Gateways for Mobile Routing in Tactical Network Deployments

R.G. Cole*, L. Benmohamed, B. Doshi
Applied Physics Laboratory
and Department of Computer Science
Johns Hopkins University
Laurel, MD, USA

Baruch Awerbuch[†]
Department of Computer Science
Johns Hopkins University
Baltimore, Maryland, USA

Derya Cansever
SI International, Inc.
Reston, Virginia, USA

***Abstract*—The US Department of Defense (DoD) is developing a Network Centric Warfighting (NCW) capability. Key to the deployment of NCW capabilities is the development of scalable networks supporting end user mobility. Initial network deployments operate either At-The-Halt (ATH) or On-the-Move (OTM) with preplanned movements. This is consistent with current networking capabilities with respect to large scale mobile network capabilities and protocols. However, future architectures and capabilities should allow for more flexible mobility models allowing for more flexible and robust NCW capabilities.**

We investigate hierarchical network models which are comprised of a high bandwidth, planned mobile core network interconnecting subtending more mobile end user networks. Standard IP routing and name and location services are assumed within the core network. The subtending and mobile end user networks rely upon highly scalable (from a mobility perspective) Beacon-Based routing architecture. The interface between the core and subtending mobile networks relies upon network concepts being developed within the Internet Engineering Task Force (IETF), specifically from IPv6 mobility and the Host Identity Protocol (HIP) rendezvous service for mobile networks. We discuss the advantageous of this architecture in terms is mobility, scalability, current DoD network plans and commercial protocol development.

I. INTRODUCTION

It has long been realized that routing in highly dynamic mobile ad-hoc networks (MANETs) represents an extremely challenging problem for protocol designers. The United States (US) Department of Defense (DoD) is developing communications capabilities for its future NetCentric Warfighter vision which relies on the deployment of large scale tactical networks, both quasi-static and mobile. While the focus of the initial developments of these communications system has been on relatively homogeneous routing domains, future interworking requires the development of a robust interworking between a highly mobile infrastructure and a quasi-static, high capacity backbone infrastructure.

A large body of work exists in the open literature and in standards development which relate to the issues of gateway design between mobile hosts and a fixed infrastructure. This body of work is not fully developed to address the needs of the US DoD due to the scale of the mobile deployment. However, we believe that current developments in MANET routing [1] [3] [4], combined with capabilities under development and discussion at the Internet Engineering Task Force (IETF), can result in a robust and scalable architecture supporting a quasi-static backbone network, large scale and highly mobile tactical networks and a gateway functionality providing interoperability between these two distinct domains. In this paper we present our initial ideas on the development of gateways for mobile routing in tactical deployments and preliminary analysis.

II. ARCHITECTURE

In this section we present our gateway architecture in a relatively abstract setting. As we will discuss below in Section III, this will allow for various specific protocol approaches based upon their specific merits. So the problem at hand is to define a robust and scalable gateway functionality between a highly mobile ad-hoc network domain and a relatively static, high bandwidth network domain for tactical environments. This is depicted in Figure 1. The US DoD plans for tactical networks involve the deployment of high bandwidth and relatively static tactical backbone networks which are surrounded by and provide internetworking to a large scale and highly mobile networks. The relatively static backbone supports satellite communications (SATCOM) and radio communications At The Halt (ATH) and On The Move (OTM) where the mobility of the nodes is relatively low speed and pre-planned. While in the tactical mobile edge, the nodes reside on small, highly mobile platforms such as Soldier Networks (SNs), Unmanned Arial Vehicles (UAVs), Manned Arial Vehicles (MAVs) and Manned Ground Vehicles (MGVs). These communications platforms comprising the tactical edge networks support SATCOM on a limited basis and more likely will rely on wireless Line Of Sight (LOS) radio communications.

Gateway architectures are being discussed which provide for interoperability between these two disparate networking domains. Example architectures include:

- *BGP Gateways* - these propose to build gateways which rely on the Border Gateway Protocol (BGP), developed for the static Internet domains. These solutions do not explicitly address the mobility issues related to ad hoc

*Robert Cole is supported by the following grant NSF-XXX-XXXXXXX.
[†]Baruch Awerbuch is supported by the following grant NSF-XXX-XXXXXXX.

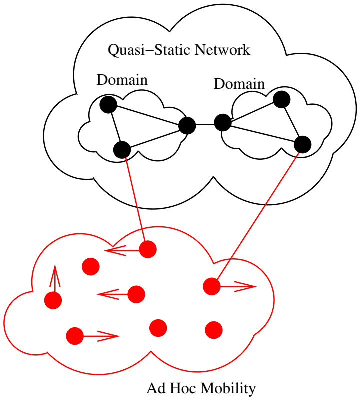

Fig. 1. Problem statement to combine mobile and quasi-static tactical network domains.

networks. Instead they assume that the mobile nodes form an associated network with aggregatable addresses and assume the existence of stable links between these mobile networks and the BGP gateways on the fixed infrastructure.

