A Cautionary Tale on Testing and Evaluating Tactical Wireless Mobile Ad Hoc Networks

Dr. John A. Stine
Operations Research and Systems Analysis Department
Acquisition and Systems Analysis Division
The MITRE Corporation, McLean, Virginia

Transformation dictates that the nature of future warfare will be network-centric where net-centricity is contingent on a ubiquitous network. At issue are the capabilities that this network must have to make network-centric operations (NCO) possible. Wireline and commercial wireless technologies have colored the expectations of what is possible and, in many cases, the requirements for the network and the applications as well. This article argues that these technologies are fundamentally different than what is required on the battlefield and, if caution is not exercised, these technologies could easily misdirect requirements and subsequent testing and evaluation strategies toward performance measures that are orthogonal to those required to enable NCO. The article reviews several contemporary discussions of NCO and networks to arrive at the thesis that the critical networking technology for the tactical edge is one that allows users to communicate with each other locally regardless of their organization and without dependence on connectivity to a network infrastructure. This article suggests test and evaluation approaches to validate this capability and to measure its effectiveness.

Tactical wireless mobile ad hoc networks (MANETs), as the means being used to network the maneuvering warfighters, are critical components of network-centric operations (NCO); however, these networks have been, and continue to be, a topic of research. There is no settled lore on design, use or performance. Meanwhile, the urgency to deliver these networks to the warfighter will require commitment to a technology. If care is not taken, this technology may not deliver the capabilities necessary for the evolution of warfare as envisioned in network-centric warfare (NCW). And worse, if fielded, it may become part of a legacy of equipment and applications that feed the inertia that will prevent the technology transformation that is desired. This undesirable end results from the tendency to create requirements based on similar technology. The purpose of this article is to explain why this is a problem; to articulate what the author believes are the critical capabilities that tactical networks must provide; and then to suggest evaluation and testing strategies to assess their achievement.

This article recounts the expectations for the tactical Internet and the testing strategy that preceded the Army's Task Force XXI Advanced Warfighting Experiment (TF XXI AWE) in 1995 and then the corrections that followed to conform to the actual technology that was delivered for the experiment in 1997. The purpose is to show an untainted vision of the networking capabilities that users thought would create a tactical advantage and also the role network design had in preventing those capabilities. Users initially thought tactical networking would enable them to communicate with each other in a local sense across organizational boundaries, but the tactical network remained hierarchical.

That hierarchy, both in a logical and physical sense, had to be maintained for the network to work. Next is a review of the observations presented in recent publications on NCO and tactical wireless networks to reveal that these original capabilities are still desired. Whereas the significant advantage of NCO is the increased operational tempo (OPTEMPO) that results from better situational awareness (SA) and command and control (C^2), new ways of fighting are born out of the social interaction of users. The social interaction of the tactical user requires the communications capabilities that were first imagined. The next two sections discuss networking technologies, first the MANET technologies and then commercial wireline and wireless technologies, highlighting the differences in the problems they try to solve and the differences in the capabilities of the technologies.

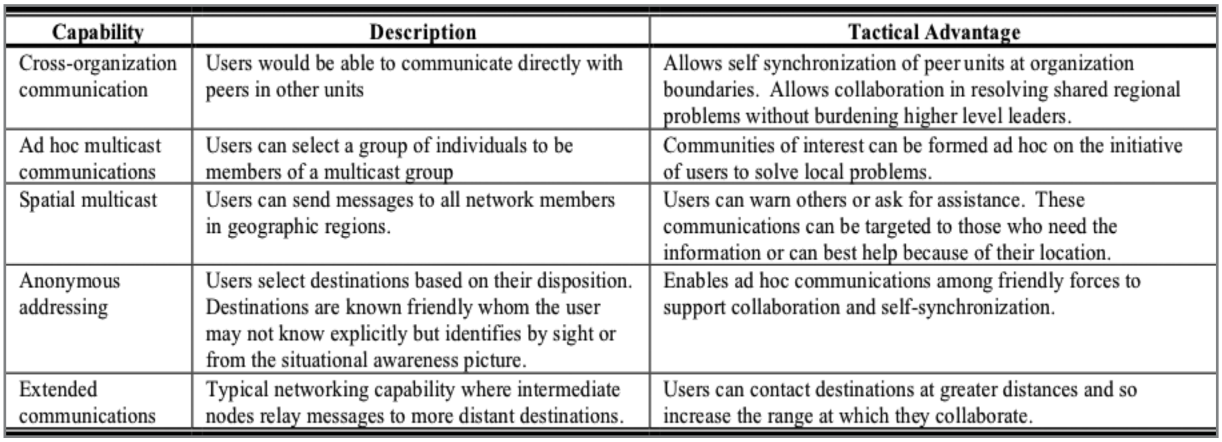
Wireline concepts that are used in network and application design are inappropriate for the mobile tactical environments and can be an impediment to NCO. They lead to the design of information systems that have static concepts of information exchange predicated on the expectation that the networking technology will support them. Tactical network technologies that are designed, tested and evaluated against this standard for performance are likely to forego providing the ad hoc communications capability that enables the local social interaction of warfighters. The warning is that the test and evaluation (T&E) community can be lured into executing T&E strategies that are complicit in promoting this end result. The author's position is that connecting to a larger infrastructure should be secondary to enabling *any subset of users* in proximity to each other to talk to each other. This latter capability should receive emphasis in T&E. At this point, the article discusses the difficulty in T&E of MANETs and reviews different strategies that are used. The author proposes a T&E strategy that he believes better differentiates the capabilities of MANET technologies and their suitability for tactical environments.

