

# Inter-domain Routing for Military Mobile Networks

Joy Na Wang, Joshua Van Hook , Patricia Deutsch

MIT Lincoln Laboratory

Lexington, MA 02420

Email: na.wang, joshua.vanhook@ll.mit.edu, Patricia.Deutsch@riverbed.com

**Abstract**—As more and more tactical Mobile Ad-Hoc Networks (MANETs) are deployed at the edge, there is a need to interconnect these heterogeneous MANETs to enable increased connectivity and robust communication services to the war fighters. Traditionally, Border Gateway Protocol (BGP) is considered the de facto standard inter-domain routing protocol. It was originally designed for wired networks and does not respond well to the challenges posed by mobile networks. With intermittent wireless links and frequent topology changes in tactical networks, BGP suffers from network partitioning, specifically the traditional Autonomous System (AS) split issue. One option is to re-architect the use of BGP to prevent AS splits as shown in [1]. A more scalable approach is to develop a new inter-domain routing protocol that fundamentally addresses BGP protocol limitations. The InterMR protocol proposed by UCLA dynamically detects and heals network splits. In this paper, we implement, demonstrate and evaluate the performance of interMR for connecting ground tactical MANETs with an airborne backbone. Implementation of the protocol required several design choice and adaptations. We use OPNET to compare the performance of the interMR protocol to a flat OSPF architecture and BGP with virtual routers under various mobility models. We show that InterMR heals network splits and provides a scalable approach for interconnecting MANETs.<sup>1</sup>

## I. INTRODUCTION

Current tactical networks heavily rely on the availability of SATCOM for Beyond Line of Sight (BLOS) communication. To improve connectivity, capacity and information sharing at the tactical edge, the Joint Aerial Layer Network (JALN) Analysis of Alternative(AoA) initiative was conducted in 2011. The goal of JALN is to augment existing SATCOM BLOS infrastructure to provide aerial layer connectivity that extends and interconnects existing tactical ground, surface and airborne networks. These networks are typically managed by independent entities and function as independent MANETs. The interconnection of these heterogeneous MANETs requires a scalable routing architecture that can support the frequent topological changes in a tactical environment. Previously we explored various routing architecture options for interconnecting these ground MANETs through the aerial layer backbone based on the mature internet protocols such as OSPF and BGP [1]. Specifically we consider the following:

- **Flat OSPF** All networks use a single converged routing layer and a proactive routing protocol OSPF is employed. Every node has information about every other node in

the network and there is no possibility of a network split. Every node is in the same MANET as shown in Fig. 1(a). Every time there is a link change, link-state advertisement (LSA) packets are flooded throughout the network, resulting in significant routing overhead as the network size increases. In addition, it is difficult to require every interconnected network to employ the same routing layer (routing protocol) especially given that the individual networks may utilize different radios or waveforms. Finally, it is not possible to enforce any policy control on a flat network.

- **OSPF with Areas** To remediate the scalability issue associated with a flat OSPF architecture, OSPF with areas can be used to limit LSA flooding as shown in Fig. 1(b). This architecture is susceptible to network splits.
- **Plain BGP** Applying BGP to the airborne scenario, the airborne backbone communicate with one or more gateways in each service network through eBGP links as shown in Fig. 1(c). In comparison to flat OSPF, the control plane traffic of BGP is lower as the dynamics in one ground service network are totally separated from the other service networks and from the airborne backbone. However, the traditional AS split issue exists as a service network can split due to mobility and/or terrain blockage. BGP will not allow communication between nodes in different subsets of the same AS in order to prevent routing loops.
- **BGP with Virtual Routers** As an extension to traditional BGP, an airborne node can spawn a virtual router for each AS domain it supports as shown in Fig. 2. In this example each airborne node has four virtual routers. Each virtual router acts as the gateway for its own AS and runs its own Interior Gateway Protocol (IGP). When a node in the service network moves out of range of its original LOS network domain but stays within range of an airborne node, it is able to communicate with the other nodes in the AS by sending data via the airborne node's virtual router. Thus, an AS never splits in this design.

