DOMAIN BASED HIERARCHICAL ROUTING FOR LARGE HETEROGENEOUS MANETS

Karthikeyan Chandrashekar[*], Raquel Morera[Ψ], Anthony McAuley[Ψ], John Baras[*]
[*] Institute for Systems Research, University of Maryland, College Park, MD, USA
[Ψ] Telcordia Technologies, One Telcordia Drive, Piscataway, NJ, USA

ABSTRACT

This paper proposes a domain based hierarchical routing for large ad hoc networks. Our approach is based on auto-configured optimized routing domains and an enhanced inter-domain routing scheme. The large heterogeneous ad-hoc network is divided into more scalable homogeneous domains where each domain can run the routing protocol that best suits its link and traffic characteristics. We here propose an inter-domain routing protocol that exploits existing messages needed to maintain the domain structure. To support heterogeneity, the inter-domain routing scheme is independent of the routing protocols running in each domain. We compare three different approaches to the inter-domain routing: a) based solely on the propagation of domain messages, b) border node based, c) dynamic border node. In this paper, OPNET simulations compare the performance of the different inter-domain routing schemes and show the benefits of the proposed approach using OLSR and DSR as intra-domain routing protocols. Results show significant reduction in protocol overhead, increased route stability and increased route availability in a dynamic heterogeneous network. It is worth mentioning that the increased route stability is not only given by the isolation of more mobile nodes from the rest in a single domain, but also by limiting the cross-layer interactions (e.g. as the routing overhead increases, collisions at the MAC layer increase and therefore more routing packets get lost).

I. INTRODUCTION

Mobile Wireless Ad Hoc Networks (MANETS) are a set of connected wireless nodes configured to form an infrastructure-less network. MANETS are extremely important to those applications were there is a need to rapidly deploy a network without any pre-existing infrastructure, i.e. future battlefield networks, sensor networks and emergency networks.

[*] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance (CTA) Program, Cooperative Agreement DAAD19-2-01-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

Multihop routing is essential to MANETs. But, scalability of routing protocols is a growing concern. As routing protocol performance (e.g. overhead, convergence time) depends on many factors (e.g node mobility, link or traffic characteristics), most MANET flat routing protocols perform well under specific conditions but do not scale well in general e.g. [2]. Even approaches to scalable routing that use multiple routing schemes [3-7] do not perform well under all conditions. It is therefore imperative to be able to choose routing protocols based on the current prevailing network conditions.

In this paper we propose a domain based hierarchical routing framework and an inter-domain routing protocol to achieve scalable MANET routing and support heterogeneity of intra domain routing. Dividing the network into smaller independent routing units (thus creating hierarchies) is a well-known approach to achieve scalable routing. Dividing the network into homogeneous domains aids network configuration and management and also improves network functions like routing, security etc [1]. This architecture allows networking functions to operate with more homogenous and limited number of nodes. Inter-domain communication is then carried out through border nodes. For inter domain routing we propose a scheme that exploits the domain maintenance protocol [11], so it does not add extra protocol overhead on the MANET, and provides stability in maintaining shortest paths. Landmark, based on dynamic hierarchies and dynamic addressing, and Fisheye routing or LANMAR based on fixed addresses are existing solutions to scalable MANET routing. However, our approach differs from those previously proposed in the literature as it allows for heterogeneity of routing protocols in the different domains, and provides an integrated solution with the configuration scheme (thus better supporting dynamic addressing).

The paper is organized as follows, in section II we describe our framework for scalable routing, and in section III we describe the inter-domain routing protocol. Section IV presents OPNET simulation results showing the benefits of our approach by evaluating protocol overhead, route stability and data delivery in a dynamic heterogeneous network. Section V concludes the paper.

II. FRAMEWORK FOR SCALABLE ROUTINIG IN MANETS

To provide scalability to the routing functions and support heterogeneity, we divide the network into independent routing domains. Routing domains are a generalization of the notion of clusters used in the literature. Each domain can run the routing protocol that best suits the characteristics of the nodes in that domain. The inter-domain routing scheme ensures that routes connecting independent domains are formed and maintained.

