CERIAS Tech Report 2002-27

HIERARCHIAL MOBILE WIRELESS NETWORK

by Yi Lu and Bharat Bhargava

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907

Hierarchical Mobile Wireless Network (HMWN)*

Yi Lu and Bharat Bhargava
Center for Education and Research in Information Assurance and Security
and
Department of Computer Science
Purdue University
West Lafayette, IN 47907, U.S.A.
{yilu, bb}@cs.purdue.edu

Abstract

Ad hoc networks may not be suitable for "non ad hoc" applications due to resource, mobility, traffic pattern and incompatible wireless MAC protocols issues. We propose the Hierarchical Mobile Wireless Network for providing flexible and scalable network services to these applications. In such a system, mobile hosts are organized into hierarchical groups. Four basic operations that are used to set up and maintain the network structure are described. An efficient protocol for group membership management is discussed. The Segmented Membership-based Group Routing protocol is presented. In this routing protocol, only local message exchanging is required. Simulation-based experiments confirm the scalability of our design.

Keywords

wireless, mobile, ad hoc, hierarchical, architecture, routing

I. INTRODUCTION

Mobile wireless networks provide users with maximum flexibility. In such networks, there is no fixed, wired infrastructure. The applications of mobile wireless networks include, but not limit to, national security operations, rescue missions, and military communications. Currently, most research efforts in this area focus on Ad hoc networks. However, many applications are not totally "ad hoc" (e.g., military communications in a battle field). Ad hoc networks may not be suitable for this kind of applications due to the following issues [1].

Resource: In an ad hoc network, all hosts are assumed to have equal capabilities (i.e., all hosts are equipped with identical communication devices and are capable of performing functions from a common set of networking services) [2]. For battle field applications, most mobile hosts are portable computing facilities such as PDA, GPS, notebook computer, etc., with portable wireless communication devices. These computing facilities have limited system resources and low computing capabilities. Lightweight batteries may power these facilities along with their communication devices. The weak power and the limited battery life will impose restrictions on the transmission range, communication activity, and computational power of the communication devices. Such mobile hosts can hardly afford the overhead of providing network services. On the other hand, there may be some movable workstations (e.g., mounted on tanks), which are powered by heavy-duty batteries, equipped with high-speed communication devices. These workstations should be utilized to provide reliable network services.

Mobility Model: Ad hoc networks assume each host moves randomly and independently. Hence, the random mobility model [3] is commonly used in the study of Ad hoc networks. According to this model, the speed and direction of the motion in the new time interval have no relation to those of the motion in the previous time interval. In the battlefield, soldiers in the same company usually move to the same trajectory at the same speed from the perspective of a battalion or a brigade, because the members among a group tend to coordinate their movements. The Reference Point Group Mobility (**RPGM**) model [4] is closer to the real world than random mobility model. RPGM partitions the network into several groups. Each group has a logical center. The center's motion defines the motion of the entire group. Each node in a group has independent random motion in addition to the group's motion.

Traffic Pattern: In an ad hoc network, the traffic pattern is random, any pair of hosts may communicate. The reality is that a small percentage of hosts in a domain are communicating outside of the domain at any given time. Many (if not most) hosts never communicate outside of their domain [5]. For example, it is much more likely that communication will

*This research is support by CERIAS and NSF grants CCR-9901712 and CCR-0001788.

take place between two soldiers in the same battalion, rather than between two soldiers in two different brigades. To take advantage of this kind of traffic pattern, the design of networks should give priority to intra-domain communications.

Different Wireless MAC Protocols: Ad hoc networks assume all mobile hosts use compatible wireless MAC protocols because any two of them may communicate directly. In large scale applications, different wireless protocols, such as bluetooth, 802.11 protocol set, or satellite, may be used and they may be incompatible. It is desirable that the network is capable of providing simultaneous and seamless support for different MAC protocols. Of course, special hosts are needed to forward packets between two groups that use incompatible protocols (like routers in wired networks).