From our simulation results, BGP with virtual routers was shown to provide a viable option for interconnecting heterogeneous MANETs to provide connectivity for intra-service and inter-service communications at the tactical edge. This architecture does not suffer from network partitioning as it prevents BGP AS splits from happening. Furthermore, this architecture places BGP links within the virtual links be-

<sup>1</sup>This work is sponsored by DoD CIO via Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, recommendations and conclusions are those of the authors and are not necessarily endorsed by the United States Government.

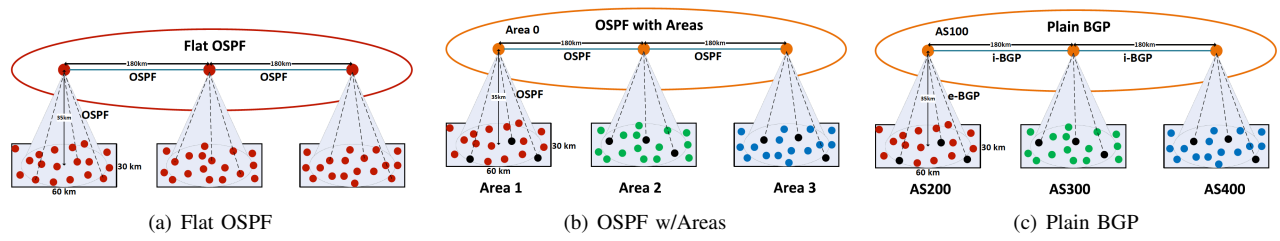


Fig. 1. Flat OSPF, OSPF with Areas and Plain BGP

tween the virtual routers, which eliminates problems arising for BGP from the intermittent connectivity characteristics of wireless links. Under various mobility scenarios, BGP with virtual routers introduces little additional overhead compared to ground networks that have no inter-domain connectivity.

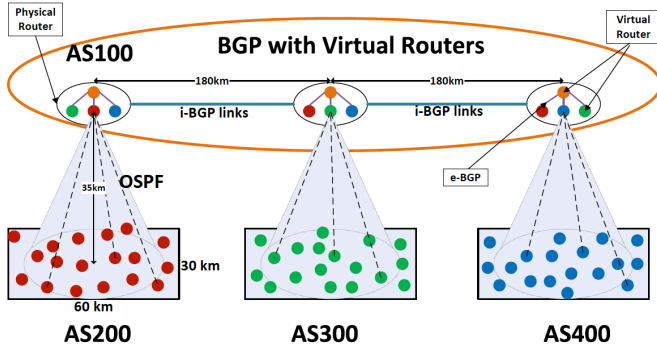


Fig. 2. BGP with Virtual Routers

However, we do recognize this solution has its own limitation as it tries to architect around BGP protocol constraints:

- **Configuration Complexity:** BGP with virtual routers requires each router to be configured to support all the AS domains within the area of the operation. The configuration can be complex as the number of potential AS's increases. If the mix of AS's were to change, the router must be reconfigured.
- **Scalability:** Theoretically, a node can be configured with as many virtual routers as are needed to cover all MANETs, but in practice the number of virtual routers is limited by the router memory. We can alleviate the issue by adding more memory to the routers but placing more hardware on the airborne node can be burdensome. There is a trade-off between the number of MANETs covered and the size, weight and power (SWaP) of the equipment. While the small networks here may not bump into a limitation on router capabilities, this approach has limited scalability.
- **Architecture limitations** BGP with virtual routers does not fundamentally address shortcomings of BGP at the tactical edge. BGP peers are still statically configured for the i-BGP wireless links.

