Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology

Jack L. Burbank, Philip F. Chimento, Brian K. Haberman, and William T. Kasch
The Johns Hopkins University Applied Physics Laboratory

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are considered by many as fundamental to realizing the Global Information Grid (GIG) and the vision of network-centric warfare. Indeed, a fully realized MANET would be powerful in enabling highly mobile, highly responsive, and quickly deployable tactical forces. However, significant technical challenges remain before this realization is viable. Addressing these deficiencies is a significant task that will require the invention and adoption of new technology. The goal of this article is not to declare these capabilities impossible to achieve. Rather, it is to manage the expectation of the capabilities achievable in the foreseeable future through edification on the technical difficulties standing between current technology and the desired capabilities. This article provides an overview of the military MANET problem space, describing the ideal military MANET solution. Several deficiencies are highlighted that exist between MANET technologies and the desired capability. Identified technical issues include system-level architecture, routing (both interior and exterior), management, security, and medium access control (MAC), with an emphasis on the former two areas.

INTRODUCTION

The military community is redefining the way wars will be fought in the future, evolving towards a Network-Centric Warfare (NCW) paradigm. In this paradigm, force is increasingly realized through the communications network and information sharing. This warfighting philosophy places a premium on information superiority on the battlefield and is predicated on the ability to achieve an Internet-like capability in operational areas, providing ubiquitous network access to enable "anytime, anywhere" communications.

This capability is to be provided by the Global Information Grid (GIG) , a varied collection of networks, including a high-capacity optical fiber backbone, satellite networks, terrestrial broadband wireless networks, shipboard, airborne, and ground-based wired and wireless local area networks, and soldier-based personal area networks. These networks will be interconnected via the Internet Protocol (IP) protocol suite. A key element of the GIG will be tactical networks, those deployed networks supporting users and platforms within the tactical operation region, hereafter referred to as the 'tactical edge'. Generally, such a region is highly dynamic in nature, consisting of a variety of network elements, largely comprised of mobile, wireless nodes on a variety of platforms, including vehicular, soldier, and temporary fixed (but nomadic) sites. Ideally, all these platforms would interconnect in a robust, reliable network system. However, the dynamic nature of the tactical edge prevents such a vision from becoming reality with current technology.

Because tactical-edge operations so often take place in locations where usable infrastructure is scarce, nonexistent, or unsuitable, MANET technology is attractive, as it would (in theory) enable the creation of networks on demand as the need arises. Notionally, a MANET is constructed from a disparate set of participants who must interact in order to complete an assigned mission. A MANET is inherently bereft of infrastructure. Members of the MANET must coordinate to perform the services typically provided by a network infrastructure (e.g., routing and data forwarding). However, the diversity of tactical operations, their scale, the wide range of equipment, the different speeds at which various parts of a tactical operation take place, as well as the environmental factors all present formidable challenges to the full and seamless deployment of MANETs in this context.

AN OVERVIEW OF THE TACTICAL NETWORKING PROBLEM SPACE

When considering the application of MANETs to the tactical space, it is necessary to consider the types of units deployed, their warfighting platforms, and their communication needs. Characteristics of these platforms have a significant effect on the design of the required solu-

 0163-6804/06/$20.00

As opposed to tame commercial environments, like café hot spots or hotel lobbies, the tactical environment is extremely harsh. A range of aircraft, from small UAVs to supersonic tactical fighters may inhabit the battlespace, introducing a different degree of mobility support at multiple layers of the protocol stack.