Figure 1 below shows a simple illustration of the above idea where a single connected network is split into two domains. Every node can belong to only one domain. Each domain is configured with a different IP address mask. The domain with IP addresses 192.0.0.X runs OLSR [8] and the domain configured with IP addresses 192.0.1.X runs TORA [9]. In the figure, there are two border routers in each domain. The border router can communicate with multiple domains at a time. Border nodes are single interface nodes on the same physical channel that other border nodes from other domains and therefore are able to communicate among themselves even they have been configured as separate domains.

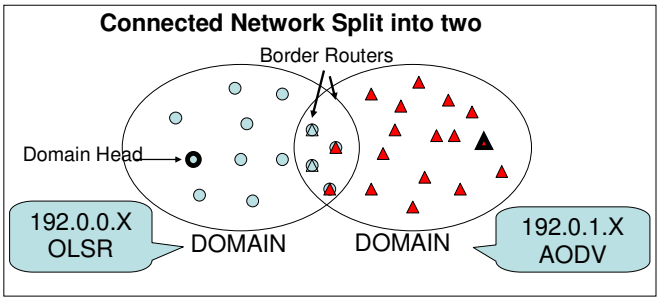

Figure 1: Multi-domain framework

A. *The Beacon Protocol*

To maintain the domain structure as nodes move and the topology changes, the network must run a domain maintenance protocol, such as the beacon protocol proposed in [11]. In every domain there is a beacon node responsible for periodically broadcasting the beacon message. The beacon message contains a field that represents the Domain Identifier ID (DID). When nodes receive a beacon message, they first check the DID to whether it corresponds to a beacon message from their current domain. If so, nodes forward the beacon message to their neighbors. Contrary, nodes first evaluate the information contained in the beacon message (e.g. priority field) to decide whether to join the new domain or remain in their current domain. Any combination of the following metrics: beacon age, node degree, number of nodes in current domain, lowest ID can be encoded in the priority field for nodes to determine if a domain change is required. Beacon messages from a different domain are not forwarded to neighbors. If a node does not hear the beacon message from its domain for a certain period of time and it hears a beacon message from a different domain, it associates to the new domain. Once a node is associated with a domain, it obtains configuration information from that domain using, for example, DRCP/DCDP [12].

Nodes receiving beacons from multiple domains become border nodes for their domains. Border routers curtail the spread of the beacon messages thereby defining the boundary of the domains. Border routers are the only nodes capable of communicating across domains even though they have only one IP interface.

B. *Intra-domain Routing*

Border routers drop packets from other domains, restricting any broadcast message within the domain boundaries. Thus routing messages are restricted within the domain boundaries. For intra-domain routing, any of the existing MANET routing protocols can be selected. The choice of the protocol clearly depends on the characteristics of the domain (e.g. traffic type and number of nodes). The key feature of the proposed domain based routing framework is that we are able to run the routing protocol best suited for the characteristics of each domain.

C. *Inter-domain Routing*

Achieving good performance of the inter-domain routing protocol is challenging, especially in MANETs where even the border nodes may consist of single interface nodes with limited bandwidth and energy. The designed inter-domain routing protocol must account for the following: a) stability of the inter-domain routes, minimize oscillation amongst different routes; b) minimize the non-optimality of the routes; c) minimize overhead in the network; d) minimize sensitivity to border router mobility (or dependency on the mobility of border routers); e) support heterogeneity of domains, i.e. be independent of the routing protocol running in each domain.

In the Internet, the Border Gateway Protocol [10] performs the inter-domain routing functions. A BGP like protocol in our context requires the external domain border routers to exchange routing, placing considerable dependency on border routers. Thus, this may not the best approach for dynamic networks where the border routers are mobile. In MANETs, several approaches have been proposed to scalable routing, e.g. Zone Routing Protocol (ZRP) [4, 5] Cluster Based Routing Protocol (CBRP) [3] and Landmark routing (LANMAR) [6][7]. ZRP uses a proactive protocol

within the local zone and a combination of a reactive routing protocol and border-cast protocol for inter-zone routing; this approach is heavily dependent on border routers. LANMAR uses Fisheye routing within the local scope. Clusters are formed based on node mobility characteristics. Cluster heads within each group become the Landmarks for inter-domain routing. Landmark-based hierarchical addressing allowing packets to be routed based on the landmark (group) as well as the host ID. However, there is no existing solution that meets all objectives of inter-domain routing aforementioned. Then, we propose the following inter-domain routing protocol described in the next section.