Taking the above discussion into consideration, we propose the Hierarchical Mobile Wireless Network (**HMWN**). The rest of the paper is organized as follows. Section II introduces related work. The network architecture and four basic operations are described in section III. The detail of an efficient membership management protocol is presented in section IV. The Segmented Membership-base Group Routing protocol is proposed in section V. In section VI, a simulation evaluation and its result is discussed. Section VII concludes the paper.

II. Related Work

Many research efforts are trying to introduce structures on ad hoc networks to provide scalable solutions for routing, location management, and resource allocation, etc. Professor Haas at Cornell University proposed the Zone Routing Protocol (ZRP) [6], where every mobile host maintains a routing zone. Researchers at University of Maryland at College Park introduced a clustering scheme for hierarchical control in wireless sensor networks [7]. An applicable hierarchy for multi-hop wireless networks for quality-of-service support is proposed in literature [8]. Most schemes assume that ad hoc networks are self-organized to discover maintain the structure. It requires extra message exchanges that may consume a big portion of the limited bandwidth. Our design utilizes the mobility model and traffic pattern to guide the establishment and maintenance of the group hierarchy, which introduces little protocol overhead. The incompatible wireless MAC protocols are addressed in the design.

III. The Network Architecture

In this section, we present the architecture for HMWN and the basic operations in a HMWN system.

A. Definitions

We present a set of definitions that will be used in the rest of the paper.

Definition III.1: A *group* is a set of mobile hosts. Each group has one representative (i.e., *agent*). A group is denoted as *group(A)*, where A is the agent. A host can not be an agent for more than one group. The Home Group (**HG**) is where the mobile host registers its membership. A Foreign Group (**FG**) is a group other than the HG. The Current Group (**CG**) is the one that the host currently attached. The corresponding group agents are called Home Group Agent (**HGA**), Foreign Group Agent (**FGA**), and Current Group Agent (**CGA**), respectively.

For every mobile host, its HG is assigned by "Grouping" operation.This relationship keeps unchanged during the life-time of the network. A mobile host's CG is changed when the "Migration" operation completes (section III-C).

Definition III.2: The groups in a HMWN system form a group hierarchy. The level of a group G represents how close it is to the root of the hierarchy, which is denoted as *lv(G)*. The lower the level is, the closer the group is to the root. The level of the root group is 0. Suppose the agent of group G_1 is a non-agent member of group G_2, then $lv(G_1) = lv(G_2) + 1$. If MH is a mobile host in group G, the level of MH is

$$lv(MH) = \begin{cases} lv(G), & \text{MH is the agent of group G;} \\ lv(G)+1, & \text{otherwise.} \end{cases} \quad (1)$$

Definition III.3: A group G_1 is a subgroup of group G_2 if and only if

1. the agent of G_1 is a non-agent member of G_2
2. or the agent of G_1 is a non-agent member of one of G_2's subgroups.

G_2 is thus a supergroup of G_1. Operators *sub(G_1, G_2)* and *sup(G_2,G_1)* are used to denote that G_1 is a subgroup of G_2 and G_2 is a supergroup of G_1, respectively.

