Considerations on the Adoption of Named Data Networking (NDN) in Tactical Environments

Lorenzo Campioni*§, Mariann Hauge†. Lars Landmark†, Niranjan Suri‡§, Mauro Tortonesi*
*University of Ferrara, Ferrara, Italy
lorenzo.campioni@unife.it, mauro.tortonesi@unife.it
†Norwegian Defence Research Establishment (FFI), Kjeller, Norway
mariann.hauge@ffi.no, lars.landmark@ffi.no
‡US Army Research Laboratory, Adelphi, MD USA
niranjan.suri.civ@mail.mil
§Florida Institute for Human & Machine Cognition, Pensacola, FL USA
lcampioni@ihmc.us, nsuri@ihmc.us

***Abstract*—Mobile military networks are uniquely challenging to build and maintain, because of their wireless nature and the unfriendliness of the environment, resulting in unreliable and capacity limited performance. Currently, most tactical networks implement TCP/IP, which was designed for fairly stable, infrastructure-based environments, and requires sophisticated and often application-specific extensions to address the challenges of the communication scenario. Information Centric Networking (ICN) is a clean slate networking approach that does not depend on stable connections to retrieve information and naturally provides support for node mobility and delay/disruption tolerant communications – as a result it is particularly interesting for tactical applications. However, despite ICN seems to offer some structural benefits for tactical environments over TCP/IP, a number of challenges including naming, security, performance tuning, etc., still need to be addressed for practical adoption. This document, prepared within NATO IST-161 RTG, evaluates the effectiveness of Named Data Networking (NDN), the de facto standard implementation of ICN, in the context of tactical edge networks and its potential for adoption.**

***Index Terms*—Information-Centric Networking (ICN), Named Data Networking (NDN), tactical networks.**

I. Introduction

Mobile military networks represent a unique subset of networks that are challenging to build and maintain. The wireless nature of these networks, and the fact that they have to operate in an unfriendly environment, results in unreliable and capacity limited performance. At the same time, we foresee a future where there is a need for more network capacity at the tactical edge and where the tactical networks often will be a complex heterogeneous network environment that exhibits frequent topology changes. Some drivers for the capacity requirements are 1) the increasing insertion of networked sensors and IoT technology (e.g., the Internet of Battlefield Things (IoBT) program [1]), 2) the increasing number of deployed autonomous nodes and swarms, 3) the adoption of new communication patterns where available information might be attractive for more receivers in an ad-hoc manner and 4) the adoption of Joint Intelligence, Surveillance and Reconnaissance (JIRS) as well as joint firing and targeting. The complex and heterogeneous nature of the tactical environment is a consequence of 1) high electronic warfare (EW) threat; 2) requirement for communications to operate on mobile nodes at increasingly longer distances and 3) the need for more data capacity. In order to achieve and maintain information superiority, it is necessary to find and deliver the most valuable information to the right recipients(s) as fast as possible [2]. This will require improved support from the tactical network and the information infrastructure.

Currently, most tactical networks use IP-based network architectures, which were designed for fairly stable, infrastructure-based networks. Since its inception, numerous patchwork modifications have been introduced to support previously not envisioned scenarios, such as mobile ad-hoc networks (MANET) to build infrastructure-less mobile networks, disruption/delay tolerant networking (DTN) [3] for very unstable networks, simultaneous transmission to a group of destinations (multicast), reliable or unreliable transport protocols, a range of information dissemination protocols (e.g., Data Distribution Service (DDS) [4]), Content Delivery Networks (CDN) [5], and Mobile IP [6] and NEMO [7] to handle node and network mobility. The result is a hodgepodge of protocols that must be in place and configured correctly in order for the network to function. Network management and control of this environment is costly and error prone. Several of these protocols also have high overhead and generate more load than can be supported by tactical military networks.

There has been much research on MANET and other wireless networks during the last three decades and many proposals, protocols, and products have been introduced that solve different aspects of the range of challenges and requirements [8] [9] [10]. One of the major problems with many of these extensions to IP and IP-based solutions is that they are not general and that different needs result in different protocols that do not generalize well [11].

Information Centric Networking (ICN) represents a clean slate approach that does not depend on stable network connections to retrieve information and provides the tools to tailor the robustness of the information collection through different

mechanisms for signaling redundancy and intermediate data storage (caching). ICN also seamlessly handles the change in traffic patterns for data meant for a single receiver and data meant for a group. This is also the case for the change in traffic patterns from fairly stable network to a network that experiences intermittent connectivity.