III. INTER-DOMAN ROUTING

In this section we propose an inter-domain routing scheme that uses the beacon protocol to discover routes to external domains. Routes within a domain are discovered and maintained by the intra-domain routing protocol. The proposed protocol is independent of the nodes characteristics (fast moving, stationary…) and the intra-domain routing scheme selected for each domain. We first described a simple inter-domain routing mechanism based only on the beacon protocol and then an enhanced scheme that includes border router information.

A. Beacon Based Inter-Domain Routing

As the goal of inter-domain routing is to ensure that every node in the network learns the existence of all subnets (prefixes), we propose the inter-domain routing protocol to use the beacon messages also as routing messages by including the DID in the IP address prefix of each domain and allowing beacon messages to cross domain boundaries rather than stopping the propagation of the beacon at the border routers. Thus, the entire network knows the DID and IP address prefixes of all domains in the network and the "direction" where domains are located. The downside of this approach however is obviously an increased protocol overhead.

To allow propagation of the beacon message across domains, we make modification to the beacon message. We add a flag to indicate whether the message is intended for domain maintenance or inter-domain routing. The flag is set to DOMAIN when the beacon message propagates within the domain boundaries and it is then used to maintain domains. Border nodes, change the flag to ROUTING and forward the message outside the domain boundaries. In the original operation of the beacon protocol border nodes would not propagate beacon messages from neighboring domains. Nodes receiving beacon messages with the flag set to ROUTING store the subnet information (or DID) in their forwarding tables. The subnet mask (or DID) is stored as the destination address and the address of the node from which the beacon is received is stored as the next-hop to that destination (see figure 2). Every node knows the next-hop node to all destination subnets in the network, so packets outside the domain are routed based on DID. Nodes may receive multiple copies of the same beacon message, as it is a broadcast message. The sequence number in the beacon message is used to discard multiple copies. As nodes only store routing information for the beacon message that arrives first, routes to the destination domains are always the fastest (shortest path and less congested).

Figure 2 illustrates the inter-domain routing protocol. Node 192.0.0.1 receives the beacon from domain 1 (subnet 192.0.1.X) from node 192.0.0.2. Thus node 191.0.0.1 stores 192.0.0.2 as the next-hop for the subnet destination 192.0.1.X.

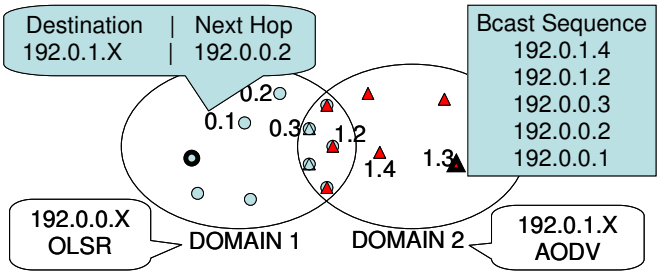

Figure 2: Beacon based inter-domain route discovery

1) Data forwarding

Routes to destinations within the domain are discovered by the intra-domain routing protocol. When the destination does not belong to the domain, packets are forwarded to the next-hop towards the destination DID. Hop by hop, packets finally reach the destination domain where these are routed to the destination node using the intra-domain routing protocol.

This scheme is simple, but the accuracy of the routes depends on the beacon update frequency, as routing tables for inter-domain routing are updated upon reception of beacon messages. When the beacon frequency is not high enough to follow the dynamics of the network (i.e. node mobility and link failures), the next-hop information to other domains may become invalid or may not be in the shortest path to the destination (i.e. "next-hop" is more than 1 hop away and the intra-domain routing find the path to it). However, refreshing the routes more frequently by increasing the beacon frequency, increases protocol overhead. In this approach link changes at any of the intermediate node pairs between a source and a destination subnet results in a change in the path between the source and the destination, creating oscillations between routes.