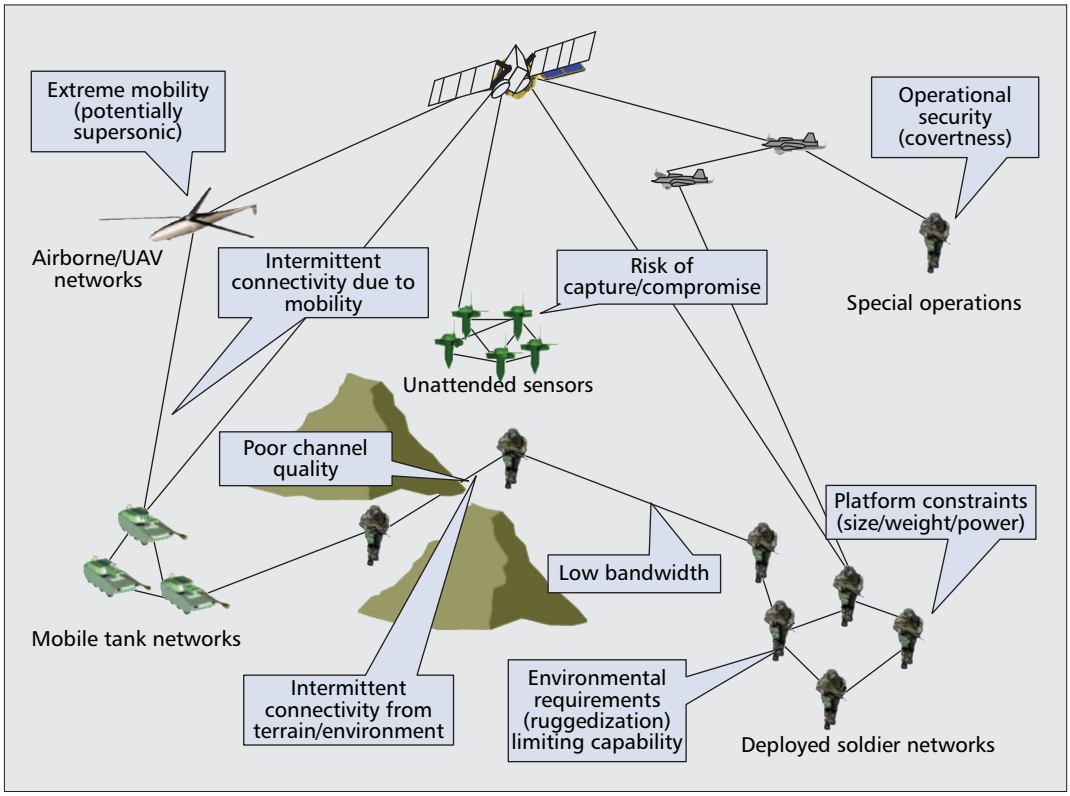

Figure 1. *The constraints of the tactical military environment*

tion. In any given operation, there may be dismounted soldiers, ground vehicles, various airborne units (unmanned aerial vehicles (UAVs), close air support (CAS) platforms, strategic fighters and bombers), and Naval platforms (both sea-based and amphibious). There will also be command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) assets that may be fixed or mobile.

To this effect, let us consider the ideal military MANET as expressed in many "vision" presentations. In the ideal military MANET, membership is dynamic, but limited only to authorized terminals. The MANET may connect to the GIG backbone or operate standalone, depending on mission and environment, with no unacceptable changes in performance or functional capabilities. GIG gateways, if available, are automatically discovered and changed during operations as required. Friendly units can almost always receive communication service from a MANET (within authorization limits) and authentication, authorization, integrity, and privacy parameters are automatically configured and negotiated in each case. Communication is secure both intra-MANET and external to the MANET. Networks may operate in anti-jam modes and in low probability of detection/interception modes. The military MANET is completely self-forming and self-healing in the sense that authorized units can join, leave, and rejoin the MANET without manual intervention (needed currently). The number of nodes in a military MANET can range from squad size or smaller to brigade size. The MANET can serve nodes moving at any speed from 5 km/hr to supersonic speeds. Nodes in a military MANET can communicate with arbitrary active and passive sensor networks as well. When there are multiple paths either within the MANET or to external nodes, the military MANET can always select a secure path, again without preplanning. This ideal military MANET is outside the scope of current capabilities and will require significant technical innovation before realization.

Figure 1 depicts some of the difficulties that the tactical space imposes on MANET technology. As opposed to tame commercial environments, like café hot spots or hotel lobbies, the tactical environment is extremely harsh. A range of aircraft, from small UAVs to supersonic tactical fighters may inhabit the battlespace, introducing a different degree of mobility support at multiple layers of the protocol stack. In addition, environmental conditions may range from desert to jungle to arctic to maritime, all of which are significantly different in RF propagation and signal characteristics. Because environmental conditions may be poor, and because of the need for covertness, bandwidth may be quite low and the connectivity may be intermittent with widely ranging communication gaps (seconds to days). Because of the risk of capture and compromise of equipment, the importance of authorization to join a MANET and the security of the communications is very high. Finally, the equipment should be lightweight, energy efficient, and easily integrated into tactical platforms (from backpacks to aircraft to aircraft carriers). Unlike the commercial world, communications equipment may also have to survive high environmental heat, dust, sand, salt water, and high terrestrial humidity, as well as very low temperatures at high altitudes. The tactical domain may also

require highly energy-efficient solutions to support long-deployed units (e.g., sensors).