- *Mobility Extensions to Standard Routing Domains* - these propose to modify some of the mechanisms of routing protocols designed for static networks to better support mobile environments. They further propose gateway functions which import topology information from the MANET into the fixed routing domain. The result is that the fixed routing domain views the MANETs nodes and their current connectivity as part of the same routing domain. These solutions seem suited for limited extensions of the fixed routing domain into the mobile environment. But these protocols are not designed *a priori* for operations in dynamic MANETs.
- *Mobile Node and Network Routing* - the IETF has developed mobile host extensions to a fixed network infrastructure in the form of IPv4 and IPv6 mobility [9] [10] and, more recently, Host Identity Protocol (HIP) and its associated Rendevouz protocols [16] [17]. These solutions are explicitly designed to handle the case of independent mobile hosts (and contained networks) which randomly attach to a fixed network infrastructure. They do not address issues associated with multihop mobile nodes providing gateway functions into a fixed infrastructure.

We have chosen to base part of our gateway architecture on this later approach to mobile networking and extend it where necessary. These solutions were particularly designed for tracking mobility of nodes and networks when moving around a relatively fixed network infrastructure. Further, similar mobile node architectures have seen large scale deployments in cellular networks. Later on we summarize this body of work. Although our architecture does not rely on one particular protocol solution to nodal mobility, we will use the language developed within the context of the Host Identity Protocol (HIP) [16] and its associated mobility extensions [17] to identify the concepts and functions required by nodes within our proposed architecture. However, we do not preclude the use of IPv4 or IPv6 mobility models instead for an actual deployment.

In this paper we discuss extensions to mobile edge networking which leverages our previous work on the design and analysis of a highly scalable and dynamic MANET routing protocol called Beacon-based Routing [1] [3] [4]. Beacon-based MANET routing relies on the presence of one (or more) distinguished node(s) which periodically beacon (transmit) a message that the mobile nodes use to construct a spanning tree within the entire connected wireless MANET. This spanning tree, which is updated on roughly the frequency of 1 Hz, can be immediately used for all routing which climbs the tree towards the distinguished node [4], can be used to boot-strap peer-to-peer path discovery [3], and immediately constructs an estimate of the local minimum connected dominating set (MCDS) for multicast applications [5], which is as good as all current distributed algorithms discussed in the literature. Further, deployments where the vast majority of unicast traffic climbs the spanning tree to a distinguished gateway node includes military tactical deployments (which are the focus of this paper) and wireless infrastructure deployment common to commercial wireless services. Hence, this Beacon-based routing approach has significant scalability advantages over other MANET routing protocols [3].

In our architecture, we propose to define the gateways as the preferred distinguished nodes within the Beacon-based routing system while simultaneously acting as Rendevouz Servers (RSs) and proxies for Locator-Addresses (LAs) to the fixed infrastructure for mobility interworking. In this sense, the gateway nodes act as a distributed server database tracking the mapping of the highly mobile nodes within the MANETs to their currently associated gateway (address) on the relatively static backbone. This is illustrated in Figure 2. Here gateway nodes bridge the highly mobile ad-hoc network components with the relatively static backbone network components. The gateways run the Beacon-based routing protocols, periodically sending beacon messages which allow the mobile nodes, i.e., UAVs, MGVs, MAVs, etc., to locate routed multihop paths to backbone nodes as well as peer mobile nodes. Further, the gateways act as RSs representing the mobile nodes to the upper network tier. So the mobility within the domain of a given beaconing gateway is handled by the Beacon-based MANET routing protocols, while the mobility between gateways (which will occur at a much lower frequency) is handled by mobile IP-like concepts. However, we propose that the Gateways nodes also act as proxy LAs for the mobile nodes; they intercept packets destine for the mobile nodes and strip off core locator addresses and inject the packets into the mobile routing domain with only their IDs. This is proposed as an overhead reduction mechanism and is not fundamental to the proposed architecture.

Next, the existing approaches to node mobility, i.e., IPv4,IPv6 and HIP, all rely on some form of dual addressing. IPv4 uses transport inside of tunnels to achieve a two layer addressing structure. IPv6 relies on header extensions to achieve

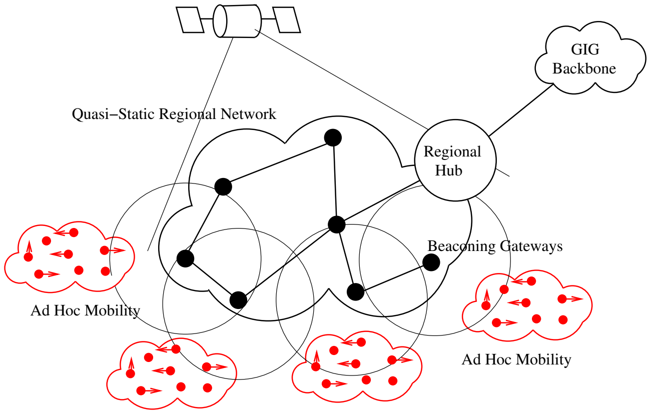

Fig. 2. Overview of proposed architecture for tactical mobility gateways.