Advantages of such an approach are a robust network architecture, a simple interface between the applications and the supporting network infrastructure, as well as simpler network management and control. The whole purpose of ICN is to make it easier to find relevant information in the network in a scalable manner. All of these benefits are also valuable for military operations. These characteristics demand a closer examination of ICN to determine whether this technology is interesting and relevant as a candidate architecture for future heterogeneous military networks.

Several ICN proposals exist with varying degrees of maturity. For the purposes of this paper, we have chosen the Named Data Networking (NDN) [12] architecture given its relative popularity and maturity. NDN is built on the Content Centric Networking (CCN) proposal in [13]. Also, NDN solutions have started attracting considerable attention from the perspective of military applications [14].

While NDN seems to offer some structural benefits for tactical environments, a number of challenges have already been identified such as information security, information naming, QoS, cache management, and coordination among nodes. Some of these challenges are fundamental to the adoption of NDN, with the result that several solutions have already been studied and addressed through different approaches. One of the objectives for the authors is to evaluate the effectiveness of NDN and these enhancements in the context of tactical edge networks. A second objective is to address the question of whether NDN, as an abstraction, simply ”shifts” the problems experienced by IP networks to different areas (i.e., does it solve some problems while creating others).

II. Related Work

There are several surveys that compare different ICN solutions such as [15], [16]. Of these, [15] is a particularly well written and comprehensive, but optimistic, survey whereas [16] represents a more critical view. Most of the ICN surveys focus on applications in high-capacity fixed Internet infrastructure, which does not align well with military tactical networks. But, [17] provides a survey of ICN-related works for wireless and mobile networks, highlighting the characteristics for these networks. There is also a handful of papers that have started to look into the use of ICN in mobile military environments [18]–[22]. All of these papers use the NDN architecture when they discuss ICN.

One of the first papers that suggests the use of NDN is mobile military networks is [18]. The paper lists opportunities but not challenges and thus does not go into technical detail and is not critical. A follow up paper [19] studies the use of NDN in two network scenarios using Emulab [23]. The reported results are encouraging; however the experiments are designed to show the benefits and do not highlight potential problems.

In [20] the authors claim that some modifications of NDN are needed to better exploit NDN’s potential. NDN is a pull-based architecture where the consumer always asks for information. Here the authors extend the architecture to also support push-based traffic. They propose to divide the content into topic based content (e.g., data files, video and audio files, etc) and spatial/temporal content (e.g., situation awareness data and sensors information) and they introduce an extra *Replay - Request* handshaking to select the data path. A simple experiment is conducted where NDN is compared with a solution for IP routing and a file sharing overlay.

NDN is compared with IP unicast (using OLSR [24]) and IP multicast (using SMF [25]) in DIL (disruptive, intermittent connectivity, and low bandwidth) environments in [21]. A very disruptive ship to shore network is built using CORE (Common Open Research Emulator) [26]. It shows how NDN outperforms IP for this scenario and how NDN can mix the unicast and multicast data dissemination models to achieve localized robustness to disruption. The paper does not discuss challenges with the NDN architecture.

In [27] the authors suggest using NDN for tactical networks in Gray Zone[1] conflicts. Two scenarios are evaluated using the mininet [28] environment. These experiments also show that NDN outperforms the other solutions as the loss-rate of the connections increases. However, as expected, the push-based IP-multicast architecture exhibits lower delays than the pull-based NDN architecture. The same testbed is reused in [29] for a similar experiment. In this paper, the authors discuss some of the advantages and disadvantages with the NDN security model. They highlight the need to encrypt the Interest messages for privacy and discuss the negative tradeoff that results with being unable to efficiently use caches.

The potential of NDN is discussed in [30] in the context of a scenario that describes a wide-area surveillance system that delivers imagery of sites of interest around a fixed location. The sensors and communication assets are owned by different coalition partners. This paper also lists some challenges that need more research; namely naming conventions, name confidentiality and policy management for NDN strategies, flow control, and access control.

NDN’s potential impact on tactical application development is discussed in [22]. The authors views are that the following characteristics of the NDN architecture can help ensure more robust mobile military networking: Host-independent behavior, multicast communication, pervasive network-accessible storage, opportunistic communication, namespace synchronization as transport, and data-centric security.