An inter-domain routing protocol designed for mobile network is needed to fundamentally address BGP constraints. A survey of existing inter-domain routing protocols [2] was undertaken to evaluate strengths and weakness at the tactical edge. Compared to various BGP modifications [3] and [4], the family of InterMR protocols, [5], [6], [7] and [8] shows

promising features for interconnecting tactical networks. In this paper, we describe our implementation of the interMR protocol and its adaptation for connecting multiple ground MANETs via an airborne backbone. The protocol implementation is general and can also be applied to the interconnection of large number of ground tactical MANETs through LOS or SATCOM links. We compare and evaluate performance of InterMR against BGP with virtual routers and flat OSPF under various tactical scenarios.

The rest of the paper is organized as follows: Section II presents a short overview of the InterMR protocol. Section III describes OPNET design and implementation of the interMR protocol. Section IV presents simulation results comparing the network throughput and routing overhead under various scenarios. Finally section V concludes the paper and describes avenues for future work.

## II. INTERMR OVERVIEW

Inter-Domain Routing for Mobile Ad Hoc Networks (IDRM) [5] was developed by a team at the University of Cambridge and IBM's TJ Watson Research center, under sponsorship from US Army Research Laboratory and the UK Ministry of Defense. It was specifically designed to handle the challenges of routing between MANETs, namely partitioning and merges of domains and dynamic neighbors where BGP does not adapt well under mobility. In order to handle the BGP AS split issue, IDRM uses a MANET ID based on domain members and is dynamically generated. MANET ID is analogous to BGP AS numbers, like AS. Each gateway periodically advertises reachable members in a digest form, which can handle network split more gracefully compared to IP prefix abstraction used in BGP. InterMR [8] is based on IDRM. InterMR uses attribute-based addressing specifically Bloom Filters for destination resolution instead of the digest form that is used in IDRM, which adds flexibility and allows to address specific content such as an army node or a medical unit. It performs dynamic gateway selection so that only a subset of gateways can be set as active to maintain connectivity while reducing control overhead. As the network changes, the active gateways can be re-selected to guarantee coverage. There are four main components of the InterMR protocol:

- **e-InterMR:** Runs on active gateways and is responsible for inter-MANET communications including gateway discovery, detection and advertising of gateway topology changes, and detection and advertising of route changes between MANETs.

- **i-InterMR:** Similar to e-InterMR but applies within a single MANET. It runs on both active and potential gateways and detects and advertises topology and route changes that occur within a MANET.
- **Gateway Selection:** Runs on all active and potential gateways and is used to dynamically select gateways for a MANET.
- **Bloom filter:** Responsible for summarizing MANET membership and destination resolution.

InterMR has four protocol messages that are implemented for both e-InterMR and i-InterMR.

- **Beacon Message:** Beacon messages are sent on a periodic basis as a keep-alive between gateways. For e-InterMR, it is sent broadcast. For i-InterMR it is sent multicast. If there are no InterMR routing changes then the only messages that are sent are Beacon messages.
- **Request Message:** When a gateway node receives a beacon from a currently unknown gateway, it sends a Routing Table Request message to that new gateway to obtain routing information. This is sent unicast.
- **Response Message:** Upon receiving a request message, the gateway then sends a Route Table Response message with its full routing information. This is sent multicast for i-InterMR and broadcast for e-InterMR.
- **Update Message:** It is an incremental update message and does not include all routes, only those routes that are to be added or deleted. The use of an update message minimizes the transmission of routing information because full routing information is only sent when a new gateway is discovered. When changes occur, only the specific, incremental changes are sent. This message is sent unicast to all known i-InterMR gateways and broadcast to e-InterMR gateways.

### III. INTERMR DESIGN AND IMPLEMENTATION

We implemented interMR using a platform independent, modular design as shown in Fig. 3. An adapter layer provides an interface to platform specific functions. This approach allows the code to be ported between platforms more easily as development is required only for a platform specific adapter and without any changes to the InterMR code itself. The first implementation is in OPNET to study the performance of the protocol in a simulation environment. The figure shows Quagga as a second possible platform and similarly other platforms could be supported as well if a specific adapter for that platform was developed.

The following section describes implementation details of InterMR protocol components described in section II. The implementation details focus on the design considerations we have to make in our OPNET implementation under JALN scenarios.

