Enabling a Data-Centric Battlefield Through Information Access Gateways

Tamer Refaei
The MITRE Corporation †
mrefaei@mitre.org

Alex Afanasyev
Florida Int'l University
aa@cs.fiu.edu

***Abstract*—Network disruptions are common in tactical networks due to a number of factors including node mobility, unfavorable RF conditions, and adversarial attacks. Even under normal network conditions, tactical links are typically characterized by their low bandwidth and high delay. Most tactical data is exchanged over TCP/IP networks and TCP/IP's host-centric approach to networking is typically challenged under such network conditions [1]. Named Data Networks on the other hand offers an alternate approach to networking, namely a data-centric approach, which has been shown to provide superior efficiency and resilience in disrupted and low-bandwidth network environments. This is due to NDN's in-network caching, stateful forwarding, and loop-free multipath forwarding services which enable efficient use of bandwidth and tolerance to disruption. In this paper, we introduce Information Access Gateways (IAGs), a network component that enables a data-centric battlefield. IAGs are NDN and IP aware components that enable seamless integration of non-NDN applications into NDN networks while offering these applications name-based services such as synchronization (for applications that adopt a group communication model) and access control (to regulate information flow across the network). We describe the different services offered by an IAG and discuss how each can be applied to a notional tactical network environment.**

***Index Terms*—NDN, ICN, data-centric network**

I. Introduction

Information-Centric Networking (ICN) and its most prominent realization Named Data Networking (NDN) have emerged in the past few years as an efficient and effective communication model for today's and future networks. Realizing that today's networks are stifled by (1) a semantically meaningless end-host addressing scheme (IP addresses) and (2) an assumption that data always resides at its producer, NDN emerged with an alternative approach to networking. NDN names data as opposed to end-hosts and its core network functions are centered around fetching and delivering data using its name. This essentially shifts the network semantics away from "*deliver a packet to a given destination address*" and towards "*fetch data identified by a given name*." This simple yet powerful paradigm shift has been shown to address some of the shortcomings of today's networks. Most importantly, it provides unmatched resilience and robustness under disrupted and low-bandwidth network conditions, which characterize today's military tactical networks.

There is a large body of research in the NDN community that has focused on the application of NDN to communication environments where a data-centric model can be of benefit. This includes environments where data tends to be confidential (e.g. mobile health), ones where group communication (e.g. multi-party chat) tends to be the norm, and others where connectivity is ad-hoc and intermittent (e.g. vehicular networks). This body of research offers solutions that address some of the challenges of today's tactical networks, where data is sensitive and requires confidentiality/integrity measures, applications that adopt a group communication model (e.g. blue force tracking) are common, and network disruptions are frequent.

In this work, we leverage some of these solutions to introduce the concept of *Information Access Gateways* (IAGs), an enabler for a data-centric battlefield. An IAG enables the integration of non-NDN applications into an NDN network and offers name-based functionalities for their traffic. For instance, an IAG can use name-based filtering to control the flow of information based on a given access control policy. Also, an IAG can use NDN Sync to synchronize the data sets of applications that adopt a group communication model.

This paper is organized as follows. In Section II, we provide a quick overview of NDN and discuss related work. For a more detailed description of NDN refer to a companion NDN overview paper [2]. In Section III, we discuss the IAG and the services it offers. In Section IV, we use a notional tactical network to show how IAG services can be integrated into the network. We conclude our work in Section V.

II. NDN Overview

The motivation of NDN is to move away from today's host-centric approach to networking towards a more dynamic distribution network that focuses on data. This approach to networking better serves today's user communication needs. Today, users are interested in the speed at which content is retrieved (in addition to its authenticity) rather than who served it. Content Distribution Networks (CDNs) address these needs by deploying IP-overlays at Internet Service Providers to bring the content closer to their users. NDN addresses these needs from within by changing the network's objective and its underlying services.