The remaining sections articulate some key challenges and limitations associated with realizing the military-grade MANET in the foreseeable future.

A Brief View of Some Issues That Impact the Near-Term Plausibility of the Ideal MANET

There are numerous actively-researched technical issues that surround the successful realization of the ideal MANET within the tactical space, including medium access control (MAC), management, security, and routing. The amount of attention these topics have received within the research community combined with the remaining lack of mature solutions is evidence of the fundamentally hard nature of these problems. A detailed treatment of all these issues is beyond the scope of this article. Rather, a brief discussion is provided on several of these areas, with references provided to more exhaustive treatments [1]. This article then goes on to focus on system-level architectural and routing issues.

Medium Access Control

The design of the MAC is critical to several of the key attributes of the ideal MANET (e.g., self-organizing, self-forming, self-healing). This is a topic that continues to receive enormous attention from the research community, with a plethora of proposed approaches and techniques [2]. Despite the activity in this area, there is not yet on the horizon a mature high-performance solution that has begun garnering community support.

Network Management

The realm of network management covers a vast spectrum. Issues such as spectrum allocation, security materials, IP configuration, and network monitoring fall under the management umbrella. While these components are not unique to MANETs, they do become more difficult when nodal mobility, dynamic network membership, and unstable links are introduced to the network. There is ongoing work within both the research and standardization communities to address topics such as IP address assignment (e.g., [3, 4]). However, solutions in this area remain immature. Centralized network management architectures fail in MANETs. Not only is the dynamic membership an issue, but more importantly, the MANET may be disconnected from the larger network for long periods of time. This renders the collection/monitoring of data in a centralized server infeasible. Dynamic networks call for management capabilities that are distributed in nature. Localized functionality reduces the dependency on infrastructure or constant connectivity to a centralized management station. However, these types of distributed management capabilities remain relatively immature.

Network Security

The security aspects of MANETs have long been a robust research area. With the amount of time, resources, and money invested in network security for the traditional Internet model, it is only natural that people wish to provide the same level of solution to the MANET environments. However, it is well understood that the existing security mechanisms do not operate well in ad-hoc scenarios [5]. Traditional network security mechanisms have a dependency on dedicated infrastructure, which may or may not be present in the case of the ideal MANET. Furthermore, the tactical space mandates that increased attention be paid to aspects such as routing security (e.g., [6]), which remains an area with relatively immature solutions.

The security aspects of MANETs have long been a robust research area. With the amount of time, resources, and money invested in network security for the traditional Internet model, it is only natural that people wish to provide the same level of solution to the MANET environments.

Integration of Tactical MANETs into the GIG Framework

A tactical network is often considered an outreach of a fixed network (either wired or wireless). The tactical subnetwork connects to the fixed network through one or more special "gateway" nodes. This gateway often takes the form of satellite connectivity, particularly for forward-deployed tactical networks. The approach often taken in design is to assume that the network and the network that it is attaching to form a single larger flat network (Fig. 2). This model introduces several architectural and system-level issues that must be addressed:

- The need for ad hoc satellite connectivity
- The need for election and management of gateway nodes
- Scalability concerns due to the single flat network view.

Tactical networks will require the use of satellites to provide reachback capability in certain scenarios. However, there is a lack of satellite systems that provide the combination of both dynamic access and significant capacity. Current Military Satellite Communications (MILSATCOM) systems require significant staff resources and expertise to plan resources ahead of a deployment. Ground terminals must be given an appropriate configuration in order to access the shared satellite. Onboard resources must also be planned to coordinate and deconflict usage. Furthermore, reallocation of resources can be cumbersome, requiring network planner intervention [7]. Significant technical innovation is required in order to decrease the preplanned nature of MILSATCOM to better align with the vision of the ideal MANET. While this remains the end goal, this capability is not envisioned to be realized in the near-term.

The concept of gateway nodes (i.e., nodes that bridge the deployed tactical network and the fixed infrastructure) introduces planning and management complexity and imposes operational constraints. Because the network only has a finite number of egress/ingress points, the force structures that can be achieved are limited (where "force structure" refers to the type of, number of, and organization of assets), and can cause bottlenecks where network performance could degrade. This is particularly true given the limited capability that may be deployable on a mobile asset (gateway nodes in wired networks can be provisioned to offset bottleneck concerns). This also creates points of failure in the network, and requires far more logistical support

To ensure the long-term usefulness of military MANETs, the concept of introducing hierarchical structure into MANETs needs to be developed and matured, both in terms of how to form hierarchies and how to maintain hierarchies in the highly mobile tactical communications environment.

