Comparisons of Inter-domain Routing Schemes for Heterogeneous Ad hoc Networks

Wenbin Ma
Department of Computer Science and Engineering
19 Memorial Drive West, Lehigh University
Bethlehem, PA 18015, USA
wem2@lehigh.edu

Mooi Choo Chuah
Department of Computer Science and Engineering
19 Memorial Drive West, Lehigh University
Bethlehem, PA 18015, USA
chuah@cse.lehigh.edu

***Abstract*— In this paper, we propose three interdomain routing schemes for communications between different ad-hoc groups (subnets), namely the implicit foreign degree based (IFD), the explicit locally optimal (ELO) and the explicit limited scope (ELS) protocols. The IFD scheme mandates that only local nodes can hear a certain number of foreign nodes are qualified to be chosen as the gateways for forwarding interdomain route requests. The ELO and ELS schemes choose the node with the highest score within its local scope as the gateway, but they differ in terms of routing protocols. The ELO uses reactive routing protocol while the ELS scheme uses a hybrid approach i.e., a proactive routing scheme within the scope and reactive scheme outside the scope. In our paper, we compared the performance between these different schemes that we proposed. Our simulation studies reveal that the explicit schemes can achieve high packet delivery ratio and good average end-to-end delay at a lower overhead cost compare to the IFD scheme. We also compared our approaches with LANMAR, an existing scalable routing protocol for ad hoc networks. The results show that our approach outperforms LANMAR in terms of the packet delivery ratio and control overhead while maintaining comparable end-to-end delay at low and medium mobility rate (less than 8m/s).**

Keywords- interdomain routing; ad-hoc network; gateway selection

I. INTRODUCTION

Wireless adhoc networks are networks that can be formed dynamically by mobile hosts without requiring any preinstalled infrastructure. Much work has been done in terms of designing flat routing schemes for ad-hoc networks [1][2]. The "flat" ad-hoc routing structure is proven to have poor scalability [3]. As the network size increases, data packets need to be routed via "long" paths which are prone to break. Thus, some hierarchical routing solutions have been recently proposed to increase the scalability of the ad-hoc networks. For example, in [4], the authors propose a two level hierarchical ad-hoc network where some "special" nodes (referred to as the backbone nodes), are assumed to have an additional powerful radio to establish long range wireless links among themselves, thus forming a mobile backbone. The backbone nodes are also moving and hence the mobile backbone is yet another ad-hoc network. The local subnets can run one routing protocol while the mobile backbone runs another routing protocol.

Most of the existing routing researches for ad-hoc networks only deal with scenarios where the nodes belong to the same administrative group. A real inter-domain routing problem studied so far is the communications between ad-hoc networks and the wired Internet. Several approaches have been proposed in [5][6]. These approaches assume that the nodes wait for a certain period of time for route replies. If no route reply is heard, the sending node assumes that the destination node is in the wired Internet and proceeds to use Mobile-IP-like protocol to register with a foreign agent that can access the wired Internet so that its packets can be delivered to the desired destination outside the ad-hoc network.

However, the inter-domain routing problems for the communications between various ad-hoc groups from different administrative domains and possibly with different network configurations have not been studied much. In this paper, we propose various routing schemes that allow nodes from different ad-hoc groups to communicate with one another without assuming the presence of backbone nodes. The ability to perform interdomain communications between different ad-hoc groups is critical in certain operations e.g. communications among different international military units in a Multinational Force; and communications between police personnels, medical personnels, and firefighters.

The rest of this paper is organized as follows: in Section 2, we discuss the assumptions made on the ad-hoc network architecture and define a few terms which we use for describing our proposed solutions. In Section 3, we describe the three routing schemes that we propose, namely the implicit foreign degree based protocol (IFD),

the explicit local optimal protocol (ELO), and the explicit limited scope protocol (ELS). In Section 4, we describe the simulation model, the traffic pattern and the mobility model that is used to evaluate all the routing schemes. Then in section 5, we present our simulation results and draw some preliminary conclusions regarding the usefulness of the three proposed schemes and the difference between them and an existing scalable routing scheme named LANMAR [7]. We also discuss the future work that we intend to explore in Section 6.

II. NETWORK MODEL

In this work, we assume that a heterogeneous ad-hoc network is composed of different subnets with various configurations. The nodes from the same organization are assumed to belong to the same subnet. Their logical grouping is reflected in their IP-like addresses <GroupID, HostID> which can be referred to as their identifiers. We also assume that the nodes can exchange hello-like messages with their 1-hop neighbors specifying their identifiers. Thus, each node can distinguish whether its 1-hop neighbors are from the same group or different groups. The nodes from different ad-hoc groups are assumed to have their own network configurations. For example, they could run different routing protocols, support different cryptography schemes, or have different authentication keys. All nodes that belong to the same group as a particular node will be referred to as the local nodes. Any 1-hop neighbor that a node can hear that belongs to a group different from its own will be referred to as the "foreign" node and the group that this foreign node belongs to will be referred to as the "foreign" or external group. In order for a node from one group to communicate with another group which may be running a different routing protocol, we assume that all ad-hoc groups support two types of common messages, namely (a) an inter-domain route request message, and (b) a special header to denote data packets. This approach is simpler than the existing proposal in [4] since the nodes from one group need not understand fully the routing protocol that the other group uses.