†Author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

NDN uses structured names to name data items. Names are semantically meaningful to the applications producing and consuming them, while also used directly by the network that treats them as an opaque set of identifiers. For example, a part of this paper published in NDN could be named as "`/MITRE/papers/Milcom2018/Refaei/pdf /version=2/chunk=3`", assuming this PDF cannot fit into a single network-level data packet. To retrieve the data that corresponds to that name, a content consumer constructs an Interest packet containing that name. The initial request for this data will result in the Interest packet being forwarded by NDN routers towards the data producer. The corresponding Data packet will be sent back through the network along the reverse path followed by the Interest packet. Every router along that path may decide to cache the Data packet, subject to its local caching policy. Subsequent requests for the same data may be served directly from a router's cache rather than its producer [3]. When multiple consumers request the same data at the same time, their Interests will be aggregated further contributing to communication efficiency.

NDN provides substantial benefits to end-user latency by allowing data requests to be satisfied by caches along the path to the data source [4]. This can also decrease the frequency of data forwarding operations which in turn decreases traffic load in the network. Finally, it enables the network to function even when an end-to-end path to a data source does not exist by allowing data to be serviced from within the network when available. All of these functions make NDN an attractive approach to networking in tactical communication environments where network disruptions are common and data links are always constrained in bandwidth.

A. Related Work

An overview of NDN and its building blocks is provided in [2], [3]. In [5], a comprehensive survey of security approaches to information-centric networks is provided, ranging from mitigating DDoS attack to creating an access control framework. The authors in [6] propose a credential-based encryption access control framework where content producers must first authenticate to a trusted authority before they can publish content to a namespace. The namespaces themselves are subject to access control; however, there are issues of scalability in terms of coordinating and maintaining access control across a large range of namespaces. The work in [7]–[9] proposes a multi-level security scheme based on attribute-based encryption. The authors in [8] propose a framework where consumers request data, embedded with attribute-based policy and then issue Interests towards a proxy. In [9], the notion of manifest-based content retrieval is proposed where a consumer first retrieves a list of data names then issues subsequent Interests to retrieve the actual data. The same manifest-based mechanism is proposed for the retrieval of keys by each consumer by utilizing key-chains.

The work in [10], [11] adopts encryption as a mechanism for access control. They propose a scheme in which the data is encrypted and disseminated but the key needs to be separately and manually requested. In [10], the focus is on the questionable availability of the producer by having intermediary nodes act as proxies whenever the producer is not reachable. They propose re-encrypting data at different points in the network to ensure confidentiality.

Finally, the concept of name-based access control (NAC) is introduced in [12]. NAC enforces access control over the data directly rather than relying on data-stores or other dedicated services to provide the enforcement. The mechanism allows a producer to secure the content it produces by encrypting it and then controlling the distribution of encryption keys to consumers who are authorized to access it.

III. Information Access Gateway

In our previous work [4], [13], we have shown how enabling a data-centric battlefield through the integration of NDN can provide both resilience and performance improvements under disrupted network conditions. When comparing the performance of applications that provide situational awareness and file sharing in a disrupted TCP/IP tactical network, NDN improved end-to-end delivery, reduced delivery delay, and utilized bandwidth much more efficiently. Even when compared to transport services that are specifically designed to improve resilience to disruption (e.g., SCPS-TP [14], NORM [15], and TFTP [16]), NDN performed better.

We define Information Access Gateways (IAGs) to be both IP and NDN devices that are meant to enable tactical networks to realize the performance gains from employing NDN while maintaining interoperability with existing IP networks. We envision an IAG to be a device that can be dropped into the network and, with minimal configuration changes, interoperate with existing devices in the network. IAGs are preloaded (and updated over the air when possible) with a policy that dictates the services it provides. These services include integration of non-NDN applications, access control, and synchronization as shown in Figure 1. We discuss each of these services in the next subsections.

A. NDNization

One of the goals of an IAG is to "NDNize" non-NDN applications. This means facilitating seamless integration of IP applications into NDN networks. NDNizing a non-NDN application can be done by simply translating its traffic from IP into NDN and vice versa without disrupting its operation or behavior. An example of an NDNization configuration is shown in Figure 2, where the IAG is configured to intercept UDP traffic to port 2200 and create an NDN Data packet with the name */video/chunk* (with an automatically appended sequence number that starts at zero) from each intercepted UDP datagram. On the receiving end (not shown in the Figure), the IAG will be configured to instantiate a synchronization service (discussed in a subsequent section) to fetch data and deliver it over IP to the receiving applications. We have demonstrated this particular functionality of an IAG in our previous work [17]. Specifically, we have shown how an XMPP Overlay (XO) application [18] (which is designed for operation in tactical

