja [20] states that this protocol is appropriate for mobile networks requiring relay nodes. The main benefit is that there is no need for a route table because the route is contained in the header of each packet sent. DSR performance is better in a static or low mobility environment. Among its disadvantages is the fact that broken links do not self-repair; this causes the most significant delay in resetting routes, taking more time than a table-based protocol. Another drawback is that each node spends considerable processing time obtaining control route information, even when there is not a destination node. This protocol has two fundamental components:

1) Route Discovery. As mentioned above, each node has a cache where it stores the most recent route searches. When a node wants to send information packets to another node, it must verify its entry in the cache. If there is access, then that route is used to transmit, and the source address is added to the packet. If there is no access while verifying the threshold or timeout has expired in the cache memory, the source node issues a route requirement packet to all neighboring nodes querying about the route to the destination, and it must wait until the path is found.

Meanwhile, the source node could execute other functions, such as forwarding packets. When the request packet reaches any relay node, it is compared to its cache or that of its neighbors to find if the destination route requirement is known or not. In case it is known, the node sends a response packet to the destination node. If unknown, the node will continue sending the same path request packet as when establishing a discovered route; the source node sends information on the destination path. The protocol adds a cache entry for future use; each node keeps the time information since the last cache entry to the actual one to know whether it is recent or not. When a packet reaches a relay node, it checks whether the packet is destined to it or not, in case it is a response packet sent; if not, the packet is forwarded as it is.

2) Maintenance. This process should be able to detect in active route or in the network if the topology has changed in such a way that

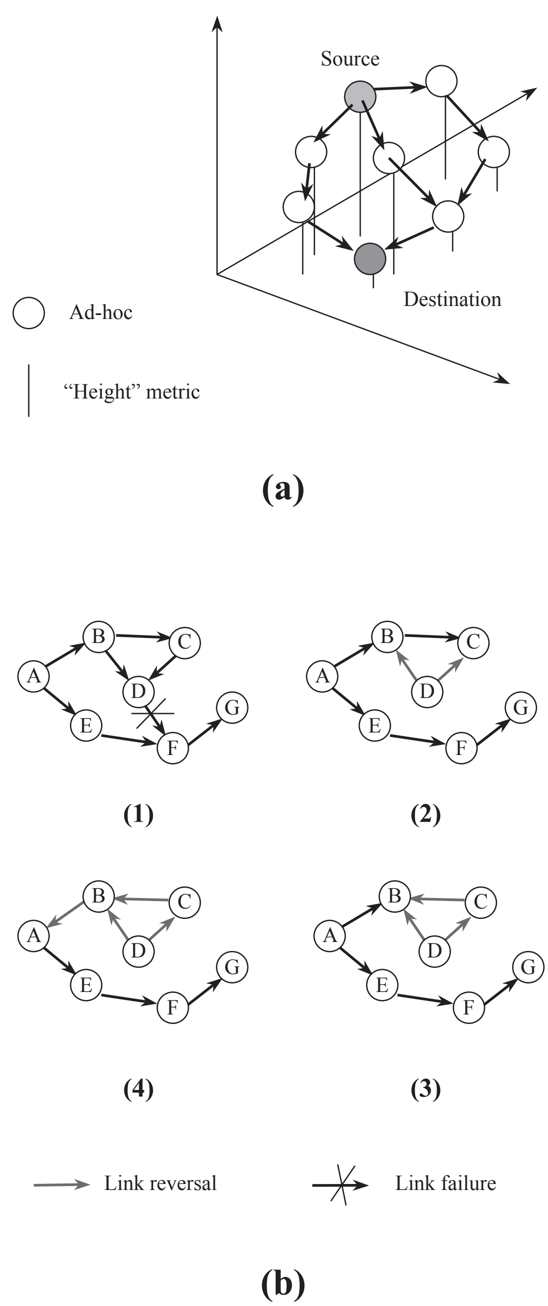
the established route is no longer available or its links do not work. At this point, the node where a fault is detected verifies if another known route to the destination exists; if not, it starts a new route search process. Either way, each node will change the entry path in the cache. The maintenance process works only during the route active time period.