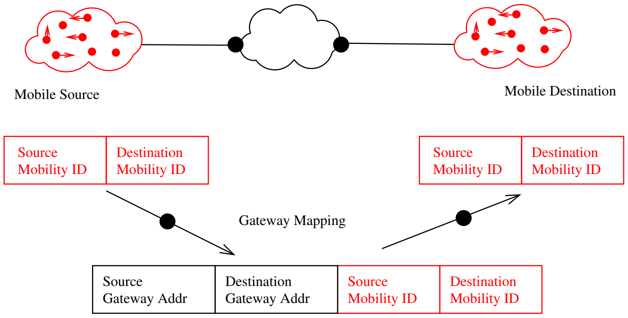

Fig. 3. Tactical mobility gateway mapping function.

a two layer addressing structure. And HIP formalizes the distinction between Identification and Address (or Locators). Here we follow these trends and rely on separate addressing structures in the mobile edge and in the relatively static core. Within the core, addressing is topologically significant and routing relies on this fact for further scalability in the tactical core. Within the mobile edge, addressing has no topological significance and routing essentially operates on host Identifiers, although these could be in the form of standard address structures such as IPv6 addresses. The Gateways provide and maintain the mapping between mobile IDs and core LAs.

The final piece to our architecture has to do with the associated addressing and naming architecture. There exists much past and current work at the IETF which rely on a two-level addressing (or addressing and ID) structure. This body of work includes a) mobile IP with host and foreign agent addresses [9] [10], b) HIP with end-point identifiers and network point-of-attachment addresses [16], and c) LISP [19] and 6/ONE [19] with core addresses and edge network addresses. All of these schemes require mechanisms to map between one set of identifiers to another set of identifiers and to provide for protocol mechanisms to carry both levels of identifiers within common packet headers. Thus the gateways will handle the mapping and encapsulation of header information as packets flow across network domain boundaries. We show this in Figure 3.

In summary, our architecture proposes the following flow for node naming, discovery and routing in a mixed mobility tactical domain.

- Node IDs are used within the mobile portion of the network, are persistent with hosts and carry no topological significance.
- Topologically significant addressing is used in the relatively static core network for routing scalability.
- DNS carries the mapping between name and ID and ID and RS address. This mapping can be dynamically updated by mobile nodes making a relatively persistent change to a new host gateway domain.
- Gateways act as RSs for the mobile nodes. This RS functionality in the gateway maintains a mapping of mobile node ID and current gateway domain (in the form of an address or locator) being visited by the mobile node.
- Gateways and mobile nodes run the Beacon-Based Routing protocol. Gateways act as a preferred Beacon node. Gateways periodically send the beacon messages for routing within the extent of the MANET within the gateway domain.
- Mobile nodes rebroadcast these beacon messages to notify downstream nodes. Mobile nodes overhear new gateway beacons and notify the local Care-Of-Gateway (COG) of its presence, its ID and its RS. The new COG updates the RS of the new location of the mobile node.
- A source node (looking for a given mobile node) queries DNS with the name and receives the node ID and RS. The source constructs a packet which contains a two-layer destination addressing scheme, the outer layer contain the RS on the core and the inner layer containing the node ID related to routing within the mobile edge. The source then forwards the first packet to the RS. The RS forwards to the current LA on the current Gateway. The COG strips the outer address and forwards into the MANET with the node ID for routing purposes.
- The current Care-Of-Gateway (COG) maintains the mapping between the mobile node's LA and the node's ID. The COG performs the mapping and encapsulation (of addresses) as required on behalf of the associated mobile node and core network routing.
- Once the destination node has replied to the original source, the two end points know their respective IDs and their LAs. The nodes/COGs can now construct packets containing two-tier packet formats as indicated in Figure 3.
- A mobile node which moves to a new Gateway domain, notifies the new Gateway which forwards this message onto the mobile nodes RS. Following HIP mobility, the mobile node also notifies its current peer corresponding nodes of its new LA. Previous COGs can timeout their mapping table entries to maintain a finite storage requirement.

This high level architectural description is just that; a high level initial description. There are numerous tradeoffs that can be made, e.g., where the construction of the outer layer of the packet headers are formed which will affect network performance or protocol architecture trades considering IPv4, IPv6 and HIP mobility functionality. These trades are the material of future study. In the next section we provide a brief discussion of current protocol developments related to our proposed Tactical Gateway architecture. This discussion is intended to give the reader an appreciation for the current networking directions in mobile and static networking and how our architecture draws upon this rich area of protocol design and research.

III. Related Work

There exists recent and interesting protocol developments within the Internet Engineering Task Force (IETF) which are associated with gateway functionality between different networking domains in a single network. Protocol work in the area of LISP [19] and Six/One [19] and IPv4 [9], IPv6 [10] and HIP [17] mobility, define and demonstrate the benefits of a layered (or tiered) architecture. In the process they develop and rely upon a layered addressing capability to achieve separation of domains and methods serving their distinct network requirements. These form a useful set of networking capability and tools for mobile tactical architectures. Finally, we overview our recent developments in light weight routing protocols for MANETs referred to as Beacon Based Routing Protocols [1] [2] [3] [4]. We overview these developments in the following subsections.

