* 1. **ICN**

(IITM, NPTEL-NOC, 2023), (Afanasyev, et al., 2018)

Information Centric Networking (ICN) is a content/data-driven approach to transferring information through a network. This is different from the traditional location-driven approach that TCP/IP adopts where IP addresses marking locations of sender and receiver are prerequisite to data transfer.

Following are 3 key ideas associated with ICN that facilitates achievement of main objectives of ICN being improving content accessibility, delivery efficiency, content availability and data authenticity.

1. **Content Naming**

Content naming is an integral part of ICN. It lies at the heart of content-driven data transfer.

Instead of senders and receivers in TCP/IP, ICN comprises puslishers and subscribers. Also, unlike TCP/IP where it’s the sender that drives transfer; here, it’s the receiver/subscriber that does this, as briefly explained below.

* When a **subscriber** requires a certain kind of data, it sends out an interest packet into the network with the “name” of the data it is looking for. The subscriber does not need to know where to find (at what address/device) to find this data.
* Data **publishers** create and introduce new data into the via **named** data packets.
* Devices in the network forward/propagate interest and data packets such that senders of interest packets with the same/similar “name” as existing data packets, receive them.

Thus, in ICN, content is retrieved based on names of desired data packets. This means content names must be globally unique and persistent. Following are popular namespace designs (strategies for naming data).

1. **Flat Naming:** This approach involves passing content to a hashing algorithm and then binding the resulting unique hash to the content along with a user generated name.
2. **Hierarchical Naming:** This convention is inspired from HTTP URLs where the name comprises portions each capturing some context regarding content separated by ‘/’s with added portions at the end that ensure uniqueness. Example: /edu/tcd/computer\_science/cs101/lecture.pdf/1 could be the name assigned to the 1st data packet related to a computer science lecture released by TCD. This type of naming is more human readable and is also more scalable than the previous one in that routers can match prefixes of the names instead of the entire name which in turn reduces size of forwarding tables.
3. **Attribute Based Naming:** This type of naming looks like HTTP GET requests. Names are created by combining various attribute values associated with a piece of data such as date, location, creator, etc.

This kind of data naming, in-effect decouples data from location, application, transportation, and storage (Datatracker, n.d.). This makes it possible to implement the following features.

1. **In Network Storage and Caching**

Nodes in an ICN network, may cache a copy of data packets that they receive and forward/use. This allows for replication. Thus, same data being available at different points in the network makes access more efficient (fewer hops required) and robust to failure (even one copy of data is unavailable, chances are, another node will have another copy of the same data). This replication and improved data availability and accessibility comes at the price of need for more storage.