- TORA, Temporally Ordered Routing Algorithm. Royer [14] defines it as a highly adaptive, non-linking, and distributed algorithm, based on the inverted link concept, designed to perform highly dynamic movable networks. Toh [1] describes the TORA protocol in section 5.8, based on the control packets broadcasting, focused on a small group of nodes close to the occurrence of a topological change in the network. The nodes must keep information about the routes of neighboring nodes to achieve this protocol goal. The protocol executes three main activities, searching or discovering the route, maintaining the route, and finally, deleting the route. During the creation and maintenance phase, the protocol uses a metric called "height," which assigns an acyclic direct graph to the destination node. Each link between the nodes sets a specific address above and below, related to the height of its neighboring nodes. Fig. 3 [1], taken from the same section of the Toh book, shows (a) the search process and (b) the maintenance process.

  If a link breaks during the maintenance process while the route is active, a new route discovery process to the destination node initiates, as shown in Fig. 3 part (b). In case of failure of the last descent direction link node, the protocol generates a new height reference, which is propagated to its neighbors. The links must invert to reflect the changes and to adapt to a new height. This also occurs if a node does not find a downlink (i.e., no longer finds neighboring nodes). The time factor is critical in this protocol because the determination of the "Height" metric depends on the logical time or time when a link breaks. TORA assumes that all nodes have synchronized clocks (probably by a GPS clock).

  The metric used by this protocol has five components (1) Logical break time, (2) unique node ID that defines the new height, (3) bit reflection indicator, (4) Propagation order parameter, and (5) unique respective node ID.

Fig. 3. (a) Route Creation, (b) Route maintenance in TORA.



Height is collectively represented by the first three, and a new height is defined whenever a node loses its downlink due to failure. In the deleting phase, this protocol floods the network broadcasting a CLEAR packet (CLR) to clear the invalid routes.

Taneja [20] mentions that this protocol uses arbitrary Height parameters to determine the direction of the link between two nodes, thus obtaining multiple paths for the same destination, none of which is necessarily the shortest. Additionally, when a node discovers that a route is no longer valid, it adjusts its height to the maximum value between neighboring nodes and thus transmits an update packet "UPDATE." If no neighbor nodes with a finite height concerning the destination are present, then it will start the process of discovering a new path that was already described.

Taneja [20] states that some of the benefits of TORA are the control of multiple routes between source and destination nodes, as well as the short time required to re-establish communication when a failure occurs by switching to another path. One of its disadvantages is that it involves clock synchronization among all network nodes. In order for this to work, it presumes that status detection, neighborhood discovery, packet delivery, and address resolution capabilities are easily accessible.

C. Hybrid Protocols.

According to Coya Rey [12], Hybrid protocols mix proactive and reactive protocols. This type of routing is performed by "cluster," i.e., intradomain and interdomain simultaneously. Proactive protocols serve for communication inside a cluster, and reactive protocols, for communication between clusters. Zone-based or cluster protocols are used in large networks with many nodes. Some examples of these protocols are the Zone-Based Routing Protocol (ZRP) and the Adaptive, Hybrid Adaptive Routing Protocol (SHARP), among others.

Zone-Based Routing Protocol (ZRP). According to Toh [1], ZRP uses the merits of reactive and proactive protocols. Routing zones are similar to a cluster, but each node acts as a zone head and, at the same time, as a member of other clusters or zones.

Zones can overlap; each node specifies a radius in terms of radius nodes; the selection of the zone size has a significant impact on the performance of the Ad Hoc network.

Coya Rey [12] mentions that in order to build a zone, each node that is one hop away and could be reached directly has to be identified. The "Neighbor Discovery Protocol" (NDP) is responsible for controlling and searching routes and indicating when a route fails. This protocol broadcasts a query packet with the message "HELLO" at a specific interval. When zone nodes identify it, route tables are modified and updated.

The radius of length x determines zone dimensions, x indicates the number of hops from the source node to the zone edge, and it is also tied to the node emission power and other parameters. The protocol performance depends on the length of the x-radius that determines the zone area: small radius for small zones in dense networks that have high mobility nodes, and larger radius for more extensive areas, dispersed systems, and low mobility nodes.

Toh, [1] in section 5.12 states that ZRP handles three sub-protocols, (a) table-driven, called IARP Intrazonal Routing Protocol, (b) Interzone Routing Protocol (IERP Interzone Routing Protocol), and (c) Border cast Resolution Protocol (BCRP). Implemented IARP uses the "Link State" or Routing Distance Vector, across the border in the routing zone disseminating information. IARP depends on the NDP protocol to detect the presence of neighboring nodes, therefore node-link connectivity, if any. Its primary mission is to ensure that each node in the zone has a consistently updated routing table that reflects the information of how each node in the zone is able to reach other nodes. IARP relies on edge nodes to execute on-demand routing to find information about nodes outside their zone. IERP uses the BCRP protocol in replacement of the query message "HELLO" when propagating within another zone.