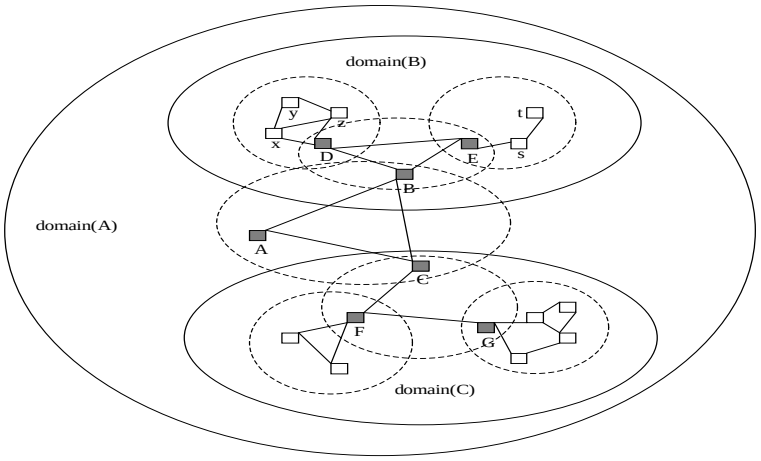

Fig. 1. Hierarchical Mobile Wireless Network

Definition III.4: A domain derived from a group G consists of and only consists of G and all its subgroups, denoted as *domain(G)*. The agent of G is also the domain agent of domain(G). Derived domains have the following property.

$$domain(G_1) \subseteq domain(G_2) \Longleftrightarrow sub(G_1, G_2) \tag{2}$$

Definition III.5: A closure domain of two groups G_1 and G_2 *closure(G_1,G_2)* is the smallest derived domain that contains G_1 and G_2. Formally, closure(G_1,G_2) = domain(G) if and only if

1. $G_1 \subseteq$ domain(G) and $G_2 \subseteq$ domain(G)
2. Derived domain(G') satisfies condition 1 $\Longrightarrow$ domain(G) $\subseteq$ domain(G')

B. An Example

Figure 1 is an example of the HMWN system. Every small square represents a mobile host and the dark ones are group agents. A solid line between two mobile hosts represents the wireless link. The dashed line circles represent groups and the solid line circles represent derived domains. The root group only contains three members $\{$A, B, C$\}$, where A is the agent. There are two level 1 groups, $\{$B, D, E$\}$ and $\{$C, F, G$\}$. B and C are group agents, respectively. D, E, F, and G are agents for level 2 groups. Figure 2 shows an alternate representation of the group hierarchy, where every group is represented by its agent at a lower level.
In this network, the domain(A) contains 7 groups and all hosts in the system. The domain(B) consists of 3 groups and mobile hosts $\{$B, D, E, s, t, x, y, z$\}$.

C. Basic Operations

The following four basic operations are defined for setting up and maintaining a HMWN system.
Grouping is the operation used to set up a HMWN system. It is only performed at the bootstrapping phase. Via "Grouping", the static membership will be established (i.e., HG will be assigned for each mobile host). The criteria for "Grouping" include

Mobility: If a set of mobile hosts are going to coordinate their movements, they may form a group.

Organization: If the owners of mobile hosts belong to the same organization, the ones in the same department may be grouped together.

Capability: Several factors are taken into account when the capability of a mobile host is evaluated, e.g., the computation capability, system resource, power level, and communication bandwidth and range. The higher the capability is, the greater the chance is that the mobile host will be chosen as an agent.

Wireless MAC protocol: If a mobile host support two wireless MAC protocols and one protocol has wider communication range, e.g., 802.11b and bluetooth. It may be chosen to be the agent for the group that use the protocol with narrower communication range (i.e., bluetooth).
The operation can be done in two different ways.