1. **Content Level Security**

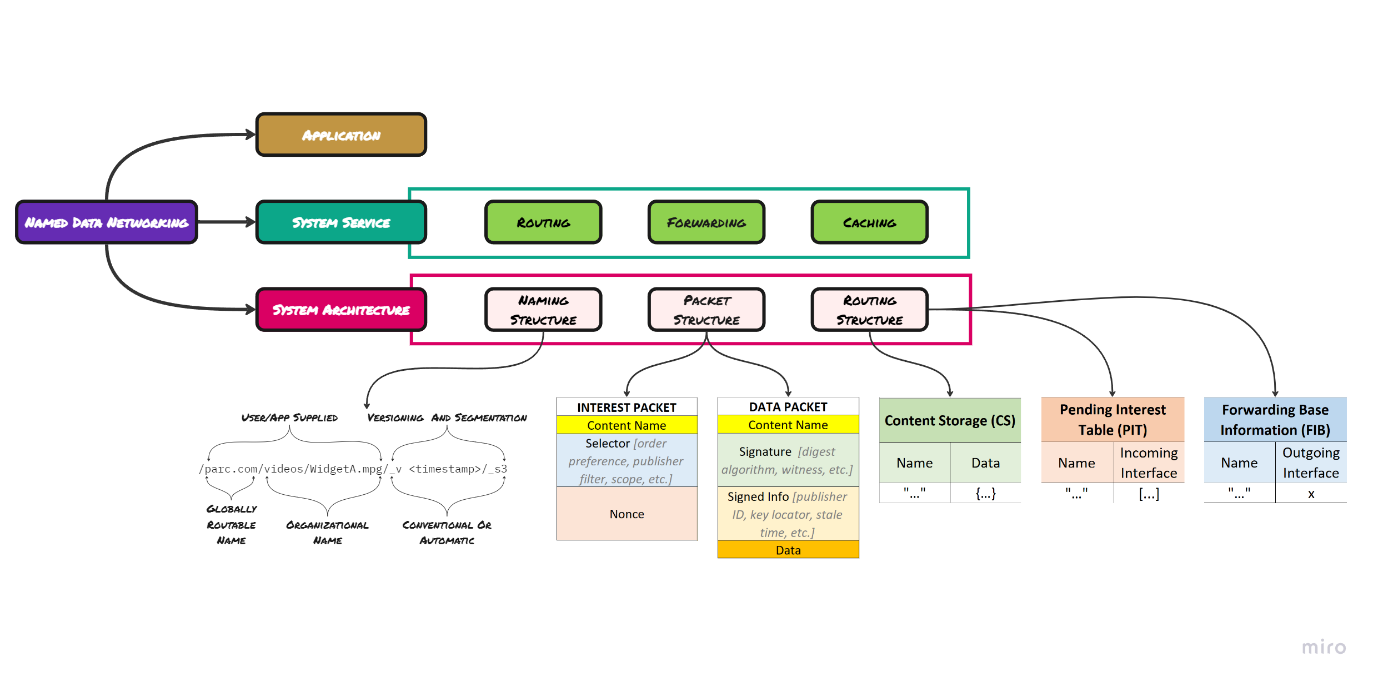
In TCP/IP security often involves securing the communication path though establishment of secure tunnels. But with ICN, it’s the data content itself that is secured (Fu, Kutscher, Misra, & Li, 2018). A simple approach to this would be to modify the classic Digital Signature Algorithm (DSA) (Scenes, 2023) each publisher adds a cryptographic signature to data packets. Subscribers verify signatures using the corresponding universal public key (all subscribers know about this key) to ensure content authenticity. Since the signature is a part of the data itself, every copy of it shall also contain the same signature. Thus, source of each copy of the data in the network can be verified (Bilal & Pack, 2020).

* 1. **NDN**

(Afanasyev, et al., 2018) (NPTEL-NOC IITM, 2023) (NPTEL-NOC IITM, 2023) (SG NDN Telkom University, 2021)

Named Data Networking (NDN) is a network architecture design that implements ICN principles.

Different applications may be built on top of the NDN architecture with characteristic naming, packet, and routing structures by leveraging system services like routing, forwarding, caching, etc, that it facilitates (SG NDN Telkom University, 2021).



**Naming Structure**

NDN does not enforce strict namespace management rules as part of the architecture. This gives one the freedom to experiment. As long as the end points in a network follow the same name assigning and querying convention, NDN can be adopted. That said, typically, NDN implementations follow a hierarchical naming convention.



**Packet Structure**

Packets may be of 2 types. An interest packet, and a data packet.

An interest packet comprises content name and can also contain conditions/rules for network devices to consider during forwarding/routing such as order in which data packets are expected, time for which this packet is valid, etc along with a nonce that facilitates linking of data packets to the interest packet that requested it.

A data packet contains content name and the data payload itself. Additionally, it may comprise meta information like the kind of content the packet contains (size, audio/video etc.), as well as security imbibing data like the signature, key locator, digest algorithm, etc.

**Forwarding/Routing Structure**

Forwarding/routing in an NDN setting is facilitated by 3 key tables/mappings as given below.