Furthermore, we assume that the nodes within a group move as a group. The different ad-hoc groups move around within a certain geographical area and may meet one another. We refer to the area where nodes from different groups can hear one another as the overlapping area. For a particular node that desires to send traffic, we refer to the group it belongs to as the source group. Similarly, the group that the destination node belongs to is referred to as the destination group.

III. INTER-DOMAIN ROUTING ALGORITHMS

In our inter-domain routing approaches, we assume that every node in the subnet can act as a gateway node. A gateway node is responsible for performing basic gateway functions e.g. relaying traffic destined to nodes in another ad hoc subnet, supporting Network Address Translation (NAT) function, tunneling and protocol translation. These can be easily applied by installing certain gateway function modules to a node. Additional gateway functionalities may be required depending on the heterogeneity among the different ad-hoc groups. Since a gateway needs to communicate with nodes from foreign/external groups, they should be elected among the nodes that can hear some foreign nodes. Different metrics can be used to select the most appropriate node to be the gateway node. In subsequent subsections, we discuss three different routing protocols that can dynamically select the gateway nodes to forward the inter-domain packets.

A. *Algorithm 1: Implicit Foreign-Degree Based Routing Protocol (IFD)*

In this algorithm, each node maintains a table that registers the number of nodes in each foreign group that it can hear. Such information can be easily obtained from the hello-like messages described in Section 2.

Whenever a node wants to communicate with any node in another foreign group, it will broadcast an interdomain route request which includes the information related to the destination and the desired gateway requirements. We will refer to the node that sends the route request as the requesting node. An example of a gateway requirement is the minimum number of nodes from the destination group that a local node can hear. Any node in the source group that hears such an interdomain route request will check its own table to see if it meets the minimum specified gateway requirements. If it does, then it will relay that interdomain route request to the destination group so that a route to the destination node can be determined. Upon hearing a favorable route reply from the destination node, this local node will respond to the original interdomain route request by claiming itself to be the gateway and attach its own identifier in the route reply message. The requesting node will use the route provided from the first route reply it receives. There are two ways to maintain the route, one is to use the same route throughout the same communication session unless a route error is received or the session ends. The other is to change the route whenever a route reply with shorter route has been received. Fig. 1 illustrates how the IFD scheme works.

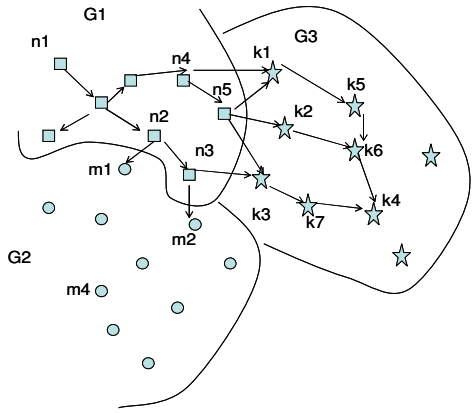

Figure 1. Implicit foreign degree based routing protocol.

Assume that node n1 from *G1* (group1) wants to send some traffic to node *k4* in *G3* (group3). Node *n1* will send an inter-domain route request for node *k4*. If the gateway requirement is such that any local node (i.e. *G1* node) with at least one 1-hop neighbor from *G3* can respond, then nodes *n4*, *n5* and *n3* can respond to this interdomain route request. If the gateway requirement is such that only nodes with at least two 1-hop neighbors from G3 can respond, then only *n5* is eligible to respond to this interdomain route request. Only those nodes that meet the minimum gateway requirements can relay the interdomain route request to the foreign group. Tradeoffs need to be made when one set this gateway requirement, e.g. requiring a node to hear more than one 1-hop foreign neighbors before it qualifies to be a gateway reduces the amount of overhead but may result in less optimal path being found.

This algorithm is simple for no explicit gateway selection protocol needs to be provided. In addition, it is adaptive to mobility since every node is allowed to pick its own gateway.

Thus, this approach is suitable for scenarios with high node mobility. The downside of this approach is the long route discovery delay especially when the destination node is at the far end of the foreign group.

There are several ways for us to enhance this simple protocol. For example, each requesting node can cache the information of the winning gateway identifier in the form (gateway node-id, foreign group-id). In the future, if the requesting node intends to send packets to other nodes that belong to the same foreign group, it would tunnel its interdomain route request directly to the gateway node rather than perform a regular route request broadcast in its local group. Intermediate nodes that lie within the route between the requesting node and the gateway node can also cache such information based on the route replies they relay. In addition, the requesting node can adaptively modify the gateway requirements to reduce the number of candidate nodes that are allowed to respond to the inter-domain route requests. For example, if the requesting node keeps count of how many route responses it receives for the same interdomain route request, it can tighten its gateway requirements to reduce the overhead when there are too many route replies. The gateway requirements can be tightened by increasing the number of foreign nodes that a local node can hear before it is allowed to respond to any interdomain route request. We refer to this number as the required "foreign degree". Tradeoffs need to be made since with fewer eligible nodes for gateway selection, less optimal paths to the destination node may be found.

Furthermore, the gateway nodes can perform local repairs whenever it receives a route error indicating that an active interdomain route is broken as shown in Fig. 2. In Fig. 2, we assume that node *n2* is the winning gateway for the communication between node *n1* from *G1* (group1) and node *m4* from *G2* (group2). When *m2* notifies *n2* that the link to *m4* is broken, *n2* will initiate a proxy route request to nearby nodes to see if they can find a route to *m4*. As shown in Fig. 2, the gateway *n2* discovers an alternative route via node *n3*.