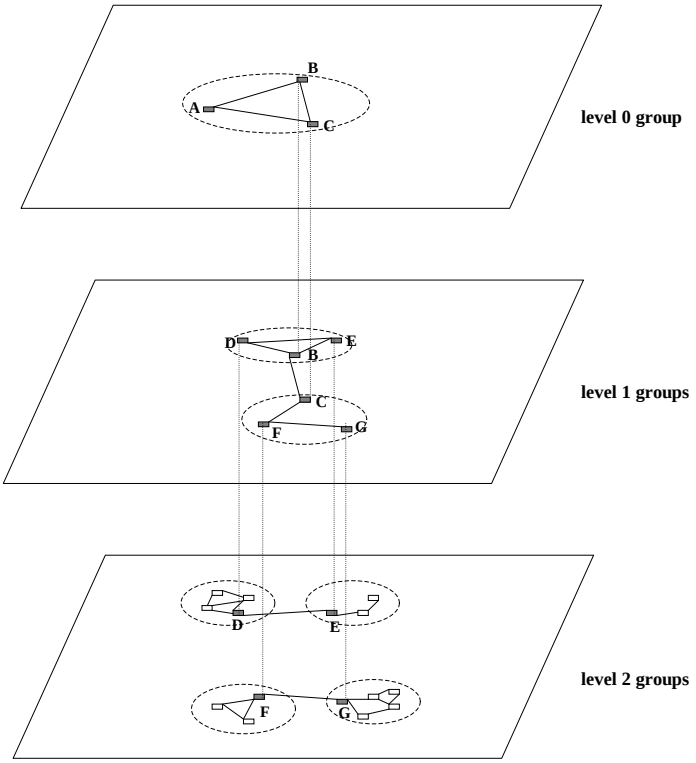

Fig. 2. Hierarchy of Groups

- Mobile hosts may autonomously organize themselves into groups, then supergroups. In the autonomous procedure, each agent will exchange the above information with its neighbors to determine the static membership relationship. This process may take a long time to complete. It is hard to obtain the optimal result.
- A trusted authority may take charge of the operation. Every mobile host reports its information to the authority. The authority employs some global optimization algorithm and distributes the result to all participated hosts.

Registration is the operation a mobile must complete before it can connect to the network. "Grouping" only determines the static membership. "Registration", along with "Leaving" and "Migration", maintains the dynamic topology of the network (e.g., CG for a mobile host). Registration takes place between the mobile host MH and its HGA. One-hop registration is recommended to reduce the risk of denial-of-service and man-in-the-middle attacks.

This operation begins with MH broadcasting the "registration" request. If the HGA is within the neighborhood, the operation continues with an identity verification process. Upon successfully registered, MH will obtain the group information such as group ID, group shared secrets, etc., and set the HGA to be its CGA. In case that MH itself is an agent of another group, all hosts in the derived domain(MH) implicitly become members of the network. MH keeps moving and sending out the request periodically if it cannot reach the HGA directly. Other hosts may provide aid to locate the HGA so that MH can adjust its movement.

Remote registration will be allowed if connectivity rather than security is preferred.

Leaving operation is completed by group agents and it may be triggered by two events.

- When a mobile host MH decides to leave the network (along with all hosts in the derived domain(MH)), it sends a "leave group" message to its CGA.
- When the agent finds out that the route to a mobile host MH is broken, it starts a Leaving Timer. If a route to MH cannot be reestablished or a "Migration"message has not received within the Leaving Interval Time as described below, the agent starts the "Leaving" operation.

$$LeavingIntervalTime = Robustness * Ad\_Interval * (Max\_Hop + 1) \quad (3)$$

The *Ad_Interval* is the time interval between the route advertisements sent out by a host. The *Max_Hop* is the hop number of the longest route in the agent's routing table. Robustness * Ad_Interval * (Max_Hop + 1) is the maximum time it will take to get MH's routing information if MH is still a member of the group. The *Robustness* allows tuning

