Experimental Evaluation of Named Data Networking (NDN) in Tactical Environments

Lorenzo Campioni*§, Mauro Tortonesi*, Bastiaan Wissingh†, Niranjan Suri‡§, Mariann Hauge¶, Lars Landmark¶
*University of Ferrara, Ferrara, Italy
lorenzo.campioni@unife.it, mauro.tortonesi@unife.it
†TNO, The Hague, The Netherlands
bastiaan.wissingh@tno.nl
‡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
¶Norwegian Defence Research Establishment (FFI), Kjeller, Norway
mariann.hauge@ffi.no, lars.landmark@ffi.no

***Abstract*—Tactical edge networks represent a uniquely challenging environment from the communications perspective, due to their limited bandwidth and high node mobility. Several middleware communication solutions have been proposed to address those issues, adopting an evolutionary design approach that requires facing quite a few complications to provide applications with a suited network programming model while building on top of the TCP/IP stack. Information Centric Networking (ICN), instead, represents a revolutionary, clean slate approach that aims at replacing the entire TCP/IP stack with a new communication paradigm, better suited to cope with fluctuating channel conditions and network disruptions. This paper, stemmed from research conducted within NATO IST-161 RTG, investigates 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. We evaluated an NDN-based Blue Force Tracking (BFT) dissemination application within the Anglova scenario emulation environment, and found that NDN obtained better-than-expected results in terms of delivery ratio and latency, at the expense of a relatively high bandwidth consumption.**

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

I. Introduction

Tactical edge networks represent a uniquely challenging environment from the communications perspective, due to their limited bandwidth and high node mobility. These formidable issues, often compounded by a hostile RF environment, make the adoption of TCP-based communications very challenging in tactical networks, and call for other solutions that can cope with these limitations.

Several middleware communication solutions have been proposed to address the issues of tactical environments, leveraging many different paradigms: from connection-oriented solutions that support session mobility and are more resilient to channel fluctuations and disconnections [1], to delay tolerant solutions based on store and forward [2], to adaptation solutions that can run with good performance and reliability levels COTS TCP-based applications without requiring any modification [3]. However, all those solutions adopt an evolutionary design approach and have thus to address quite a few complications in order to provide applications with a network programming model suited for tactical edge environments while building on top of the TCP/IP stack [4].

Information Centric Networking (ICN), instead, represents a revolutionary, clean slate approach that aims at replacing the entire TCP/IP stack with a new communication paradigm. ICN provides several tools to tailor the robustness of data retrieval connections through different mechanisms for signaling redundancy and intermediate data storage (caching). Within an ICN architecture data producers, data location and transport means become transparent. This enables to seamlessly switch between different traffic patterns for data meant for single receivers and data meant for a group of recipients, or even to adapt traffic from fairly stable networks to intermittently connected ones.

Several ICN proposals exist with varying degrees of maturity [5]. The most mature, popular, and relevant solution for the purpose of supporting tactical communications is arguably Named Data Networking (NDN) [6]–[8], which builds on the concepts developed by the Content Centric Networking (CCN) proposal [9]. In fact, NDN-based solutions have recently started attracting considerable attention from the perspective of military applications [10], [11].

The NATO STO IST-161 Research Task Group (RTG) on Efficient Group and Information Centric Communications in Mobile Military Heterogeneous Networks is interested in evaluating NDN as a possible foundation for tactical communications. To this end, the IST-161 RTG analyzed at the architectural and capabilities levels the opportunities and challenges presented by the adoption of NDN in tactical environments [11]. This theoretical evaluation highlighted the fact that NDN offers some structural benefits for tactical environments in terms of: support for disruption tolerance, node mobility, multicasting and multihoming, compelling synergies with IoT, and of a programming model well suited for tactical appli-

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MILCOM47813.2019.9020843

cations. However, the evaluation also identified a number of fundamental challenges to address such as the need to develop: sensible information naming schemes, new security, reliability, performance tuning, and congestion control solutions as well as a strategy layer suited for the tactical environment.

This paper extends our previous analysis by presenting an experimental evaluation of NDN within the Anglova scenario emulation environment (see section IV). More specifically, we focus on the evaluation of the NDN capability to support Blue Force Tracking (BFT) dissemination in an emulated environment. To this end, we developed a simple NDN-based BFT dissemination application that bridges the mismatch between the push-based nature of BFT applications and the pull-based semantics of NDN by assuming isochronous (and known) BFT generation times.