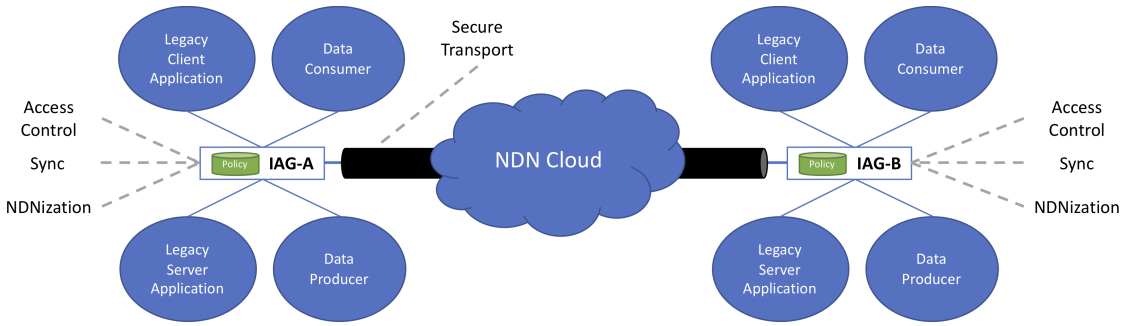

Fig. 1. Services Offered by an Information Access Gateway

networks) can be seamlessly integrated, with no configuration or code change, into an NDN network. We have also shown how XO benefited from NDN's disruption tolerance when operated in a disrupted network. The NDNization function is designed to be generic but configurable to recognize and translate specific application traffic patterns into NDN packets. Our experience has shown nevertheless that simple configurations can be created to NDNize simple applications (e.g., Cursor-on-Target [19], which we will illustrate in Section IV), but the configuration can be more complex for other applications such as web browsing where traffic tends to be more dynamic and conversational.

```
"producers": [
        {
        "class": "UDPProducer",
         "ip": {
                "application": "videostream",
                "protocol": "udp",
                "port": "2200"
        },
        "ndn": {
                "name": "/video/chunk",
                "argv": "default"
        }}
],
```

Intercept all UDP datagrams to port 2200

Translate to NDN Data packets with name /video/chunk/{counter}

Fig. 2. Illustration of the NDNization Service

B. Synchronization

Synchronization (Sync) is a concept that has evolved within the NDN architecture with the realization that there is a class of applications that operate asynchronously but require their datasets to be synchronized in a timely manner. Chat is an example of this type of applications that has presence in the battlefield. Sync services operate as NDN applications that ensure that specific datasets (i.e. name prefixes) are always synchronized. Whenever new data is generated by an application it is pushed to its local Sync service, which then informs other Sync services about the existence of new data. Remote Sync services then fetch the new data over NDN. This functionality simplifies end user applications as they do not need to fetch or deliver data but rather rely on the Sync service to do that on their behalf. Different NDN Sync protocols have been recently developed such as ChronoSync [20], VectorSync [21], PSync [22], and others [23].

The synchronization service offered by the IAG can either be pre-configured or offered upon demand. For instance, an IAG can be pre-configured to synchronize all chat NDN data if it is assumed that it will be needed by some or all applications operating within its domain. On the other hand, a synchronization service can be offered upon demand for a multi-party chat session that is instantiated dynamically to support an on-going mission. This is beneficial in a severely disrupted tactical network environment; one where a functional end-to-end path between a consumer and a producer may not exist at any point in time. This can be viewed as a realization of the concept of Named Function Networking (NFN) [24], which extends the notion of naming data to services and enables their instantiation as needed.

C. Access Control

Access control is a fundamental security requirement in tactical networks due to the sensitive nature of the data generated and exchanged. Various protection mechanisms are typically employed for the purpose of controlling access to data such as end-to-end encryption, packet filtering, as well as user authentication. In NDN, some of these mechanisms need to be replaced with others that fit the nature of a data-centric network. For instance, traditional packet filtering mechanisms based on addresses, port numbers, and protocols need to be replaced with others that operate based on names. Accordingly, IAGs utlize two name-based services to regulate access to data: authorization and filtering.

