

Network Virtualization for Military Application: Review and Initial development of conceptual design

Jiradett Kerdtri*, Komwut Wipusitwarkun**

*Computer and Programming Laboratory, Defense Technology Institute, Thailand

**School of Information, Computer, and Communication Technology (ICT), Sirindhorn International Institute of Technology, Thailand

jiradett.k@dti.or.th, komwut@siit.tu.ac.th

Abstract— Networking Technology, undoubtedly, plays a vital role in modern warfare especially in Network Centric Operations (NCOs) and Global Information Grid (GIG) concept. However, the current popular network infrastructure, mainly TCP/IP architecture, is in fact unsuitable with advanced military communication especially in tactical operation networks. The key characteristics of military communications are classified as delay/disruption/disconnection tolerant networks (DTNs) which are long and variable delays, high error rates and greatly heterogeneous. As a result a call for new type of network architecture emerges to support such peculiar characteristics of military communication network. This paper reviews the current approaches in network technology of military communication and proposes the conceptual design of Virtualization Network (VN) for military communication to address the limitation of current network infrastructure. The implementation of Military Network Virtualization Environment (MVNE) introduces the crucial two new key features of military tactical network: information classification and movable nodes. These features along with essential research challenges must be analyzed to realize a viable virtualization network for military communications.

Keywords— Network Virtualization, GIG, Military, Tactical Network, Communication

I. INTRODUCTION

In the modern Information era, the military operation accomplishment relies heavily on the advantage of information technologies especially on the network technology. Although TCP/IP protocol has played an important role in military communication network for a couple decades, this popular network protocol based on end-to-end path is actually unsuitable for military communication network [1], [2]. The common features of military communication are long/variable delay, high error rates and significantly heterogeneous [3], [4]. As a result, the implementation of TCP/IP network based on the assumptions of low transmits delays, low error rates and existing end-to-

end path undoubtedly contradicts the key characteristics of military communication network. To address mentioned limitations, it is remarkably necessary to design new network architectures along with correlative researches. This paper proposes the use of network virtualization technology on the design of military communication network, which is classified as Disruption Tolerant Network (DTN) [3], [5]. The rest of paper is organized as follows. Section II gives the overview of military communication. Sections III introduces the related researches that consist of GIG, DTN, and Network Virtualization. Section IV illustrates the initial conceptual design for military network. Finally, section V presents the research challenges for designing the system for Military Virtualization Network and conclusion in section VI.

II. MILITARY COMMUNICATIONS

A. Key Characteristics

In general, military communication network is different from civilian communication network in the Concept of Operations (ConOps). In combat environment, the ability to rapidly collect, assimilate, and distribute intelligence across the battlespace has led to a dramatic improvement in the effectiveness of forces and their ability to deploy to counter emerging threats and to deliver precision effects in a timely manner [6]. Consequently in NCW concept, military network technologies must provide key characteristics such as self-organization and decentralization, which speed information flow to increase situational awareness [1]. In battlefield, the primary features of military communication networks are long and variable delays, arbitrarily long periods of link disconnection, high error rates, large bidirectional data-rate asymmetries and heterogeneous connections because of the nature environment of battlefield [3]. Most of military applications have to deal with unstable links with limited bandwidth and variable latency [2], [7]. For example, the use of satellite as a mean of communication in rural area is significantly slow and unstable which significantly decreases the efficiency of operations [8] - [10]. All in all, to maintain the information dominance the key characteristics of military

communication network are focused on long/variable delay and disruptive connection, high error rates and heterogeneous environment

B. Difference in Network ConOps

Principally, military networks are built from ad hoc wireless connections between mobile nodes [11], which are highly dynamic network environment. Compare with citizen communication network [12], the military communication network hold following differences [3]:

1) **Heterogeneous nodes**: In the network centric environment, various types of communication transmissions occur between diverse nodes such as command and control centers, sensors, radar or communication relays. Therefore, the military communication nodes comprise of numerous devices, which are function differently in combat network system.