B. *Border router and beacon based inter-domain routing*

We enhance the previous protocol by making the next-hop node to other domains be a border router rather than the neighbor from which the beacon message for a specific domain was received. The list of next-hop nodes is now a set of border routers that need to be traversed to reach the destination from the source. A node retains its border router status while keeps receiving domain maintenance beacon messages from more than one domain. To incorporate this enhancement we add a new field to the beacon message, named LAST_BR. When a border router retransmits the beacon of a different domain it adds its address to the LAST_BR field. A node that receives the beacon checks if a valid LAST_BR field exists, if so, the node adds the LAST_BR address to the forwarding table as the next-hop to the destination domain.

1) Data forwarding

As before, destinations within the domain are handled by the intra-domain routing protocol. For an out of domain destination the next-hop address is that of a border router. The intra-domain routing is now responsible for finding the shortest path to the border router. This process continues until the destination domain is reached.

Clearly with this enhancement the number of link changes is limited to the set of neighboring border routers and hence we expect that near-shortest-path routes will be maintained between the source and the destination. In this approach routes to other domains are more stable, but the protocol is sensitive to border router mobility.

IV. SIMULATION ENVIRONMENT AND RESULTS

We have implemented the beacon protocol and the inter-domain routing in OPNET. We set up a simple domain based network to emphasize the benefits of domain based routing in terms of overhead and convergence properties of the routing. We then evaluate our inter-domain routing scheme in terms of data delivery and overhead.

We first compare the performance of the network when running flat routing (i.e. without any domains) and with domains. The comparison metrics are routing overhead, convergence time and data delivery. To this end, we design a simplistic scenario with 26 nodes as shown in Figure 3; where the network is split into four domains. Three of these domains are encompassed by fixed nodes and domain (4) consists of moving nodes. The nodes in each domain are automatically configured to belong to different subnets. The beacon protocol is used to maintain domains and the beacon nodes or domain heads are pre-configured. In this scenario, nodes 1,8,13 & 15 are the beacon nodes for the 4 domains. The beacon frequency is 5 seconds. Nodes in the moving domain (4) move according to the Billiard mobility model. The node speed varied from 0 – 10 m/s. Sources in the network generate UDP traffic 10 kbps flows with the packet size being 300 bytes. There are 3 sources in the network and they are chosen such that there is a source from each of the 3 static domains. The 3 corresponding destinations are chosen from the moving domain (4). For simplicity we run OLSR in all domains. In the non-domain case OLSR is used as the flat routing protocol across the network and in the domain case OLSR runs within the local scope defined by the domains. The inter-domain outing protocol implemented is the beacon based inter-domain routing protocol. 802.11b is used as the MAC layer.

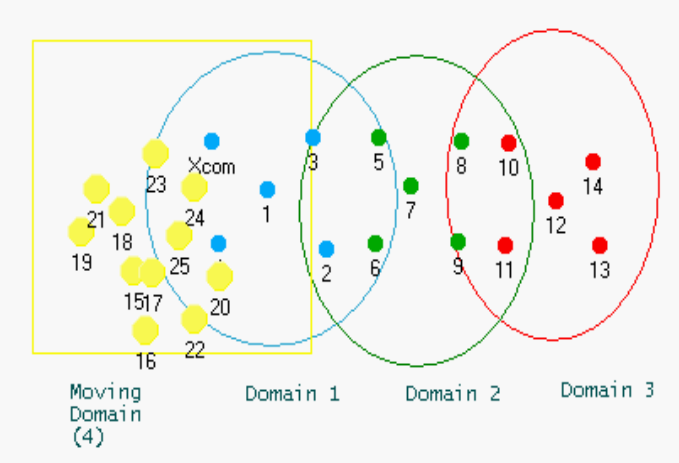

Figure 3 Simulation Scenario

Figure 4 shows the comparison of the total routing traffic (OLSR traffic) received by all nodes in the network for the single domain case (flat routing) and for the case where the network is split into different domains. For each case, there are two graphs, one when all nodes are static, and another one when some nodes in domain (4) are mobile. In this case there is no user traffic.