According to Haas [36], one consideration about ZRP is that it handles different protocols according to zones, and this affects the performance efficiency of interzonal communication, and the route search can be unstable and challenging. Without proper query control, ZRP can have reduced performance than typical protocols based on "flooding." Inside a zone, a route failure due to node mobility is treated with a proactive protocol; the node reports the loss to every zone node, which, upon information reception, update their route tables. If route failure is due to an edge node or a different zone node, route repair runs like a new route search. In the worst case scenario, the failure route message is sent to the source node.

The last lines describe the protocol operation and compare the algorithm's main characteristics. Now some differences will be exhibited. Time complexity is smaller in WPR than in DSDV because the latter informs only the neighboring nodes about the link status changes when a link fails. When additional links are established, the "HELLO" packet is used as a presence indicator to allow the entry to update the routing table affecting the neighboring nodes exclusively.

In the CGSR, the routing performance depends on the status of specific nodes (cluster heads, output nodes, or normal nodes). Link failure time complexity is associated with a cluster head and is higher than in the DSDV protocol due to the need for extra time to select a new cluster head. In the same way, this applies to the selection of new nodes links that are associated with cluster heads.

In terms of communications complexity, since the DSDV, CGRS, and WRP use shorter Path Distance Vector protocols, all of them have the same degree of complexity during link breakouts and additions.

Reactive Protocols comparison in Table 4 shows that the AODV protocol, like the DSR, use the same procedure to find a source to destination node path. However, it differs from the fact that DSR has a higher load in each used packet to carry established route information. In contrast, the AODV only carries the destination route information. This also happens with packet responses and in-memory loading of each protocol. AODV is the only compared protocol that can perform multi-broadcast.

The requirement of link symmetry between nodes is a drawback of the AODV protocol being unable to use asymmetric links routes, unlike DSR, which is able to use asymmetric links when symmetric ones are not available.

The DSR [23] protocol performs best on moderate mobility nodes networks concerning packet transmission latency, and this presumption provides a small network diameter, which allows all nodes to become receiving nodes. Hence, the network management software receives any packet without a filter or restriction provided by the destination address.

The DSR does not perform periodic broadcasting requirements saving bandwidth and power consumption. Therefore, this protocol is not overloaded when there are no network topology changes. Additionally, it allows each node to keep information of all routes established to the destination node in its cache. Thus, when a link is broken, relay nodes can check their cache for another path. If not found, the protocol invokes the algorithm to find a new route. In the DSR, the recovery of a route is faster than in other algorithms. However, due to the DSR small diameter, it is not scalable to vast networks.

The TORA is an "inverted link" type algorithm, according to Park [24]. This protocol is best suited to large networks with a dense node population. DSR and TORA are the only two protocols capable of establishing more than one route between the source and destination nodes. Rebuilding routes is not necessary until all possible paths have been considered valid. Therefore, bandwidth is retained. Another advantage of TORA is the multicast capability, which, unlike in AODV, is

Table 2. Comparison of Reactive Protocols.