#### A. e-InterMR Implementation

e-InterMR is responsible for routing and topology change detection between MANETs. Each active e-InterMR gateway sends a periodic beacon via one-hop broadcast. This beacon

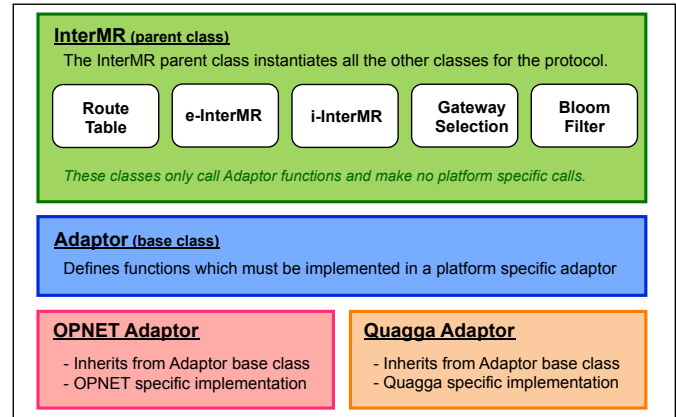


Fig. 3. InterMR Implementation Architecture

serves as a keep-alive and supports new gateway discovery. Each gateway builds a list of MANETs it is directly connected to through e-InterMR. If a gateway is not heard from in a configurable amount of time, e-InterMR will declare that neighbor dead and remove its routes from the local routing table as well as propagate those changes to its one-hop e-interMR neighbors. In addition, any update and response message can also take the place of the keep-alive and discovery functionality of a beacon. This helps reduce overall routing overhead.

If a gateway hears a new MANET ID advertised by a neighbor, the local gateway will send out a route request message asking the neighbor for its complete routing table. Upon receiving a request message, a gateway replies with a response message. This message contains all the InterMR routes with a complete path vector and is sent one-hop broadcast. Upon receiving routing information, e-InterMR recalculates the path length to each destination and selects the shortest route as the active routes. Any route changes are then sent broadcast to this gateway's one-hop neighbors via an update message.

#### B. i-InterMR Implementation

Like e-InterMR detecting neighboring gateways across MANETs, i-InterMR detects gateways inside a MANET. It makes sure the gateways share a common view of the network. The beacons in i-InterMR have been extended slightly to include connectivity information for use with gateway selection in our implementation. This design choice is made to ensure both active and inactive gateways have current connectivity information. The information in i-interMR beacons must be disseminated throughout the local MANETs. Since gateways may be multiple intra-MANET hops away, involving non-gateway nodes that do not understand interMR, multicast is necessary to flood this information across the local MANET. In this implementation, an OPNET SMF (Simple Multicast Forwarding) implementation was used, but SMF relies on flooding that is not efficient. Ideally a better wireless multicast protocol is needed, but this is still an area of research which is out of scope of this paper.

Like e-InterMR, requests, responses and updates work in a similar fashion. They allow the gateways inside a MANET to

have a consistent view of the network to effectively make routing decisions. Request messages are sent unicast to the newly discovered gateway. Response messages are sent multicast to the other gateways in the MANET. Update messages are sent unicast to each gateway within the MANET as discovered through the beacon process. We choose to use unicast for update messages because they can be large and frequent if there is a lot of churn in the local MANET. Since the architecture has few gateways this is favorable compared to something like flooding through SMF.

In addition, i-InterMR detects splits and merges in the local MANET and updates MANET ID accordingly. The MANET ID is determined from the lowest node ID of gateways in the local MANET. If the gateways cannot hear the gateway with the lowest node ID or if a new gateway with lower node ID is discovered, a MANET split or merge, respectively, is detected. This will trigger the gateways to select a new MANET ID. When the MANET ID changes, e-InterMR and i-interMR must send out route updates. Since the MANET ID selection is based on information obtained through beaconing, no additional signaling is required to trigger a change.

