**Intro**

* Can be used for low extensive embedded devices
* Due to lack of resources current structure have overloads and packet loss.
* NDN a request-response scheme can be used to solve this problem.

**Security and Safety**

* Current structure rely on private cloud with dedicated users with a “secure communication channel”.
* As users increase with different data access permissions ,we cant rely only on channels.
* Solution “protect data instead of way of transmission”.
* In Emergency we can not rely for information with a single uplink.
* Embedded devices have limited capability so vulnerable to DDoS attacks.
* ICN provides ability to recover locally and confine attack to only end devices.

**Security by NDN**

Data access

* Data is stored in both gateway and nodes.
* Network is Delay Tolerant.
* Ability to recover.

Robustly secure network

* NDN encrypts content instead of channel.
* Data chunks are stored at nodes and can get delivered whenever internet connectivity is back.

DDoS

* Initially assumed it to be a completely DDoS resistant architecture but that was not the case.
* Can be done by User generated names and content Requests.
* Can be prevented by pre configuring PIT tables according to well understood communication flows.

**Comparison**

MQTT

* Publish Subscribe protocol where message is deleted after delivery.
* MQTT-SN for low end IoT devices.
* No end to end security between publisher and subscriber threatens message integrity

CoAP

* Constrained Application protocol.
* Use polling, push and observe operations.
* Servers are maintained by single administrator so it can vulnerable. While in ICN attacking specific content source is important.

Caching

* IN CoAP and ICN not in MQTT

Packet delivery

* Most successful in NDN.

Object Security

* In built security in ICN, trust not based on contracts.

Infrastructure

* Amplification attack on spoofed ip(victim) in CoAP(due to UDP) but difficult in MQTT(TCP) but not in MQTT-SN(UDP).
* While in ICN there is no End-To-End.

End Node Protection

* MQTT and CoAP both vulnerable to end to end but here ICN is not end to end thus protect end devices.

Name privacy

* Neither in MQTT nor in coAP.
* For now not even in ICN.

**Expenses of content Security**

* Signing and verifying chunks using light weight SHA-256 keyed with hash message authentication code(HMAC).
* Processing time in miliseconds but just a few packets sent per second so not a problem.
* Energy constrain may be there.