The Content Store (CS) maps content name to data received. This often acts as the cache. When a node does not contain requested data, it maps content identifier of received interest to one or more incoming interfaces in the Pending Interest Table (PIT) to keep track of all interested parties for a specific content. The Forwarding Information Base (FIB) table maintains a dictionary of interest packet content names mapped to the outgoing interface that it was forwarded to.

**Caching**

NDN implements in-network caching which means that network devices may choose to store a copy of content received within data packets locally. This means that on subsequent hits, a subscribers can find data previously requested by itself/another subscriber on a device that is physically closer to itself (reachable in few, ideally a single hop). This greatly reduces response time. However, there must be some mechanism to clear the cache from time to time to minimize storage overhead.

**Forwarding/Routing**

The core idea behind flow of packets through an NDN based network can be summarised as follows.

|  |  |
| --- | --- |
| *Receive Interest Packet* | *Receive Data Packet* |
| 1. Check CS. 2. If corresponding data is found in CS, send this data in a data packet to interested party/parties. 3. Else, add interested party to PIT. 4. Check FIB to see if known outgoing interface for this interest exists. 5. If so, forward packet out through this interface. 6. Else, pick a suitable interface (not the one the interest came from) to forward the packet to if possible. 7. If valid outgoing interface identified, populate FIB and forward interest packet our chosen interface. | 1. Check PIT for any parties interested in received content. 2. If no pending interest is found, drop packet. 3. For every pending interest found, forward data packet. 4. Possibly cache content in CS. |

All data transfer, staying true to ICN, is receiver driven. Whenever a node (subscriber) requires information, it sends an interest packet into the network for corresponding data packet. Network devices then forward this interest packet until it gets to a node which contains requested data (publisher/in-network cache). This data then arrives back to the subscriber via reverse path forwarding (right hand side column in above table).

# References

Afanasyev, A., Burke, J., Refaei, Wang, T., Zhang, L., Zhang, B., & Lixia. (2018). A Brief Introduction to Named Data Networking. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*.

Bilal, M., & Pack, S. (2020). Secure Distribution of Protected Content in Information-Centric Networking. *IEEE Systems Journal, 14*(2), 1921-1932. doi:10.1109/jsyst.2019.2931813

Datatracker. (n.d.). *Charter for Research Group* . Retrieved from datatracker.ietf.org: https://datatracker.ietf.org/rg/icnrg/about/

Fu, X., Kutscher, D., Misra, S., & Li, R. (2018). Information-Centric Networking Security. *IEEE Communications Magazine, 56*(11), 60-61. doi:10.1109/mcom.2018.8539022

IITM, NPTEL-NOC. (2023, May 12). *Information Centric Networking - Part 1*. Retrieved from YouTube: https://www.youtube.com/watch?v=F\_NpB6trbzo&list=PLyqSpQzTE6M9voigbAaFzKiybgN7Xgvka&index=64

NPTEL-NOC IITM. (2023, May 12). *Information Centric Networking - Part 2*. Retrieved from YouTube: https://www.youtube.com/watch?v=aVZw1Qd6RLo&list=PLyqSpQzTE6M9voigbAaFzKiybgN7Xgvka&index=65

NPTEL-NOC IITM. (2023, May 12). *Named Data Networking - Part 1*. Retrieved from YouTube: https://www.youtube.com/watch?v=OM-cBILswZk&list=PLyqSpQzTE6M9voigbAaFzKiybgN7Xgvka&index=67

NPTEL-NOC IITM. (2023, May 12). *Named Data Networking - Part 2*. Retrieved from YouTube: https://www.youtube.com/watch?v=Eh5yHPeqBI0&list=PLyqSpQzTE6M9voigbAaFzKiybgN7Xgvka&index=69

Scenes, B. B. (2023, January 17). *What is Digital Signature Algorithm ?* Retrieved from medium.com: https://medium.com/@21\_000\_000/digital-signature-algorithm-60c8318cf9b6

SG NDN Telkom University. (2021, October 2). *NDN vs IP*. Retrieved from YouTube: https://www.youtube.com/watch?v=ud9YOlekH6c