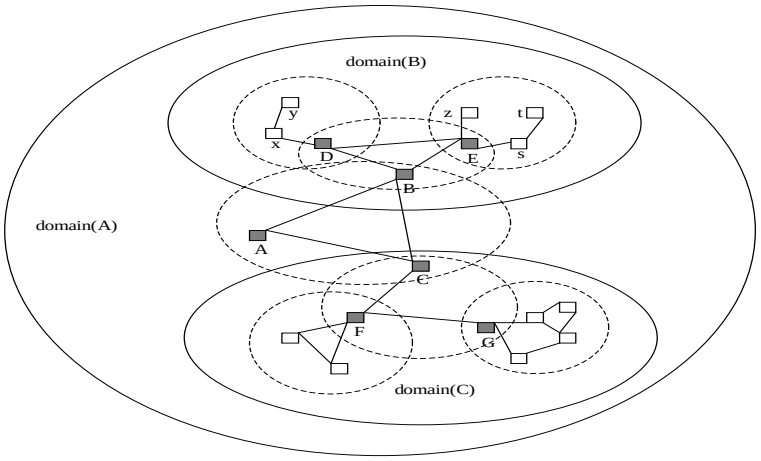

Fig. 3. Migration

for the expected packet loss on wireless links. If the system is expected to be lossy, the Robustness may be increased. The leaving operation is able to tolerate (Robustness - 1) failures. Thus Robustness must be greater than 1.
After the CGA of MH updates the membership information (Section IV-C), the CGA will forward the ”leave group” message to its own CGA.
Migration operation is initiated by a mobile host that decides to leave its current group and join a foreign group. Usually, when a host MH realizes that the CGA is no longer reachable, it starts this operation by sending out a “Migration” request. Foreign agents that are in the neighborhood reply this request based the policy, MAC protocol compatibility and capacity. MH chooses the FGA whose reply comes first, set it to be the CGA, and invokes the hand-off procedure. Every agent that replies the request will start a timer. When the timer expires, the agent will cancel the operation.

Figure 3 illustrates the topology of the example HMWN system shown in Figure 1 after mobile host z migrated from group(D) to group(E).

IV. Membership Management

Maintaining the structure in an efficient way is significant in a HMWN system. Essentially, it is a membership management problem because the mobile hosts are organized as hierarchical groups. The following subsections present an efficient membership management protocol.

A. Data Structure

The membership information is mainly used for two purposes. The first is to verify the identity of a host (i.e., the static membership). The second is to help routing protocols to determine the proper route to forward packets (i.e., the dynamic membership). Each agent maintains two separate tables.
Static_Member_Table contains the identification information of mobile hosts whose HGA is the table owner. This table is mainly used by security protocols. The table has an entry for every potential member, which is a 3-tuple {*ID*, *shared_secret*, *public_key*}. Initially, an entry only contains the ID and the shared_secret. After registration, the public key of the member will be recorded in the entry.
Current_Member_Table contains the information of all the mobile hosts that currently belong to the domain whose agent is the table owner. The entry of the table is a 3-tuple {*ID*,*intermediate_host*, *home_agent*}. The intermediate_host is the group-mate whose Current_Member_Table contains the mobile host. This table is used by the routing protocol to locate mobile hosts.
Depend on the size of the tables and the available memory, these two tables can be stored using a hash table or a ordered list to accelerate the searching process.

B. Registration

Upon successful registration, the host will get the group information from the agent. The host sets the agent to be its CGA. In case that security protocols are deployed, a mutual challenge-and-response process will be initiated to verify

the identity of the host. If verification succeeds, the agent will record the host's public key in the corresponding entry of Static_Member_Table, the host will get the group key, the agent's public key, and other information required by the security protocols such as a certificate.
The host will send a list of all members in its Current_Member_Table to the agent. This list will be forwarded via the path from the agent to the root of the hierarchy. Every agent on the path will add the members to its own Current_Member_Table.

C. Leaving

When a member is leaving this group, the process is much simpler. The host will send a list of all members in its Current_Member_Table to the agent. This list will be forwarded via the path from the agent to the root of the hierarchy. Every agent on the path will remove the members from its own Current_Member_Table.

D. Migration

When a mobile host MH is leaving the current group G_1 and joining another group G_2, both the CGA and the FGA will update their Current_Member_Table. If MH is an agent, all mobile hosts in domain(MH) also implicitly leave domain(G_1) and join the domain(G_2). After joining the foreign group, MH will send messages to the CGA and the FGA to help them update the membership.

D.1 Update at FGA side

MH sends the following message to the foreign agent.

[ADD, ID, previous_agent, member_list]

where ID is the identification of MH, previous_agent is MH's CGA before joining the group, member_list is MH's Current_Member_Table.
The FGA invokes the following process to update the membership.