2) **Multi-links**: The links between nodes in military communication compose of different medium such as radio, satellite, cable, etc. Depend on the mission requirement military networks usually consist of a variety of multi-links. Thus, links and nodes in military network are materially heterogeneous.

3) **Time-varying topology**: Normally in military operation, communication nodes move relentlessly causing the network topology structure to change dynamically. This provides unstable links to the battlefield network, causing the latency and disruptive service [4].

C. Military Multilevel Security

Multilevel security (MLS) is the ability to distinguish subjects according to classification levels to determine the degree to which they can access confidential objects [13]. MLS was developed by the US military in the 1970's to allow users to share some information with certain classes of user by labelling data with classification and assigning fixed clearances to users [14]. The term classification and clearance in the context of military system refers to the security levels Top Secret (TS), Secret (S), Confidential (C), Restricted (R) and Unclassified (U) according to British definitions [15]. In military communication network it is necessary to accommodate the different classification level to transmitted data as well as different clearance levels to users. Therefore, the ideal military network must handle diverse class of data differently such as broadcasting unclassified data while multicasting confidential or restricted data.

D. Current Network Limitation

In 1982, the U.S. Department of Defence declared TCP/IP to be the standard communication s protocol for all military computer networking and the general trend across NATO communications systems is to move away from TDM-based systems to everything over IP approach [6]. However, current communication network is a generation old and no longer effective in meeting the emerging requirement imposed by the next-generation military applications [3]. There has been a great deal of correlative research designed to meet peculiar characteristics of military communication such as Mobile Ad

hoc Networks (MANET) or DTN [2], [8], [16], [17]. Military forces around the globe have applied one or the other networking paradigm with varying degrees of success to their own problems of mobility at lower tactical level [4]. The obvious problem is the limitation of traditional transport network protocol which based on certain assumptions and application scene, such as, low transmit delays, low error rates and existing end-to-end paths [3]. In MANET the nodes locations are arbitrary, and the network topology is dynamic. In MANET protocol, all nodes are synchronously connected and depend on existing end-to-end path between the sender and receiver before any communications can occur. On the other hand, DTN do not make any assumption about end-to-end path; instead DTN assumes the nodes will be eventually connected. As a result, DTN is suitable only for non-real time, messages or bundle based communication [4]. However, those types of network do not cover the necessity characteristics of military network especially multilevel classification information.

III. RELATED WORK

A. Global Information Grid

The Global Information Grid (GIG) is defined as a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy maker, and support personnel [18]. The underlying backbone of the GIG infrastructure is the convergence over Internet Protocol (IP). Recently, U.S. DoD has specified the use of the IP as the standard data interchange format for network implementation, requiring that any applications or sensors that interface with the network or transmit over the network do so via an IP format [6]. Overall, GIG represents the integration of network-aware applications and systems that can exploit the information available to and from each node through adapting to the dynamically changing communications environment in which they are expected to operate. The GIG integrates and exchanges intelligence feeds from across the U.S military community (US Army's LandWarNet [19], US Air Force's C2C ConstellationNet [20] and US Navy/Marine Corps FORCENet [21]), DoD networks, and non-military sources

B. Delay/Disruptive Tolerant Network

The common definition of Delay and disruptive Tolerant Network (DTN) is no guarantee of a contemporaneous end-to-end path from source to destination [22]. DTN is a class of network architecture intend for network which connection is periodic, intermittent, and/or prone to disruption. The "store-carry-forward" scene is used in DTN to address the TCP limitation [3]. This type of transmission is similar to postal office system in which the data is transmitted hop-by-hop until reaching the final destination. Moreover, the intermediate nodes will always store data regardless of whether the link is connected before sending the data. Consequently, this will significantly improve the data transmission reliability. The

main goal of DTN is for deep space communications, which successfully implemented and tested recently [23]. Recently, several researches proposed DTN as a viable solution to optimize the military communication network, concerned with networks that experience long transmission delay or periods of disruption [3], [4]. However, DTN is asynchronous in operation and are suitable only for non- real time, message or bundle based communications [4]. In addition, military communications require a network that dynamically adapts to a variety of mobility situation as well as the ability to prioritize them to the correspondent sensitivity level of military security. Finally, security must be embedded into the core infrastructure of military network.