The routing overhead of OLSR is due to the exchange of the HELLO, TC (Topology Control) and the HNA (Host-Network Address) messages. As expected, we observe that the overhead due to the exchange of routing messages is lower in the domain based network than the non-domain network (less than 40%). In the domain based network routing messages are contained within the domain whereas in the non-domain network the routing messages are propagated throughout the network. As OLSR is a proactive protocol, route updates are initiated periodically and the routing overhead is independent on link changes. This is also shown in the bottom graph of Figure 4.

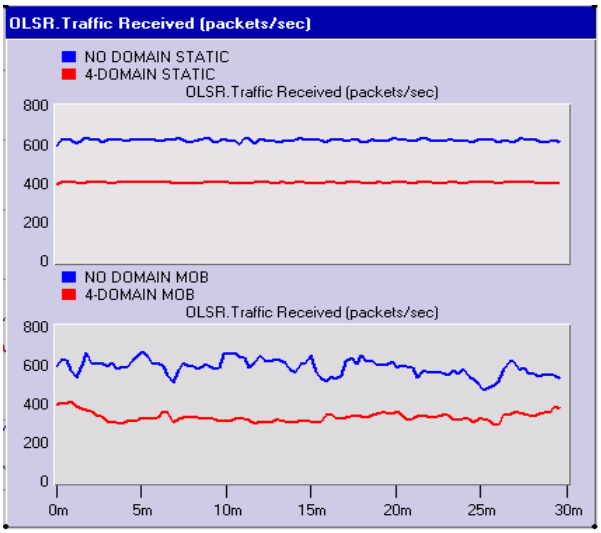

Figure 4: Routing overhead

To account for overhead introduced by the beacon protocol used for inter-domain routing in the case of multiple domains, Figure 5 shows the total traffic (routing and beacon) load at the MAC layer. This is an indication of the total control protocol overhead as there is no data traffic in this scenario. Clearly, we see that the domain based network has lesser overhead than that of the flat non-domain network despite the overhead of the beacon messages. Mobility has no impact in these conclusions. We observe some fluctuations in the curves originated by MAC layer collisions of broadcast messages, thus loss of the signaling packets.

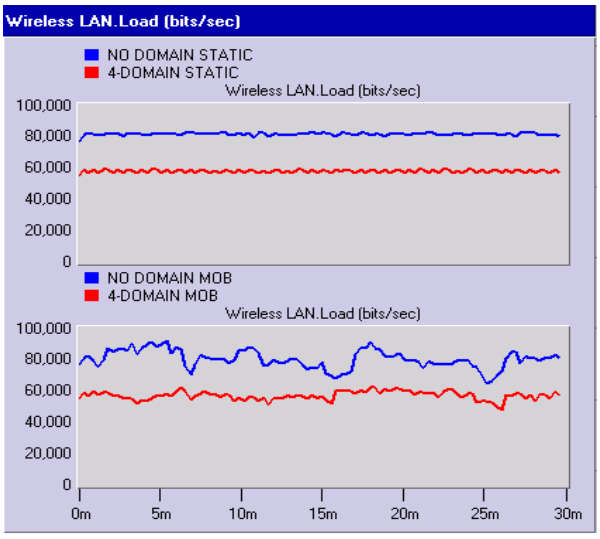

Figure 5: Total overhead

Convergence time must also be considered when evaluating scalability and stability of routing protocols. Figure 6 shows the convergence properties of OLSR routing in the non-domain and the domain case. Convergence activity is an event that results in the addition, update or deletion of an entry in the routing table. The routing is said to have converged if there is no convergence activity for a fixed duration T. We would like to point out that convergence activity does not mean that there are unknown routes still being discovered, it just implies that the routes are being updated as better paths are being discovered. In the graph a transition from 0-1 indicates the start of a new convergence period and the transition from 1-0 the end of the period, the corresponding abscissa value indicated the duration of the convergence period. We see that the non-domain static scenario has several convergence windows of significant duration (order of minutes) whereas the domain static network has convergence windows that converge quickly (order of seconds). This indicates that localizing the routing information can improve the convergence properties. We see that mobility exaggerates the situation with the domain based network also experiencing significant convergence activity. Also both networks have continuous convergence activity after some time which is indicated by the lack of lines on the graph (at time 12m for the non-domain case and at time 16m for the domain based network). Mobility can significantly affect the convergence properties of the routing and again we see that the domain based network is better than the non-domain network as the convergence activity is now restricted to the local routing scope. Then, the effect of changes has also more limited scope.