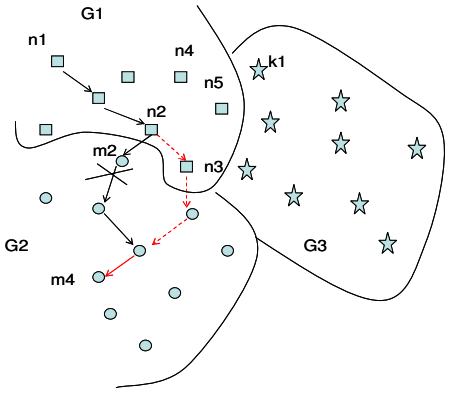

Figure 2. Gateway local repair.

B. Algorithm 2: Explicit Locally Optimal Routing Protocol (ELO)

In this design, each node calculates a score for each foreign group based on the self-maintained table that registers the number of nodes in each foreign group that it can hear. A new type of message is defined called the self-nominating gateway message (*SNGM*). The *SNGM* contains the GroupID and the score for each foreign group this node can hear. The *SNGM*s are piggybacked to

the normal hello messages that are exchanged between each node and its 1-hop neighbors.

Again, the routing approach in this scheme is reactive-based. Whenever a node wants to communicate with any node in a foreign group, it will broadcast an interdomain route request. Each node in the source group that hears the interdomain route request will check the scores for that foreign group from the latest *SNGM*s it received from all its neighboring nodes, and compare them to its own score. If it has the highest score which is at least equal to 1, it will declare itself as the wining gateway and relay that interdomain route request to the destination group.

Consider the scenario in Fig. 3, nodes *n5*, *n7* and *n3* will send out their self-nominating gateway messages. Node *n5* and *n7* will be selected as the gateway for comunication requests from *G1* to *G3*, since *n5* can hear the largest number of foreign nodes from *G3* in its neighborhood (*n4, n5, n6*) and *n7* can hear the largest number of foreign nodes from *G3* among its one-hop neighbors (*n3, n6*) as well.

When node *n1* wants to communicate with node *k4* in *G3* (group 3), both node *n3* and node *n7* will relay the interdomain route request to the nodes in *G3* to find a route to the destination node *k4*.

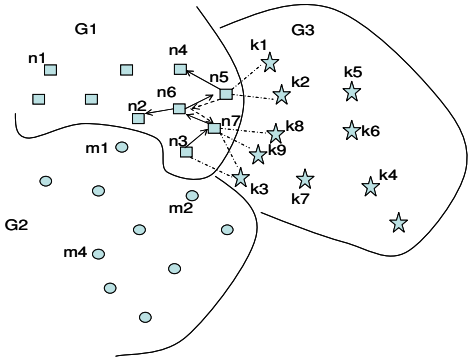

Figure 3. Self-nominating gateway Procedure.

This approach works as a reactive routing protocol with the local optimal gateway selection process. It has all the advantages of the reactive routing protocols like optimal route choosing, but it also suffers from the disadvantages like larger route discovery delay.

C. Algorithm 3: Explicit Limited Scope Routing Protocol (ELS)

In this approach, each node maintains the route information to every destination node of the same group that is certain hops away (the hop number is refer to as the scope). To do this, traditional proactive routing protocol is used for routing within the scope and reactive routing protocl is used to reach the nodes outside the scope.

Similar to the ELO scheme described in section 3.2, each node will maintain a score table based on the number of nodes in each foreign group that it can hear. These score information will also be sent out using the *SNGM*s. The difference is that we can either piggyback the *SNGM*s to the route update packets sent out within the scope, or broadcast them separately within the scope at certain frequency. If a node hears a packet with the header that indicates that another node in its scope can hear a larger number of foreign nodes from the same foreign group, then it will consider itself not a capable gateway, otherwise it will be selected as the winning gateway. Only the winning gateway is allowed to respond to the interdomain route requests and will forward the interdomain route requests to the foreign group.

Consider the same scenario in Fig. 3, nodes *n5*, *n7* and *n3* will send *SNGM*s. If the gateway scope is set to two-hops, then node *n7* will be selected as the gateway for comunication requests from *G1* (group 1) to *G3* (group 3), since it can hear the largest number of foreign nodes from *G3* (the number is 3) among (*n2, n3*, *n5*, *n6, n7*).

When node *n1* wants to communicate with node *k4* in *G3* , only node *n7* will relay the interdomain route request to the nodes in *G3* to find a route to the node *k4*. Even though setting the gateway scope to a higher number could reduce the overhead, less optimal routes may be found since the number of eligible gateway nodes is reduced and only the selected gateways are allowed to relay the interdomain route request.

Since proactive routing is involved in this protocol, we are hoping to get better performance both in terms of routing overhead and average delay.

IV. SIMULATION MODEL

In this section, we describe the simulation model that we used to evaluate the performance of the routing schemes; including the scenario generation, the traffic pattern and the mobility model.