FGA Membership Update

```
for each entry e in member_list
  if a corresponding entry e' does not exist in the Current_Member_Table
    add the entry e';
  set intermediate_host of e' to ID;
  set intermediate_host of e to my_id;
if previous_agent is not in the Current_Member_Table
  send out a message [ADD, my_id, previous_agent, member_list] to its CGA;
```

Every agent that receives the message will invoke the same process.

D.2 Update at CGA side

MH sends the following message to the current agent.

[REMOVE, ID, foreign_agent, member_list]

where ID is the identification of MH, foreign_agent is the agent of the foreign group, member_list is MH's Current_Member_Table.
The CGA invokes the following process to update the membership.

CGA Membership Update

```
if foreign_agent is not in the Current_Member_Table
  for each entry e in member_list
    remove the corresponding entry in the Current_Member_Table;
  send out a message [REMOVE, my_id, foreign_agent, member_list] to its CGA;
```

Every agent that receives the message will invoke the same process.

Figure 4 shows the difference between "Registration", "Leaving" and "Migration" with respect to the modification of Current_Member_Table. The small circles represent the mobile host. For "Registration" and "Leaving", the effect will

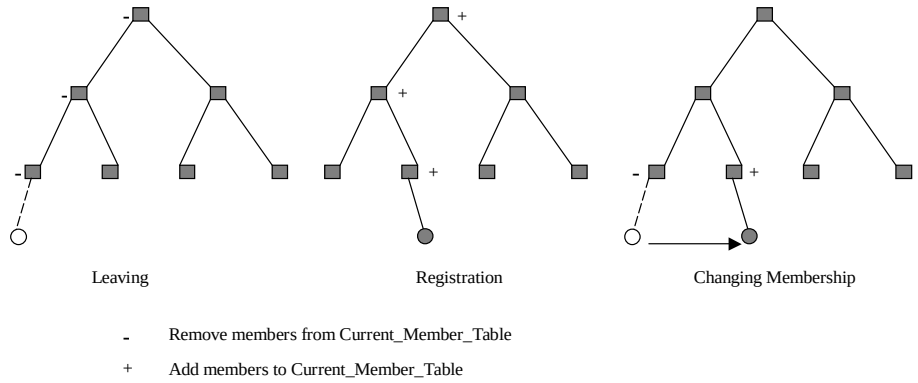

Fig. 4. Membership Modification

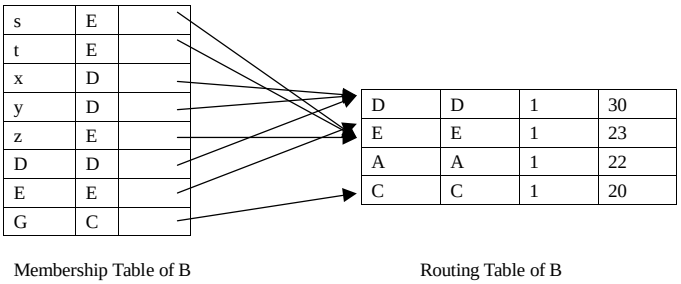

Fig. 5. Membership Table and Routing Table

be propagated to the root of the hierarchy. Thus lv(A)+1 unicasts are required, where A is the agent. For "Migration", the effect is only propagated to the agent of the domain closure(previous_agent, foreign_agent). The number of required unicasts is

$$lv(previous\_agent) + lv(foreign\_agent) - 2 * lv(closure(previous\_agent, foreign\_agent)) \quad (4)$$

V. Segmented Membership-based Group Routing

We propose a Segmented Membership-based Group Routing (SMGR) protocol for the HMWN system to take advantage of the hierarchical group structure.

A. Data Structure

SMGR protocol requires two tables. One is the routing table, in which each entry is a 4-tuple <*destination*, *next_hop*, *distance*, *sequence_number*>. The sequence_number represents the freshness of the route. Each host maintains a sequence_number for itself. This number is monotonically increasing. Only routes to the group-mates are maintained in the routing table. These routes are updated using DSDV [9] protocol.