"Right-sizing expectations for Task Force XXI"

In the spring of 1995, excitement was high among the experimenters (the users, developers and evaluators) that were selected to participate in the Army TF XXI AWE. The centerpiece concept that was being evaluated was a brigade-wide network dubbed the tactical Internet. There was a shared sense of responsibility that it was a collective task to demonstrate the immense advantage that such a network could provide. In his zeal, the assistant division commander (ADC) of the experimental force (EXFOR) called in the testers to clarify their task well before the issues and criteria for the experiment had been established. Having given much thought to the problem, he realized that the advantages would not be apparent unless the users knew how to take advantage of them, and the testing events put the EXFOR into situations where the network could allow solutions not previously possible.

There were two primary benefits that the network and the "Applique"[1] application were expected to provide: improved SA and a better communications capability. *Table 1* lists the fundamental new communications capabilities that the experimenters thought the network would provide. In addition, some legacy communications capabilities were expected to survive the transition, specifically the ability to eavesdrop on C^2 nets and the ability to move from one C^2 net to another. The eavesdropping capability was used frequently by higher-level commanders to assess the activities of lower organizations and lower-level organizations to learn of impending operations. The content and the perceived stress in vocal communications were key components in their developing an SA. Further, moving among C^2 nets was necessary for operational flexibility.

From the better SA and communications came a vision of a much more dynamic and fast-paced type of warfare where lower-level leaders could have much greater initiative because they could collaborate and self-synchronize among themselves. A very interesting anticipated capability was that of reconstitution, where the improved SA and communications capability would allow battle survivors to self-organize into effective fighting organizations for follow-on operations. This task demanded the flexible communications of Table 1. It was clear that the EXFOR ADC envisioned a tactical advantage would result from this type of flexible communications among tactical users. He expected the EXFOR to be trained to seek advantages



Capability	Description	Tactical Advantage
Cross-organization communication	Users would be able to communicate directly with peers in other units	Allows self synchronization of peer units at organization boundaries. Allows collaboration in resolving shared regional problems without burdening higher level leaders.
Ad hoc multicast communications	Users can select a group of individuals to be members of a multicast group	Communities of interest can be formed ad hoc on the initiative of users to solve local problems.
Spatial multicast	Users can send messages to all network members in geographic regions.	Users can warn others or ask for assistance. These communications can be targeted to those who need the information or can best help because of their location.
Anonymous addressing	Users select destinations based on their disposition. Destinations are known friendly whom the user may not know explicitly but identifies by sight or from the situational awareness picture.	Enables ad hoc communications among friendly forces to support collaboration and self-synchronization.
Extended communications	Typical networking capability where intermediate nodes relay messages to more distant destinations.	Users can contact destinations at greater distances and so increase the range at which they collaborate.

Table 1. Expected networking capabilities for Army Task Force XXI

using these communications capabilities, for the testing scenarios to create opportunities for their demonstration, and for the testers and evaluators to be astute enough to look for them.

Unfortunately, the first tactical Internet did not measure up to this vision of agility—it was quite inflexible. The architecture hardwired the organization together, required a significant engineering effort to configure and was fragile. Not only did it not provide the capabilities listed in Table 1, it prevented the previous capabilities of eavesdropping and moving between C^2 nets.[2] Nodes (and thus, users) had a position in the network that translated into a near-permanent task organization. The network was designed primarily to transport SA data, and the C^2 communications remained the traditional hierarchical voice nets.

Meanwhile, the testing scenarios were driven by the objective to observe improved OPTEMPO by a brigade-sized force as opposed to demonstrating any particular new communications capability. It was impractical for testers to try to steer the activities in the force-on-force events to create situations that would reveal an improved agility as the ADC had promoted. The subsequent development of the issues and criteria for the experiment were constrained by these realities. The focus of data collection and evaluation was directed toward measuring improvements in SA and OPTEMPO. Testers emphasized instrumenting the network and placing subject matter experts throughout the EXFOR to make these assessments (Sayre et al. 1998). The performance of the network was observed, but there was no effort to identify or test new communications capabilities such as those listed in Table 1.

The point of this story is threefold. First, networks have two characteristics that are important to transformation: their ability to move data across a network and their ability to support collaborative peer-to-peer communications. Second, without knowledge of the networking technology, the experimenters felt an advantage of tactical networking would be the ad hoc communications they could execute among themselves. And third, there is a tendency to evaluate networks by focusing on their ability to move data for the applications that use them as opposed to verifying communications capabilities of the technology. The remainder of this article will attempt to show that, in evaluating tactical networks, assessing whether a flexible communications capability exists is the more important task and that measuring capacity and support of application information exchange can easily become a distraction.

NCO tactical networking requirements

NCO is a new theory of warfare based on exploiting information technology and is the core concept that guides the transformation of the U.S. military. It is summarized by the tenets of NCW that were articulated in the Executive Summary of the Department of Defense (DoD) Report to Congress in 2001. They state that "a robustly networked force improves information sharing and collaboration, which enhances the quality of information and shared situation awareness. This enables further collaboration and self synchronization and improves sustainability and speed of command which ultimately result in dramatically increased mission effectiveness." (Garstka and Alberts 2004) It is well understood that this transformation will require simultaneous changes in doctrine, organization, training, material, leadership development, personnel and facilities (DOTMLPF). This breadth of change implies a commitment, and such a commitment requires a vision of what the network will deliver and how to access these capabilities.