A. Traffic Pattern and Mobility Model

We use GlomoSim [8], which is a scalable simulation environment designed for wireless ad hoc and sensor networks, as a tool to evaluate our protocols. In our experiments, the MAC layer is implemented using the distributed coordination function of IEEE 802.11 [9]. Data packets are sent using CSMA/CA mode. The radio

model is consistent with the existing commercial Wireless LAN offerings (e.g. Cisco Aironet). The radio transmission range is 350 meters and the channel capacity is 2Mbit/sec. The simulation area is 1500*1500 meter square. Each simulation lasted for 20 minutes of simulation time. There are two groups of nodes and each group has eighteen nodes.

B. Traffic Pattern and Mobility Model

We had tried both 20 traffic sessions and 40 traffic sessions. For 20 traffic sessions, the source and destination nodes are randomly chosen from different ad hoc groups. To increase the load in the network, we also tried 40 traffic sessions. In this scenario, 20 traffic sessions whose source and destination nodes are randomly chosen in the same group are added to the previous 20 inter-group traffic sessions. Traffic is UDP and the size of each packet is 512 bytes. The interarrival time of the data packets on each source/destination connection is 20 seconds.

The mobility model used in our simulation is the Reference Point Group Mobility (RPGM) model described in [10] and [11]. It defines the concept of a reference point (group center) that moves according to the random waypoints model, and the group members experience a random deviation from this group motion. We modified a mobility scenario generation tool called BonnMotion [12] to generate our simulation scenarios. In the simulation, the group center moves towards a randomly picked destination at a constant speed. Once the destination is reached, another destination will be randomly chosen and the group will start moving towards the new destination after a certain period of pause time. The nodes in the same group follow their reference point. The distance between each node and its group reference point is chosen from a uniform distribution within range [0, maximum diversion distance]. This behavior is repeated for the whole duration of the simulation. In our simulation, the group moving speed is varied to simulate different group mobility.

V. PERFORMANCE EVALUATION

To evaluate the performance of our approaches, we use the following metrics:

- *Packet delivery Ratio* – the ratio of the number of received data packets to the number of data packets sent by the sources.
- *Control Packet Overhead* – The number of control packets that our protocol sent out for gateway selection, route discovery and route maintenance. This overhead includes the hello-like messages used in all the schemes.
- *Average end-to-end packet delay* – the time from when the source generates the data packet to when the destination receives it.

All these metrics reflect the efficiency of a routing protocol. Good routing schemes should have a high packet delivery ratio but low control packet overhead.

In all our simulation experiments, we use two ad-hoc groups with eighteen nodes each. Since the overlapped area where nodes from different groups can hear one another is needed for different ad hoc groups to communicate with each other, we should wait for some time after the simulation starts to ensure that the starting locations of the nodes will not affect much the performance of the inter-domain routing schemes. Thus, we include some warm up period before collecting the statistics in our simulations. We set the minimum node mobility to 2m/s.

A. Performance of IFD

We use the IFD in the first two experiments. In the first experiment, the radio transmission range of the node is 350m. In the second experiment, we vary the transmission power of the radio to study the impact of radio transmission range on the three performance metrics. We also vary the settings for the required foreign degree in IFD to see how these settings impact the routing performance.

1) Packet Delivery Ratio:

Fig. 4 plots the packet delivery ratio as a function of mobility when IFD is used. As we can see in Fig. 4, the results of data packet delivery ratio linearly decrease when the mobility increases; the highest packet delivery ratio is achieved when the mobility is 2m/sec. This is because when the mobility rate increases, the frequent changes of the network topology in each group and the overlapped area between these groups create more impact on the end-to-end routes. Thus, the packet delivery ratio drops as mobility increases which is similar to the typical behavior observed for the ad-hoc routing protocols for a single ad-hoc network.

It is also observed from Fig. 4 that, as the gateway score requirement is tightened (by setting the required foreign degree to higher number), the data packet delivery ratio decreases. This is because setting the required foreign degree to a higher number may reduce the number of eligible nodes for gateway selection and hence reduce the possibility for the requesting node to

find a route to the destination in foreign ad-hoc groups. With increasing mobility, there are more frequent changes in network topology and link failures. Thus, there are fewer nodes that can meet the stringent gateway requirement and hence we observe that the packet delivery ratio drops more with a more stringent gateway requirement as mobility increases.

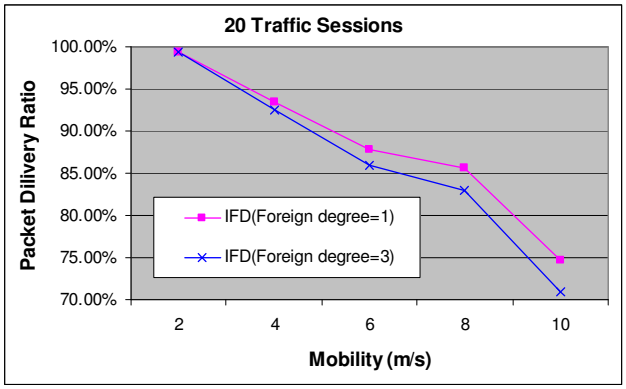

Figure 4. Mobility vs. Delivery Ratio (18 nodes/Group)

2) Routing Overhead and Average Delay:

The control packet overhead and the average end-to-end delay for the first experiment are plotted respectively in Fig. 5 and Fig. 6 respectively.