The results obtained show that NDN achieved better-than-expected performance, both in terms of delivery ratio and delivery latency, at the expense of a non-negligible bandwidth consumption. These promising results stimulate us to further evaluate NDN by overcoming the isochronous BFT generation times assumption, possibly through the adoption of synchronization extensions such as ChronoSync [12], and considering other types of tactical applications, e.g., sensor data and document exchange.

II. Related Work

In the literature several surveys provide a comprehensive comparison of different ICN solutions. Surveys such as [13] offer an overall optimistic point of view on ICN, while other surveys, like [14], include quite a few critical considerations. Most of the surveys focus on applications design for high-capacity fixed Internet infrastructure, which present different characteristics with respect to military tactical networks. Amadeo et al.'s work represent an exception, which surveys ICN-related solutions in wireless and mobile networks [15]. A handful of papers have also started to look into the use of ICN in mobile military environments [6], [16]–[19].

NDN has been suggested to address the challenges for mobile military networks in [16]. The paper lists opportunities for ICN but does not provide technical details. That study, however, has been extended in [17] with an experimental evaluation of NDN in two network scenarios using Emulab [20]. The results provided are encouraging but the experiments are designed to show the benefit of the architecture and do not highlight potential challenges.

S. Y. Oh et al. claim in [18] that some modifications of NDN are required to better address MANET challenges. NDN is a pull-based architecture where the consumer always asks for data. The authors propose to support push communication model by dividing 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* handshake 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 [21]) and IP multicast (using SMF [22]) in DIL (disruptive, intermittent connectivity, and low bandwidth) environments in [19]. A very disruptive ship to shore network is built using CORE (Common Open Research Emulator) [23]. It shows promising results in which NDN outperforms IP based communication and presents how NDN can mix a unicast and multicast data dissemination model to achieve localized robustness to disruption. The study however does not discuss any possible challenges that must be addressed with the NDN architecture.

NDN's potential impact on tactical application development is discussed in a number of publications [6]–[8]. Evans et al. present the mininet [24] based evaluation of two different scenarios [25]. The results show that NDN outperforms other examined solutions as the reliability of the connection (e.g. radio link) decreases due to high loss-rate. However, the work also indicates that a push-based multicast architecture exhibits lower latency in data transmission that the NDN pull-based architecture. The authors of [25] also discuss various properties of the NDN security model which can have a negative impact on the communications since it limits an efficient use of the caches. In [8] the authors provide a small scale comparative evaluation between NDN, WS-Notification, and MQTT. The results show that NDN exhibits a higher bandwidth consumption compared to MQTT, and that WS-Notification has the highest overhead. However, the manuscript does not investigate NDN broker-less design which as the authors suggests, would be more suitable for tactical networks.

III. NDN

NDN is a clean state communication paradigm that does not follow the host centric architecture of the classical Internet [26] but focuses on allowing to retrieve information (content) irrespectively of its originating location. This is done *by addressing the information by name rather than by its source (host name or IP address)*. To enable such design, information naming must rely on a solid naming scheme provided by the applications. As a result, the first step in NDN application development is defining a naming scheme that fits the content characteristics and the application's particular needs.

Once the naming scheme is defined, applications can share information through the two basic NDN primitives: they request specific content by sending an *Interest* packet containing the name of the content, and respond to Interest messages with the matching data in a *Data* packet. When the consumer has issued an Interest message, the latter is forwarded through the network in search for a node that holds the desired content. When the content is found, it is wrapped in a Data packet, which is then transmitted through the reverse path of the Interest packet back to the consumer.

The management of this process is implemented in the forwarding engine in all network nodes (routers, consumers, and producers) within the NDN architecture. In NDN, the interfaces over which content can be transmitted and received are called *Faces*. A Face is an abstraction of a internal interface towards higher layers (applications), a network interface, or

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MILCOM47813.2019.9020843

other types of connections, like a TCP connection in case of hybrid NDN/IP solutions.

More specifically, when an application issues an Interest, the message reaches the local forwarding engine over an internal Face. First, the forwarding engine checks if the requested content is available in the local *Content Store*, the 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 register the Interest, as well as the originating Face, in an internal table called *Pending Interest Table* (PIT). In case that the Interest was already registered in the PIT,it is a policy decision if the forwarding engine does should forward the Interest to other nodes or not. If the choice is to discard the Interest since the content has already been requested, it simply adds the new Face to the PIT in order to forward back the Data message to all interested consumers.