1) Authorization: In order to control access to data, an IAG performs authorization checks using names and identity information of consumers. When data is requested by a consumer, an Interest packet is sent from the consumer to its corresponding IAG (i.e., consumer IAG). The consumer IAG would then check the authorization policy (which defines how data can be accessed globally throughout the network) to check if the given consumer is allowed access to the data requested. To enable such a verification process, IAGs require all Interest packets to be signed. If a consumer is allowed access to that data, the request is either served from the IAG's local cache if that data is available or forwarded to another IAG where the data may be available. Otherwise, a NACK packet is generated and sent back to the consumer. This verification process is also applied at other IAGs through which the Interest packet

TABLE I
EXAMPLE NAME-BASED FILTERING POLICY

Action	Face ID	Filter	Description
Allow	1	"/mov/G"	allow access to G-rated movies
Allow	1	"/mov/PG"	allow access to PG-rated movies
Deny	1	"/"	deny everything else
Allow	2	"/"	allow everything

is forwarded. An additional level of authorization can be added by relying on mechanisms such as name-based access control [12], where access control is provided by encrypting the NDN Data and ensuring that decryption keys are only disclosed to authorized consumers.

2) Filtering: A name-based filtering service in a data-centric network is the equivalent of a firewall service in a host-centric network. It allows for regulating the type of data that flows between different parts of the network. For instance, a policy can be devised as shown in Table I for controlling access to movie data based on their ratings. Assuming all movie Data packets have a "`/mov`" prefix followed by a rating, this policy dictates which movies can be streamed through a given NDN face ("kids" devices are connected through face 1 while "adults" are connected through face 2).

D. Secure Transport

All IAGs communicate with each other over secure transports providing confidentiality and integrity for entire NDN packets (Interest, Data, and NACK). IAGs also use secure transports to communicate with consumers and producers as well. This ensures that the data is protected in transit between IAGs as well as between IAGs and producers/consumers. We rely on existing protocols, such as the Datagram Transport Layer Security (DTLS) [25] and the Media Access Control Security (MACSec) [26], that provide security for point-to-point channels to realize the secure transports. Note that secure transports can be cascaded to support the two-layers of encryption requirement mandated by the Commercial Solutions for Classified NSA program [27] for confidentiality of data.

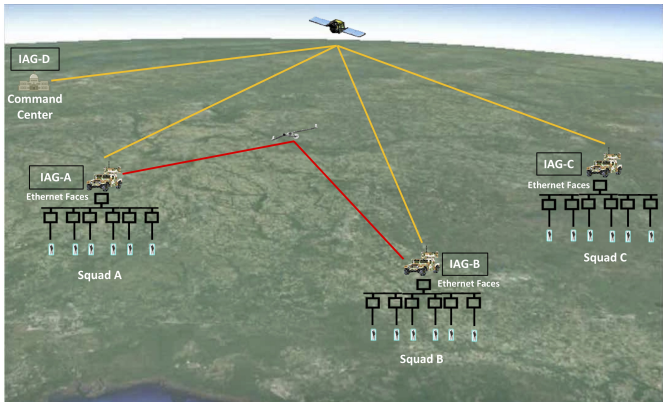

Fig. 3. Notional Tactical Network Scenario

IV. APPLICATION TO A NOTIONAL TACTICAL NETWORK

In this section, we consider the notional tactical network shown in Figure 3 and discuss how IAGs can be applied to it. In this network, a command center (top left) is connected to three different squads through a satellite link and three vehicles that serve as gateways to each of the squads. A drone provides additional connectivity between squad A and squad B. The producers of the data in this scenario are the soldiers within each squad. The consumers are both soldiers and the command center. We consider two applications used by the soldiers in each squad: (1) Cursor-on-Target [19] as a non-NDN application, (2) an NDN-based chat application. Squad A and squad B are participating in the same mission, so they are expected to be able to exchange track information. Nevertheless, the access control policy dictates that friendly tracks should not flow through the drone. The command center on the other hand should be allowed to receive tracks from all squads. Chat is allowed between all parties.

In order to realize NDN into this network, we place an IAG on all vehicles and at the command center and do the necessary configuration to make it function as the gateway node on each. This enables each IAG to process all ingress and egress traffic. We will assume that all NDN data produced by a given application will have the name prefix: "`/<squadId>/<deviceId>`". Routes to a given name prefix can be defined statically for a small network or simply rely on self-learning functionality of NDN [28]. Alternatively, an IAG can run a routing protocol like the Named Data Link State Routing Protocol (NLSR) [29] to advertise name prefixes.