As we can see in Fig. 5, the results of the control packet overhead are related to the results of the packet delivery ratio shown in Fig. 4. The higher the data packet delivery ratio, the smaller the overhead is. When the link fails or the nodes move, the end-to-end path may break and hence packets are lost. Since we are using reactive-based routing protocols, such path breakages will trigger route repair or new route discovery events which result in increasing overhead.

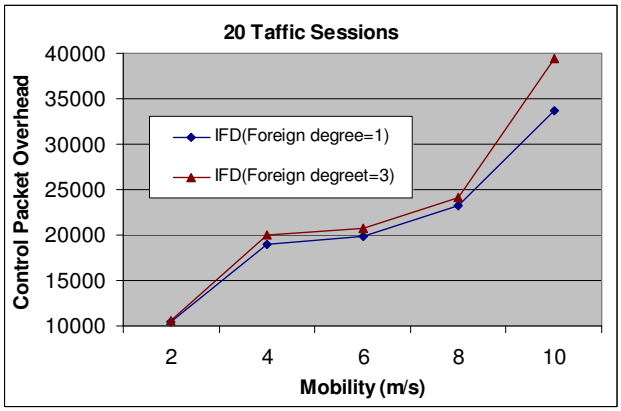

Figure 5. Overhead vs. Delivery Ratio

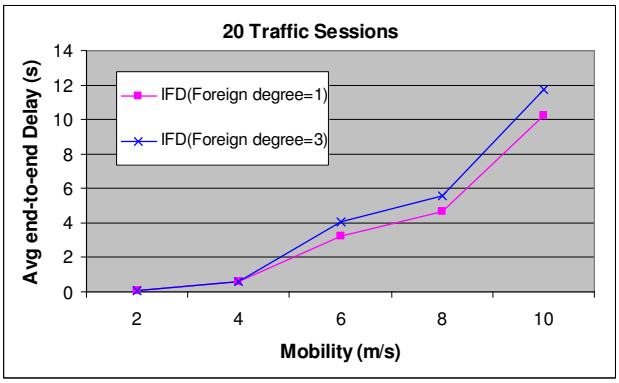

Figure 6. Average Delay vs. Mobility

From Fig. 6, we see that the average delay increases as the gateway requirement is tightened. When the gateway requirement is tightened, the number of nodes eligible to be gateways reduces and hence less optimal routes may be found for the inter-domain communications which results in the increase of the average delay.

3) Impacts of Radio Transmission Range:

We also study the impacts of changing the radio transmission range on the routing performances. In this simulation experiment, the mobility is set to 2m/sec and the required foreign degree is set to 1. Fig. 7 to Fig. 9 plot the packet delivery ratio, the control packet overhead and the average delay results respectively as the radio transmission range is varied from 140m to 350m.

Since the maximum deviation distance for a group is fixed and all the traffic sessions are between different groups, changing the radio transmission range actually affects the possible overlapped area between different groups. When the radio transmission range is small like 140m, there is not much overlapping area between the two ad hoc groups, and hence some connections cannot be completed. On the other hand, as the radio transmission range keeps increasing, the communication ability of our solution becomes more efficient and there will be more chances to set up the connections between different ad hoc groups. As proved by the results, the packet delivery ratio increases while the overhead and average delay decrease.

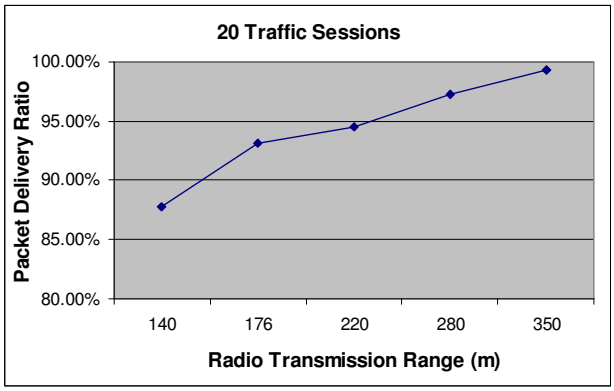

Figure 7. Packet Delivery Ratio vs. Radio Transmission Range

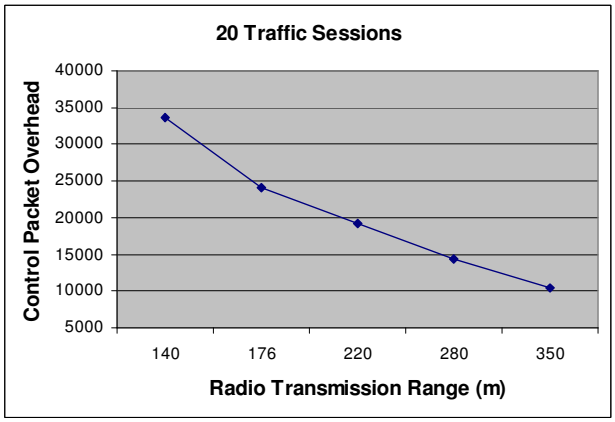

Figure 8. Overhead vs. Radio Transmission Range

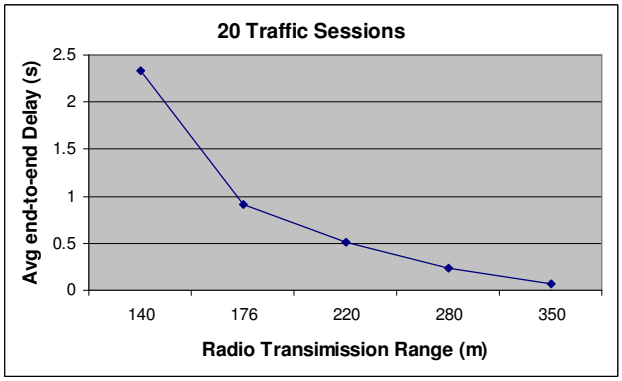

Figure 9. Average Delay vs. Radio Transmission Range

B. *Performance of ELO and ELS*

We use similar settings as in experiment 1 to evaluate the performance of the ELO and ELS schemes. For ELO, we set the scope to 1; and for ELS, the gateway scope is set to 2.