If 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. To perform Interest forwarding the engine is sided by another module in NDN architecture called the *Strategy Layer*. The Strategy Layer enables NDN to perform intelligent forwarding decisions such as forwarding on multiple Faces, name-driven caching and forwarding mechanism.

This forwarding procedure is repeated in all 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 produces the information, it resolves the Interest by sending back a Data packet following 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 satisfy the PIT entry and may 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.

IV. Anglova Scenario

The NATO STO IST-161 RTG has been using the Anglova scenario [27] [28] to evaluate the relative performance of a variety of Group Communications Protocols to disseminate information within a tactical domain [29]. The Anglova scenario is a purposely designed testbed that allows to evaluate the performance of communication solutions in a realistic tactical environment in a controlled and reproducible way. It consists of an emulated scenario that depicts an operation conducted by a battalion after receiving reconnaissance data alerting of an attack by insurgent forces against coalition forces in an operational zone. The Anglova scenario is instantiated using the Extendable Mobile Ad-hoc Networking Emulator (EMANE), and provides node mobility and network connectivity for a military operation across three vignettes designed to highlight the challenges related to tactical networks. The vignettes have the same actors and role but define different set of operations and events. The first vignette covers all the intelligence preparation action such as sensor deployment and information gathering. The second vignette describes the deployment of the coalition forces. In this vignette the forces move into the operational zone and so the connection between the nodes is discontinued due to the increasing distance between them. The final vignette describes war-events in the network with: neutralization of insurgents, medical operation and even attacks of the enemy position.

So far, the experiments conducted within NATO IST-161 RTG activities focused on a part of the Anglova scenario. More specifically, we considered Company A from the second vignette in which troops are deployed in the operational zone. This part of the scenario reenacts the behaviour of 24 vehicles that exit the Headquarters area to reach the operation zones. While limited in terms of number of nodes involved and duration of the scenario, the set of played events includes multiple mobile nodes, exhibiting disconnectivity and limited bandwidth issues, and thus provide a clear and effective stress test to evaluate group communication solutions for tactical environment. More specifically, the connectivity between forces is provided by VHF connections. However, while forces move away from the starting area they might lose connectivity with other stationary nodes and they have to switch SATCOM links or rely on moving tactical UAVs used as communication link.

To mimic the behaviour of tactical applications leveraging group communication protocols [29], we built a test harness that disseminates three types of information objects: Blue Force Tracks (BFT), sensor data and documents and identified 3 key performance measures: delivery ratio, delivery latency, and bandwidth utilization. BFT are small size messages, from 128 to 512 Bytes, and disseminated every few seconds (usually 5 to 10). A BFT messages represent a sort of position update messages or hello messages disseminated with best effort policies and all nodes produce and should receive these type of messages. Sensor data and document messages are larger messages that require specific transmission policies and are occasionally generated (every few minutes).

V. BFT Dissemination using NDN

To evaluate the effectiveness of NDN in the context of tactical edge networks, we extended the test harness presented in [29] and discussed in the previous Section to support NDN-based communications. This allows to compare NDN with different data dissemination solutions designed for tactical environments.

To bridge the mismatch between the push-based nature of tactical applications and the pull-based semantics of NDN, we decided to focus only on BFT dissemination which arguably represents the most challenging component of a tactical application for NDN. As a result, we implemented within our test harness a simple NDN-based BFT dissemination application based on the assumption of isochronous (and known) BFT generation times. More specificially, BFT information is published by each node every 10 seconds, and consumed by all other nodes. The payload of the BFT messages is 128 Bytes, resulting in a setup with 24 publishers and 24 subscribers.

In order to address these differences we designed the following naming scheme:

```
/anglova/blue_force/<node_id>/<seq>
```

where *anglova* is the root, *blue force* is the topic, *node id* is the node identifier and *seq* is an incremental value that distinguishes each data item the node has published. This scheme allows to uniquely identify the data published by each node while allowing each consumer to request it without the need of a content discovery mechanism. For example if a consumer needs the 16^{th} content item published by node 4 it can simply send an interest specifying the following name:

```
/anglova/blue_force/node_4/16
```

with the assumption of isochronous generation of BFT information each consumer can issue interests at the same rate as data is produced and thus emulating a push communication model through proactive Interest dissemination.