### C. Bloom Filter and Digest Mode

InterMR as presented in [8] used attribute-based addressing in the form of Bloom Filters. Its predecessor, IDRM, however, uses a digest mode. The digest mode was claimed in [5] to be sufficient for MANETs up to 1000 nodes.

Bloom filters are probabilistic data structures that hash a number of field such as MANET ID, node ID, IP address, etc. into a bit array. One can then determine definitely if a node is in the array or probably if it is not. There is a non-zero probability that a false positive will occur. This is governed by the number of hash functions, length of the Bloom filter and number of elements stored.

A simple analysis was conducted based on InterMR packet sizes and a typical neighbor change rate of less than 10 per second for each MANET within our network. These neighbor changes are the addition or loss of gateway neighbors, which are distinct from OSPF link changes. Bloom Filter based addressing did not reduce overhead for a low false positive rate. As such, the Bloom Filter implementation was deferred and the digest mode is currently employed. A more detailed analysis of the implications of increased network overhead due to a non-zero false positive probability as well as memory requirements of the digest mode is needed for future work. Bloom Filter based addressing, however, also has some potential benefits for policy expressiveness. Attributes such as node type (i.e. medical unit) could be included in the hash procedure. With that in mind, a richer policy can be employed than the typical BGP AS-based approach through the use of bloom filter.

### D. Gateway Selection Implementation

The InterMR routing protocol includes dynamic gateway selection as an important feature. In a MANET, it is difficult to statically assign gateways because coverage is not guaranteed. This could be mitigated by having a large number of gateways,

but this in turn produces more overhead for the network. The best solution is to employ dynamic selection of gateways so that a low number of gateways can be set as active while maintaining connectivity. As the network changes, the active gateways can be re-selected to guarantee coverage. Gateways are selected as active based on their connectivity to other MANETs. The goal is to have at least one active gateway for all known external MANETs. Information about connectivity is gathered from beacon messages and this is used by each gateway to decide whether or not it should be active. Both active and inactive gateways exchange i-interMR beacon messages to obtain connectivity information such as lists of connected MANETs and number of intra-MANET one hop neighbors.

We solve the gateway selection algorithm as a set cover problem. We propose a greedy algorithm running on every gateway node. Gateway selection is based on an ordered list of potential gateways using the following criteria:

- **Uncovered inter-MANET connectivity (Ordered from high to low):** Preference is given to gateways with more one-hop connectivity to uncovered MANETs.
- **Total inter-MANET connectivity (Ordered from high to low):** Preference is given to gateways that have more total one-hop inter-MANET connectivity while their uncovered inter-MANET connectivity may be the same.
- **Previous Gateway Status:** This helps to maintain certain stability of the protocol by preferring the currently active gateways with 1 as active and 0 as inactive
- **Intra-MANET connectivity (Ordered from high to low):** Preference is given to a densely connected gateway. This attempts to reduce the average path length in the local MANET.
- **Node ID (Ordered from low to high):** This serves a deterministic tie-breaker.

Each gateway builds the list of MANETs to cover and the list of gateways ordered per the criteria from above. The top gateway on the gateway list is selected as active, the list of uncovered MANETs is updated to exclude the MANETs covered by that active gateway. The list of gateways is then re-ordered and the top gateway on the list is then selected as active. This continues until all MANETs are covered.

This algorithm runs in a distributed fashion. Every gateway starts as active and after a configurable amount of time, the first gateway selection takes place. This is intended to give the routing protocols time to stabilize before selection takes place. After the initial selection, gateways selection runs only in response to network changes such as inter-MANET connectivity changes and intra-MANET splits or merges. In our current evaluation of the JALN scenario, the number of gateways is very small and therefore dynamic gateway selection is not used. However, we believe dynamic selection can improve the protocol performance when more gateways are present in the network.