A. IPv4 and IPv6 Mobility

IPv4 and IPv6 mobility addresses the case of a single node moves about a fixed network infrastructure. NEMO [11] extends IPv4 nodal mobility to the case where a given network is mobile. As the node moves, it picks up new network attachment point addresses. Within the IETF, standards exist for both IPv4 and IPv6 network layers. These standards define several common terms:

- *Mobile Node (MN)* the roaming node.
- *Home Agent (HA)* a static node which maintains a repository of network information related to the MN.
- *Foreign Agent (FA)* a static node which temporarily is acting as a gateway to the MN based upon the MNs current point of attachment address.
- *Home Addresses* this is the static, home address associated with the mobile node and which is related to the HA subnet.
- *Care-of-Address* this is the temporal address of the MN which is topologically associated with the FA, in the case of IPv4 , or of the MN in the case of IPv6.
- *Corresponding Node (CN)* a node (static or mobile) which is currently communicating, i.e., maintaining a transport level connection, with the MN.

We discuss each network layer, i.e., IPv4 and IPv6, separately below.

IPv4 Node Mobility: The IETF RFC 3344 [9] defines the IPv4 standards for a single mobile node moving around a fixed network infrastructure. The routing model for IPv4 is as follows(see Figure 4). Initially, the MN builds an association with the HA. The HA will maintain a data repository relating the MN static address with it current FA address. As the MN moves to another network point of attachment, the MN temporarily associates with the FA and notifies the HA of the address of the new FA. The HA updates its data repository based upon this new information. The FA is now responsible for forwarding data packets from the HA to the MN. The HA and FA accomplish this by building a tunnel between them. CNs send packets, destine for the MN, using the MN static address. These are intercepted by the HA, which encapsulates them into the HA-FA tunnel using the FA address. When the FA receives the packets, it decapsulates the packet and forwards to the MN. The MN may act as its own FA, hence the MN and FA are coincident. Or the FA and MN may be non-coincident. When the MN responds to the CN, the packets carry the CN as the destination address, and hence the normal routing path is followed. Hence, due to the CA sending to the static MN address which is forwarded through the HA to FA tunnel, and the MN packets following normal routing to the CN, asymmetric routing results.

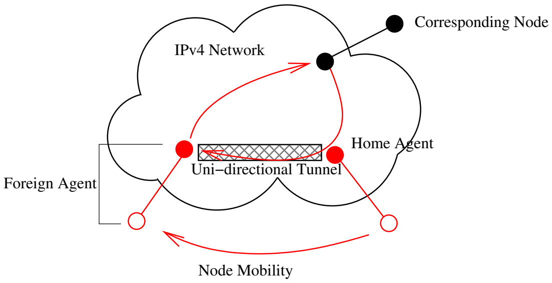

Fig. 4. IPv4 mobility approach.

Clearly this routing model has the highly desirable benefit of allowing the MN and CN nodes to maintain data sessions while the MN moves throughout the network infrastructure. The CN node is oblivious to the fact that the mobile node is changing its network point of attachment address as it moves around the static network infrastructure. However, several network inefficiencies results. These include (RFC 4830 [14]):

- *Inefficient routing* due to the reliance upon HA-to-FA tunnels, the path from the CN to the MN is not the most efficient as defined by the normal routing path.
- *Aggregate QOS* in a static network environment reach with QoS support, the existence of the tunnel between the HA and FA can defeat the benefits of the QoS policies.
- *Reliability* HA redundancy is not defined within the current standards.
- *Other Issues* - including interference with existing anti-address spoofing filters in the network, hand over latency on moving to new FAs, additional signaling, control and messaging overhead, and potential location privacy concerns.

NEMO Network Mobility: NEMO addresses Domain Mobility within a fixed network infrastructure. Here it is assumed that a group of nodes move about the fixed infrastructure together. The architectural model for NEMO's network mobility closely follows the IPv4 nodal mobility model discussed previously with a few exceptions. One prominent exception is the reliance upon bi-directional tunnels between the HA and the FA. This is because mobile network addresses are hidden from the FA attachment gateway. Hence, the HA uses standard routing within the fixed core to advertise the mobile network address.

IPv6 Node Mobility: The IETF RFCs 3775 [10], RFC 4068 [12] and RFC 4866 [15] define the base IPv6 standards for a single mobile node moving around a fixed network infrastructure. The routing model described in these standards is similar in some aspects to the IPv4 nodal mobility model, but adds several new features which address some of the deficiencies identified in the IPv4 section above. In IPv6 nodal mobility model, two routing modes are supported. One maintains a bi-directional tunnel between the CO-address and the HA-address. In this case all traffic between the CN and the MN travels through the bi-directional tunnel and hence routing is asymmetric. In the other, more desirable mode, direct communications between the CN and the MN is maintained. This is accomplished through additional IPv6 capabilities. In the direct communication case (see Figure 5), the address binding update sent from the MN to the HA, when the MN picks up a new point of attachment address, is also sent to the CN address. The CN maintains a local cache binding the MN-HA to the MN-COA. The CN relies upon the IPv6 header extension support for the placement of the MN-HA in an option field while carrying the COA in the destination address field from the CN. Hence, the Home Agent is maintained to enable new session establishment, while the new IPv6 features allow for ongoing, direct communications between CNs and MNs. RFC 4866 [15] extends this capability by minimizing handoff delays, increasing aspects of security and reducing overall control overhead.