For ELO, reactive routing with local optimal gateway selection process is used. The *SNGM*s are piggybacked to the hello messages exchanged between the network neighbors. For ELS, a proactive routing scheme is used within the scope and a reactive routing scheme is used to reach nodes outside the scope. The *SNGM*s are piggybacked to the route update messages that are broadcasted within each node's scope.

In our third experiment, the mobility is varied to evaluate the routing performance of ELO and ELS. The results shown in Fig. 10 to Fig. 12 indicate that the packet delivery ratio for the ELO is better than that achieved by ELS. This may be due to the fact that fewer nodes qualify to be the gateway nodes when the optimal gateway node is chosen within a larger scope, and the same gateway node may be chosen again when the previous end-to-end route breaks. The results also show that ELS has better performance in terms of overhead and average delay. This is because unlike the ELO scheme which uses a reactive routing scheme that incurs large overhead and long delay for high mobility scenarios; the ELS scheme uses proactive routing schemes within the scope and thus can achieve smaller overhead and lower average delay.

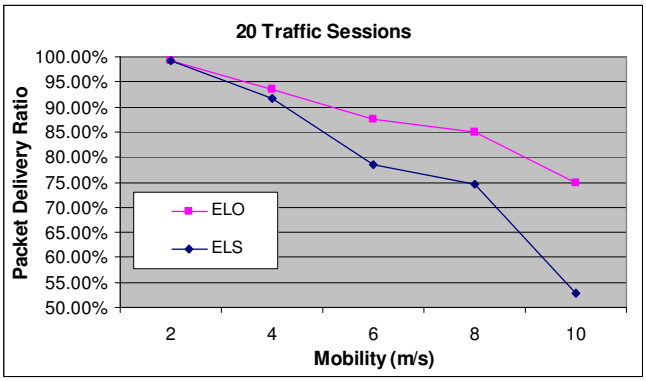

Figure 10. Packet Delivery Ratio vs. Mobility for the two schemes

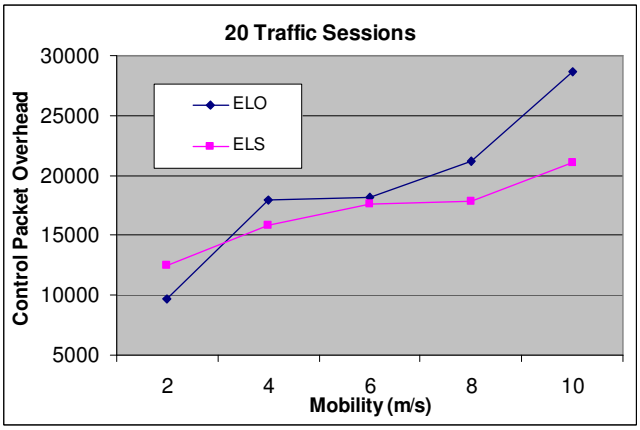

Figure 11. Overhead vs. Mobility for the two schemes

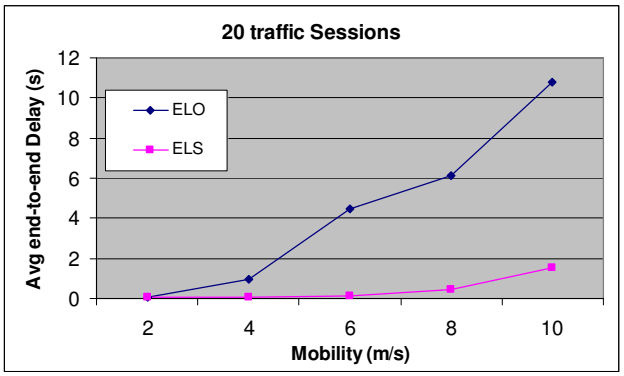

Figure 12. Average Delay vs. Mobility for the two schemes

C. *Comparison of IFD, ELO and ELS*

To compare the three schemes proposed in this paper, we plot the packet delivery ratio, the overhead and the average delay results we obtained for the three schemes on the same curve in Fig. 13, Fig. 14 and Fig. 15 respectively.