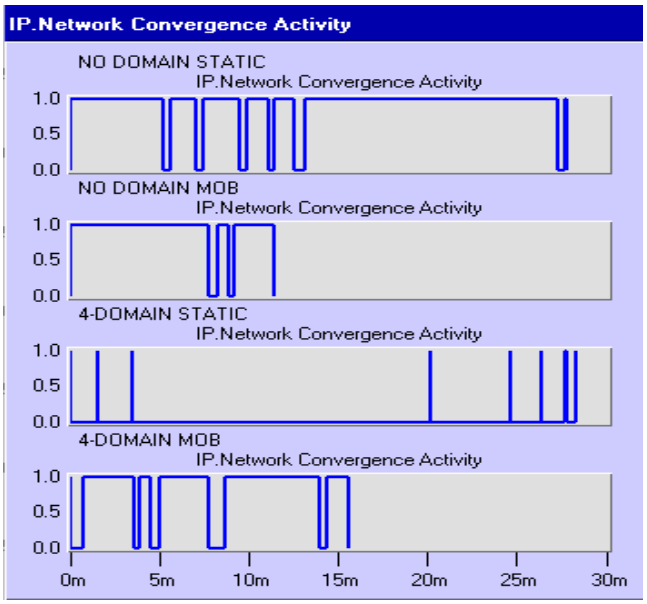

Figure 6: Convergence activity

A better understanding of the behavior of the convergence activity can be obtained by looking at the number of packets dropped due to collisions at the MAC layer. Figure 7 shows that a significant number of packets are dropped due to collisions in the non-domain network when compared to the domain based network. This is due to the extra traffic

generated in the network, result of the excess propagation of the routing messages in the non-domain network. Furthermore we see that mobility also affects the number of collisions as the 1-hop neighborhood is now continuously changing. Localizing the routing within domains also reduces the impact of the MAC.