C. Network Virtualization

Since the key characteristics of military communication network are different from civilian communication network, these distinctive features of tactical networks call for Network Virtualization approaches to realize complex, adaptive, and fault-tolerant applications to be deployed in the battlefield. A concept of Network Virtualization (NV) has been promoted in recent years as a new infrastructure to overcome the limitation of existing Internet, which consists of conflicting goal and policies among stakeholders [5], [24], [25]. Network Virtualization is the process of integrating hardware and software network resources and functionality into a single, software-based administrative entity. By allowing multiple heterogeneous network architectures (service provider) to cohabit on a shared physical substrate (infrastructure provider), network virtualization provides disruptive technology, which can aid designing diversity complex network architecture [26]. As a result, NV is an ideal infrastructure for designing such network architecture for military communications. The idea of multiple coexisting logical networks can be categorized into four main classes: VLANs, VPNs, Active and Programmable Networks, and Overlay Networks [26].

IV. DESIGN

A. Design Goal

The overall goal of the design is to address the distinctive characteristics of military network with VN capability. With the advance in computing technology currently, it is possible to implement desired complex network functionality in heterogeneous virtual networks on a shared physical infrastructure. In order to materialize this proposed virtualization network environment, each of these design goals must be fulfilled: security embedded, disruptive and disconnected services tolerant, ease of use, heterogeneous structures interoperability and dynamic network environment adaptive.

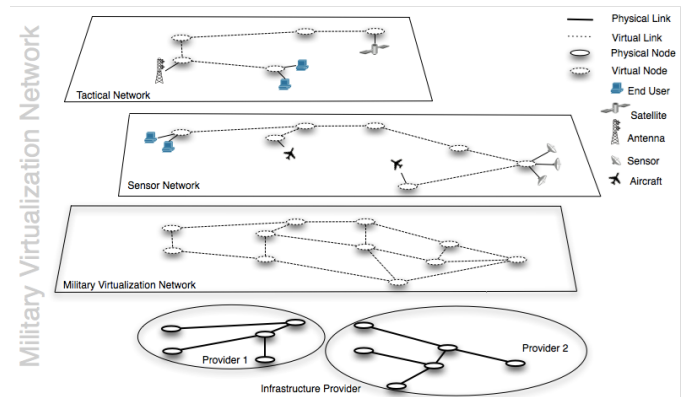


Figure 1. Military Virtualization Network Environment

A Virtual Network is a group of virtual nodes connected together by a set of virtual links to form a virtual network topology [26]. The underlying physical topology from infrastructure provider distributes the necessary resources to logical network. Physical nodes host virtual nodes while physical links provide network infrastructures and resources for virtual links. Figure 1 illustrates the basic entity of Network Virtualization Environment (NVE) to form a model of Military Virtualization Network Environment (MVNE) for military applications utilizing the network resources from infrastructure provider. A similarity of concepts in MVNE and GIG is their role to create an environment in which uses can access data on demand at any location by plug-and-play network [6].