The IPv6 nodal mobility model resolves some of the identified issues with respect to the IPv4 mobility model. Specifically, the routing inefficiency due to routing asymmetry is eliminated by both modes. The bi-directional tunnel mode forces all communications between the CN and the MN through the tunnel. The direct communication mode eliminates the need for tunneling all together. Further, the ingress anti-spoofing address filtering problem is eliminated due to the use of the IPv6 header extension to place the MN HA, hence the network attachment points only see the CoA in the MN-to-CN packets. Finally, the direct communications mode solves issues related to aggregating packet-level QoS handling, discussed above for the IPv4 case. Some issues, e.g., the HA redundancy question, remain to be resolved.

B. Host Identification Protocol

The Host Identification Protocol (HIP) [13] formalizes the separation between address, related to network point of attachment, and host identity (ID) which is persistently attached to the host. HIP develops a shim protocol layer between network and transport layers which manages the binding of the transport layer to the ID and to the network layer address. HIP additionally defines a mobile node capability be defining a Rendevouz server, similar in function to the IPv6 HA [13].

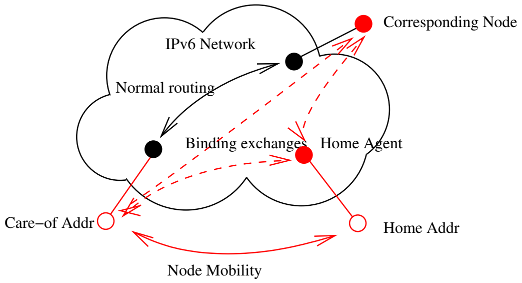

Fig. 5. IPv6 mobility approach.

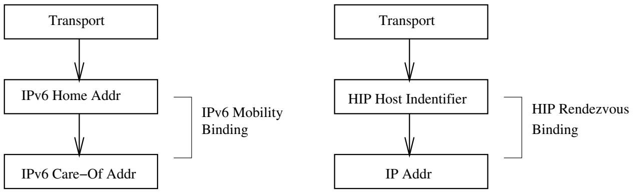

Fig. 6. Mobility binding to persistent identifier.

HIP defines several common terms, but somewhat differently from IPv4 and IPv6 mobility standards. Specifically, HIP defines the following:

- *Host Identification (ID)* - a persistent host identification.
- *Host Identity Tag (HIT)* a cryptographic hash of a host identity (ID).
- *Locator Address (LA)* a topologically significant address used for routing in the context of the core, fixed network infrastructure.
- *Rendevouz Server (RS)* like the HA in IPv4 mobility, a server holding the mapping information between the node's HIT and the node's current LA.
- *Peers* corresponding nodes in current communications with the focus node.
- *Care-Of-Gateway (COG)*[1] the current gateway associated with the node's LA.

Like IPv4 and IPv6 mobility, HIP allows for the continuance of active socket bindings while the end-points are mobile. However, HIP binds sockets to the HIT, rather than host addresses. Figure 6 compares the Mobile IPv6 and HIP/Rendevouz methods of maintaining transport bindings during node mobility.

C. LISP and Six/One

The Internet routing in the core network is being pushed to its limits due to a rapid explosion of prefixes exposed to core

[1] This is not actually a HIP term, but instead a term we use in the description of our mobility gateway architecture

routing. This is a result of the increase use of dual homing for end-to-end redundancy. The introduction of an additional address structure, i.e., IPv6, will exacerbate this situation. To address this problem, researchers have proposed LISP [19] and Six/One [19] routing architectures. These minimize the core routing prefixes through the creation of a two tier network structure. Like our Tactical Gateway Architecture for Mobile Networks, the gateways between these tiers provide a mapping and encapsulation function to provide a logical separation between core routing requirements and edge routing requirements. For example, LISP gateway routers perform a mapping function by querying a mapping service (like provided by our distributed mobility gateways). Once the gateway discovers the mapping, it encapsulates the original packet inside a m-GRE tunnel to the far-side gateway responsible for the destination host. Hence, routing in the core Internet, will only have to handle the set of prefixes associated with the core routers acting as LISP gateways. While these proposals, e.g., LISP and Six/One, are focused on addressing Internet routing scale, they propose separation architectures which rely upon network tiers, each addressing a different set of requirements. In this sense, our two tier architecture follows these in define separate tiers addressing separate functions.