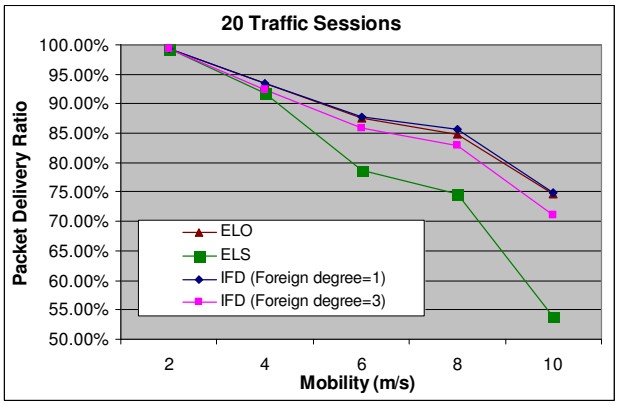

Figure 13. Packet Delivery Ratio vs. Mobility for the three schemes

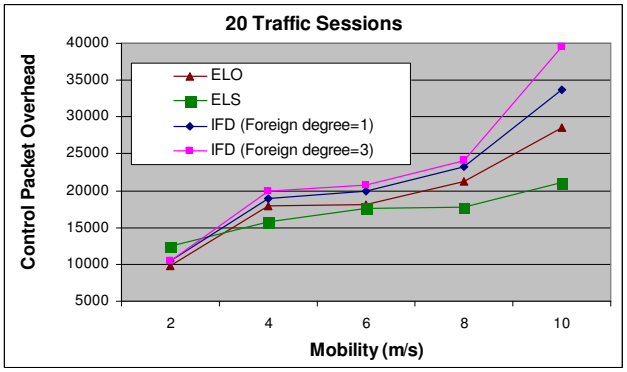

Figure 14. Overhead vs. Mobility for the three schemes

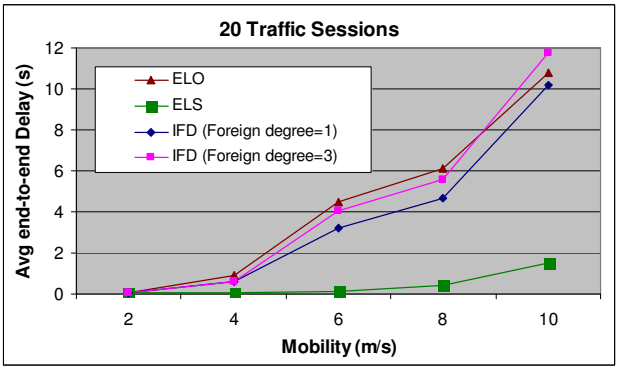

Figure 15. Average Delay vs. Mobility for the three schemes

As we can see, comparing to IFD, ELO scheme shows similar packet delivery ratio and average delay performance but smaller overhead, while ELS scheme gives comparable packet delivery ratio performance but with significantly smaller overhead and average delay.

D. *Comparison of IFD, ELO, ELS and LANMAR*

LANMAR [7] is a scalable routing protocol designed based on fisheye protocol. In LANMAR, there is a two-level fisheye for each node, link state updates within the scope is performed at a certain frequency, and the distance vectors of all the landmarks and drifters in the entire network are updated globally at another frequency. This means that every node in the network needs to maintain the distance vectors for the landmarks of all the logical groups and drifters of its own logical group. Since the route update packets for landmarks and drifters need to be flooded over the whole network, using LANMAR actually make the assumption that there is a global setting for all the nodes in the network. Thus, it can not fulfill the requirement for inter-domain routing where different ad-hoc groups may have different settings. In our approaches, only hello-like messages are exchanged between neighbors, which can be easily implemented. Based on the information exchanged in these messages, only qualified nodes (gateways) will be selected to relay packets between different ad hoc groups.

To show the improvement introduced by our design, we studied the performances of LANMAR [7] protocol using the commercial version of Globosim [8], and compare them to the performances of our schemes. In this experiment, 40 traffic sessions scenario is used. The fisheye scope for LANMAR is set to 2 hops and the update frequency within the fisheye scope is the same as the update frequency of the hello-like messages used in our approaches. The results are shown in Fig. 16, Fig. 17 and Fig. 18.