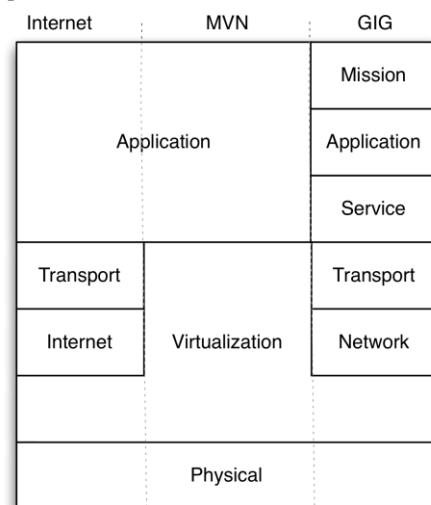


Figure 2. Comparing of Internet, MVN and GIG protocol stack

The Internet Protocol is the principle communication protocol and most widely used for today network. The GIG relies on the common IP network but adds the mission layer and service layer next to the application layer. On the top, a mission layer provides the specific aggregation of applications from the application layer necessary to perform a particular military mission. Below application layer, a service layer acts as an interface between different applications ensuring data in a correct format is presented participating applications [18]. In

Figure 2 the virtualization layer acts as a data link layer in GIG and Internet protocol stack to manage the two-way communications protocols among users. This approach aims to deliver a universal network that comprises all communications and computing systems and services, applications, data, security services and other associated services necessary to achieve information superiority during peace. On the other hand, during war or tactical operation, virtualization layer in MVN acts as an interface between application and physical layer to address the limitation of TCP in battlefield environment.

B. Initial Conceptual Design

The goal of MVN is to address the limitation required for military communication in addition of increasing the efficiency of operation. The concept of operation for military network (NetOps) normally divides into board two parts under conventional warfare. The military operations during peace is the normal mission that military supports the other parts in the nation and international such as domestic disaster relief, humanitarian assistance, counter terrorism etc. Thus, the Global Information Grid (GIG) concept of globally information sharing is utilized [27]. The NetOps of GIG is to understanding the environment and delivering trustworthy service to all users, anytime and anyplace [28]. The Internet and several means of communications are used to form a gigantic overlay network. The military operation during war is the battle environment such as global conventional war and regional conventional war. As a result, the military network under this circumstance must survive the peculiar characteristics of dynamic topology and disruptive. The conceptual design aims to support the operations of these two parts. During peace, packets from application layer in the Internet protocol or service layer in GIG protocol are transmitted to physical layer through traditional transport layer, network layer (TCP/IP basically) and virtualization layer. In GIG, the virtualization layer provides functional point-to-point data transfer between two or more logical connected devices, enabling reliable data delivery between heterogeneous nodes via virtual links. In addition, virtualization layer is integrated in to the stack to append more functionality to the data transmission. This will guarantee the interoperability among heterogeneous military devices as well as information sharing. On the other hand, the communication stack utilizes virtualization layer from the top application layer to address the limitation of legacy transport protocol during the war. The data from application layer transfers to virtualization layer directly to encapsulate with programmable header which making executable packet

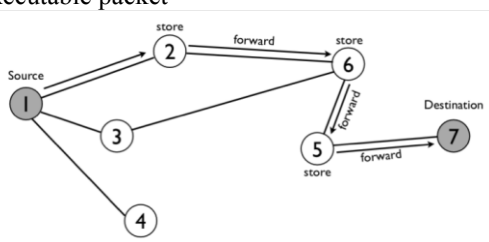


Figure 3. Virtual Network Transmission

From figure 3, each virtual node is assigned with unique number. The intermediate nodes cache the data sending to them and wait for the available node to transmit. The virtual node incorporates the ability of packet execution to make routing decision. The delivery semantics may be multicast; unicast or anycast depends on the level of information security [29]. This scenario works the same way as a car with GPS that can go to any destination via any road available comparing with legacy transport protocol as a train which require a railway so the train can go to the destination.

