Opportunities and Challenges for Named Data Networking to Increase the Agility of Military Coalitions

Christopher Gibson
IBM UK
Project 3
gibsoncr@uk.ibm.com

Pablo Bermell-Garcia
Airbus Group, UK
Project 3
pablo.bermell@airbus.com

Kevin Chan
ARL, USA
Project 3
kevin.s.chan.civ@mail.mil

Bongjun Ko
IBM T.J. Watson Research Center, USA
Project 3
bongjun_ko@us.ibm.com

Alex Afanasyev
UCLA, USA
Project 3.
aa@cs.ucla.edu

Lixia Zhang
UCLA, USA
Projec3
lixia@cs.ucla.edu

***Abstract*— the objective of this paper is to summarize the opportunities and challenges for adopting Named Data Networking (NDN) in the specific context of military coalition operations and tactical networks, to improve the analytics capacity of the network and to speed up and improve the quality of distributed decision making. The characteristic properties of tactical networks are high dynamics in multiple dimensions. Furthermore, coalition networks must provide secure and efficient communication across coalition boundaries and mitigate the impact of adversarial entities attempting to obstruct the mission. By treating payloads, cryptographic keys, and policies all as semantically named and secured data packets, NDN integrates storage and processing into the networking layer and natively supports ad hoc, disruption tolerant networking with built-in security.**

I. Introduction

The success of military coalitions depends on, to a large extent, the ability to exchange relevant information between their assets in a secure and timely manner. While military forces are already operating in the highly challenging network environments of the tactical battlespace, the federated nature of coalitions brings additional challenges of controlling information flow across various boundaries, including problems of information discovery and sharing, and managing access privileges to information with high granularity. While digitalisation in recent years has undoubtedly increased our ability to capture battlefield information in multimedia forms with fine granularity, it has also raised the requirements to collect, process, and analyze that information to derive the most informed decision making available, and to share information with coalition partners under constraints imposed by policy control. Although today's operational TCP/IP network architecture, developed 40 years ago, can still work effectively in meeting the society's needs for large scale data dissemination over well engineered network infrastructure, it has shown its limitations in meeting the requirements of highly dynamic tactical networks. Hence new technologies and architectures are needed, that can exploit the increased capacities in data capture and processing, and increase the agility of distributed analytics in coalition operations [1].

II. Named Data Networking

The adoption of Named Data Networking (NDN) design [2] can effectively achieve this goal by raising the level of abstraction in networking. In NDN, the focus of networking is lifted from forwarding packets to destination nodes identified by IP addresses to directly accessing secured data by names. This fundamental change in communication model not only decouples information from its containers, but more importantly both removes applications' information access from the dependency on lower layer naming (e.g., IP addresses), and removes security control from the dependency on data containers and communication channels. NDN moves web semantics—fetching data by names (URLs)—from application layer to network layer, so that named and secured application data becomes the focus of all network operations, allowing the network to provide flexible and efficient ways to utilize all available network resources to satisfy applications' needs.

III. Motivational scenarios

To illustrate the communication requirements, and to identify the challenges in providing secure, resilient data collection and analytics by adopting NDN in military coalition environments, we use a field trial scenario from the Coalition Warfare Program (CWP) of the Office of the Secretary of Defence (OSD) [3]. The goal of this project was to demonstrate the seamless integration of a previously disparate set of coalition assets into a single data-to-decision (D2D) system. Through coalition asset integration, the trial aimed to achieve rapid assembly and deployment of a system with seamless control and highly granular, policy-controlled data sharing and

dissemination. At a high level, this example scenario is a wide-area surveillance system aiming to deliver imagery of sites of interest around a given location (specifically the sources of acoustic events around a facility). The available assets consist of two sets of acoustic unattended ground sensors (UGS), a fixed camera with pan-tilt-zoom functionality, a mobile camera mounted on an autonomous unmanned aerial vehicle (UAV), a second UAV tasked to harvest information from one set of low power UGS, and several software services providing analytics functionality. These assets are collectively provided by three coalition partners, each with varying sharing policies.

IV. Research questions

The adoption of NDN in tactical networks is a novel area of research. There remain a number of topics that require further research and investigation in order to bring NDN and its advantages into operational reality in such environments.

(1) **Naming Conventions**. NDN relies on well-defined naming conventions to enable each data consumer to automatically construct the proper name to fetch its required data. Naming conventions and standards are critical for seamless integration of networking, storage, and processing in an efficient and decentralized way. In addition to being used at the network layer for packet forwarding, data names are also used for security purposes. Thus, how best to design the namespace standards remains an open question. We are still in the early stages of developing general guidelines and hope to gain more insights by experimentation with a larger number of diverse application scenarios.

(2) **Information Discovery**. Because tactical coalition environments are highly heterogeneous and highly dynamic, establishing naming conventions may not eliminate cases where consumers express interests using names that do not match to the names of the content being produced, especially when the content is not an exact match to the query, although could be highly relevant. It is important to investigate, and validate novel methods and tools to enable NDN interest forwarding to accommodate multiple, approximate naming schemes, possibly through iterative learning from consumers' acceptance or rejection of retrieved data. Such adaptive learning has the potential to be very useful in mitigating the uncertainty of namespaces across coalition networks.

(3) **Name Confidentiality**: NDN enables powerful mechanisms for fine-grained and data-centric confidentiality, i.e., the content stays confidential and can only be accessed by the parties who are authorized. However, battlefield communication may also require name confidentiality: a mechanism to prevent unauthorized observers from understanding the nature of the requests and retrieved data. An approach to addressing this problem is to encrypt all communications among coalition entities to obscure all packet exchanges. Given all the entities in an NDN network must possess valid certificates, we can explore designs that utilize naming conventions to facilitate/automate the encryption key management. In other words, a plain-text communication with "signed Interests" [4] can be used to authentically request the encryption key, then completely encrypted Interest/Data exchanges are used for all future (potentially multi-point in nature) communication.

(4) **Policy Management**. NDN can facilitate policy management and dissemination. Whilst policy management is not yet an active research area in NDN, it is critical in realizing resilient and secure collection and processing of data in coalition environments. Therefore, it is vital to investigate novel methods to (a) use policy to secure and manage access to named data, (b) use NDN to distribute policy updates across the network, and (c) apply the ideas to specific deployment scenarios to verify the relevance and feasibility of the identified ideas.

V. Conclusions

Although Named Data Networking (NDN) as a new Internet architecture is still under active research, multiple research initiatives have been launched recently to explore its applicability and advantages in highly dynamic, highly heterogeneous environments. NDN is expected to excel in such environments because of its resilient delivery of named, secured data, independently from individual nodes, channels, or locations. This paper aims to motivate the research to exploit the use of NDN to improve the capability of distributed coalition systems. Since this is a new field of study, as a next step we must choose appropriate methodologies to validate and evaluate the perceived advantages of NDN and thoroughly examine the remaining issues.

Acknowledgment

This work is partially supported by the U.S. Army Research Laboratory and the U.K. Ministry of Defense under Agreement Number W911NF-16-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defense or the U.K. Government.

References

[1] 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 Proceedings of Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations (DAIS), 2017.

[2] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named Data Networking," ACM Computer Communication Reviews, June 2014.

[3] F. Bergamaschi and D. Conway-Jones, "ITA/CWP and ICB technology demonstrator: a practical integration of disparate ISR/ISTAR assets and technologies," in Proceedings of SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2012.

[4] NDN Team, "Signed Interest," Online: https://named-data.net/doc/ndn-cxx/current/specs/signed-interest