NDN properties can effectively be exploited to enable and

[1]“Gray Zone conflicts happens somewhere in the ”Gray Zone” of the continuum between strict diplomacy at the lowest intensity of the spectrum and open warfare at the highest intensity. Often there is ambiguity on the exact nature, specific parties, and ultimate goals of the conflict, but a critical aspect of Gray Zone operations is sharing of information in order to modify the perceptions and beliefs of the involved parties” [27].

improve Wireless Sensor Networks (WSN). An interesting solution is proposed in [31], which exploits NDN caching and Interest data aggregation to create a mechanism that provides dataset synchronization. This allows to increase the data availability for environments with intermittent connectivity, including ad-hoc networking or delay/disruption tolerant scenarios.

III. NDN

In the classic Internet protocol stack, IP represents the "glue" in the network. IP is host centric, which means that IP addresses are used to locate the requested information. Information is therefore bound to the one unique IP address of the server where it is produced or stored.

NDN is a clean slate architecture that does away with the host centric architecture of the classical Internet [32]. In NDN the focus is on finding the information (content) that a client wants to retrieve irrespective of where it is stored. This is done by addressing the information by name rather than by its source (host name or IP address).

In NDN, the content naming scheme is a fundamentally important and application specific design choice. This means that the first step in NDN application development is defining a naming scheme that fits the content characteristics and the application's particular needs. For instance, in a tactical application, the content name can be built hierarchically and be human readable. An example would be:

```
[Mission_network_xx/Intelligence_reports/
Geographic_area_x,y/role_xx/today]
[Mission_network_xx/weather_sensor/
Geographic_area_x,y/windspeed/current]
```

While this forces software engineers to address information production and consumption related aspects early on in the development process, it also affords considerable liberty to explore a wide range of naming schemes, from simple hierarchical to tag- and/or keyword-based ones [33], to find the best suited one for the particular application. Of course, the names must be commonly agreed upon by all the consumers and producers in the information domain where they operate (e.g. mission network, national network, etc.).

NDN is built on two simple basic primitives; request for a specific content and the response with the matching data. In NDN the two packets that perform these primitives are called *Interest* and *Data*. In order for any content to flow in the network, the consumer must issue an *Interest* that specifies the name of the content that the consumer in looking for.

When the consumer has issued the Interest for the required content, the Interest is forwarded through the network in search for a node that holds the content. When the content is found, it is wrapped in a Data packet, which follows the reverse path of the Interest packet back to the consumer.

The Interest and Data management primitives are implemented in a forwarding engine that is installed in all network nodes (routers, clients and servers) in the NDN architecture, as shown in Fig. 1. In NDN, an interface over which content is transmitted or received is called a Face, which can be an internal interface towards higher layers (the application), a network interface, or other types of connections, like a TCP connection in case of hybrid NDN/IP solutions.

When an Interest is generated by the application, it reaches the forwarding engine of the node over an internal interface (Face 2 in Fig. 1). First, the forwarding engine checks if the requested content is available in the Content Store, an internal cache that stores copies of the recent Data packets received or forwarded. If the content is not available in the Content Store, the forwarding engine registers the Interest, as well as the originating Face, in an internal table called Pending Interest Table (PIT). If the Interest was already registered in the PIT, the engine simply adds the new Face in order to forward back the Data message to all interested consumers.

In case the Interest is not already in the PIT, the forwarding engine checks its Forwarding Information Base (FIB) to see which Faces to forward the Interest on in order to start looking for the content in the network. The FIB is similar to the routing table in IP architectures. The Interest is forwarded on one or several of the Face(s) that the FIB points at. This procedure is repeated in all forwarding nodes until the Interest arrives at a node where the FIB points at the Face to the application that produces the information or there is a match in the Content Store.

When a node is able to fulfill the request, meaning it either has content in its Content Store or is the node that produced the information, it resolves the Interest by sending back a Data packet. During this phase there is no need of FIB since the Data packet simply follows the bread crumb trail from the path taken by the Interest. In fact, each node in the path has stored the Face(s) that received the Interest so once they receive the Data packet they update the PIT, and since the Interest is resolved, they cache the content (to increase data availability and performance when the same content is requested in the future), and forward back the message through the Face(s) that received the Interest packet. This simple procedure is repeated for all content the consumer wants.

Forwarding in NDN is stateful, which enables NDN to perform much more intelligent forwarding decisions than IP (which is stateless). This functionality, managed by the Strategy layer, can be used to enable access control (only allow Data with certain names to be forwarded), intelligent caching (cache and forward data based on its priority, which can be name-driven), as well as robustness to disruption (cache data based on known delay/disruption on the incoming link).

IV. Advantages in Military Tactical Networks

With the basic principles of NDN established, this section discusses some aspects of NDN that makes the architecture appealing for heterogeneous military networks, particularly with mobile nodes.