In defining the network requirements, the NCW tenets state that the network must be robust, referring to a comprehensive and reliable connectivity of all networked entities. The expectation that this statement creates is actually a problem. While the network is being invented, developers of applications and middleware have assumed, or tried to specify, network capabilities. In 2004, a study of Army bandwidth needs (Joe and Porche 2004) states that the bandwidth the Army demanded was not achievable. The study's recommendation was for the Army to reassess its information demands and to determine what information truly contributes to mission success. The JASONs, a group of academics that assembles each summer to consider DoD technology problems, was asked in 2005 to assess the state of the art for MANETs, to identify gaps between the Army's stated requirements and what MANETs can support, and to provide recommendations.

The group's conclusion in (Weinburger et al. 2006) was that MANET technology could not currently, nor would it in the foreseeable future, support the communications capabilities envisioned. Its recommendations called for the following: In the short-term, scale back the requirements and build to those, while simultaneously investing in a large research program with emphasis on enabling commanders to reliably predict the behavior of their networks. The point is that a concurrent transition across DOTMLPF is risky. All solutions will be constrained by what the networking technology can provide, but because those constraints are not known, development of battle command systems must assume capabilities or specify their requirements. The reports previously mentioned say that this is what had happened—information demands had overreached what technology could deliver.

The question now is whether this is the appropriate path to the development of network-centric systems, and if not, then what is the alternative? The author's position is that the network is the core technology of tactical NCO; it should be the focus of development; and applications should be designed once the capabilities of the network are known. The remainder of this article attempts to identify what capabilities this network must achieve, and it also tries to contrast these capabilities with those that have driven the development of networks thus far. Evidence is presented in the next section indicating that a communications capability of a networking type (one that is accessible to users) is a key enabler of NCO.

Significance of social domain and social networks

Domains are used to categorize network-centric phenomena. The physical domain covers the infrastructure that supports NCO, the physical activities of the forces and the place where those forces are to have an effect. The information domain is where information resides and the processes that create, manipulate and share it. The cognitive domain "encompasses perceptions, awareness, understanding, decisions, beliefs and values of the participants." The social domain is "where force entities interact, exchange information, form awareness and understanding, and make collaborative decisions." (Garstka and Alberts 2004)

The first three domains—physical, information and cognitive—were the domains that were used to describe information warfare in (Alberts, Garstka, Hayes and Signori 2002). Through their subsequent study of the effectiveness of forces with NCO capabilities, (Garstka and Alberts 2004) observed that there was an increased effectiveness that could be attributed to two factors. The first is greater agility. Agility is the ability to quickly and nimbly adapt and respond to changing circumstances and to develop innovative solutions to problems. The second is that people, not technology, are what adapt, respond and develop innovative solutions. Technology is only an enabler. This pushes the discussion of what causes NCO into the social domain, and so it was added to the domains of NCO.

Similar to domains in NCO, networks can be divided into different classes: physical, communications, information and social. Physical networks refer to the components that connect entities to each other. Communications networks are the logic and protocols that govern how communications move in a physical network. Information networks encompass the logic and processes that control the collection of information, its fusion and manipulation into an information schema, and then the information distribution in the network. Finally, social networks encompass the social structures that form about individuals, groups and their cultures. These networks tend to be built upon each other, social on information, information on communications, and communications on physical (Committee… 2005).

In studying the value of network science as a research discipline for the Army to fund, the Committee on Network Science for Future Army Applications made two observations relevant to this discussion. First, the committee stated, "The value of NCW is said to be the greatest at the intersection of the four domains. Analysis of recent military operation in Iraq and Afghanistan suggests, however, that only the information domain is represented." (Committee… 2005, 21) Second, it states, "As a consequence of its discussions with Army and DoD representatives, the committee has come to realize that the fundamental problems underlying effective network-centric operations (NCO) lie in the social domain." (Committee… 2005, 40) It is interesting how this matches the observations of what happened in the TF XXI AWE. Improvements in effectiveness in the AWE were also the result of better SA and doing things faster rather than as a result of changes in the social interactions among warfighters.

So, what is the social network that would cause new ways of fighting, and why is it not being observed? The research of (Barabási 2002) indicates that social networks tend to converge at individuals who know the most people, have the most capability or broker the most power yielding a scale-free connectivity. This observation seems attractive, especially with those that confront the scalability of MANET-routing protocols, but there is a simple reason why this is not the paradigm: capacity. Commanders do not have the capacity to directly lead an indefinite number of entities. The hierarchical C^2 structure has evolved from this experience. Similarly, the wireless physical networks are constrained by capacity, and it would be debilitating to cause traffic to converge at a node.

The alternative is actually seen in the prescient ideas of the EXFOR ADC during the TF XXI AWE. The social network should also include all nodes that are in proximity to each other. The motivation for social interactions among actors in proximity to each other is that they are in a position to most impact each other's area of interest, either intentionally or unintentionally. Benefits come from the opportunities to warn, to assist and to cooperate. The killer application of the network is to enable users to network with each other on their own terms. The reason why the latter social network is not enabled is that the network architecture: physical, communications and information, match the hierarchy of the chain of command and are focused on providing transport for applications. In many cases, despite proximity, cross-organization communications are impossible. Traditional social relationships are the only ones that the networks and applications support.