TABLE I  
SIMULATION DEFAULT PARAMETERS

MAC	Mobile nodes: TDMA
Number of Nodes	93: 30 nodes per MANET and 3 Airborne nodes
Traffic Pattern	Intra-MANET: all to all Inter-MANET: Mesh between mobile nodes
Number of Runs	20
Propagation Model	Free space path loss
Mobility Model	Preplanned group mobility; random waypoint
MANET Routing	OSPF-MDR

#### IV. PERFORMANCE EVALUATION

InterMR was implemented in OPNET Modeler 17.1 [9]. Fig. 4 depicts part of a 93 node scenario used in the simulation. The airborne nodes are placed 35 km from the center of their respective ground network and are spaced 180 km apart from each other to cover the entire theater. Three gateway nodes (shaded black in Fig. 4) are selected in each ground network and are configured to run two TDMA networks: Ground-to-Ground TDMA network and Air-to-Ground network. Ground-to-Ground TDMA networks run distributed slot assignment with roaming disabled, while Air-to-Ground TDMA networks are running centralized scheduling with roaming enabled. The air nodes act as a hubs in this case. Each TDMA network runs on an independent frequency. There are seven TDMA networks configured in the simulation. Table I shows the default simulation parameters. Each MANET runs OSPF-MDR as its Interior Gateway Protocol (IGP) for comparison and consistency.

In the following section we evaluate InterMR in terms of its functionality as well as its overhead cost of interconnecting ground MANETs. Specifically we study whether InterMR can heal network splits under mobility. We measure the average throughput per flow under a group mobility scenario. Packet drops indicate a route does not exist or is incorrect. It is found that InterMR can heal network splits without experiencing throughput drops just like flat OSPF and BGP with virtual routers, while OSPF with areas and plain BGP cannot heal network splits [1]. Next we focus on the cost of each routing option which is routing overhead associated with interconnecting ground MANETs under random mobility scenarios. As we focus on how the ground network traffic affects the JALN backbone, the air nodes are stationary in our evaluation scenario.