A. Disruption Tolerance

Several solutions, adopting both COTS and purposely developed approaches [9], have been proposed to address disrupted

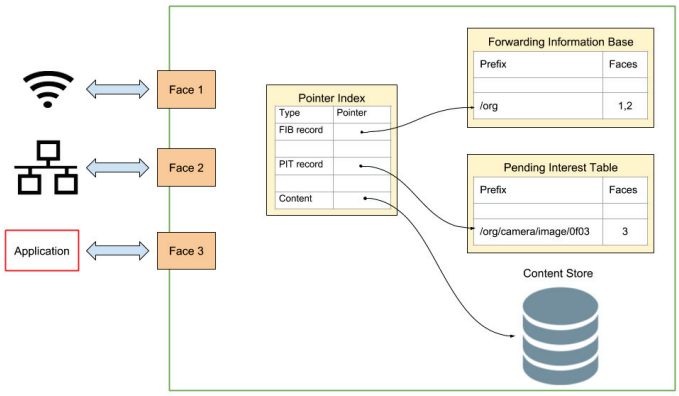

Fig. 1. Overview of the forwarding engine in a NDN node.

communications in tactical networks. Unlike native IP, the store and forward functionality of NDN enables it to withstand disruptions without the need for any specific extensions.

In fact, NDN adopts a communication model that decouples information producers and consumers and is not dependent on a stable connection between them. If at some point in time an Interest message can get to the producer or a Content Store that holds the content, the responding Data packet can start its way back to the consumer and will be stored at each hop. If the Data message is lost due to broken links, the consumer can simply reissue the Interest after a timeout.

This approach provides a simple mechanism for communication reliability. In fact, after the first Interest, each successive Interest sent has a higher likelihood of succeeding since the content is now likely stored in a Content Store closer to the consumer.

B. Node Mobility

Node mobility is a significant challenge for IP due to the dual nature of IP addressed being identifiers and locators. Supporting mobility requires purposefully developed solutions to enable connections to withstand node mobility [8] or to support multipath communications [34]. Instead, NDN copes significantly better with mobility.

Node mobility can be split in consumer mobility and producer mobility. Consumer mobility is handled automatically by NDN. A consumer that has moved simply asks for new content in the standard way by issuing an Interest. The Interest builds a path from the new position of the consumer to the first node that holds a copy of the content and the Data packet follows the reverse path back to the new node position. If a node moves after it has issued an Interest and before it has received Data, then the application can resend the Interest after a timeout. In this way the new Interest will research the content required from the new position established and thus generating the new path necessary to the Data packet to reach the consumer.

Producer mobility is more problematic. In fact, when a Mobile Producer (MP) moves to a new position, a consumer might be unable to fulfill its Interest since the path to the MP might become invalid. To address this problem, the MP might hasten the creation of a new Interest path by generating a "breadcrumb trail" to a rendezvous node to enable Interests to trace content at its the new position. The rendezvous node can also be used as a deposit for content, allowing it to resolve consumers' Interests while the routing strategies have not aligned to the new position of the MP. Furthermore, consumers and router nodes can also adapt their behaviour for this particular situation by choosing more aggressive Interest flooding strategies in order to find the new location of the producer.

C. Multicasting and Multihoming

The NDN architecture seamlessly handles the dissemination of content to a single consumer or to a group of consumers. As introduced in Section III, NDN manages all the interfaces over which data are sent or received with components named Faces. Each Face can be connected to higher layer entities, such an application, a physical network interface or even a virtual link, such as a TCP connection in hybrid NDN/IP architectures. As a result, NDN supports multicast communications out of the box.

Furthermore, NDN overcomes the well-known problems that IP architectures presents with multihoming. In fact, since Interest routing is based on the content name, NDN works out of the box in heterogeneous network environments with multiple channel technologies and is capable of aggregating Interests received from different faces, so that only one Interest per content is sent over a shared communication link. Furthermore, nodes with multiple networks interface are also profitable in term of caching. When a Data packet is sent back to the consumer, NDN leaves a copy of the message in the local Content Store of all nodes along the reverse Interest path. Popular content is then automatically made available close to its consumers.

D. Synergies with IoT

NDN presents interesting synergies with IoT applications [35]. In fact, while NDN was designed with *"one Interest, one Data"* semantics, other ICN implementations (most notably PURSUIT) were specifically designed to support publish/subscribe communications. As a result, borrowing on concepts and tools from the aforementioned ICN implementations, and through the clever adoption of specifically designed naming schemes [33], NDN could be extended to realize publish/subscribe communications with support to topics and distributed caching - a communication model that is particularly well suited for IoT.