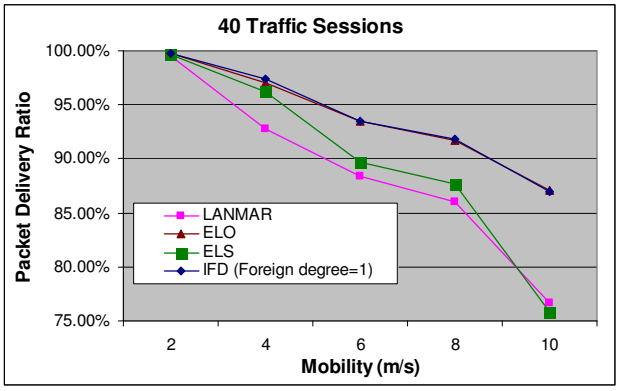

Figure 16. Packet Delivery Ratio vs. Mobility for the four schemes

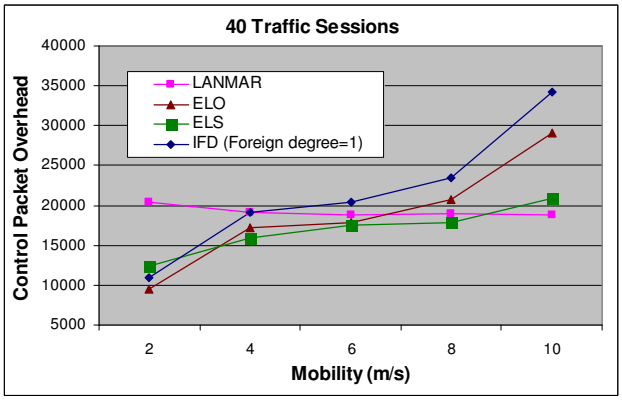

Figure 17. Overhead vs. Mobility for the four schemes

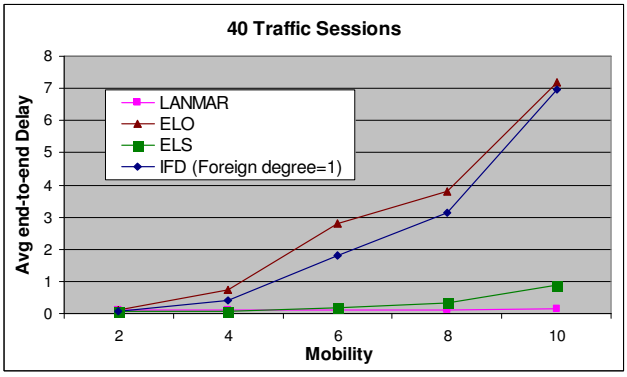

Figure 18. Average Delay vs. Mobility for the four schemes

The studies show that our inter-domain routing approaches can achieve comparable performance as LANMAR, a scalable routing scheme designed for a single network. Although in our approaches, only nodes that meet the gateway requirements are allowed to relay the interdomain route requests which results in longer route discovery time, our approaches can still allow different adhoc groups to communicate efficiently with high delivery ratio and low routing overhead, especially in low to medium mobility scenarios (less than 8m/s).

VI. Conclusions and Future Work

In this paper, we have proposed three interdomain ad-hoc routing schemes, two of which are reactive-based schemes while the third is a hybrid proactive-reactive based scheme. The two reactive-based schemes are the implicit foreign-degree based routing scheme (IFD) and the explicit locally optimal (ELO) routing scheme. In these two schemes, the number of the nodes that can respond to the interdomain route requests are dynamically restricted such that a high packet delivery ratio and relatively low end-to-end delay can be achieved without incurring a high routing overhead that is experienced by typical flooding style routing protocols. Our simulation results indicate that the ELO scheme achieves similar packet delivery ratio and end-to-end delay as those achieved using IFD scheme but with lower overhead. We also propose another scheme i.e. the Explicit Limited Scope (ELS) routing scheme which uses hybrid proactive/reactive approaches. Among the three schemes, the ELS scheme is the best scheme in terms of achieving high packet delivery ratio at low routing overhead and average delay. The ELS scheme also provides better packet delivery ratio and routing overhead than the LANMAR scheme, a hierarchical routing scheme proposed in the literature, with mobility lower than 8 m/s.

In this paper, we use the same routing protocol for the different ad-hoc groups in the simulation. In future, we intend to study the performances of the interdomain routing scheme using different intradomain routing protocols. In addition, we only consider using the number of foreign nodes as a metric for the gateway requirement in this paper. In future, we intend to use other metrics like remaining power as well. For interdomain communications, security issues are also important e.g. how we can prevent adversaries from pretending to be a node in a foreign group and hijack the traffic. Such issues need to be addressed and we leave them for our future work.

References

[1] D. Johnson, D. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks", Proceedings of ACM Sigcomm, August 1996.

[2] C. Perkins, E. Royer, "Ad-hoc On-Demand Distance Vector Routing", ACM WoWMoM, Seattle, WA, pp. 26-33, August 1999.

[3] S. Das, C. Perkins, E. Royer, "Performance Comparison of Two On-demand Routing Protocols", Proceedings of IEEE Infocom, March 2000.

[4] K. Xu, M. Gerla, "A Heterogeneous Routing Protocol Based on a new stable clustering scheme", Proceedings of Milcom, 2002.

[5] Y. Sun, E. Royer, and C. Perkin, "Internet Connectivity for Ad Hoc Mobile Networks," International Journal of Wireless Information Networks special issue on Mobile Ad hoc Networks, 9(2), April 2002.

[6] M. Ergen and A. Puri, “MEWLANA – Mobile IP Enriched Wireless Local Area Network Architecture”, Proc. IEEEVTC, September 2002.

[7] Mario Gerla, Xiaoyan Hong, Li Ma, and Guangyu Pei, “Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks”, IETF Internet Draft, MANET Working Group, draft-ietf-manet-lanmar-05.txt, November 2002.

[8] M. Takai, L. Bajaj, R. Ahuja, R. Bagrodia, and M. Gerla, “GloMoSim: A Scalable Network Simulation Environment”, Technical report 990027, UCLA, Computer Science Department, 1999.

[9] IEEE Computer Society LAN/MAN Standards Committee, “Wireless LAN Medium Access Protocol (MAC) and Physical Layer Specification”, IEEE Std 802.11-1997. The IEEE, New York, NY, 1997.

[10] X. Hong, M. Gerla, G. Pei, C. Chiang, “A Group Mobility Model for Ad-hoc Wireless Networks”, Proceedings of the 2nd ACM International Workshop on Modeling and Simulatoin of Wirelss and Mobile Systems, 1999.

[11] K. Wang, B. Li, “Group Mobility and Partition Prediction in Wireless Ad-hoc Networks”, ICC 2002 IEEE International Conference on Communications, pp. 1017-1021, April 2002.

[12] C. de waal, M. Gerhaz, “BonnMotion: a mobility scenario generation and analysis tool”, Communications Systems group, Institute of Computer Science IV, University of Bonn, Germay, http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion/, 2003.