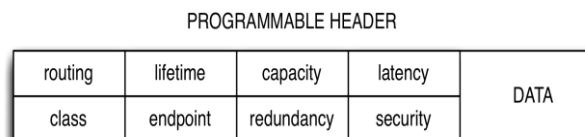


Figure 4. Packet in MVN

Since the military communication network is classified as a class of DTN, the network transmission protocol must be adapted to fit the key characteristics. The size of transmission data packets in military communication is relatively compact such as geo-location, message or image. As a result, such packets can be redesigned to incorporate more capability by increasing the overhead size. As of figure 4, a packet overhead is embedded with a programmable header, which can be executed at each virtual node that this intelligence packet visits on the network. In fact, a concept of these intelligence/smart packets was proposed in several active/programmable network researches area for a couple decades [30], [16]. However, most techniques are still based on the use of TCP and Ethernet encapsulation, which greatly limit the functionality of programmable header. With emerging in NVE, the virtual node and link is basically a logical software based infrastructure that can be simply customized to fit any complex requirements. A code inside packet is a program that can be executed at nodes on the path to destination. By combining DTN concept [16] with NVE infrastructure, the packet can determine the following function at virtual node:

1) Routing: The routing capability in military communication is crucial especially when the mobility, environmental factors, or jamming causing the disconnection. Each packet must find the best available path to the destination.

2) Lifetime: The time on packets and nodes must be in synchronizing. The data expiration is supported by timestamp and instruction program. Each node can determine packet expiration based on the class of data content. For example, the longevity of data with top-secret class is shorter than unclassified class for security purpose.

3) Capacity: DTN architecture does not expect links to always available or reliable thus node must incorporate ability to store data until the links become available. A program inside each packet must control the storage required to execute and cache data when dealing with different capacity on heterogeneous nodes.

4) Latency: Because of the characteristics of military operation, dealing with high propagation delay is the main goal of new network design. Especially in battlefield, the delay may be caused by plan or unplanned. Thus this program must handle the delay based on the situation and data class.

5) Level of information class: This function offers the same service as priority classes in DTN architecture. The code offers degree of information sensitivity measurement for the data, which can be classified by the level of military security (Top Secret, Secret, Restrict, Classified and Unclassified). Consequently, these priorities affect the delivery urgency and assurance.

6) Endpoint: Each node is assigned by unique number to make a distinction among nodes. This is a similar concept of Endpoint Identifiers (EIDs) in DTN [16]. By knowing the unique number of Endpoint, the program can select the proper path to the destination.

7) Redundancy: The path failure is the main problem in DTN routing. Other causes of data loss in DTNs include link transmission errors, message drops due to insufficient buffer space, or failure of a node along the path. Early research on DTN routing has mainly focused on utilizing precisely known network dynamics, which does not account for message losses due to link failures, buffer overruns, path selection errors, unscheduled delays, etc.[10]. Therefore, in this scene the proper data replication system is necessary to cope with the data loss problem.

8) Security: In military tactical networking, security and privacy is the most crucial factor in every aspect of operations. Therefore, the code program must ensure the confidentiality, integrity and availability of data on the network.

The virtual node and packet is customizable software that can program to suit the requirement of the situation. As a consequence, the situation aware NVE is the best fit for the uncontrollable and unpredictable scenario such as battlefield.

V. RESEARCH CHALLENGES

A. Opportunistic Routing

The peculiar characteristics of military communication network are the main focuses on the design of MVNE. There are several concerned issues for the implementation in this network especially in routing. In fact, routing is clearly the most difficult issue to deal with. A distinctive characteristic of MVNE is a lack of consistent end- to-end paths due to interruptions that may be either planned or unplanned. The most research challenge in this type of networks is selecting routing paths [10]. The approach of using opportunistic routing technique based on data context to improve the route selection is one of great interesting idea. In opportunistic network, virtual nodes are enabled to communicate with each other even if an existing path never exists [31].

B. Network Formation

Because of the heterogeneous environment and greatly dynamic topology, the military network formation is one of the difficult research challenges. In the battlefield, various

tools are used for networking and communication such as sensors, radio, portable computing devices, etc. In addition, the scenario constantly alters to the current situation. Therefore, the network formation that can adapt to the current situation and topology requires to be designed.