More specifically, an IoT application based on NDN could adopt naming schemes that, for example, organize devices and the information they generate in a strict hierarchy or adopt less restrictive taxonomies that can generalize multiple devices. This would allow directly using naming schemes to as part of the basic discovery mechanisms by investigating the header of the Data requested or even information cached in the local content store without deploying dedicated discovery protocols.

In the tactical environment, this means that NDN could become an interesting enabling technology for IoBT [1]. More specifically, the NDN capability to leverage locally available information is likely to become a sought-after feature for military operations in the future where information is expected to be scattered all over the network and the challenge lies in finding the right information.

E. Interface between application and network layer

TCP/IP applications leverage a range of solutions including unicast, multicast, and DTN, to implement realize a wide range of communications patterns. However, those solutions are mostly designed to masquerade network behavior from the application – leading to poor performance in tactical environments unless specifically developed solutions proposing an enriched network programming model are adopted [9] [10].

Instead, NDN provides applications with a simple but powerful programming model that allows tuning application behaviour to the current network performance. More specifically, by properly tuning the Interests transmission rate, a node can attempt to mitigate node mobility issues and control the traffic flow according to the available network resources. This gives NDN a flexible flow control function that works in a distributed manner and can make local decisions.

In addition to application specific configuration, node level configurations also represent convenient "knobs" for performance tuning. For example, a router can for example set a limit on the number of pending Interest that it allows on an outgoing Face, or the number of Data messages that are forwarded back.

V. Challenges in Military Tactical Networks

Clearly, the previous section has identified a number of advantages of NDN over traditional IP networks. Howerver, NDN raises a number of new issues that must be studied further to evaluate its utility in heterogeneous military networks. This section lists some of the important topics within NDN that need further examination.

A. Naming

Naming is one of the most challenging tasks in NDN application design. While it is certainly impossible to devise a standardized naming scheme that applies to a wide range of application domains for traditional Internet applications, we believe that this problem could at least be partially addressed for military networks. In fact, military applications consider a significantly smaller amount of content types than Internet ones. Furthermore, military information already present standardized formats that provide common information structures, which can be used to regroup contents and obtain content taxonomies. These properties will simplify the design of naming schemes, and also potentially increase its effectiveness since it is directly tailored to the information. Nevertheless, this topic requires much attention.

B. Security

The NDN security architecture [36] is very flexible but raises some challenges - particularly for mobile military networks. In NDN, information security (INFOSEC) is placed on the content. Each content chunk is signed and optionally encrypted. This is flexible but introduces overhead. The public key of the signer, a certificate for that public key or a pointer to them must be sent with the packet and a trust chain must be in place. For low data rate mobile connections this can be problematic. Traffic analysis is also a challenge, in NDN the Interest is sent in clear text. This is not adequate for military networks [29]. The security model does not handle network security (NETSEC). There must be functions in place that perform network security. The security discussion in [16] and [17] shed some light on some of the security challenges. Some traditional solutions for mobile military networks such as preloaded keys and link level encryption can solve some of these problems but more research is needed.

C. Strategy

The strategy layer is a powerful component in the NDN architecture but must be studied and tuned to achieve its full potential. The flexibility introduced by this layer enables to tailor the forwarding policy of Interest and Data to the application specific requirements. In fact, NDN allows to implement a wide range of strategies, from naive ones that simply mimic standard IP communication mechanism (e.g. unicast, multicast) to more sophisticated ones that continuously analyze their performance and self-learn how to improve their performance.

For instance, FIB can be based on overheard traffic such that the Interests might sent on one or several Face(s) in the direction of where Interest for similar content has been resolved before. However, strategies that introduce high redundancy in the Interest distribution should be carefully adopted for networks where links capacity is limited or present different resource constraints. Strategies should be designed to achieve the best tradeoff between delay in fetching the information and network resource utilization. At this matter, proactive routing solutions that announce cached content might allow the strategy layer to improve the Interest forwarding toward nearest producers and thus reduce resource utilization.

Finding the best trade-off between complexity, efficiency and robustness is crucial to exploit the flexibility of the strategy layer to adapt it to the network properties and communication requirements. At this matter, the experience from the vast research on routing in MANETs can be reused and extend to NDN strategy for mobile networks. The survey in [17] gives a comprehensive overview of different routing approaches for mobile NDNs. The policies of the strategy layer as well as the supporting routing functions are still an open research area.