Metric	PERFORMANCE AREAS		Reactive PROTOCOLS AODV	DSR	TORA
I. Package Sent Ratio	1	Network mobility		Moderate related to latency	High mobility
	2	Route type.	On-demand.	Multiple.	Multiple.
		Shorter/more congested ratio	Always selects the least congested route.		
		Complexity in time	Initialization 0(2d), fails 0(2d)	Initialization 0(2i) Post fails 0(2d) or 0*.	Initialization 0(2i) Post fails 0(2d)
		Complexity communications.	0(2N)	0(2N)	Initialization 0(2N) Post fails 0(2x)
	3	Network and route information Availability	Available when needed	Available when needed	Available when needed
II. TDL Delays between the source node and the destination node.	4	Delays and latency	Higher message delay than proactive in the route discovery process,	Higher message delay than proactive in the route discovery process,	Higher message delay than proactive in the route discovery process,
	5	Bandwidth Consumption	Higher than usual due to the issuance of the HELLO message.	Low consumption	Just as the DSR is smaller
	6	Route Metric	Freshest and shortest path	Shortest path	Shortest path
		Route Maintenance	Route Tables	Route caches	Route Tables
		Multi-route possibilities	No	Yes	Yes
		Route Reconfiguration	Delete route; notify the source	Delete route; notify the source	Link reversal; route repair
		Periodic route update	Not Required	Not Required	Not Required
III. Loading in messages	7	Network size and number of nodes	Small, few nodes	Small, non-scalable for large networks, few nodes	Small, It handles high node density
	8	Traffic associated load. frequency TX/RX	Static	Static	Static
	9	Multicast Capability	Yes, even motion nodes.	Yes	No, but, supports through LAM (*4),
	10	Routing Philosophy and Critical Nodes	Flat, No	Flat, No	Flat, No
	11	Message load	It does not set additional loads on the network	Proportional to the distance of the link/ carries all the complete information of the route / s	
		Reaction to link failures	Quickly responds to topologic changes.	Does not repair the links locally reset is longer than proactive	Quickly, but if it has to restart, the discovery process is the slowest.
		Net Saturation	Saturated due to the flooding technique.		
		Signaling traffic generated	Grows with the increasing mobility of active routes		
	12	TX update Frequency and Updates TX to:	N/A	N/A	N/A

IV. Energy consumption	13	Power consumption		Hight power consumption	
V. General features that do not affect performance	14	Exclusively dedicated capacity of relay nodes	Not simultaneous due to nodes detecting emissions between each other.		
	15	Clock synchronization			Needs Synchronization time
	16	Loop free	Yes	Yes	Yes

Table 3. Comparison of Proactive Protocols.

Metric	PERFORMANCE AREAS		Reactive PROTOCOLS		
			DSDV	CGRS	WRP
I. Package Sent Ratio	1	Network mobility		High density	
	2	Route type.	The ones on the TABLE	The ones on the TABLE	The ones on the TABLE
		Shorter/more congested ratio	Shorter route selection	Shorter route selection	Shorter route selection
		Complexity in time	0(d)	0(d)	0(h), Low compared to DSDV
		Complexity in communications.	0(x = N)	0(x = N)	0(x = N)
	3	Network and route information Availability	Nodes have route information in two tables regardless of need. (*1).	Nodes have route information in two tables regardless of need. (*1). It is hierarchical, and a node at some point cannot be a relay node.	Nodes have route information in four tables regardless of need. (*1).
II. TDL Delays between the source node and the destination node.	4	Delays and latency		Less delays than reactive	
	5	Bandwidth Consumption	Can be higher because of the use of tables	Can be higher because of the use of tables	High because of the need to be sending Hello packets
	6	Route Metric	Freshest and shortest path	Shortest path	Shortest path
		Route Maintenance	Route Tables	Route Tables	Route Tables
		Multi-route possibilities	Yes	Yes	Yes
		Route Reconfiguration		No need route already reconfigured in the tables.	
		Periodic route update	Required	Required	Required
III. Loading in messages	7	Network size and number of nodes	High- permanent route availability limit the number of nodes that can connect to the network grows in an O(n2) order.	Small, few nodes can be connected	High due to the permanent availability of routes.
	8	Traffic associated with load and frequency of emission and reception		Inefficient due to the need to be periodically transmitting a network update regardless of how many times the network topology changes	
	9	Multicast Capability	No	No (4*) does it through a sub-algorithm	No

	10	Routing Philosophy and Critical Nodes	Flat, No	Hierarchical,	Flat (*4), No
	11	Message load		Equal to the DSDV/ WRP, the load is even higher because it requires maintaining four tables.	
		Reaction to link failures	The updating process is slow because it has a lot of information on each node, significant when the link is dropped. / DSDV Requires constant updating as there are no changes in the topology.		
		Net Saturation	Not saturated		
		Signaling traffic generated	Higher than reactive routing		
	12	TX update Frequency and Updates TX to:	Periodically and as needed. Neighbors	Periodically and Neighbors and cluster head	N/A Periodically and as needed. Neighbors
IV. Average energy consumption	13	Power consumption	Moderate power consumptions, eventually high		
V. General features that do not affect performance	14	The exclusively dedicated capacity of relay nodes			
	15	Clock synchronization	No need	No need	No need
	16	Loop free.	Yes	Yes	Yes, but not instantaneous

not incorporated in the essential operation but performed by means of a dedicated sub-algorithm called Lightweight Adaptive Multicast Algorithm (LAM). TORA and LAM enable the multicast capability. TORA depends heavily on node clock synchronicity. Network nodes must have a GPS or any other mean to control time to allow performance.