Once we addressed the incompatibilities between our test harness and the NDN communicating model we had to properly configure the network stacks to allow information sharing. NDN supports different mechanisms to transmit messages to other nodes via the so called *NDN face system* that allows seamless handling of native communication that bypasses IP or message encapsulation in COTS transport protocols such as UDP. For our experiment we decided to leverage UDP Multicast for message transmission. In this way, applications will broadcast Interests to all reachable nodes in the network that, if they have cached the requested content, will broadcast back the Data message. While this approach could limit the possibility of interest aggregation or data caching, due to the synchronous dissemination of interest, it will allow to obtain a first coarse grained evaluation of NDN capabilities to be refined in the future wit more sophisticated schemes and configuration.

VI. Experimental Evaluation

We analyzed the behavior of our naive NDN-based BFT application according to 3 key performance indicators: delivery ratio, delivery latency, and bandwidth utilization. We compared NDN's performance with that achieved by two other group communication solutions: DisService and NATS, which we believe represent important and relevant baseline references. As shown in [29], DisService outperforms many other group communication solutions, in terms of bandwidth utilization, delivery latency, and delivery ratio, in tactical environment conditions. Although BFT message transmission typically leverages best-effort communications, in our experiments we evaluated DisService in both unreliable and reliable message transmission configurations. We refer to those two configurations with the names DisService and DisService Reliable respectively. Furthermore, we also included NATS in the comparison since, even if not as effective as DisService, it proved to be best performing broker based group communication solutions in our previous experiments [29].

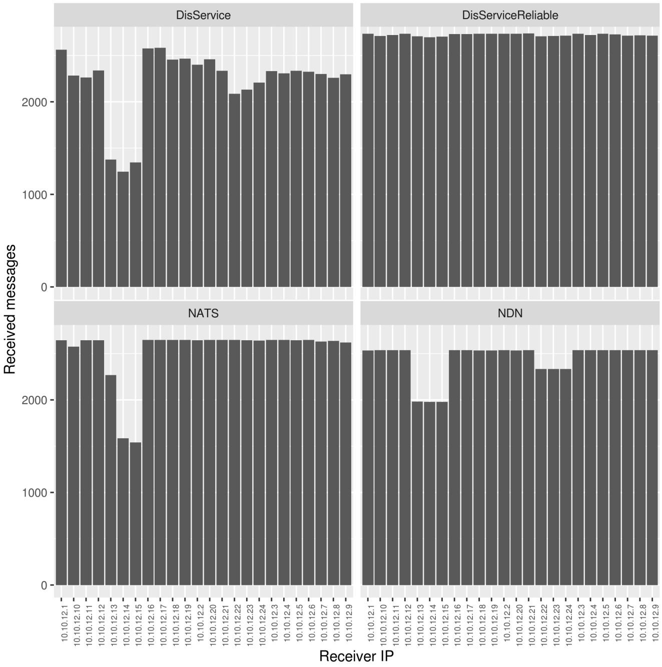

Fig. 1. Number of messages received by each node.

Fig. 1 depicts the total number of messages received per node. The figure clearly shows that one group of nodes receive a smaller amount of messages. This is caused by the events of the scenario, that frequently disconnect nodes 13, 14, and 15 from the other nodes. Almost all the group communication solutions we examined are very sensitive to this disconnection and fail to deliver a significant amount of messages to these nodes. However, NDN seems less affected by this issue and delivers more messages to nodes 13, 14, and 15 compared to DisService and NATS.

Fig. 2 further illustrates the effectiveness of protocols in delivering BFTs by showing the delivery ratio of messages, i.e., the ratio of nodes that actually received the BFTs. To better illustrate the dynamics of the protocol behavior throughout the duration of the scenario, the figure divides messages in 20 categories, according to the respected minute of generation time. Each category of messages is depicted using a Boxplot that allows to graphically evaluate the distribution of delivery ratios in the messages of each category. The Boxplots allow us to clearly describe the sets of data we gathered using their quartiles and thus highlighting dispersion and asymmetries. Due to the

Fig. 3 completes the effectiveness analysis of the group communication solutions from the application perspective by presenting the distribution of delivery latency. The figure uses the same format of Fig. 2, which classifies messages according to their relative minute-of-simulated-time of their generation