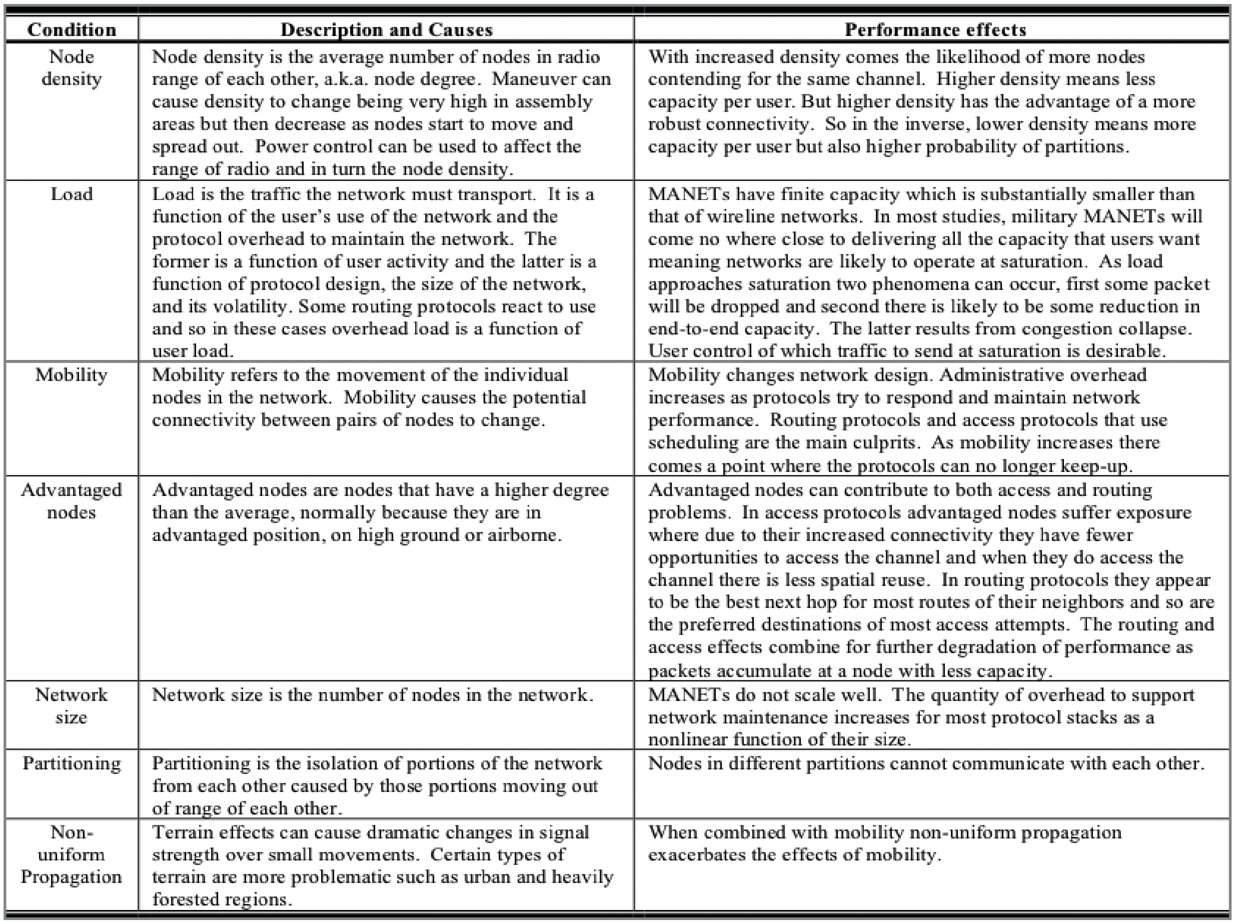
Dominant effect of scenario on network performance

The networking technology that will be implemented at the tactical front is referred to as a MANET. Although there are many different visions about what paradigms, protocols and radio frequency (RF) technologies should be used to build MANETs, there is a common understanding of their properties—there is no infrastructure, and they are self-forming and self-healing. Unlike wireline networks that are designed to provide a capability, MANETs adapt to provide as good a capability as the situation allows. The actual design of the network is a function of the disposition of the nodes, and this disposition can greatly affect the performance of these networks. *Table 2* lists some critical dependencies between MANET performance and use scenario. Simply put, users design their own networks by how they maneuver. Robust connectivity is a goal, not a guarantee.

This dependence between network performance and maneuver begs the question to what extent should average users understand and be concerned about how their collective behavior affects network performance. The configuration of networks is not easily understood and is usually managed by a central authority, so developers would prefer users be concerned only with using the network. Unfortunately, the physics of tactical wireless communications offers a very different reality. A pleasing observation that is made later in this article is that a solution that solves the social networking problem will also allow a user to understand his network, and both can be made quite intuitive.