D. Beaconing Routing for MANETs

The Beacon-Based Routing (BBR) for MANETs [18] [3] [4] is a generalization of the Pulse Protocol [1] [2] originally developed for infrastructure and sensor-based wireless networks. The BBR protocol is an opportunistic, light-weight routing protocol for MANETs which simultaneously builds a single spanning tree structure for the majority of the unicast routing and an estimate of the minimum connected dominating set (MCDS) for the multicast routing. These structures are periodically updated with a network overhead cost of M, the number of mobile nodes in the MANET. All other known MANET routing protocols generate overhead which grows like M^2. For tactical networks, where the bulk of the traffic flows up the command hierarchy, these routing structures are extremely efficient. For peer-to-peer traffic, the BBR protocols use the single spanning tree to bootstrap shorter paths between the peers [3] resulting in good routing efficiency.

In the BBR protocol, a distinguished node is elected which periodically broadcast a beacon message containing the beacon ID, also forming the instance ID of the local MANET. Nodes receiving this message, not the presence of the sending node, place their local ID, and retransmit the beacon message. Nodes which have transmitted the beacon message, listen for following beacon rebroadcasts containing their local node ID. These messages indicate that the local node should act as a member of the MCDS. The rebroadcasting of the beacon message builds an instance of a spanning tree whose root is the original beacon node.

Routing efficiency studies of BBR protocols have been performed [5]. As an example, Figure 7 shows a random deployment of mobile nodes and their radio ranges. If two circles touch, then the nodes are assumed to have radio communications. The upper right hand plot shows the resulting connectivity map, while the lower two plots show two instances of the spanning tree construction resulting from a random selection of beacon nodes.

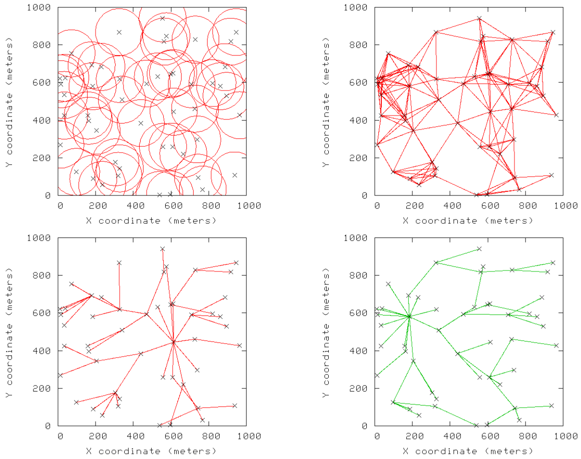

Fig. 7. Example random topology and resulting Beacon-Based Routing spanning tree.

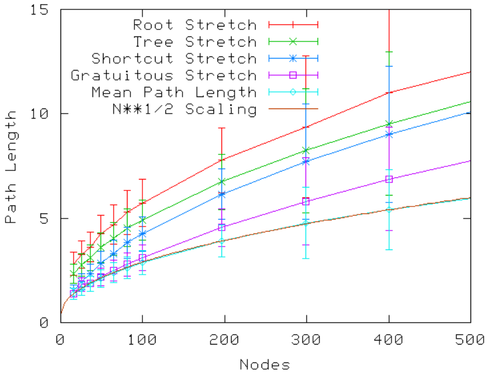

Fig. 8. Results for Beacon-Based Routing peer-to-peer path construction.

The BBR protocols use these trees for routing when communicating up the spanning tree (or command hierarchy). For peer-to-peer routing the BBR protocols use an efficient bootstrap method [3] method. Figure 8 shows simulation results which estimate the efficiency of the bootstrap method by computing the routing stretch, which is the ratio of the resulting path length to the optimal path length.

As previously mentioned, the BBR protocols simultaneously construct an estimate of the MCDS for multicast applications. Figure 9 shows simulation results demonstrating the effectiveness of the BBR protocols to construct the MCDS in comparison to other prominent methods. Note that all methods shown to be better than the BBR protocol in the figure are methods which rely upon full network topology information and hence generate protocol overheads scaling like M^2. With the MCDS computed the BBR routing protocols use this to provide a Core-Based Tree multicast capability [5].

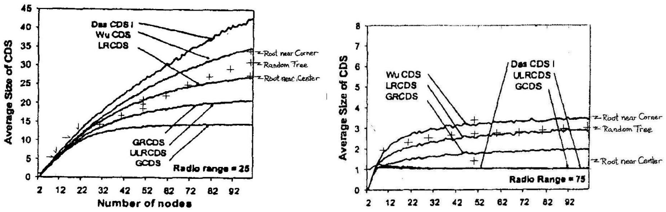

Fig. 9. Results for Beacon-Based Routing MCDS construction.

So, the IETF is relying upon domain (and associated address) separation to provide for i) routing scalability and ii) nodal mobility. The BBR MANET routing protocol has been demonstrated to be highly efficient in high mobility situations and especially in hierarchically organized networks as found in tactical deployments. Hence, it seems very natural to combine these two protocol developments into an integrated architecture for mobility management in tactical radio networks as be present in this paper. We believe that our gateway architecture is highly scalable, flexible and supportable in large scale tactical deployments. We now discuss some initial architecture analysis results in the next section.