DOI til publisert versjon/DOI to published version: 10.1109/MILCOM47813.2019.9020843

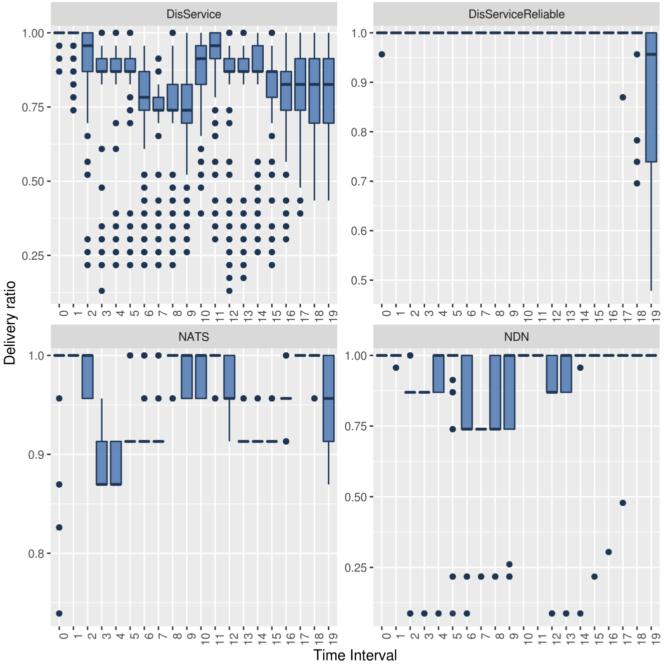

Fig. 2. Delivery ratio per minute.

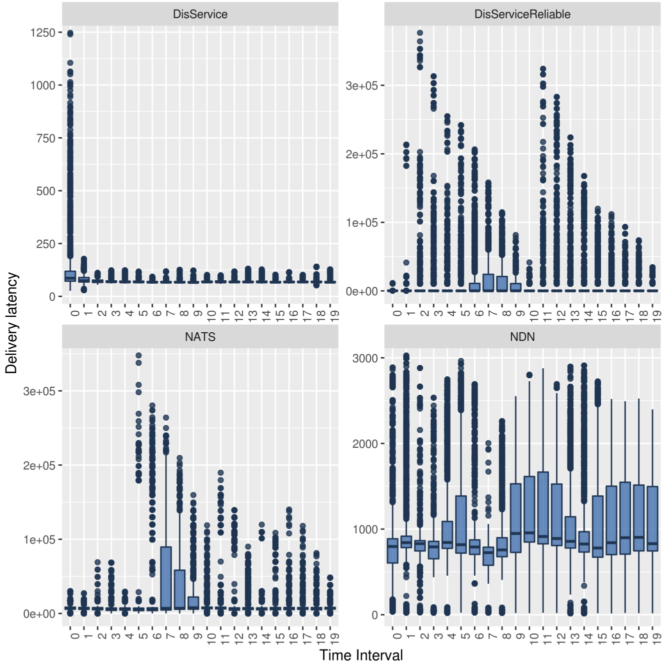

Fig. 3. Delivery latency per minute.

and using Boxplots to present the distribution of delivery latency minute-by-minute. In this case, the graphs present different scales for the y axes since NATS and DisService Reliable presented outliers with high delivery latency values. However, even if DisService and NATS deliver some message after more than 10 seconds, the majority of BFTs is received quickly after their initial generation. NDN instead seems slightly slower in delivering messages, requiring on average 1 second for delivery. This might be caused by the proactive interest dissemination approach that we adopted to reenact push communication model. In fact, due to the NDN communication model, producers do not proactively push content to the consumers after it has been generated but instead wait to receive Interests from the consumers before transmitting data – with the result of increasing the overall delivery times.

Finally, we present the total amount of outgoing traffic in Fig. 4, as metric to evaluate and compare the network resource consumption of each protocol. This measure is obtained as the sum of the average amount of bits per second sent by each node. The figure shows that the naive message dissemination strategy that we adopted for our NDN-based application causes considerable pressure on the network. In fact, even when NDN relies on UDP Multicast and thus can leverage link-local multicast dissemination of data, it still presents a high overhead compared to DisService and DisService Reliable. We speculate that this might be caused by the absence of tailored caching, Interest aggregation and forwarding strategy configurations that could theoretically reduce the bandwidth consumption of NDN while at the same time increase its effectiveness.