Suitability of commercial technologies

Without a clear understanding of the limitations of MANET technologies, commercial technologies drive both the expectations of performance and the paradigm on which applications are conceived and developed. Multiple problems arise because there is a fundamental difference in the physics, logic and purpose of these technologies as compared to



Condition	Description and Causes	Performance effects
Node density	Node density is the average number of nodes in radio range of each other, a.k.a. node degree. Maneuver can cause density to change being very high in assembly areas but then decrease as nodes start to move and spread out. Power control can be used to affect the range of radio and in turn the node density.	With increased density comes the likelihood of more nodes contending for the same channel. Higher density means less capacity per user. But higher density has the advantage of a more robust connectivity. So in the inverse, lower density means more capacity per user but also higher probability of partitions.
Load	Load is the traffic the network must transport. It is a function of the user's use of the network and the protocol overhead to maintain the network. The former is a function of user activity and the latter is a function of protocol design, the size of the network, and its volatility. Some routing protocols react to use and so in these cases overhead load is a function of user load.	MANETs have finite capacity which is substantially smaller than that of wireline networks. In most studies, military MANETs will come no where close to delivering all the capacity that users want meaning networks are likely to operate at saturation. As load approaches saturation two phenomena can occur, first some packet will be dropped and second there is likely to be some reduction in end-to-end capacity. The latter results from congestion collapse. User control of which traffic to send at saturation is desirable.
Mobility	Mobility refers to the movement of the individual nodes in the network. Mobility causes the potential connectivity between pairs of nodes to change.	Mobility changes network design. Administrative overhead increases as protocols try to respond and maintain network performance. Routing protocols and access protocols that use scheduling are the main culprits. As mobility increases there comes a point where the protocols can no longer keep-up.
Advantaged nodes	Advantaged nodes are nodes that have a higher degree than the average, normally because they are in advantaged position, on high ground or airborne.	Advantaged nodes can contribute to both access and routing problems. In access protocols advantaged nodes suffer exposure where due to their increased connectivity they have fewer opportunities to access the channel and when they do access the channel there is less spatial reuse. In routing protocols they appear to be the best next hop for most routes of their neighbors and so are the preferred destinations of most access attempts. The routing and access effects combine for further degradation of performance as packets accumulate at a node with less capacity.
Network size	Network size is the number of nodes in the network.	MANETs do not scale well. The quantity of overhead to support network maintenance increases for most protocol stacks as a nonlinear function of their size.
Partitioning	Partitioning is the isolation of portions of the network from each other caused by those portions moving out of range of each other.	Nodes in different partitions cannot communicate with each other.
Non-uniform Propagation	Terrain effects can cause dramatic changes in signal strength over small movements. Certain types of terrain are more problematic such as urban and heavily forested regions.	When combined with mobility non-uniform propagation exacerbates the effects of mobility.

Table 2. Scenario effects on MANET performance

MANET technologies and the networking problems of tactical environments. One must consider each.

■ *Physics*

The wireline medium is profoundly different than the wireless medium. It is dedicated to a selected subset of nodes; it can have immense bandwidth that is expandable; it is highly reliable; and it is static in its connectivity. If bandwidth is insufficient, more can be purchased. Bandwidth is inexpensive compared to the costs of other components in the network. In contrast, wireless capacity is comparatively miniscule and is a finite resource that must be shared, so it is the most valuable resource. Connectivity between a pair of nodes is a function of proximity and the use of the media by others. It is much less reliable, and its reliability changes with mobility.

Commercial wireless technologies do not provide a model for tactical networking. They are primarily used as a last-hop technology where access into an infrastructure network is achieved through single-hop wireless transmissions between wireless nodes and an access point. As a result, the access point can be used to arbitrate access and maximize channel utilization. All routing is within the infrastructure and does not involve the use of the wireless media. Access points are static, and the only issues that result with node mobility are changing their association with access points as they move, and then informing the infrastructure of this change. These technologies do not seek to enable direct peer-to-peer connectivity as is necessary in tactical networks.

■ *Logic*

Commercial networks, both the Public Switched Telephone Network (PSTN) and Internet Protocol (IP) networks are logically hierarchical networks. Switching and routing move up a series of networking levels to the first common network level, then across that level, and back down the hierarchy to the distant end. These hierarchies are articulated in telephone numbers and IP addresses. The logic of these hierarchies is the foundation of network design. Network designers articulate their intended movement of traffic by how they connect nodes and assign addresses.

In contrast, MANETs have no permanent logical design. Connectivity cannot be chosen *a priori*, so designers cannot specify the movement of traffic *a priori*. The hierarchical logic of network design and configuration does not apply. Efforts to make it apply deny the mobility of nodes except to within the range of routers that span hierarchies and limit direct connectivity to peers in the same hierarchy.

Further, in the case of IP networks, the logic of a link is the fundamental building block of networks. Most protocols that reside above IP assume a reliable interconnection of links beneath IP. This paradigm is the foundation of routing, multicasting, quality of service and security protocols in IP networks. The link assumption is not true in MANETs, which makes most of these protocols inappropriate for tactical networks (Stine 2006).

■ *Purpose*

The value of most networks is a function of the larger infrastructure. It already has value, and the user benefits by connecting to it. Thus, users want to connect to the network to obtain access to e-mail services, corporate applications, the World Wide Web or the PSTN. This is certainly the case for commercial wireless technologies. WiFi provides access to a LAN, WiMax to the Internet, and cellular telephony to the PSTN. Additionally, most all popular applications have an infrastructure base, including those that give the illusion of peer-to-peer connectivity such as messaging and chat rooms.