The other is the membership table, in which every entry is a 3-tuple <*final_destination*, *intermediate_host*, *routing_entry*>. *routing_entry* is a pointer to the entry in the routing table that specifies the route to the *intermediate_host*. Every entry in Current_Member_Table has a corresponding entry in this table.

Take host B at Figure 3 as an example, figure 5 shows the routing table, the membership table, and the pointers.

The size of the routing table is bounded by the size of the group, which is nearly a constant.

SMGR protocol will add a header, which is a 4-tuple <*source*, *final_destination*, *intermediate_host*, *next_hop*>, to each packet. The header is used to route the packet.

B. Routing

When a host receives a data packet, either from another host or from a application running on itself, it takes the following steps to forward the packet. Here we assume that the routing table is up-to-date.

SMGR protocol

```
if it is the final_destination
  send the packet to the corresponding application;
else if it is the next_hop
  find out the route to the intermediate_host;
  change next_hop and send out the packet;
else if it is the intermediate_host
  search the Current_Member_Table;
  if an entry e exists for the final_destination
    set the intermediate_host to e.intermediate_host;
    get the routing table entry re;
    set the next_hop to re.next_hop;
    send out the packet;
    if the packet comes from a host which is in the same group of e.intermediate_host
      send a "redirect" message to the host;
  else
    if the packet comes from a host of which it is the agent
      set the intermediate_host to CGA;
      send the packet to CGA;
    else
      send out a "membership expires" message to the source;
else if it is the source
  search the Current_Member_Table;
  if an entry e exists for the final_destination
    set the intermediate_host to e.intermediate_host;
    get the routing table entry re;
    set the next_hop to re.next_hop;
    send out the packet;
  else if it is not the root of the hierarchy
    set the intermediate_host to CGA;
    send the packet to CGA;
  else
    drop the packet and notify the application;
else
  drop the packet silently;
```

A host will removes the corresponding entry from the membership table when it receives a“membership expires” message.

When a host receives a “redirect” message, it adds an entry in the membership table, set intermediate_host to be the redirected host.

VI. Simulation-based Evaluation

Currently, we have implemented a simplified version of SMGR in ns2 (network simulator) [10]. In this version, the membership modification is completed through broadcast instead of unicast. It is predictable that more protocol overhead will be introduced by the simplification. We have also implemented the computation delay component to simulate different computation capabilities. The purpose of the experiments is to evaluate the scalability of HMWN.

A. ns2 Simulation

In this preliminary experimental study, we take the normalized protocol overhead (protocol overhead divided by throughput) [11] as the metric to evaluate the scalability of routing protocols. Since SMGR utilizes distance vector, we compare it with two popular Ad hoc routing protocols, DSDV [9] and AODV [12], which also utilize distance vector. The experiments simulate a 1000m x 1000m area. Random mobility model is used to generate hosts’ movements, the maximum speed is 5m/s, the pause time is 3s. The number of end-2-end connections is equal to the host number and every Source-Destination (S-D) pair is randomly chosen. For each host number ranging over $\{20, 30, 40, 50, 60\}$, five scenario are created. Every simulation runs 1000 seconds. The normalized protocol overhead is extracted from the generated trace file.