D. Reliability

NDN does not provide an integrated solution for a reliable communication. As a result, unlike the TCP/IP model in which reliability functions are provided by transport layer

protocols, in NDN the responsibility to recover a lost message relies on applications – thus complicating the task of software engineers.

However, NDN properties allow to manage reliability through the already available mechanisms used for the nodes interaction. For example, a mechanism to provide reliability can be performed by issuing a new Interest packed if the previous Interest for the same content was not resolved within a certain timeout period. In this way application can achieve reliable information sharing with a simple and lightweight mechanism. This mechanism allows application to have full control to the timeout period and thus adapt this to the network capacity, QoS needed and so on.

E. Performance Tuning

Since NDN is a relatively new technology, the performance tuning of NDN applications is an aspect that still needs to be thoroughly investigated.

For instance, cache replacement strategies for Content Stores and values for several timeouts (including Interest retransmission) are critical parameters for application performance and robustness (as they not only influence delay and jitter of the requested Data but availability as well). Cache replacement strategies of classic IP architectures are a mature research field and this knowledge can be reused here. But more work is needed to learn which strategies are best to use for which routing strategy and for different data types. Furthermore, applications might reissue the an Interest if no Data has been received within a certain timeout. This parameter must be properly tuned to fit traffic requirements and network properties. More experience that can result in guidelines for how to set the parameters, are needed. [37] is one example reference that discuss Cache replacement strategies for NDN.

Chunk size is another very relevant performance related research topic in NDN. How large data elements should the consumer be able to ask for in one Interest? The NDN architecture promotes tiny chunks, as small as single voice samples or video frames. The advantage of this is a very responsive network. The Interest can be routed a different way for each voice sample and thus be able to handle mobility and avoid network congestion (do flow control) etc. very quickly. This comes at the cost of a large overhead; this Interest packet and headers in the Data packet (that includes a security certificate) for each tiny chunk of data. Larger chunk sizes such as whole documents or videos reduce the overhead but also reduce some of NDN architectures qualities. In fact, with larger chunks it is more likely that the forwarding of Data will fail.

F. Congestion Control

NDN adopts a radically different communication model than TCP/IP. Hence, it cannot easily leverage the immense knowledge base built over decades by researchers investigating end-to-end congestion control solutions such as those designed for TCP [38] [39]. As a result, NDN has to leverage other congestion management solutions, including receiver-based congestion control, hop-by-hop congestion control, and hybrid methods.

At the moment of this writing, hop-by-hop congestion control methods, based on the automatic slow down of Interest forwarding at the router level in case of overloading, seem to be the most commonly proposed ones. However, those methods typically do not consider numerous important factors, such as the influences that caches have on transport traffic, multi-path transport, etc.. Overall, congestion management definitely represents one of the aspects that are most in need of further investigation to foster practical adoption of NDN based solutions.

VI. Proposed Method to Evaluate ICN

The NATO STO IST-161 RTG has been using the Anglova scenario [40] [41] to evaluate the relative performance of a variety of Group Communications Protocols to disseminate information within a tactical domain [42]. We have developed a test harness that measures three key performance measures - delivery ratio, latency, and bandwidth utilization - in the context of disseminating three different types of information objects - Blue Force Data, Sensor Data, and Documents. Our objective in the near future is to incorporate NDN as another protocol to evaluate within this scenario and test harness, so that it can be compared with more traditional approaches that use either centralized brokers or decentralized delivery over IP multicast. This would allow us to better characterize where NDN sits in the overall space of dissemination protocols - especially with respect to tradeoffs between delivery coverage, latency, and communications overhead.

After this initial evaluation, we also plan to explore NDN-specific alternatives to see their relative impact on performance. One challenge within routing is service discovery in heterogeneous networks. Should search for data be based on traditional topology/service discovery or be more based on hint based? That is, services are announced/hinted by the use of ongoing traffic.

Another interesting question is how to best use the different NDN faces in mobile multihop wireless networks. Broadcast is superior in small networks, but less suitable in larger networks. We are particularly interested in considering the effectiveness of NDN in heterogeneous networks and the mixing of different strategies (e.g., broadcast in small networks) and how to find, if any, the tradeoffs of using caching/multi-path search compared to traditional topology discovery.

Finally, Security is a key requirement for most tactical network communications. Traditionally, NDN uses signatures, which add overhead. We plan to explore different security models for NDN and explore ways to reduce the signature overhead if it indeed turns out to be a problem.

VII. Conclusions

In this survey we discussed the capabilities and challenges that NDN presents for in tactical environments More specifically, we observed that the continuous evolution of tactical

networks due to the central role of information and the use of new technologies that increase the amount of information gathered and transmitted can profit of NDN properties. However, NDN architecture needs a deeper investigation in order to increase the overall effectiveness of the protocol. This is one of the planned activities for the NATO IST-161 Research Task Group.