Here is the important view that governs the position of this article. The primary purpose of the wireless tactical network is to provide a means of communications among local actors to solve local problems. Its secondary purpose is to connect to the infrastructure. In tactical environments, users cannot rely on a fully connected network and so cannot rely on access to any infrastructure or infrastructure-based applications either. Any *2, 3* or *n* neighboring users should be able to form a network, exchange information among themselves and collaborate to solve problems, without depending on connection to a network external to themselves.

Meanwhile, the dominance of the infrastructure view of information systems and their supporting networks is causing the networks of tactical NCO systems to be designed in a way that does not give emphasis to this objective. Recall that there are several classes of networks: physical, communications, information and social, and that each class is built upon the other in that order. Currently, the information network is being designed first; it is the easiest place to start.

Driven by system engineering views of business processes, developers hypothesize the information exchange requirements (IER) necessary for operations. Meanwhile, policy, urgency and these IERs guide the communications network development. The need for compatibility with the larger Global Information Grid (GIG) and the abundance of applications that are already available for IP-based networks make extending wireline networking principles down to the tactical edge a goal. In the end, physical networks are expected to conform to the communications network concepts, and social networks are expected to evolve from the information networks.

There is no better case study of the problem than current systems. Say a new network was delivered to be used with FBCB2: How would it be evaluated? The concept of how FBCB2 supports battle command would not change. The transport and dissemination of information would follow the same logic. The time to initialize the system, currently over three months (Sprinkle and Black 2006), would stay the same at best. There would be no new social networks formed or business processes possible. The only observable difference would be in the transport capabilities.

The T&E conundrum is that this combination of expectations and requirements leads to a prototypical set of measures of effectiveness and performance of the network (for example, interoperability, capacity, latency and so forth) that alone do not capture the networking capabilities that are necessary for NCO at the tactical edge (that is, the ability of users to create and maintain a network that supports the information and social networks needed for operations). A description of the dependencies of MANET performance on scenario precedes this section to make clear that there is dependence between the former types of measures and use. If the users are not given the ability to understand how their activity affects their networks and to adapt, these measures are as much an indication of the difficulty of the scenario as they are the performance of the networking technology. This dependence diminishes the utility of test results of this type.

MANET T&E strategies

At this point, four themes have emerged. First, the performance of a tactical wireless network is a function of its use and so should be designed with features that allow users to understand and manage this interaction. Second, a critical capability of tactical networking technology is ad hoc communications among local actors where building these networks is the application. Third, battle command systems will be developed while oblivious to the first two capabilities, but are most likely to dictate the testing objectives for the network. And fourth, if the third story dominates, then the resulting T&E will measure transport capabilities, will likely confound networking technology effects with scenario effects and will learn nothing about the first two capabilities.

Here, a fifth scenario is introduced: An alternative T&E approach is not really known. MANETs are complex systems. Users will react to whatever communications capability they are given. There will be a give and take where maneuver will respond to network performance leading to emergent behavior. Evaluation of these systems will need to assess whether the users are merely reacting to the network performance or understand what causes good performance and, as such, manage their maneuver to balance their communications needs with their mission. Better yet, they can assess whether they can exploit their communications ability to obtain the advantage as envisioned for NCO. The author is unaware of any T&E approach that seeks to understand and evaluate the effectiveness of emergent behavior in MANETs.

The remainder of this section proposes T&E approaches that accomplish two objectives. First, they measure the quality of the MANET technology in terms of capacity and robustness across a continuum of scenarios; and second, they discern whether the technology provides users with the capabilities to build and maintain the social networks necessary for NCO. Determining whether the emergent behavior will cause new and better ways of fighting will be a process of discovery. T&E can assume a new, important role in system development by assisting developers and users in understanding these dependencies.

■ *Simulation techniques*

The most common technique to evaluate MANET technology is simulation. The cost of building a multinode network makes alternatives impractical, especially in development. The disadvantage of simulation is that there is so much dependence on the simulation environment and scenario (as in live exercises), that the results are very difficult to repeat and are suspect (Andel and Yasinsac 2006). Additionally, simulation environments for communications systems do not model emergent behavior. Scenarios are scripted and, at best, have threaded traffic where a thread consists of a series of exchanges, one contingent on the reception of the previous. The author is not aware of any high-resolution communications models that include the emergent behavior that results from communications. Combat simulations that attempt to link user activity to communications do not model networks with sufficient fidelity for this evaluation. Thus, there is no settled approach to evaluate networks using simulation. Simulation tends to be more of an engineering tool that supports the development of the technology. It helps identify shortcomings so that they may be addressed, but it offers little proof of suitability.

Much effort has been directed toward improving simulation. There are two general themes: (1) make network simulations more realistic; and (2) enable simulation environments to handle larger-sized networks. Both address concerns about the fidelity of the results. However, the author subscribes to a contrary view. The larger and more realistic a simulation is made, the more heterogeneous the scenario. It quickly becomes difficult to discern whether technology or scenario effects are the cause of the performance. If there is an indication of poor performance, there is no easy way to determine the reason except to trace through the simulation to find the cause. This can be as difficult as debugging code. These heterogeneous simulations do not lend themselves to developing lessons learned that could help users optimize the performance of their networks. It is believed to be much more useful to use simulation to characterize the performance of a networking technology. Characterizations map network performance to user behavior and use of the network rather than simply test whether the network technology is suitable for some set of test scenarios.