IV. Architecture Analysis

In this section we present some initial estimates of the capacity of the proposed architecture to address a typical deployment. We use as a background model, that of a fictitious US Army Division deployment. Figure 10 show our idealized view of such a network deployment. The key components of the model (and routing architecture) are:

- *DNS* - responsible for the source host (somewhere in the greater network) name (or ID) to RS (Gateway) responsible for the target mobile destination host. These DNS queries occur infrequently, only when the source host does not already have a cached DNS entry for the RS of this destination. Regardless of the location of the source host (i.e., on the relatively stable network or in the relatively mobile edge), DNS supports this translation request.
- *Gateways, Rendevouz Servers (RSs)* - RSs are responsible for maintaining the mapping of name (ID) of the mobile node to its current gateway domain. If the mobile node is visiting a foreign domain, then this gateway will forward the packet onto the node's LA associated with the Care-Of-Gateway (COG). The COG queries for current mobile location occur only when the source initially wishes to establish communications with the destination mobile node. Once communications is established, the destination node is responsible for updating both its RS and all the node's active peer communicating partners.
- *Gateways, Foreign Agent (FA)* - If a mobile node moves between gateway domains, it must notify its new COG and RS of the move. This ensures that the distributed gateway information regarding mobile node location is up to date.

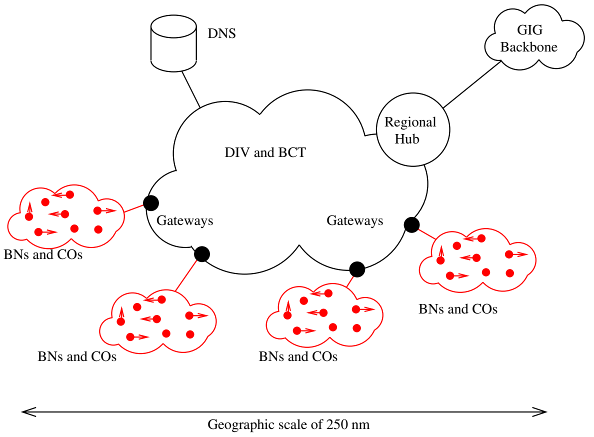

Fig. 10. Model deployment for analysis of scale.

TABLE I
Size estimates for projected deployment.

Entity	Soldiers	Number per DIV
Division (DIV)	$1 - 2 \times 10^4$	1
Brigade Combat Team (BCT)	$4 - 5 \times 10^3$	4
Battalion (BN)	$0.5 - 1.5 \times 10^3$	16
Company (CO)	$75 - 200$	64
Plantoon (PL)	$30 - 50$	256

- *Routing Core* - the routing core of the relatively stable backbone routes based upon the address of the node (if directly affixed to the core routing backbone) or of the current Gateway Address of the mobile node. This allows for scalability and stability of routing within the core.
- *Edge Routing* - the routing in the edge is totally based upon the IDs (or names) of the mobile nodes and attached gateways. This routing is design for full ad hoc, mobile networking within the edge tactical networks.

Table I presents our force projections for this typical deployment. We use a rule of four to multiple the number of lower level entities comprising the next higher level entity, e.g., we assume four COs per BN, etc.

We assume that the gateway nodes defining the boundary between the stable core and the mobile edge networks are located in all DIV, BCT, BN and in some CO units. The mobile edge nodes support the PL and CO units. Define the follow parameters of the model (Table II).

The default values obtained above follow from the values of N and A and the assumption of uniform deployment. We assume there are roughly 64 Gateways deployed; this comes from the assumption of 4 BCTs/DIV, times 4 BNs/BCT, times 4 COs/BN. The value of M_{GW} is obtained by dividing N by N_{GW} yielding roughly 1.5×10^3. So each gateway nodes is responsible for an area whose diameter is roughly 36 nm. Note, this does not imply that the beaconing range has to be 36 nm. Assuming a typical mobile node speed of 50 $knots$, then the minimum time the node resides within the domain of a given Gateway node is $1\ hr\ = D_{GW}/S$. Hence, an conservative estimate (for the purpose of engineering) of

TABLE II
MODEL PARAMETERS.

Parameter	Definition	Default Value
N	Number of Mobile Nodes	6×10^3
N_{GW}	Number of Gateway Nodes	64
M_{GW}	Mobile Nodes per GW Domain	1.5×10^3
A	Total Deployment Area	$6.5 \times 10^4\ nm^2$
D	Effective Diameter of Deployment Area	2.8×10^2
A_{GW}	Responsible Area of a Gateway	$1 \times 10^3\ nm^2$
D_{GW}	Effective Diameter of Gateway Area	$36\ nm$
S	Average Speed of Mobile Node	$50\ knots$
ν_{GW}	Frequency of GW Changes (new FAs)	2.8×10^{-4}
ν_{DNS}	Frequency of DNS Record Changes	TBD

the frequency of total changes to the Gateways' distributed database of ID to FA mappings is $N \times \nu_{GW} \approx 5/second$. This is a relatively small load to manage on the distributed GW database and amounts to only one update per 13 seconds per GW node (pair).

When a mobile node wishes to change its RS gateway affiliation, it must issue a dynamic DNS record update signifying this change. It is hard to predict the load this would generate on the overall DNS infrastructure of the DIV. However, it is hard to image that the frequency of this type of change would be large.