ACKNOWLEDGEMENTS

This paper presents the results of work conducted by the authors within the NATO STO IST-161 Research Task Group on Efficient Group and Information Centric Communications in Mobile Military Heterogeneous Networks.

REFERENCES

[1] S. Russell and T. Abdelzaher, "The internet of battlefield things: The next generation of command, control, communications and intelligence (c3i) decision-making," in *IEEE MILCOM*, 2018, Conference Proceedings, pp. 737–742.

[2] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, and L. Sadler, "Exploring value-of-information-based approaches to support effective communications in tactical networks," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 39–45, 2015.

[3] Y. Cao and Z. Sun, "Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges," *Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 654–677, 2013.

[4] O. M. G. (OMG). Data distribution service (dds). [Online]. Available: https://www.omg.org/omg-dds-portal/

[5] F. Guidec and Y. Maheo, "Opportunistic content-based dissemination in disconnected mobile ad hoc networks," in *UBICOMM*, 2007, Conference Proceedings, pp. 49–54.

[6] C. P. (Ed.), "Ip mobility support for ipv4, revised," IETF, Electronic Article RFC5944, Nov. 2010. [Online]. Available: http://www.ietf.org

[7] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (nemo) basic support protocol," IETF, Electronic Article RFC53963, Jan. 2005. [Online]. Available: http://www.ietf.org

[8] N. Suri, E. Benvegnu, M. Tortonesi, C. Stefanelli, J. Kovach, and J. Hanna, "Communications middleware for tactical environments: Observations, experiences, and lessons learned," *IEEE Communications Magazine*, vol. 47, no. 10, pp. 56–63, 2009.

[9] N. Suri, G. Benincasa, M. Tortonesi, C. Stefanelli, J. Kovach, R. Winkler, R. Kohler, J. Hanna, L. Pochet, and S. Watson, "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *IEEE Communications Magazine*, vol. 48, no. 10, pp. 60–69, 2010.

[10] M. Tortonesi, A. Morelli, C. Stefanelli, R. Kohler, N. Suri, and S. Watson, "Enabling the deployment of cots applications in tactical edge networks," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 66–73, 2013.

[11] K. Scott, T. Refaei, N. Trivedi, J. Trinh, and J. P. Macker, "Robust communications for disconnected, intermittent, low-bandwidth (dil) environments," in *IEEE MILCOM*, 2011, Conference Proceedings, pp. 1009–1014.

[12] N. D. N. project. Named data networking (ndn) - a future internet architecture. [Online]. Available: https://named-data.net/

[13] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *ACM CoNEXT*. 1658941: ACM, 2009, Conference Proceedings, pp. 1–12.

[14] C. Gibson, P. Bermell-Garcia, K. Chan, B. Ko, A. Afanasyev, and L. Zhang, "Opportunities and challenges for named data networking to increase the agility of military coalitions," in *2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Aug 2017, pp. 1–6.

[15] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2014.

[16] A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan, and J. Wilcox, "Information-centric networking: seeing the forest for the trees," in *ACM HotNets*. 2070563: ACM, 2011, Conference Proceedings, pp. 1–6.

[17] M. Amadeo, C. Campolo, A. Molinaro, and G. Ruggeri, "Content-centric wireless networking: A survey," *Computer Networks*, vol. 72, pp. 1–13, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614002497

[18] B. Etefia and L. Zhang, "Named data networking for military communication systems," in *IEEE Aerospace Conference*, 2012, Conference Proceedings, pp. 1–7.

[19] B. Etefia, M. Gerla, and L. Zhang, "Supporting military communications with named data networking: An emulation analysis," in *IEEE MILCOM*, 2012, Conference Proceedings, pp. 1–6.

[20] S. Y. Oh, D. Lau, and M. Gerla, "Content centric networking in tactical and emergency manets," in *IFIP Wireless Days*, 2010, Conference Proceedings, pp. 1–5.

[21] M. T. Refaei, S. Ha, Z. Cavallero, and C. Hager, "Named data networking for tactical communication environments," in *IEEE NCA*, 2016, Conference Proceedings, pp. 118–121.

[22] J. Burke, A. Afanasyev, T. Refaei, and L. Zhang, "Ndn impact on tactical application development," in *IEEE MILCOM*, 2018, Conference Proceedings.