C. Multilevel Security

This degree of information sensitivity of delivery service is extremely significant in military communications and operations. Most military services have been deployed concept of MLS. However, the major problem with MLS system is that the limited demand for them does not compensate for high costs of developments and certification. Rydal Research and Development [32] proposed the use of virtualization to manage multiple level of military security by placing security labels in network packet headers and specialized processing structures built into switches. Thus virtualization network is one promising research in the area of MLS.

D. Security

Security, unquestionably, is the most important function in military communication. Take DTN for an example; according to its features such as multi-hop transmission or frequently interruption, it faces several security concerns, for instance denial of service attack, information fragmentation and private information issue. The traditional encryption mechanism based pseudonyms or layered encryption does not apply to this on-demand routing [3]. Therefore, the security can be simply implemented in logical nodes and programmable packets to address the security issue in DTN.

E. Application Timeout

The communication in this disruptive/delay environment consists of several issues to address especially in application timeout. The delay in military communication network may greatly vary, sometimes disconnected. The nodes may have to store packet with a long period of time until the nodes eventually connected again. As a result, the appropriate timeout must be analyzed in detail. The timeout for highly classified data and unclassified data should be different. The longer the node caches sensitive data, the more chance it will leak. In addition, most current applications do not handle a very long time out since the design of those applications does not cope with much latency.

VI. CONCLUSION AND FUTURE WORK

The key characteristics of military communications—unstable links, variable latency and greatly heterogeneous—make it distinctive among other types of networking. These characteristics make virtualization network architectures a better fit for tactical networks than traditional TCP designs. By combining the concept of DTN with network virtualization architecture, the Military Network Virtualization Environment (MVNE) is propose in this paper. Several research challenges are suggest as a realization of a practical implementation toward the network centric operation. MVNE can substantially benefit military tactical network with a focus on

security and data delivery. The concept of VN is relatively new. However, with the advance in networking technology, it is possible for a realization of MVNE. In future work, the initial of MVN conceptual design will be simulated and analysed focusing on the routing and MLS.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contribution of Sirindhorn International Institute of Technology and Defense Technology Institute.