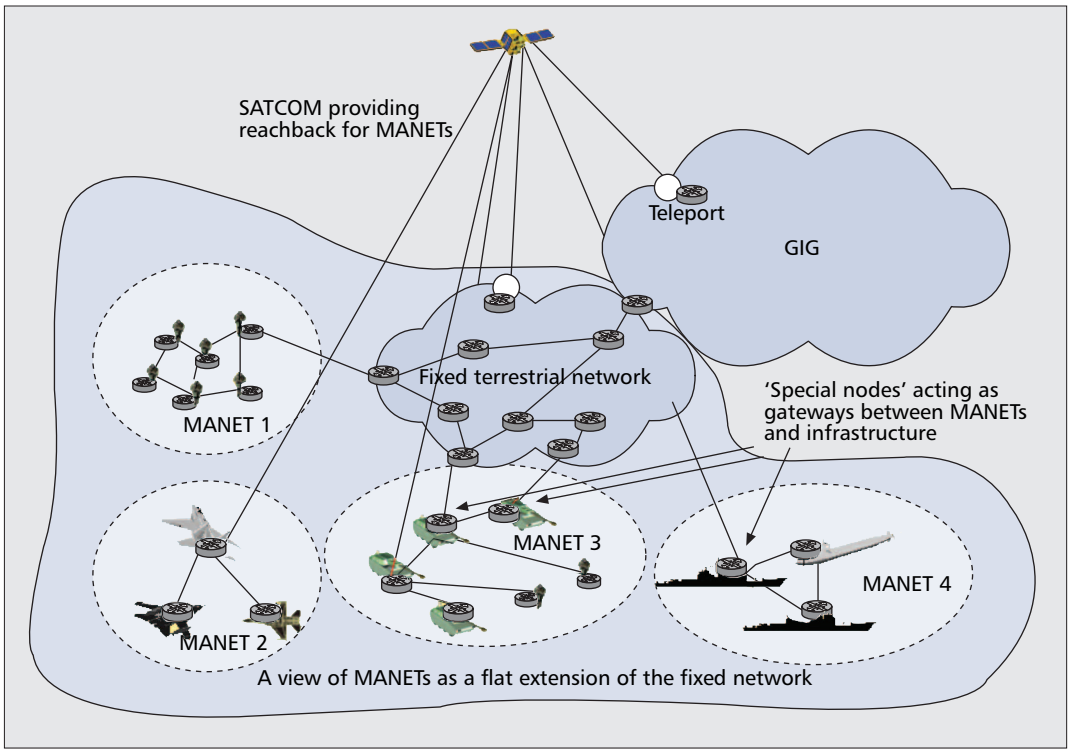

Figure 2. *A view of MANETs as a flat extension of the network infrastructure.*

and maintenance because different network assets are deployed. The number of gateway nodes and their logical placement in the network will affect performance.

In the ideal military MANET, every deployed asset could potentially operate as a gateway. However, this approach introduces significant technical complexities. Mechanisms must be in place to allow for the autonomous election/re-election of gateway nodes as required, and the dissemination of gateway information to the rest of the MANET. This is a complex capability that will require technical innovation beyond what is available today.

The view of the tactical network as a flat extension of the fixed network poses significant problems. First, the flat network could grow substantially as multiple MANETs interconnect, placing a burden on nodes within the fixed network. Furthermore, MANET nodes may require a large number of fixed node address entries in their routing tables. In addition, MANET link instability will require routing nodes within the larger network to remain robust, even with the introduction of potentially many unstable links.

Many emerging MANET solutions assume a flat-routed network with thousands of members. Such an approach simplifies the solution space within the context of configuring boundaries and hierarchies. However, the potential problems far outstrip the benefits obtained from such an approach. Drawbacks include security, management, and routing. A particular concern of large MANETs is the performance and stability of the routing protocol. Large networks that are flat-routed have limited performance. Experience from Internet routing research strongly suggests that hierarchy in network design increases network nodal capacity and decreases the operational expense of maintaining the network [8]. This includes not only the management aspects but also routing protocol performance. Without aggregation, network control traffic increases because of nonaggregated address advertisement routing exchanges among all nodes within the network. From the operational perspective, route flaps and topology changes (especially as mobility increases) have a greater impact on flat networks than hierarchical ones.