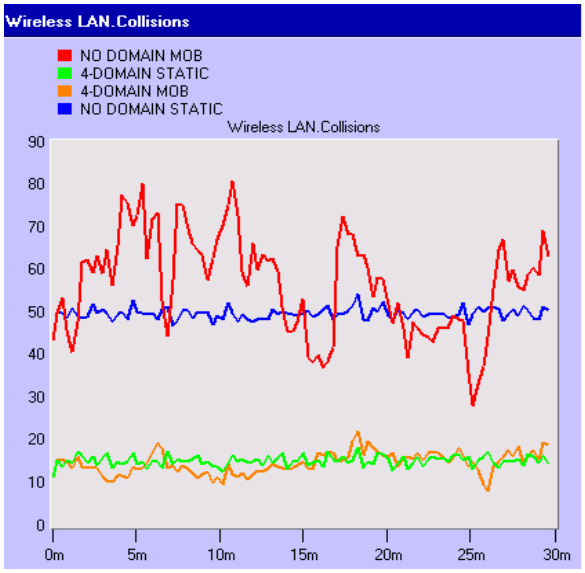

Figure 7: Packets dropped due to MAC collisions

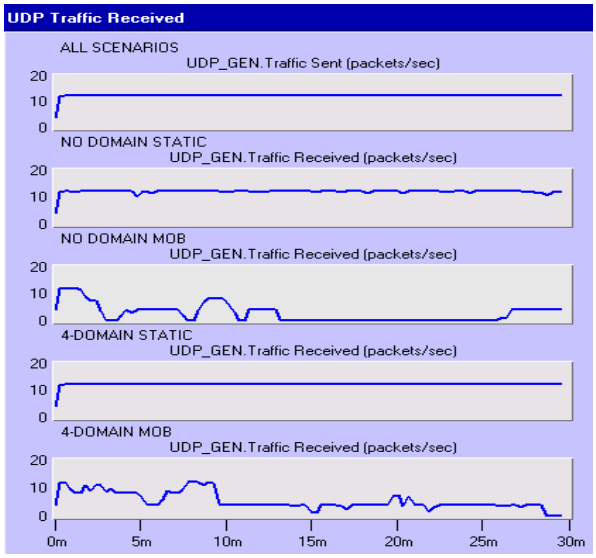

Figure 8: Data traffic sent and received

Figure 8 shows the data sent and received in the various scenarios. The domain based static network receives all the traffic sent by the sources. The non-domain static network experiences slight losses due to MAC collisions. In the mobile scenarios (remember the destinations are in the mobile domain) there is a significant loss in data received; this is due to a combination of lack of routes to destination as well as MAC layer collisions. We see that the domain based mobile network performs significantly better than the non-domain mobile network. The partitioning of networks into domains also improves data delivery.

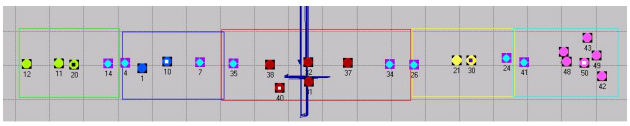

Figure 9: test scenario

We now construct a simple test scenario shown in Fig 9 consisting of 5 domains all with fixed nodes except for nodes in the center domain (31&32), with 31 having a horizontal motion pattern and 32 having a vertical motion pattern. The sources are in the leftmost domain and the destinations are in the rightmost domain. The objective is to show the resilience of the border router based inter-domain routing to link changes of the nodes in the center domain. This follows from the idea that this form of routing depends only on the path of border routers between the source and the destination.

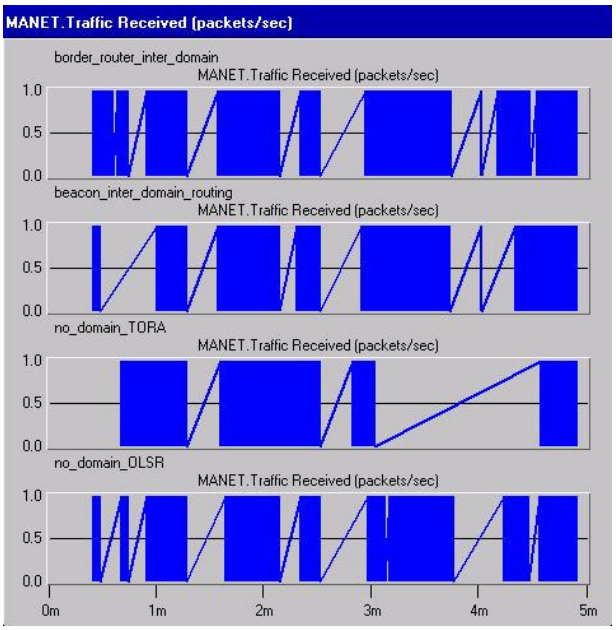

Figure 10: Traffic received

Fig 10 shows the data packets received at the destination as a 0-1-0 transition. Clearly, the border router based inter-domain routing protocol performs better (more 0-1-0 crossings) than the plain beacon based routing protocol which will be affected by the link changes of the moving nodes. This shows the intrinsic benefit of using the border router information. Furthermore, the domain based routing schemes perform better than the single domain network case for both the proactive (OLSR) and reactive (TORA) routing protocols. This further highlights, our argument that dividing networks into domains can benefit routing whether be it proactive or reactive.