Characterizing the performance of a protocol stack is still a topic of research. It would be done using relatively unrealistic scenarios that are statistically homogeneous. Characteristics of the simulations that are changed from simulation to simulation include the number and density of nodes, their mobility, their load, the average path length of end-to-end traffic and a location-varying pathloss rate. Each scenario, that is, set of characteristics, provides a data point in the characterization.

Some of these characteristics, such as network size and node density, and some intermediate measures such as the average lifetimes of links and paths, become measures of difficulty. The protocol stack would then be characterized across these measures of difficulty, ranging from easy to hard. Measures of performance would evaluate how well access protocols arbitrate access including their "goodput," fairness and service delivery, as well as how well routing protocols track the topology and the quantity of overhead they generate to do so.

Such characterizations of protocol stacks would make it very easy to compare MANET technologies. The factors that influence performance and the sensitivity of performance to scenario will be obvious. These characterizations can be used as guides on how to regulate maneuver to maintain network performance. In turn, they give an indication as to whether the types of NCO envisioned by the military are feasible with the technology.

■ *Capabilities assessment*

The performance of the networking technology over the range of scenario conditions is only half of the evaluation. The second half is an assessment of capabilities. The following questions provide a starting point for evaluating capabilities.

(1) Does the network require a large initialization?

If a large initialization is required and if the details of the initialization are dependent on military organization, then this is an indication that the technology is not very flexible. FBCB2 epitomizes the problem. Initialization of a battalion requires creating a configuration data base, testing that database, configuring each piece of equipment as specified, and then populating the larger centralized Army-wide master database (Shane and Hallenbeck 2005). This is the antithesis of agility. Smaller initializations such as TRANSEC codes, frequency hop sets and IDs are not seen as debilitating. The network technology and the applications should avoid the need to maintain a depository of configuration data and allow the network to discover its configuration, since it is necessarily dynamic.

(2) Can users communicate with their peers and do so easily?

These types of capabilities are articulated in Table 1. In addition to these, the networking technology should still allow eavesdropping on C^2 networks. Further, every node should be able to communicate with every other node as long as they are in range of each other.

(3) Can users select their network participation?

A frequent requirement in dynamic organizations is to change C^2 relationships. Such reorganization involves moving to different C^2 nets, either voice or data. There should be minimal effort to make these changes and, ideally, the users involved should be able to do it on their own in a way that is as simple as changing a channel.

(4) Does the network support a flat architecture?

In a flat architecture, no node is dependent on another to be useful. A contrary example is an access point network. Loss of the access point renders all nodes in the network useless.

(5) Does the technology provide understandable feedback on the network state?

The networking technology should provide users with feedback about their network. A commercial example is the signal strength indicator on cell phones, that is, bars. Users can employ this feedback to move to locations where they can become connected. Similarly, a graphical feedback of the network topology could help users to understand who they can reach and possibly provide feedback on how they might maneuver to close communications with others. Over time, this type of feedback will result in users developing methods to maintain robust connectivity.

(6) Does the networking technology support integration with IP networks?

The MANET itself does not have to have an IP-based solution but should support the use of IP to integrate the MANET with the GIG. The role of IP is to enable interoperability. IP applications should be able to coexist in the MANET. A standardization effort to support this objective that leaves open the design of the MANET technologies is proposed in (Stine 2006). Meanwhile, IP-based MANET solutions do not provide a pass, as they are unlikely to provide the other capabilities listed previously.

■ *Live testing*

Ultimately, the purpose of live testing is to verify that systems provide the advertised capabilities, that these capabilities are accessible by representative users, that they enable these users to do things better, and to allow random and possibly unexpected events to reveal deficiencies of the technology. Simple scenarios can verify most of the aforementioned capabilities. In the case of tactical networking and information technologies, there is risk of collapse where performance declines because of excessive or extreme use.

The conditions that cause it to occur should be revealed in the characterization. Live testing should attempt to reveal the OPTEMPO that creates these conditions. It should also attempt to reveal the vulnerability of the network to loss of components and the operational impact. Finally, a quality that can only be tested live is whether the emergent behavior the technology engenders will debilitate or enhance operational capability. For example, a technology that causes units to remain in tight formations to keep things working would be preferred less than one that allows users to work as a team over large expanses.

Research in delivering capabilities

A dilemma in evaluating transformational technologies that results from pushing the limits of technology is assessing whether a technology that falls short of the vision represents sufficient improvement to warrant fielding. This warning is that if care is not taken, especially with networking technologies, the current trend in acquisition programs will result in the fielding of communications systems that will fall short of the mark but will still be an improvement. If fielded, they will be used for years to come and cause inertia in the effort to achieve the transformation desired because of the cost of their replacement. With time, the problem will only become worse as development of applications to use the network will further entrench the U.S. armed forces in its paradigm. To assist testers and evaluators in facing this dilemma, there are many research programs that are attempting to reinvent wireless networking.

■ *Defense Advanced Research Projects Agency (DARPA) research*

DARPA has multiple projects that address networking. Specifically, the Control-Based MANET program is seeking a network that overcomes the limitations of IP networks and seeks a "tabula rosa" rethinking of MANET technology. The type of ideas they espouse are a single-layer network that optimizes the network across physical, medium-access control and routing functions. The Wireless Network after Next (WNaN) program is attempting to build networks using inexpensive radios that are enhanced by the networking technology.