To ensure the long-term usefulness of military MANETs, the concept of introducing hierarchical structure (such as that described in [8]) into MANETs needs to be developed and matured, both in terms of how to form hierarchies and how to maintain hierarchies in the highly mobile tactical communications environment. This is a key area that requires active research if large-scale MANETs are to be achieved, yet an area in which little activity is currently observed.

MANET Routing

Of all network functions, routing illustrates the challenges of the military MANET quite clearly. We have touched on the difficulties of MANET routing already, but this section provides a more focused discussion on the difficulties of routing in the military MANET problem space. We divide our discussion of routing into two parts: routing within MANETs (interior MANET routing), and routing between MANETs and to other networks (exterior MANET routing).

Interior MANET Routing

By "interior MANET routing" we refer to the problem of routing among ad hoc mobile nodes, rather than routing to or between base stations or otherwise reaching the Internet, or in the case

of DOD tactical networks, the GIG. We do not imply that a MANET is equivalent to an autonomous system (AS).

The principal challenge in interior MANET routing is scalability. We must consider several different aspects of scalability:

- Scoping by mission (i.e., limiting most communications to a set of nodes involved in performing a specific mission)
- Scalability with respect to the number of units in the tactical space
- Scalability with respect to the capacity of the employed waveforms
- Scalability with respect to the forwarding capabilities of the nodes in the MANET
- Scalability with respect to the network and protocol traffic induced by the operational conditions and the platforms in use

The latter issue refers to the effect of operational conditions on the routing protocols themselves — specifically, the effect of speed and intermittency on the number of routing updates or new routes that must be computed for tactical MANETs. The combination of large numbers of nodes acting as routing peers and the large number of link changes (due to varying channel conditions and the speed of the platforms involved) work together to pose a significant challenge.

The topic of MANET routing has been a topic of significant research and standardization efforts. Efforts within the Internet Engineering Task Force (IETF) have produced several experimental protocols with current efforts to develop standards-track solutions. Furthermore, there exists a wide variety of interior MANET routing proposals within existing literature; far too numerous to exhaustively survey in a single article. There are many papers that summarize MANET routing protocols and their performance (e.g., [9]) and it is not our intention here to duplicate their efforts. Despite this intense research activity, mature solutions to this problem space have yet to emerge, even within the commercial problem space. In fact, research increasingly demonstrates that path stability is critical for the high performance of MANET routing protocols [9]. This suggests that

- Emerging approaches to MANET routing are not highly effective in the tactical environments for which they are most desperately needed
- The responsibility for high performance is placed onto MAC design, an area which is already known still to be immature

The interior routing problem is exacerbated by specific issues in the tactical networking space that should be addressed, and to our knowledge have either not been addressed or not addressed fully enough to demonstrate that the solutions being considered meet the requirements. Among these issues are the coexistence of potentially many MANETs of many different types and capabilities in the tactical space. This is an issue in several ways: scant attention has been given to the mechanisms and policies for different military MANETs merging together from a routing point of view. Can we expect, for example, that as a mobile unit network passes a battlefield-sensor network, that they will merge into a single routing domain and update their routing tables in a surge? Similarly, will a fly-by MANET of tactical aircraft merge with every network that it passes and can see in an area of operations? If we view this as undesirable, how do we prevent it from happening with current MANET routing technology?

Portions of a tactical MANET may become disconnected for long periods of time. By the time it reconnects, its routing information will be stale and it will require a refresh. Again, we can expect surges of routing information to flow between these networks at a time when units are joining together and possibly need to trade other application- and mission-critical information. Many of the RF links in tactical MANETs are bandwidth poor. The policies for the use of those links as transit links for applications that one service may consider critical and another not, have not even been discussed, much less mechanisms developed for implementing and enforcing those policies.

Another key issue in MANET routing is efficient multicast routing. Situational awareness (SA) information has potentially many producers and even more consumers in the tactical space. In addition, life-critical SOS and emergency information needs to be broadcast. While there is some work on MANET multicast protocols (e.g., [10]), it is still in its early stages. As it develops, it will need to scale in order to work in the tactical networking space.