Table 1 below shows the percentage of MANET traffic successfully delivered for various protocols in a scenario with 5 domains, each consisting of 10 nodes. Standard protocol settings were used for TORA, DSR and OLSR. The beacon interval was 20 seconds. The results shown in Table 1 are for a static scenario. For the border node interdomain routing approach we tried two configurations that we name "BR" and "BR_dynamic". In the former, fixed nodes near the boundary between domains are explicitly designated as border router. This results in a fixed number of border routers per domain, one per boundary. In the latter scheme, nodes become border routers based on the beacon messages they receive. The dynamic scheme could result in several border routers per domain, thereby, increasing reliability and the number of stale border routers. We observe that DSR, a reactive protocol performs the best. DSR is an on-demand routing protocol and for the data traffic carried in this scenario has less overhead than OLSR (a proactive routing protocol). Figure 7 shows that there are a large number of MAC collisions that generated routing packets losses and therefore route fluctuations. Table 1 shows that beacon based inter-domain routing and dynamic BR interdomain routing perform better than the non-domain OLSR case. This is because domains reduce overhead and moreover the border router based scheme is more stable to route fluctuations. However, the fact that the BR inter-domain routing performs poorer than non-domain OLSR is counterintuitive. This is due to the fact that in this topology we only have a single BR per domain, therefore, a single point of failure. If the beacon message is lost due to MAC collisions, the inter-domain routing is severely affected. Plain OLSR provides more diversity in such scenario. However, with dynamic BR, the overall throughput is better due to the reduction in the overhead and limiting the number of collisions.

Routing Scheme	**% data delivered**
No_domain_OLSR	45%
No_domain_TORA	32%
No_domain_DSR	88%
Domain_plain	53%
Domain_BR	38%
Domain_BR_dynamic	61%

Table 1: MANET traffic delivered

V. CONCLUSIONS

The domain based framework for routing in ad hoc networks can provide scalable routing. Moreover, the network supports diversity in choosing the intra-domain routing protocols. We see that the domain framework enhances routing by reducing overhead and enhancing data delivery. The inter-domain routing protocol is independent of the intra-domain routing and is based on the beacon protocol. We see also suggest an enhancement to the inter-domain routing protocol that incorporates the border router set to improve path stability. Results show that the total overhead in a domain based network including the cost for maintaining domains is still less than that of non-domain or flat networks. Even for a simple network split into 4 domains we can reduce the routing overhead by 25%. Work is currently in progress to set up experiments with multiple routing protocols running in different domains. We are also studying the stability of critical nodes like domain heads and the border routers.

REFERENCES

[1] R. Morera & A. McAuley, "Flexible Autoconfigured Domains for more Scalable, Efficient and Robust Battlefield Networks", In *proceedings of IEEE MILCOM,* OCT 2002

[2] S.R. Das, C.E. Perkins and E. M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks", In *Proceedings of IEEE INFOCOM* 2000, Tel Aviv, Israel, Mar. 2000, pp. 3-12.

[3] M. Jiang, J. Y. Li, and Y. C. Tay. Cluster based routing protocol (CBRP) functional specification. *IETF Internet draft*, Aug. 1999. http://www.ietf.org/ietf/draft-ietf-manetcbrp-spec-01.txt.

[4] Z.J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," In *Proceedings of IEEE ICUPC'97*, San Diego, CA, Oct.1997

[5] Z.J. Haas and M. R. Pearlman "Determining the Optimal Configuration for the Zone Routing Protocol", In *IEEE Journal on Selected Areas in Communications*, Aug. 1999, pp. 1395-1414.

[6] G. Pei, M. Gerla and X. Hong, "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility," in *Proceedings of IEEE/ACM MobiHOC 2000*, Boston, MA, Aug. 2000, pp. 11-18.

[7] M. Gerla, X. Hong, G. Pei, "Landmark Routing for Large Ad Hoc Wireless Networks", *IEEE GLOBECOM 2000*, San Francisco, CA, Nov. 2000.

[8] T. Clausen and P. Jacquet "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group, October 2003.

[9] V.D. Park and M.S. Corson, "A Highly Adaptive Distributed RoutingAlgorithm for Mobile Wireless Networks," In *Proceedings of IEEE INFOCOM'97*, Kobe, Japan, Apr. 1997, pp. 1405-1413.

[10] Rekhter, Y., and T., Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[11] R. Morera, et al, "Robust Router Reconfiguration in Large Dynamic Networks", MILCOM 2004

[12] A. McAuley, D. Chee, J. Chiang, S. Das, K. Manousakis, R. Morera, L. Wong, K. Young, "Automatic Configuration and Reconfiguration in Dynamic Networks," Army Science Conference, December 2002.

[ii] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government