Route recovery is not as expeditious in TORA as in other protocols due to potential oscillations within this period, which can cause long delays until a new route is determined.

Proactive protocols are based on routing tables that store information for all possible routes demanding this information to be broadcasted continuously or table updates being issued. These activities require higher power consumption, broader bandwidth, and produce considerable delays. These demands provide the advantage of more robust links that remain without breakouts for much longer.

Information management based on demand corresponds to reactive protocols, so their efforts are materialized only when necessary, either to establish a new route or to repair a broken link. Reactive protocols' advantages are low power consumption, less data traffic improving bandwidth exploitation. However, unlike proactive protocols, these routes are less robust, and rebuilding routes takes much longer, causing delays or link loss. Finally, this comparison will be analyzed later for benchmarks and the simulation process to meet the main objective of this work, which is to recommend as far as possible the best protocol to be implemented in the CTDL.

Conclusions and future work

In reactive protocols, broadband usage is optimized because of less load on messages. On-demand traffic, no requirements for continuous updates, and low traffic assure the protocol's excellent performance. Thus, reactive protocols perform better than proactive ones in the update and link-breaking recovery processes since the proactive ones require constant table updating, and therefore information traffic becomes congested. Among reactive protocols, TORA and AODV have the multicast capability, while among proactive protocols, only the CGRS has this capability through a secondary algorithm. Bandwidth consumption is lower, especially in TORA and DSR, because the messages are only sent on demand, in contrast with them being sent continuously in proactive protocols.

All the routing protocols keep links between nodes as long as route information is maintained; however, Table-Driven protocols work better because the information is always available. Considering the aforementioned theoretical performance algorithms, it can be concluded that proactive protocols have a lower delay in messaging. Another advantage of proactive protocols is that they usually select the shortest path, which is the most powerful to create stronger links. Regarding node quantity, relatively few protocols have improved performance, particularly the DSDV protocol.

There are many features of routing protocols that are not actually usable by the network posed in this maritime scenario, as well as others that would not differ in their implementation, such as power usage because the participating nodes have a constant power supply. Both reactive and proactive protocols perform well in small networks of moderate traffic and low density, but as the system grows in density and traffic, advantages and disadvantages show up. In terms of latency, routing protocols would be well implemented on the network because actual usage dynamics allows delays for up to two minutes without being critical. The CTDL implemented features clock synchronization via GPS used to determine node position and media access control when required. This capability would be available if the TORA protocol is implemented. Regarding network size for simplicity purposes, flat and non-hierarchical protocols should be implemented.

This study allows us to infer that reactive protocols might work better than proactive protocols in CTDL, mainly because of bandwidth consumption. This issue is critical because of the hardware limitations mentioned in the CTDL for maritime scenarios. Hence, according to the analysis for this type of reactive protocol (On-Demand), the DSR might perform better.

Validation of this preliminary study employing a simulation tool that allows for adjustment of results with the obtained data is required as future work.

Bibliography

[1] C.-K. TOH, Ad Hoc Mobile Wireless Networks, Protocols and Systems, Upper Saddle River, New Jersey: Prentice-Hall, 2002.

[2] S. M. L. S. M. T. GUSTAVO PEREZ VALDEZ, "Desarrollo de un Enlace de Datos Tactico, Fsae 1: Prototipo," COTECMAR, Cartagena, 2012.

[3] I. BOLT BERANEK AND NEWMAN, "A History of the ARPANET," DARPA, Arlington, Virginia, 1981.

[4] J. P. O. GRADY AND A. MCDONALD, "State of the Art: Ad Hoc Networking," *M-Zones Deliverable 1*, vol. State of Art Surveys, no. 2, pp. 16-26, Mayo 2003.

[5] C. L. G. JR., "Data Link Communications Tactical Air Command and Control Systems," *IEEE JOURNAL SELECTED AREAS IN COMMUNICATIONS*, vol. SAC 3, no. 5, pp. 779-790, 1985.

[6] J. M. GOMEZ T., W. A. CASTRO C, G. PEREZ V, S. MARRUGO LL. AND J. VILLEGAS D, "Codesarrollo de un Sistema De red Tactica Naval .....," COTECMAR, Cartagena, 2015.