Finally, military mobility is quite different from mobility in the commercial environment. This implies that the random waypoint model is probably not sufficient to evaluate MANET routing protocols for tactical networking. On both large and small scales, we can expect military mobility to be much more coherent and directed and that nodes will be in general more concentrated, rather than more dispersed (though in some operational scenarios, just the opposite will be true).

Our assertion is not that these problems cannot be solved; it is merely that they need to have research attention before envisioned tactical networks meeting all the projected requirements will be real.

On both large and small scales, we can expect military mobility to be much more coherent and directed and that nodes will be in general more concentrated, rather than more dispersed (though in some operational scenarios, just the opposite will be true).

Exterior MANET Routing

In order for MANETs to be used effectively in tactical communications, there must be an overall network architecture that determines how MANETs function with the rest of the communications networks. Most attention so far in MANET research has been focused on the MAC layer and specific routing protocols within the MANET. Little attention has been given to how MANETs interoperate within the larger network. However, in the tactical space, MANETs must often operate in concert with other networks.

The operation of MANETs within the context of the larger GIG requires some scoping of the routing domain between interior and exterior for scalability, as with wired networks. MANETs cannot necessarily predict how many and which other networks they will need to connect to. MANETs cannot grow arbitrarily and simply absorb all other MANETs operating in the same tactical space or be absorbed into a single flat routing domain. A given MANET may have multiple points of attachment to a fixed or semi-fixed infrastructure. However, given mobili-

The dynamic nature of BGP speakers and peer networks also impacts the ability to use current BGP security solutions. Because of the capability of nodes to join and leave MANETs, if fixed addresses are used, route summarization becomes very difficult because MANET membership can be dynamic.