In the next sections, we discuss how to NDNize CoT and the access control/Sync configuration for this network.

A. NDNization of CoT

CoT data is simple and can be easily NDNized. CoT messages are an XML representation of a target [19]. Information about the target is represented as an event and includes its type and location. The simplest approach to NDNize a CoT event is to use the key information that describes an event such as *type* and *uid* (event unique identifier) to construct a name. The name is then used to generate a Data packet that encapsulates the entire event in its content. Figure 4 shows a sample CoT event of a *friendly* ground target and how it can be NDNized. In the example, IAG-A intercepts all CoT data that is generated (UDP with destination port 18200) and produces an NDN Data packet out of each by applying a naming scheme that includes the squad (squad A) and the device identifiers (1290) as well as the *type* and *uid* fields. The IAG also can leverage the value of the *stale* field to set the freshness period of the generated NDN Data packet.

On the receiving end, an IAG generates a request for a synchronization service for the NDNized data. The configuration shown in Figure 4 instructs IAG-B to synchronize data with the name prefix */SquadA/1290/CoT/Event*. Any received data is then sent back over UDP/IP to a receiver at 10.0.0.1:1820. Note that multiple receivers can be defined or data can be sent out over to a multicast address.

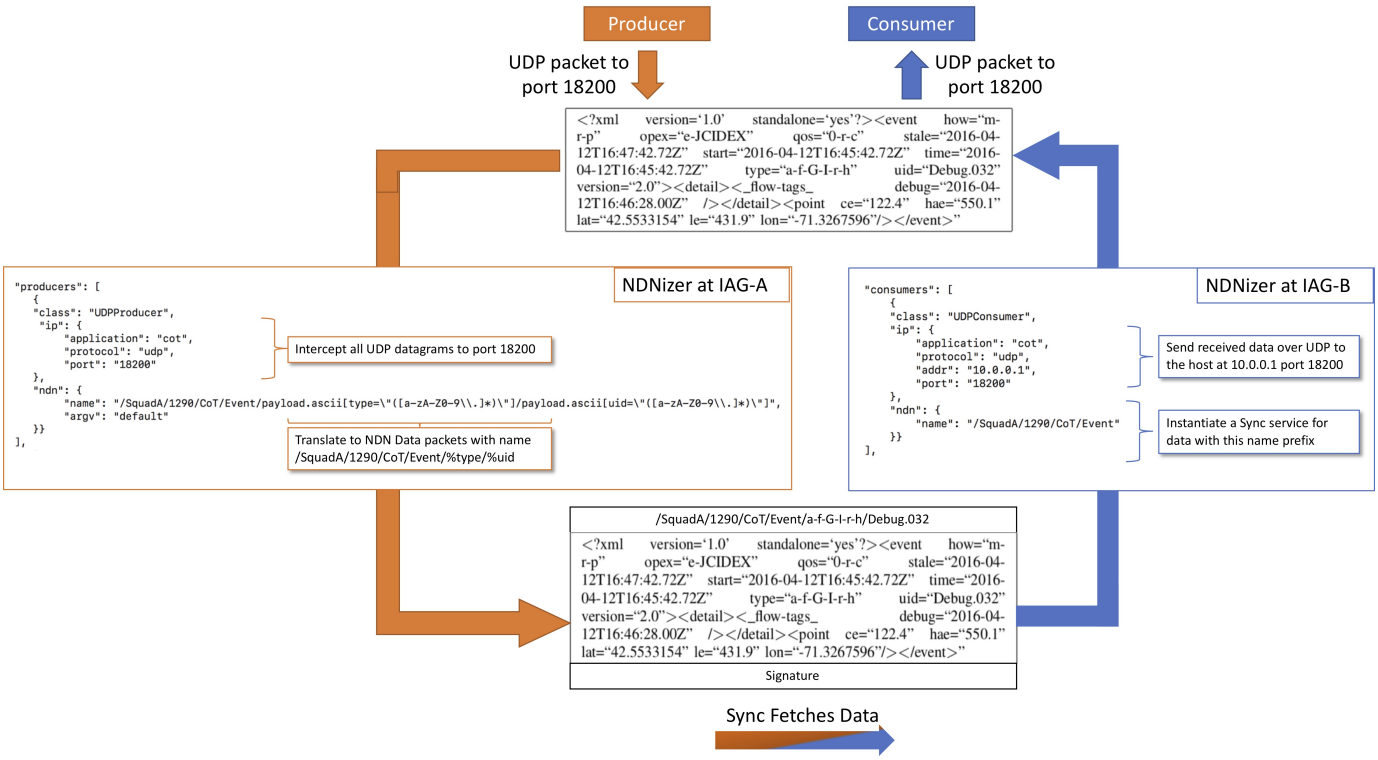

Fig. 4. NDNization of a CoT Event at IAG-A

B. Synchronization

As mentioned before, chat is an excellent example of an application where a synchronization service can prove to be beneficial. For global chat sessions, it makes sense to use a pre-configured synchronization service. For chat sessions that are instantiated dynamically based on mission needs, on-demand synchronization can be leveraged.

C. Access Control

In order to control access to data, NDN applications will need to be configured with a single Ethernet face pointing to its corresponding IAG. This creates a hub-and-spoke architecture where all Interest and Data packets flow through the IAG first before being serviced. To fully protect communication between the NDN applications and the IAGs, a secure transport based on MACSec can be used between each and its corresponding IAG. For a fully data-centric network policy, all data that is not NDN or does not have an NDNization policy (with the exception of control traffic) can be dropped.