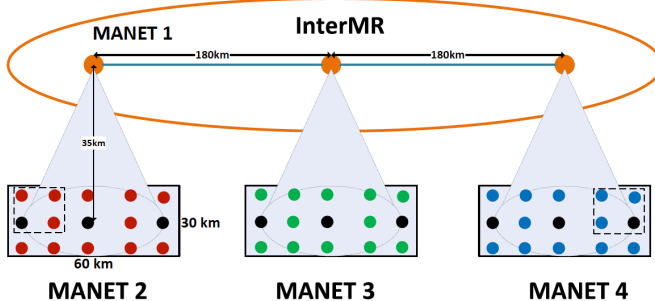


Fig. 4. InterMR Group Mobility Scenario

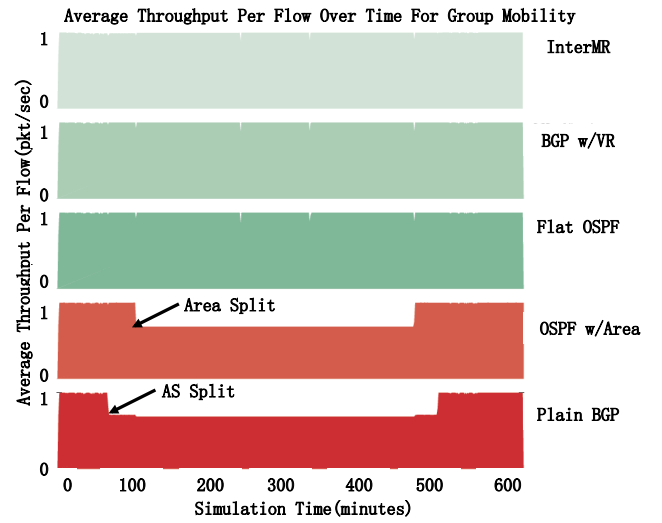


Fig. 5. Group Mobility Average Throughput Per Flow Vs Simulation Time

##### A. Group Mobility Scenario

The pre-planned group mobility as shown in Fig. 4 is used to study how InterMR adapts to node mobility in the network. The mobility pattern is as follows: MANET 2 nodes move with a constant speed of 50 mph towards MANET 4 and then move back to their original position, concurrently MANET 4 nodes move with the same speed towards MANET 2 and then back to their original position. The specific nodes that move are depicted in the figure in the dashed boxes. The results of this scenario for InterMR are compared with the results for the other four architecture options (BGP with virtual routers, flat OSPF, plain BGP and OSPF with areas). Fig. 5 shows the average throughput per flow versus time for various routing architecture options under group mobility. A y-axis value of 1 indicates 100% throughput. The graph shows that for OSPF with areas and plain BGP mobility may cause an AS split or an area split resulting in an effectively partitioned network and significantly reduced throughput. InterMR, BGP with virtual routers and flat OSPF do not suffer from this problem.

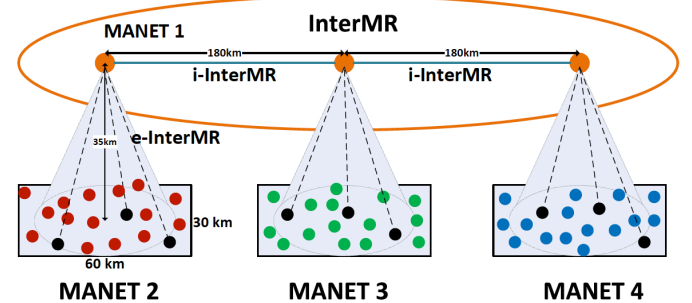


Fig. 6. InterMR Random Mobility Scenario

##### B. Random Mobility Scenario

As can be seen from the previous section, InterMR, flat OSPF and BGP with virtual routers are able to adapt to network partitions. In this section, we study the scalability of these routing architectures in terms of control plane traffic



in the presence of high mobility. We expect that InterMR overhead will increase with the size of the network as its digest size will increase because this corresponds to more route updates to be distributed across InterMR gateways. We evaluate its scalability under random mobility scenario. The random mobility scenario is configured as follows: Every node in each of the ground service networks starts at the same position and then moves randomly within a rectangle of 60 km x 30 km with a constant speed of 20 m/s, following the random waypoint mobility model. Fig. 6 provides a notional picture of the scenarios. The simulations had three ground MANETs of 30, 45, 60, 90 and 120 nodes and three air nodes for a total of 93, 138, 183, 273 and 363 nodes. Fig. 8 shows the total overhead (ground and air combined) for InterMR, flat OSPF, and BGP with virtual routers. Fig. 8 shows that the total network overhead increases as the size of the network increases. The overhead for flat OSPF increases much faster than that of InterMR and BGP with virtual routers.