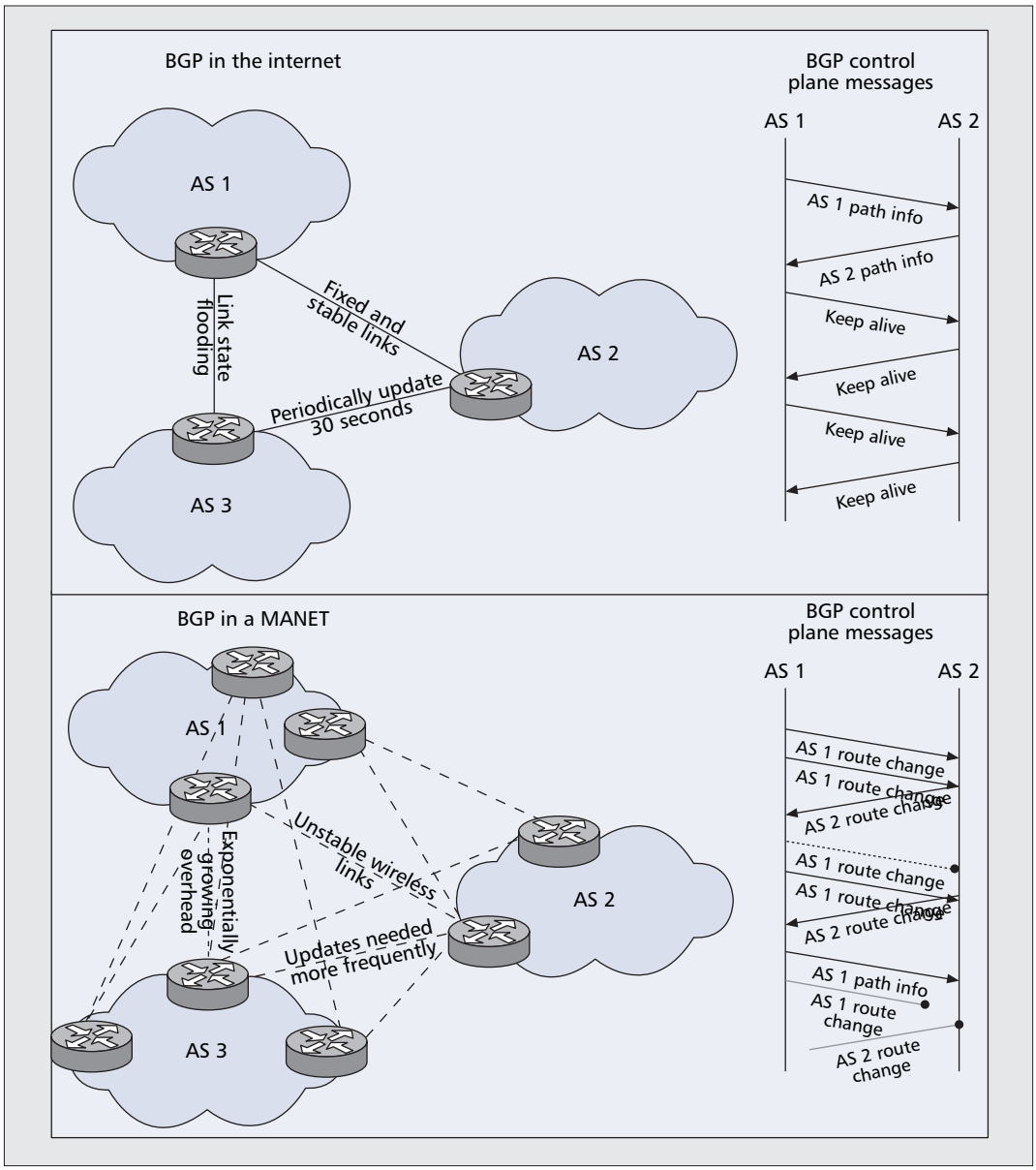

Figure 3. *Issues surrounding BGP employment in a MANET.*

ty and varying quality links, the MANET may not be able to maintain internal connectivity. Consequently, there may be the phenomenon of internally disconnected fragments of a single MANET routing domain that are connected to the same infrastructure network.

These issues argue that an exterior MANET routing protocol is needed. We note that Border Gateway Protocol (BGP) is not that protocol. BGP is not able to detect and connect dynamically to arbitrary peers (it is less flexible than OSPF in that respect) and the degree of mobility that would be found in a tactical MANET environment demands that it do so. In addition, the instability of links and peers will require a prohibitive amount of routing information to be exchanged for limited bandwidth connectivities in the tactical environment [11]. Additionally, BGP peering sessions are established over statically configured TCP connections. Dynamic membership and mobility within a MANET inhibits the configuration of BGP peering sessions given the lack of a priori knowledge of which node within the MANET is capable and available to establish a BGP peering relationship with an arbitrary peer network. The dynamic nature of BGP speakers and peer networks also impacts the ability to use current BGP security solutions. Because of the capability of nodes to join and leave MANETs, if fixed addresses are used, route summarization (which is required for BGP scalability) becomes very difficult because MANET membership can be dynamic. Assigning a prefix to the MANET to simplify summarization requires an ability to automatically configure that prefix in all nodes as they join the network. Such auto-configuration is an open research topic. Equating a MANET routing domain with an AS may lead to AS fragments (internally disconnected) attaching to other multiple ASes, causing problems with the inter-domain routing system [12]. These issues are illustrated in Fig. 3, where path information (PI) messages now form the bulk of BGP control

plane messages, as opposed to the wired case of predominance of much smaller keep-alive (KA) messages (|PI| >>> |KA|).

For these reasons, it is argued that a new approach to interdomain routing must be developed for MANETs that, at a minimum, have the characteristics summarized in Table 1. This is a critical research area for MANET routing that is currently receiving (relatively) little attention. Without proper attention to the aspect of exterior routing, deployed tactical networks could be significantly limited in terms of its capability to internetwork with other networks within the GIG.

1. Dynamically discover, authenticate and connect to routing peers
2. Auto-configuration capabilities
3. Parsimony of routing information on exchange, including suppression of route exchange on re-connection.
4. Strong authentication, information protection and resistance to hostile, perhaps Byzantine attacks on the protocol.
5. Ability to accept and form multihomed attachments with other networks

Table 1. *Requisite interdomain MANET protocol characteristics.*

CONCLUSIONS

Key areas, such as MAC design, routing, management, and security pose significant technical challenges that require substantial innovation before military MANET solutions will be realized that are consistent with the long-term vision of NCW. From the wide variety of proposed solutions to these problem areas, it is becoming increasingly evident that this is a poorly understood problem space.

Equally daunting challenges are presented in the effective internetworking of these tactical MANETs, an area not yet receiving significant interest. How does the MANET communicate with other networks within the GIG? What is the proper architectural view of the tactical MANET within the context of the larger GIG? How can the concepts of hierarchy that have helped the Internet scale be built into tactical MANETs? How can military assets such as satellites be made less preplanned in nature to match the same type of (desired) ad hoc nature in the tactical network itself. These are all fundamentally hard problems that have no clear path forward in terms of solutions. At this stage, many of these issues are still at the point of basic research. Requirements and usage cases must be articulated in order to better understand the problem space.