[23] T. U. of Utah. Emulab. [Online]. Available: https://www.emulab.net/

[24] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg, "The optimized link state routing protocol version 2," IETF, Electronic Article RFC7181, Apr. 2014. [Online]. Available: http://www.ietf.org

[25] J. Macker(ed.), "Simplified multicast forwarding," IETF, Electronic Article RFC6621 (Experimental), May, 2012. [Online]. Available: http://www.ietf.org

[26] Common open research emulator (core). [Online]. Available: https://www.nrl.navy.mil/itd/ncs/products/core

[27] J. B. Evans, S. G. Pennington, and B. J. Ewy, "Communication networks for the tactical edge," in *SPIE Defense + Security*, vol. 10205. SPIE, 2017, Conference Proceedings, p. 9.

[28] Mininet - an instant virtual network on your laptop (or other pc). [Online]. Available: http://mininet.org/

[29] J. B. Evans, S. G. Pennington, and B. J. Ewy, "Named data networking protocols for tactical command and control," in *SPIE Defense + Security*, vol. 10651. SPIE, 2018, Conference Proceedings, p. 7.

[30] C. Gibson, P. Bermell-Garcia, K. Chan, B. Ko, A. Afanasyev, and L. Zhang, "Opportunities and challenges for named data networking to increase the agility of military coalitions," in *IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI*, 2017, Conference Proceedings, pp. 1–6.

[31] T. L. Xin Xu, Haitao Zhang and L. Zhang, "Achieving resilient data availability in wireless sensor networks," in *May 2018 - IEEE International Conference on Communications (ICN-SRA)*, 2018, Conference Proceedings.

[32] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014. [Online]. Available: http://doi.acm.org/10.1145/2656877.2656887

[33] O. Ascigil, S. Reñé, G. Xylomenos, I. Psaras, and G. Pavlou, "A keyword-based icn-iot platform," in *Proceedings of the 4th ACM Conference on Information-Centric Networking*, ser. ICN '17. New York, NY, USA: ACM, 2017, pp. 22–28. [Online]. Available: http://doi.acm.org/10.1145/3125719.3125733

[34] A. Bouacherine, M. R. Senouci, and B. Merabti, "Multipath forwarding in named data networking: Flow, fairness, and context-awareness," in *E-Business and Telecommunications*, M. S. Obaidat, Ed. Cham: Springer International Publishing, 2017, pp. 23–47.

[35] D. Mars, S. Mettali Gammar, A. Lahmadi, and L. Azouz Saidane, "Using information centric networking in internet of things: A survey," *Wireless Personal Communications*, Jan 2019. [Online]. Available: https://doi.org/10.1007/s11277-018-6104-8

[36] D. Smetters and V. Jacobson, "Securing network content," PARC, Tech Report, Oct. 2009.

[37] G. Carofiglio, V. Gehlen, and D. Perino, "Experimental evaluation of memory management in content-centric networking," in *IEEE ICC*, 2011, Conference Proceedings, pp. 1–6.

[38] Y. Ren, J. Li, S. Shi, L. Li, G. Wang, and B. Zhang, "Congestion control in named data networking a survey," *Computer*

Communications, vol. 86, pp. 1 – 11, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366416301566

[39] K. Schneider, C. Yi, B. Zhang, and L. Zhang, "A practical congestion control scheme for named data networking," in *Proceedings of the 3rd ACM Conference on Information-Centric Networking*, ser. ACM-ICN '16. New York, NY, USA: ACM, 2016, pp. 21–30. [Online]. Available: http://doi.acm.org/10.1145/2984356.2984369

[40] N. Suri, A. Hansson, J. Nilsson, P. Lubkowski, K. Marcus, M. Hauge, K. Lee, B. Buchin, L. Msrholu, and M. Peuhkuri, "A realistic military scenario and emulation environment for experimenting with tactical communications and heterogeneous networks," in *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2016, pp. 1–8.

[41] N. Suri, J. Nilsson, A. Hansson, U. Sterner, K. Marcus, L. Misirliolu, M. Hauge, M. Peuhkuri, B. Buchin, R. in't Velt, and M. Breedy, "The angloval tactical military scenario and experimentation environment," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2018, pp. 1–8.

[42] N. Suri, R. Fronteddu, E. Cramer, M. Breedy, K. Marcus, R. i. '. Velt, J. Nilsson, M. Mantovani, L. Campioni, F. Poltronieri, G. Benincasa, B. Ordway, M. Peuhkuri, and M. Rautenberg, "Experimental evaluation of group communications protocols for tactical data dissemination," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Oct 2018, pp. 133–139.