■ *Advanced Tactical Networking research*

The MITRE Corporation's ATN project is well on its way to delivering all the capabilities described in (Stine and de Veciana 2004). ATN is reinventing MANETs using spatial context. The access protocol arbitrates the use of an RF channel in space, and the routing protocol captures topology by tracking node locations and their observations of their environment. Through this different paradigm, networking capabilities such as spatial reuse, prioritized access, reserved access, preemptive access and multicasting are all possible. Voice, video and data can all be merged. The spatial context of nodes and their connectivity make it easy to provide a graphical display of the network that matches the actual positioning of nodes. Such a display provides the feedback that users need to maintain their network and to identify the individual nodes or groups of nodes they might want to talk to. All destinations can be made accessible through the graphical user interface (GUI) without prior knowledge of the destination's address or the user's identity.

Conclusion

This article has combined multiple stories to describe the network that is needed at the tactical edge to achieve the capabilities necessary for NCO. Unfortunately, these capabilities are not well articulated in requirements for future networks, nor well understood by developers of network-centric systems. It explains that the current trend in network design does not seem to be addressing these capabilities and that evaluators and testers will be put in the difficult position of assessing these technologies when the requirements that are most important are not specified. The purpose of this article is to warn testers and evaluators of this situation, but more important, to provide enough background information so they can try to do something about it. Additionally, the article provides an approach to test and evaluate MANETs that can determine if the technologies will ultimately be able to support NCO. ❑

DR. JOHN A. STINE received a bachelor of science degree in general engineering from the United States Military Academy at West Point, New York, in 1981. He received master of science degrees in manufacturing systems and electrical engineering from The University of Texas at Austin, Texas, in 1990, and later a Ph.D. in electrical engineering, also from The University of Texas at Austin, in 2001. He served in the U.S. Army for 20 years, branched as an engineer officer with a functional specialty of operations research and systems analysis (ORSA). He served as an ORSA in the EXFOR Coordination Cell during the Army's Task Force XXI AWE, where he managed the effort to collect and select the issues and criteria to be evaluated in the experiment. He also was a member of the electrical engineering and computer science faculty at West Point, where he taught courses in communications. He has been with The MITRE Corporation in McLean, Virginia, since 2001, where he conducts research in wireless mobile ad hoc networking (MANET) and consults on projects concerning ad hoc networking, spectrum management, and modeling and simulation of wireless communications networks. Dr. Stine is a member of the IEEE and a registered Professional Engineer in the state of Virginia.

Endnotes

[1] Applique was the first instantiation of Force XXI Battle Command, Brigade-and-Below (FBCB2).

[2] The original tactical Internet combined data into the voice SINCGARS nets, thus fixing them in the architecture and discouraging movement from voice net to voice net, because it would break the data services. The difficulties with contention between voice and data resulted in the isolation of voice networks from data networks in subsequent designs, which solved this problem for voice nets. Because future technologies intend to combine data and voice services, this shortcoming may again need to be resolved.

References

1. Alberts, David S., Garstka, John, Hayes, Richard E. and Signori, David T. 2002. *Understanding Information Age Warfare*. Washington, D.C.: CCRP Publication Series.

2. Andel, T. R. and Yasinsac, A. July 2006. "On the Credibility of MANET Simulations." *IEEE Comp. Magazine*. Pp. 48-54.

3. Barabási, A. L. 2002. *Linked*. Perseus Publishing: Cambridge, Massachusetts.

4. Committee on Network Science for Future Army Applications. National Research Council. 2005. *Network Science*. The National Academies Press: Washington, D.C.

5. Garstka, J., and Alberts, D. 2004. Network Centric Operations Conceptual Framework Version 2.0. Vienna, Virginia: Evidence-Based Research, Incorporated.

6. Joe, L. and Porche III, I. 2004. *Future Army Bandwidth Needs and Capabilities*. Rand Corporation.

7. Sayre, R. G., Fletcher, D., Barbee, S., Kass, R., Lee, M. and Lopez, G. September/October 1998. "Collecting Data for the Army's Task Force XXI Advanced Warfighting Experiment." *The ITEA Journal of Test and Evaluation*.

8. Shane, R. and Hallenbeck, P. 2005. "Managing Data for Interoperability: The Army C4ISR and Simulation Initialization System (ACSIS)." 9th International Command and Control Research and Technology Symposium.

9. Sprinkle, R. B. and Black, C. September 2006. "Joint BC & Simulation Systems Initialization Process." *Proceedings of the Fall Simulation Integration Workshop*.

10. Stine, J. A. and de Veciana, G. September 2004. "A Paradigm for Quality-of-Service in Wireless Ad Hoc Networks Using Synchronous Signaling and Node States." *IEEE J. Selected Areas of Communications.* Vol. 20, No. 7, 1301-1321.

11. Stine, J. A. October 2006. "Cross-Layer Design of MANETs: The Only Option." *Proceedings, IEEE MILCOM.*

12. Weinburger, P., et al. 2006. "Army MANET, JSR-05-135." JASON Group Report. The MITRE Corporation.

Acknowledgments

The author would like to acknowledge the thoughtful reviews and helpful suggestions of Fred Stein and Phillip Hallenbeck of The MITRE Corporation.