This model also indicates the number of nodes within the ownership of a given RS. This quantity is determined as $M_{GW} = N/N_{GW} = 1.5 \times 10^3$. This is a reasonable number of nodes given a BBR MANET routing with respect to routing overhead (although it seems quite large for traditional link state routing protocols). However, there are many other considerations and studies required to understand the scalability of our tactical mobility architecture. For example, traffic considerations may result in bottlenecks at the gateway nodes. This would require the deployment of more gateway nodes or increased bandwidth into the gateway nodes. Clearly this analysis is very cursory and much more analysis is necessary.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we present an a new gateway architecture for mobility management in large tactical network deployments. Our proposal relies upon recent protocol developments in i) nodal mobility management at the IETF in the form of IPv4 [9], IPv6 [10] and HIP mobility [17], ii) routing scalability in the core Internet in the form of LISP and Six/One proposals, and iii) recent developments in light-weight MANET routing protocols in the form of Beacon Based Routing (BBR) [1] [2] [3] [4]. Our proposal relies on the development of gateways between a relatively static core tactical network and highly mobile BBR MANETs. The gateway nodes act as Beacons in the context of the highly mobile nodes in the MANETs. Hence, our gateways refresh the definition of the MANET domains and MANET routing at a frequency of roughly 1 Hz. This results in an extremely flexible and dynamic tactical network architecture. We discussed our proposal in the context of related protocol developments. We also presented an initial architecture analysis model and results, validating the utility of our approach.

Clearly, this is an initial description of our system with initial analysis. Much work is required to fully flesh out the protocol specifics and to finalize the analysis prior to moving to the prototype phase. But we are very encouraged by our analysis to date and will continue to pursue the development of our tactical gateway architecture.

REFERENCES

[1] Awerbuch, B., Holmer, D. and H. Rubens, *The Pulse Protocol*, IEEE Infocomm 2002, August, 2002.

[2] Awerbuch, B., Holmer, D. and H. Rubens, *The Pulse Protocol: Mobile Ad Hoc Network Performance Evaluation* Infocomm'05, San Francisco, CA, USA, October 2004.

[3] Cole, R.G., Awerbuch, B., Holmer, D. and H. Rubens, *Analysis of Multiple Trees on Path Discovery for Beacon-Based Routing Protocols* IEEE PacRim'07 Conference on Communications, Victoria, BC, Canada, August 2007.

[4] Cole, R.G., Awerbuch, B., Holmer, D. and H. Rubens, *Beacon-Based Routing for Tactical Networks* IEEE MILCOM'07 Conference, Orlando, FL, USA, October 2007.

[5] Cole, R.G. and B. Awerbuch,, *Beacon-based MANET Routing and Minimum Connected Dominating Sets for Multicast* JHU Technical Report, December 2007.

[6] Moy, D., *OSPF - Anatomy of an Internet Routing Protocol* Addison-Wesley Press, New York, January 1998.

[7] Clausen, T. and P. Jacquet, *Optimized Link State Routing Protocol (OLSR)* IETF Request for Comment 3626, October 2003.

[8] Perkins, C.E. and E.M. Royer, *Ad-hoc On-Demand Distance Vector Routing* Infocomm'99, San Francisco, CA, USA, September 1999.

[9] Perkins, C.E., *IP Mobility Support for IPv4*, IETF Request for Comments 3344 (Proposed Standard), Aug, 2002, Updated by RFC 4721.

[10] Johnson, D., Perkins, C. and J. Arkko, *Mobility Support in IPv6*, IETF Request for Comments 3775 (Proposed Standard), Jun, 2004.

[11] Devarapalli, V., Wakikawa, R., Petrescu, A. and P. Thubert, *Network Mobility (NEMO) Basic Protocol Support*, IETF Request for Comments 3963 (Standards Track), January, 2005.

[12] Koodli, R., *Fast Handovers for Mobile IPv6*, RFC 4068 (Experimental), Jul, 2005.

[13] Moskowitz, R. and P. Nikander, *Host Identity Protocol (HIP) Architecture*, IETF Request for Comments 4423 (Informational), May, 2006.

[14] Kempf, J., *Problem Statement for Network-Based Localized Mobility Management (NETLMM)* IETF Request for Comments 4830 (Informational), April, 2007.

[15] Arkko, J., Vogt, C. and W. Haddad, *Enhanced Route Optimization for Mobile IPv6*, IETF Request for Comments 4866 (Proposed Standard), May, 2007.

[16] Moskowitz, R. and P. Nikander, *Host Identity Protocol (HIP) Architecture*, IETF Request for Comments 4423 (Informational), May, 2006.

[17] Laganier, J. and L. Eggert, *Host Identity Protocol (HIP) Rendezvous Extension*, IETF Request for Comments 5204 (Experimental), April, 2008.

[18] Rubens, H. and D. Holmer, *Private Communications* 2006.

[19] Internet Research task Force (IRTF), *Routing Research Group* http://www3.tools.ietf.org/group/irtf/trac/wiki/RoutingResearchGroup, 2008.