[7] B. TANG, BAOLIU YE, L. SANGLU, G. SONG AND I. STOJMENOVIC, "Latency-optimized Broadcast in Mobile Ad Hoc Networks without Node Coordination," in *MobiHoc 2014*, Philadelphia, PA, USA, 2014.

[8] K. A. JAGADEV, K. B. PATTANAYAK, K. M. MISHRA AND M. NAYAK, "Power and Delay Aware On-Demand Routing For Ad Hoc Networks," *IJCSE International Journal of Computational Science and Engineering*, vol. 02, no. 04, pp. 917-923, 2010.

[9] M. GERLA, L.-J. CHEN, Y.-Z. LEE, B. ZHOU, J. CHEN, G. YANG, AND S. DAS, "Dealing with node mobility in Ad Hoc wireless. Network," UCLA, Computer Science Department, Los Angeles, California, 2005.

[10] NORTHROP GRUMMAN, LINK 22 Guidebook Overview, San Diego, California: Space & Mission Systems Corp., 2010, p. 120.

[11] P. KUOSMANEN, "Classification of Ad Hoc Routing Protocols," Helsinki.

[12] L. COYA REY, T. O. LEDESMA QUIÑONES AND W. BALUJA GARCIA, "Protocolos de enrutamiento aplicables a redes MANET," *REVISTA TELEM@TICA*, vol. 13, no. 3, pp. 59-74, 2014.

[13] M. VENKAT AND N. KASIVISWANATH, "Routing Protocols for Wireless Mesh Networks," *International Journal of Scientific & Engineering Research*, vol. 12, no. 8, 2011.

[14] C.-K. T. ELIZABETH M. ROYER, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46-55, April 1999.

[15] S. MURTHY AND J. GARCIA-LUNA-ACEVES, "A Routing Protocol for Packet Radio Networks," *Proceedings of ACM First International Conference on Mobile Computing & Networking MOBICOM95*, Noviembre 95.

[16] S. MURTHY AND J. GARCIA-LUNA-ACEVES, "An efficient Routing Protocol for wireless Network," *ACM Mobile Networks and App. J.*, no. Special on Routing In Mobile Communication Network, pp. 97-183, Octubre 1996.

[17] A. TANENBAUM, Computer Networks, vol. 3, Englewood, New Jersey: Prentice-Hall, 1996, pp. 357-358.

[18] C. -C. CHIANG, "Routing In Clustered Multihop, Mobile Wireless Networks with Fading Chanel," in *IEEE SICON 97*, Singapore, April 1997.

[19] M. SHOBANA AND S. KARTHIK, "A Performance Analysis and Comparison of various Routing Protocols in MANET," in *Proceedings International Conference on Pattern Recognition, Informatics and Mobile Engineering*, Tamilnadu, India, 2013.

[20] S. TANEJA AND A. KUSH, "A Survey of Routing Protocols in Mobile Ad Hoc Networks," *International Journal of Innovation and Technology*, vol. 1, no. 3, pp. 279-285, August 2010.

[21] M. SHOBANA AND S. KARTHIK, "A Performance Analysis and Comparison of various Routing Protocols in MANET," in *International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)*, Tamilnadu, India, 2013.

[22] H. T. DUYEN, W. BENJAPOLAKUL AND P. D. MINH, "Performance evaluation and comparison of different ad hoc routing protocols," *Computer Communications*, pp. 2478-2496, 4 May 2007.

[23] D. JOHNSON AND D. MALTZ, "DYNAMIC SOURCE ROUNTING IN AD-HOC WIRELESS NETWORKS," in *Mobile Computing*, T. Imielinski, and H. Korth, Kluwer, 1996.

[24] V. PARK AND M. CORSON, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in *INFOCOM 97*, Kobe, Japan, 1997.

[25] S. MURTHY AND J. GARCIA -LUNA-ACEVES, "Loop-Free Internet Routing Protocol Using Hierarchical Routings tress," in *INFOCOM '97*, Kobe, Japan, 1997.

[26] C.-C. CHIANG, M. GERLA, AND L. ZHANG, "Adaptative Shared Tree Multicast in Mobile Wireless Networks," in *GLOBECOM 98*, Sidney, Australia, 1998.

[27] L. JI AND M. CORSON, "A lightweight Adaptive Multicast Algorithm," in *GLOBECOM 98*, Sidney, Australia, NOV-1998.