For intra-IAG communication, a secure transport based on DTLS can be defined between each pair. Note that there will be two different transports defined between squad A and squad B to capture the fact that they are reachable through the satellite link (face 1) as well as through the drone (face 2). A policy that restricts CoT event of type *friendly* from being sent/received through the drone is shown in Table II.

TABLE II
COT NAME-BASED FILTERING POLICY FOR IAG-A

Action	Face ID	Filter	Description
Allow	1	"/"	allow all
Deny	2	"/*/Cot/Event/.-f-.*"	deny type "Friendly"
Deny	2	"/*/Cot/Event/.-a-.*"	deny type "Assumed Friendly"
Allow	2	"/"	allow everything else

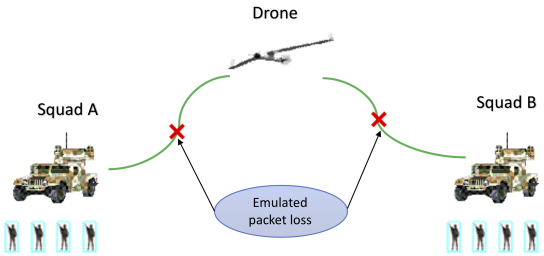

Fig. 5. Evaluation of IAG

D. Evaluation

We have implemented some of the functionalities of the IAG and demonstrated it in [30]. The current implementation supports the NDNization and the synchronization services only. Figure 5 shows an emulation of a portion of the network shown in Figure 3 where CoT events are sent from squad A to squad B through the drone. CoT was used without modification and generated approximately 100 tracks. The drone's mobility was structured such that it is connected to both squads A and B only 20% of the time. Otherwise, it is connected to only one

of them. As expected, when the IAG was not used, only about 20-30% of the tracks were delivered. When the IAG was used (on the vehicles and the drone), all trackes were delivered.

V. Conclusion and Future Work

In this paper, we have introduced Information Access Gateways, an enabler for a data-centric battlefield that provides a non-disruptive transition path from the host-centric approach to communication that is adopted by today's network and towards the more efficient data-centric model. IAGs facilitate seamless integration of tactical IP applications into NDN networks. We have discussed the design of IAGs and the services they offer. We have also implemented some of the services of the IAG and demonstrated in [30]. Our future plans are to incorporate additional services to the IAG (e.g. QoS service for name-based prioritization) and apply them to a representative tactical communication network to assess its benefits as well as integration challenges.

References

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

[2] A. Afanasyev, T. Refaei, L. Wang, and L. Zhang, "A brief introduction to Named Data Networking," in *submission to MILCOM 2018*.

[3] 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.

[4] M. T. Refaei, S. Ha, Z. Cavallero, and C. Hager, "Named Data Networking for tactical communication environments," in *Proc. of IEEE NCA*, Oct 2016.