REFERENCES

- [1] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications*, 2003.
- [2] M.-J. Sheng, K. I. Park, R. Manfreedy, and T. Mak, "Analysis of ECN on TCP Performance Enhancing Proxy performance for satellite networks," in *Military Communications Conference*, 2008. MILCOM 2008. IEEE, 2008, pp. 1–7.
- [3] Z. Lu and J. Fan, "Delay/Disruption Tolerant Network and its application in military communications," in *Computer Design and Applications (ICDDA)*, 2010 International Conference on, 2010, vol. 5.
- [4] P. Holliday, "NOMAD A Mobile Ad Hoc and Disruption Tolerant Routing Protocol for Tactical Military Networks," *Distributed Computing Systems Workshops*, 2009. ICDCS Workshops '09. 29th IEEE International Conference on.
- [5] S. Farrell, "Security in the Wild," *Internet Computing*, IEEE, vol. 15, no. 3, pp. 86–91, 2011.
- [6] R. S. Deakin, *Battlespace Technologies: Network-Enabled Information Dominance*. Artech House, 2010.
- [7] K. Lund, E. Skjervold, F. T. Johnsen, T. Hafsoe, and A. Eggen, "Robust web services in heterogeneous military networks," *Communications Magazine*, IEEE, vol. 48, no. 10, pp. 78–83, 2010.
- [8] M. Allman, C. Hayes, and H. Kruse, "TCP performance over satellite links," in *Proceedings of the 5th ...*, 1997.
- [9] Y. Chotikapong, H. Cruickshank, and Z. Sun, "Evaluation of TCP and Internet traffic via low Earth orbit satellites," *Personal Communications*, IEEE, vol. 8, no. 3, pp. 28–34, 2001.
- [10] S. Jain, M. Demmer, and R. Patra, "Using redundancy to cope with failures in a delay tolerant network," *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, vol. 35, no. 4, 2005.
- [11] P. Holliday, "SWARMM - a mobility modelling tool for tactical military networks," in *Military Communications Conference*, 2008. MILCOM 2008. IEEE, 2008, pp. 1–7.
- [12] L. Kant et al., "Network science based approaches to design and analyze MANETs for military applications," *Communications Magazine*, IEEE, vol. 46, no. 11, pp. 55–61, 2008.
- [13] M. Choudhary and P. Sharma, "Secure multicast model for ad-hoc military networks," *Networks*, 2004.
- [14] R. Ramachandran and D. Pearce, "AspectJ for multilevel security," Bonn, 2006.
- [15] P. Ushman, *Marking Classified National Security Information*. Washington, DC: The Information Security Oversight Office, 2011, pp. 1–46.
- [16] D. Tennenhouse and J. Smith, "A survey of active network research," *Communications Magazine*, IEEE, vol. 35, pp. 80–86, 1997.
- [17] N. Suri et al., "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *Communications Magazine*, IEEE, vol. 48, no. 10, pp. 60–69, 2010.
- [18] M. U. Charlie I Cruz, *NETWARS BASED STUDY OF A JOINT STARS LINK-16 NETWORK*, AIR FORCE INSTITUTE OF TECHNOLOGY, 2004.
- [19] U. S. A. C. I. O. G.-6. A. A. I. Center, "Army Enterprise Architecture Network," *architecture.army.mil*. [Online]. Available: <http://architecture.army.mil/technical-view.html>. [Accessed: 29-Nov.-2011].
- [20] C. N. Sweet and S. Kanefsky, "The C2 Constellation A US Air Force Network Centric Warfare Program" in *2004 Command and Control Research and Technology Symposium*, 2004, pp. 1–31.
- [21] FORCENet A Functional Concept for the 21st Century. US Navy.
- [22] B. Walker et al., "The state of DTN evaluation," *CHANTS '10: Proceedings of the 5th ACM workshop on Challenged networks*, 2010.
- [23] A. Jenkins, S. Kuzminsky, K. K. Gifford, R. L. Pitts, and K. Nichols, "Delay/Disruption-Tolerant Networking: Flight test results from the international space station," in *Aerospace Conference*, 2010 IEEE, 2010, pp. 1–8.
- [24] K. Oberle, M. Kessler, M. Stein, T. Voith, D. Lamp, and S. Berger, "Network virtualization: The missing piece," in *Intelligence in Next Generation Networks*, 2009. ICIN 2009. 13th International Conference on, 2009, pp. 1–6.
- [25] G. Schaffrath, C. Werle, and P. Papadimitriou, "Network virtualization architecture: Proposal and initial prototype," in *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, 2009.
- [26] N. Chowdhury, "A survey of network virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, Apr. 2010.
- [27] A. Thomas, T. Turner, and S. Soderlund, "Net-Centric Adapter for Legacy Systems," *IEEE Systems Journal*, vol. 3, no. 3, pp. 336–342.
- [28] "The Global Information Grid: Enabling the Transformation to Net-Centric Operations," *dtic.mil*, 24-Mar.-2005. [Online]. Available: <http://www.dtic.mil/ndia/2005netcentric/monday/guthrie.pdf>. [Accessed: 26-Aug.-2011].
- [29] S. Nelson and R. Kravets, "Achieving anycast in DTNs by enhancing existing unicast protocols," *CHANTS '10: Proceedings of the 5th ACM workshop on Challenged networks*, 2010.
- [30] N. M. M. K. Chowdhury and R. Boutaba, "Network virtualization: state of the art and research challenges," *Communications Magazine*, IEEE, vol. 47, no. 7, pp. 20–26, 2009.
- [31] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *Communications Magazine*, IEEE, vol. 44, no. 11, pp. 134–141, 2006.
- [32] D. L. Hecht and W. A. Rosen, "Military Embedded Systems," *mil-embedded.com*. [Online]. Available: <http://www.mil-embedded.com/pdfs/Rydal.July07.pdf>. [Accessed: 26-Nov.-2011].