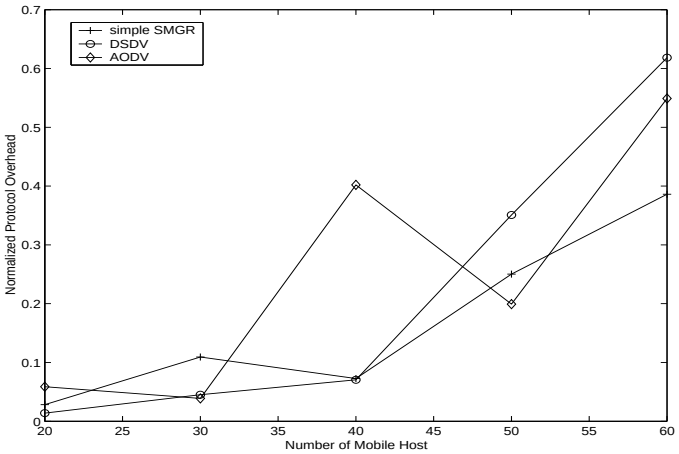

Fig. 6. Normalized Protocol Overhead vs Number of Mobile Host

B. Normalized Protocol Overhead

The result of the experiment is shown in figure 6. The curves present the mean value of the normalized protocol overhead for each protocol. The curve of AODV protocol has sharp changes when host number is 40 and 50. A possible reason is that ADOV works in a on-demand fashion and the chosen of S-D pairs will heavily affect its performance in terms of protocol overhead. For DSDV and simple SMGR, when the host number is less than 50, they have similar performance. When the host number reaches 60, the difference is greater 50%, which means simple SMGR is more scalable than DSDV. Considering the random mobility model and the random traffic pattern that are used for the experiments prefer Ad hoc architecture, and the simple SMGR introduces more protocol overhead, we may expect the HMWN supported by SMGR routing protocol to be more scalable.

VII. Conclusion

In this paper, we present the Hierarchical Mobile Wireless Network. Our motivation is to provide flexible and scalable network services to ”non ad hoc” applications. In an HMWN system, mobile hosts form hierarchical groups. Four basic operations that are used to set up and maintain the hierarchy have been discussed. The detail of an efficient membership management protocol is presented. The Segmented Membership-base Group Routing (SMGR) protocol for HMWN is proposed. An experimental study is carried out to compare the scalability of SMGR with AODV and DSDV Ad hoc routing protocols in terms of normalized protocol overhead. The SMGR outperforms these two protocols for about 50% when host number reaches 60.

References

[1] Yi Lu and Bharat Bhargava, “Achieving flexibility and scalability: A new architecture for wireless network,” in *Proceedings of International Conference on Internet Computing*, June 2001, pp. 1105–1111.

[2] Zygmunt J. Haas and Marc R. Pearlman, “Providing Ad-Hoc connectivity with reconfigurable wireless networks,” *Ad Hoc Networks*, 2000.

[3] M. M. Zonoozi and P. Dassanayake, “User mobility modeling and characterization of mobility patterns,” *IEEE Journal on Selected Areas in Communications*, pp. 1239–1252, September 1997.

[4] Xiaoyan Hong, Mario Gerla, Guangyu Pei, and Ching-Chuan Chiang, “A group mobility model for Ad Hoc wireless networks,” in *Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, 1999, pp. 53 – 60.

[5] Kjeld Borch Egevang, Cray Communications, and Paul Francis, “The ip network address translator (nat),” *RFC 1631*, May 1994.

[6] M. R. Pearlman, Z. J. Haas, and S. I. Mir, “Using routing zones to support route maintenance in ad hoc networks,” in *Proceedings of Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE*, September 2000.

[7] Suman Banerjee and Samir Khuller, “A clustering scheme for hierarchical control in multi-hop wireless networks,” in *Proceedings of IEEE Infocom 2001*, April 2001.

[8] R. Ramanathan and S. Steenstrup, “Hierarchically-organized, multihop mobile wireless networks for quality-of-service support,” *Mobile Networks and Applications*, vol. 3, no. 1, June 1998.

[9] Charles E. Perkins and Pravin Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers,” in *Proceedings of the SIGCOMM’94 Conference on Communications Architectures, Protocols and Applications*, August 1994, pp. 234–244.

[10] “The network simulator - ns-2,” *http://www.isi.edu/nsnam/ns/*.

[11] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marine, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Personal Communications*, vol. 8, no. 1, pp. 16–28, Febuary 2001.

[12] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad hoc on-demand distance vector (aodv) routing," *IETF Internet Draft of AODV, version 10, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-10.txt*, 2002.