[5] R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[6] B. Hamdane and S. G. E. Fatmi, "A credential and encryption based access control solution for Named Data Networking," in *Proc. of IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015.

[7] M. Ion, J. Zhang, and E. M. Schooler, "Toward content-centric privacy in ICN: Attribute-based encryption and routing," in *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*, 2013.

[8] R. S. da Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in Named Data Networking using attribute-based encryption with immediate revocation of privileges," in *Proc. of IEEE CCNC*, January 2015.

[9] J. Kuriharay, E. Uzun, and C. A. Wood, "An encryption-based access control framework for Content-Centric Networking," in *Proc. of IFIP Networking*, 2015.

[10] C. A. Wood and E. Uzun, "Flexible end-to-end content security in CCN," in *Proc. of IEEE CCNC*, Jan 2014.

[11] T. Chen, K. Lei, and K. Xu, "An encryption and probability based access control model for Named Data Networking," in *Proc. of IEEE IPCCC*, December 2014.

[12] Z. Zhang, Y. Yu, A. Afanasyev, J. Burke, and L. Zhang, "NAC: Name-based access control in Named Data Networking," in *Proc. of ACM ICN*, 2017.

[13] Milcom 2017 tutorial: A data-centric battlefield: Leveraging named data networks in tactical networks. [Online]. Available: https://named-data.net/publications/tutorials/

[14] Consultative Committee for Space Data Systems, "Space communications protocol specification-transport protocol," https://public.ccsds.org/Pubs/714x0b1c1s.pdf, May 1999.

[15] B. Adamson, C. Bormann, M. Handley, and J. Macker, "NACK-oriented reliable multicast (NORM) transport protocol," RFC 5740, https://tools.ietf.org/html/rfc5740, November 2009.

[16] "The TFTP protocol (revision 2)," RFC 1350, https://tools.ietf.org/html/rfc1350.

[17] T. Refaei, J. Ma, S. Ha, and S. Liu, "Integrating IP and NDN through an extensible IP-NDN gateway," in *Proc. of ACM ICN*, 2017.

[18] Naval Research Labs, https://www.nrl.navy.mil/itd/ncs/products/xo, June 2013.

[19] M. J. Kristan, J. T. Hamalainen, D. P. Robbins, and P. J. Newell, "Cursor-on-Target message router user's guide," The MITRE Corporation, Technical Report MP090284, November 2009.

[20] Z. Zhu and A. Afanasyev, "Let's ChronoSync: Decentralized dataset state synchronization in Named Data Networking," in *Proc. of IEEE ICNP*, October 2014.

[21] W. Shang, A. Afanasyev, and L. Zhang, "VectorSync: Distributed dataset synchronization over Named Data Networking," in *Proc. of ACM ICN*, 2017.

[22] M. Zhang, V. Lehman, and L. Wang, "Scalable name-based data synchronization for Named Data Networking," in *Proc. of IEEE INFOCOM*, May 2017.

[23] W. Shang, Y. Yu, L. Wang, A. Afanasyev, and L. Zhang, "A survey of distributed dataset synchronization in Named Data Networking," NDN, Technical Report NDN-0053, May 2017.

[24] C. Tschudin and M. Sifalakis, "Named functions and cached computations," in *Proc. of IEEE CCNC*, 2014.

[25] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," RFC 6347, https://tools.ietf.org/html/rfc6347, January 2012.

[26] "IEEE standard for local and metropolitan area networks: Media access control (MAC) security," *IEEE Std 802.1AE-2006*, Aug 2006.

[27] Commercial solutions for classified. [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/

[28] J. Shi, E. Newberry, and B. Zhang, "On Broadcast-based Self-Learning in Named Data Networking," in *Proc. of IFIP Networking*, 2017.

[29] L. Wang, V. Lehman, A. M. Hoque, B. Zhang, Y. Yu, and L. Zhang, "A secure link state routing protocol for NDN," *IEEE Access*, vol. 6, 2018.

[30] T. Refaei, J. Ma, S. Ha, and S. Liu, "Integrating ip and ndn through an extensible ip-ndn gateway," in *Proceedings of the 4th ACM Conference on Information-Centric Networking*, ser. ICN '17. New York, NY, USA: ACM, 2017, pp. 224–225. [Online]. Available: http://doi.acm.org/10.1145/3125719.3132112