### 3 Disconnected OSPF Networks

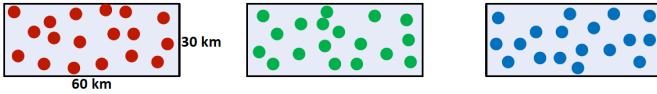


Fig. 7. Three non-connected MANETs

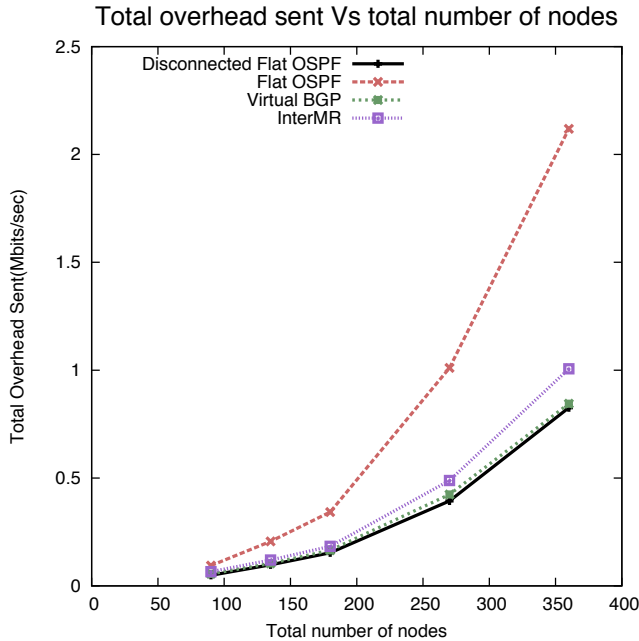


Fig. 8. Total Overhead for InterMR, Flat OSPF and BGP with Virtual Routers

We are not only concerned with the total overhead of the network, but also the cost of interconnecting ground MANETs under different routing architectures. InterMR is proposed to fundamentally address BGP's constraints in the wireless mobile environment. BGP with virtual routers is an architectural solution to avoid the AS split problem. However, we must also understand the cost in term of overhead that

these two solutions have for interconnecting the MANETs. To do this, a network architecture approach, a baseline scenario, was also considered. This network approach has three non-connected ground MANETs running OSPF as their routing protocol as depicted in Fig. 7, which captures the routing traffic generated by simply running OSPF in each MANET. Fig. 8 shows that InterMR and BGP with virtual routers incur little cost for connecting the MANETs as the overhead for InterMR and BGP with virtual routers is not much higher than the case of the non-connected ground networks. InterMR overhead is slightly higher than BGP with virtual routers, which is because of i-interMR overhead across the backbone comparing i-BGP traffic within virtual routers in the case of BGP with virtual routers. This demonstrates that InterMR is a scalable approach for interconnecting MANETs due to its low overhead in combination with its ability to network mobility.

### V. CONCLUSION

The dynamics of mobile ad-hoc networks pose challenges for inter-domain routing with BGP due to the frequent topology changes and intermittent wireless links. This paper compares several approaches for addressing BGP's known AS split issue. The focus of this paper was on the development and performance of an implementation of interMR. We found that interMR was able to adapt to network changes under a group mobility scenario designed to induce network splits. In addition, InterMR added little additional overhead for connecting ground networks. The overhead from InterMR, however, was slightly higher than BGP with virtual routers due to underlying beaconing processes. More work is needed to understand how InterMR performs under various traffic patterns.

### REFERENCES

- [1] J. Wang, A. Narula-Tam, and R. Bryan, "Interconnecting heterogeneous manets at the tactical edge," in *Military Communication Conference*, 2014.
- [2] T. Gibbons, J. V. Hook, J. Wang, and T. Shake, "A survey of tactically suitable exterior gateway protocols," in *Military Communication Conference*, 2013.
- [3] S. Hares and R. White, "BGP dynamic AS reconfiguration," in *Military Communication Conference*, 2007.
- [4] M. Kaddoura, B. Trent, and R. Ramanujan, "BGP-MX: Border Gateway Protocol with mobility Extensions," in *IEEE Military Communication Conference, MILCOM2011*, 2011.
- [5] C.-K. Chau, J. Crowcroft, K.-W. Lee, and S. H.U.Wong, "Inter-domain routing for mobile ad hoc networks," in *3rd international workshop on Mobility in the evolving internet architecture*, 2008.
- [6] B. Zhou, Z. Cao, and M. Gerla, "Cluster-based Inter-domain Routing (CIDR) Protocol for MANETs," in *IEEE/IFIP WONS 2009, Snowbird, UT, Feb. 2009*.
- [7] B. Zhou, T. A., K. Zhu, Y. Lu, and M. e. a. Gerla, "Geo-based Inter-Domain Routing (GIDR) Protocol for MANETs," in *IEEE Military Communication Conference, MILCOM2009*, Boston, MA, October 2009.
- [8] S. H. Lee, S. H. Y. Wong, K. L. C. Chau, J. . Crowcroft, and M. Gerla, "InterMR: Inter-MANET Routing for Heterogeneous MANETs," in *The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010)*, 2010.
- [9] "Riverbed OPNET Modeler (Release 17.1) [Software]. (1986-2012). San Francisco, CA Riverbed Technology Inc." [www.riverbed.com](http://www.riverbed.com).