VII. Conclusions

During the thorough testing of our specifically developed naive NDN-based BFT dissemination application within the Anglova scenario, NDN has shown promising performance, both in terms of delivery ratio and delivery latency.

However, these results were achieved assuming isochronous (and known) generation times for BFTs, which might be impractical for some applications, and at the expense of significant bandwidth consumption. In fact, despite that these results look promising, more evaluation is needed to further validate NDN as a viable approach for group communications in tactical environments.

Future works will consider non-isochronous BFT generation and analyze implementations of naming strategies and information sharing solutions that support more complex scenarios. In this context, an interesting approach could be to adopt some form of NDN synchronization, such as ChronoSync. In addition, we will consider setups that are not based on UDP multicast, but instead leverage Ethernet Multicast/Unicast directly (possibly using NDNLPv2) as well as improved caching configuration, Interest aggregation and forwarding strategies. We will also consider to further extend the scenario with more sophisticated topologies in which nodes might require multiple hops to transmit information and to permit experiments focused on different NDN strategy mechanisms.

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.

DOI til publisert versjon/DOI to published version: 10.1109/MILCOM47813.2019.9020843

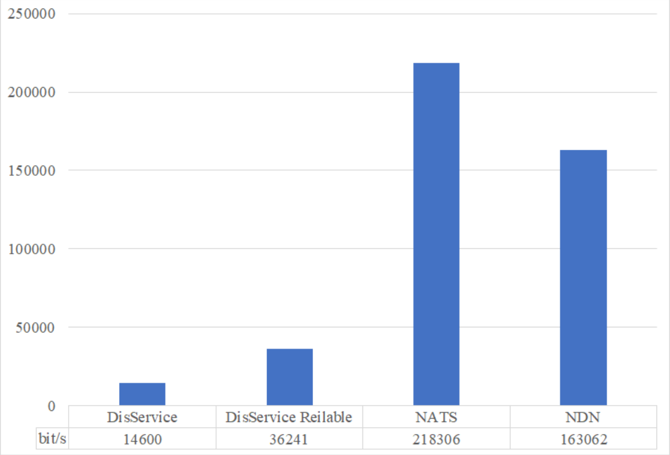

Fig. 4. Cumulative bandwidth consumption per second.

The authors would like to thank Prof. Lixia Zhang from University of California Los Angeles and Prof. Alex Afanasyev from Florida International University for their invaluable support in the proper setup of NDN for the experiments conducted in this work.

References

[1] 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.

[2] 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.

[3] 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.

[4] G. Benincasa, A. Morelli, C. Stefanelli, N. Suri, and M. Tortonesi, "Agile communication middleware for next-generation mobile heterogeneous networks," *IEEE Software*, vol. 31, no. 2, pp. 54–61, Mar 2014.

[5] M. Tortelli, D. Rossi, G. Boggia, and L. Grieco, "Icn software tools: Survey and cross-comparison," *Simulation Modelling Practice and Theory*, vol. 63, pp. 23 – 46, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1569190X15300654

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

[7] 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.

[8] F. T. Johnsen, L. Landmark, M. Hauge, E. Larsen, and . Kure, "Publish/subscribe versus a content-based approach for information dissemination," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Oct 2018, pp. 1–9.

[9] 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.

[10] 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.

[11] L. Campioni, M. Hauge, L. Landmark, N. Suri, and M. Tortonesi, "Considerations on the Adoption of Named Data Networking (NDN) in Tactical Environments," in *2019 International Conference on Military Communications and Information Systems (ICMCIS 2019)*, May 2019, pp. 1–8.

[12] Z. Zhu and A. Afanasyev, "Let's chronosync: Decentralized dataset state synchronization in named data networking," in *2013 21st IEEE International Conference on Network Protocols (ICNP)*, Oct 2013, pp. 1–10.

[13] 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.

[14] 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.

[15] 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

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

[17] 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.

[18] 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.

[19] 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.

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

[21] 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

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

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

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

[25] 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.

[26] 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

[27] 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 2016)*, May 2016, pp. 1–8.

[28] 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 2018)*, May 2018, pp. 1–8.

[29] 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.

DOI til publisert versjon/DOI to published version: 10.1109/MILCOM47813.2019.9020843