The authors believe that the ideal MANET is indeed a good goal, and is the eventual requisite capability for the tenets of NCW to ever become fully realized. However, the reality is that MANET technology is still in an early stage of evolution and is too immature to provide the ideal MANET. A more realistic expectation is that infrastructure and much preplanning is required for the foreseeable future. MANET technologies will mature over time at an uneven rate (i.e., certain aspects of MANET technologies will mature faster than others), and tactical networks can leverage these technologies to evolve towards the ideal MANET. During this evolution, the scale of MANETs should remain limited, with sufficient infrastructure in place to guarantee adequate performance and protection. Does this provide the ideal capability? No. Does this provide a positive way forward that guarantees a reasonable capability that can evolve and improve over time? Yes, and that is likely the best anyone should expect for the foreseeable future.

REFERENCES

[1] I. Chlamtac, M. Conti, and J. J-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," *Ad Hoc Networks*, 2003, pp. 13–64.

[2] Raja Jurdak *et al.*, "A Survey, Classification and Comparative Analysis of Medium Access Control Protocols for Ad Hoc Networks," *IEEE Commun. Surveys*, vol. 6, no. 1, 1st Quarter 2004.

[3] P. M. Ruiz, F. J. Ros, and A. Gomez-Skarmeta, "Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges," *IEEE Commun. Mag.*, Oct. 2005, pp. 118–25.

[4] M. R. Thoppian and R. Prakash, "A Distributed Protocol for Dynamic Address Assignment in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 1, Jan. 2006.

[5] L. Zhou and Z. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, 1999, pp. 24–30.

[6] J. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Commun. Mag.*, Oct. 2002.

[7] C. Sbarounis *et al.*, "Dynamic Bandwidth and Resource Allocation (DBRA) for MILSATCOM," *2004 IEEE Military Commun. Conf.*, 31 Oct.–3 Nov. 2004, vol. 2, pp. 758–64.

[8] J. Yu, "Scalable Routing Design Principles," RFC2791, July 2000.

[9] K.-W. Chin, "The Behavior of MANET Routing Protocols in Realistic Environments," *2005 Asia-Pacific Conf. Commun.*, Oct. 2005, pp. 906–10.

[10] J. Macker *et al.*, "Simplified Multicast Forwarding for MANET," Internet Draft, work in progress.

[11] E. Fleischman and W. Furmanski, "Mobile Exterior Gateway Protocol: Extending IP Scalability," *Military Commun. Conf.*, Oct. 2005.

[12] J. P. Macker and V. D. Park, "Heterogeneous Architecture Support for Wireless Network Dynamics and Mobility," NRL Report RL/MR/5520—00-8513, Nov. 2000.

BIOGRAPHIES

JACK L. BURBANK (Jack.Burbank@jhuapl.edu) received his Masters of Science in electrical engineering in 1998 from North Carolina State University and supervises the wireless networking section at The Johns Hopkins University Applied Physics Laboratory. His recent work is in the areas of wireless network electronic attack, sensor networking, and mobile ad hoc networking. He is a professor of networking and telecommunications in the Johns Hopkins University Part Time Engineering Program, and a member of the IEEE and the ASEE.

PHILIP F. CHIMENTO [SM] is a senior technical staff member at the Johns Hopkins University Applied Physics Laboratory. He received an A.B. degree (magna cum laude) from Kenyon College, an M.Sc. degree from Michigan State University, and a Ph.D. degree in Computer Science from Duke University. He has spent more than 25 years in the field of computer communications, in both industry and academia. He is a member of the ACM.

BRIAN K. HABERMAN is currently a Research Staff member at the Johns Hopkins University Applied Physics Laboratory and a Doctoral Candidate in the Johns Hopkins University Whiting School of Engineering. His research interests include IPv6, mobility, sensor networks, inter-domain routing, and multicast. He is the co-chair of the IETF's IPv6, MAGMA, and NTP Working Groups. He holds a B.S. in computer science from Clemson University and an M.S. in computer science from North Carolina State University.

WILLIAM T. KASCH received a B.S. in electrical engineering at the Florida Institute of Technology in 2000 and an M.S. in electrical and computer engineering at the Johns Hopkins University in 2003. His interests include various aspects of wireless networking, including MANET, IEEE 802 technology, and cellular. He participates actively in both the IEEE 802 standards organization and the Internet Engineering Task Force.