In Class Assignment

21_AIE_302

Advanced Computer Networks– SEM-V

Professor – Jaysooraj Sir

Submitted By: Vikhyat Bansal [CB.EN.U4AIE21076]

Information-Centric Networking for The Internet of Things

Introduction

The definition of the Internet of Things (IoT) is still under debate, but there is a large consensus on attributing IoT a primary role in providing global access to services and information offered by billions of heterogeneous devices (or things), ranging from resource-constrained to powerful devices (and/or virtualized everyday life objects) in an interoperable way.

Despite great efforts and valuable achievements, the large-scale deployment of IP-based IoT solutions still provides challenges. The limited expressiveness of IP addressing simultaneously serving as locator and identifier, the need for a resolution system, complex mobility support, multicast, and massive access under the stringent performance requirements of IoT (e.g., scalability, energy efficiency) are just a few examples.

ICN v/s IP based networking

Information-centric networking (ICN) has been recently proposed for this purpose and is inspiring the design of the future Internet architecture. Unlike the IP-address-centric networking of the current Internet, in ICN every piece of content has a *unique*, *persistent*, *location-independent name*, which is directly used by applications for accessing data. This *revolutionary* paradigm also provides content-based security regardless of the distribution channel and enables in-network data caching.

ICN matches a wide set of IoT applications that are *information-centric* in nature, since they target data regardless of the identity of the object that stores or originates them.

For example, road traffic/environmental monitoring applications are oblivious to the specific car/sensor that provides the information. ICN *names* can directly address heterogeneous IoT contents and services, such as vehicular/home services and environmental data. Unlike IP addresses, such names are independent of the location of content/service producers, thus facilitating delivery operation in the presence of nodes mobility.

By caching data closer to consumers, ICN can reduce data retrieval delay and network load, and limit massive access to resource-constrained devices. For instance, once home appliances have been triggered about their energy consumption, the retrieved information can be cached at intermediate nodes and be available for later requests.

Information-Centric Networking

Common core of ICN principles that can be summarized as follows:

- Content-based naming and security
- In-network caching
- Name-based content discovery and delivery
- A connectionless receiver-driven communication model

In the given figure below, Therein, ICN consumers (C1 and C2) specify which named content they seek and not where it is provided. Both hierarchical and fl at names are possible in ICN, with the former appearing as uniform resource identifier (URI)-like identifers with variable lengths, while the latter comprises fixed-length identifiers with no semantic structure. Moreover, the use of unique names makes each content packet a self-identifying unit and drives request forwarding toward content provider(s) (typically the closest one), thus enabling anycast retrieval.

Content-based security makes each data a self-authenticating unit, with protection and trust implemented at the packet level rather than at the communication channel level. The security mechanisms are closely related to the naming scheme. When hierarchical naming is used, security-related information (e.g., the publisher signature) is embedded into a separate field of the content unit, thus requiring a public key infrastructure (PKI) for integrity checks. Flat namespaces instead enable the use of self-certifying names, allowing integrity checks without the need for a PKI.

Since each data packet is self-consistent, in-network caching is enabled, with potentially every network element caching the processed data packets and making them available for future requests; for example, consumer C2 in figure below is immediately served by router R6.

Distributed caching makes communication connectionless by not requiring consumers and producers to be simultaneously connected.

In contrast to the current Internet, where senders control data transmission, ICN data retrieval is receiver-driven, consisting of two phases: the discovery triggered by a consumer to find the content or its replication, and its delivery back to the interested consumer. Content discovery can be supported in two main ways: via name-based routing (NBR) or through a look-up-based resolution system (LRS).

With NBR, the consumer sends a content request packet (i.e., the so-called Interest), hop-by-hop relayed by the forwarding nodes by looking up a name match into their forwarding information base (FIB). Once the content is found, it follows the soft-state traces on the reverse path back. By recording the pending requests until the Data packets are received, each forwarder can measure delivery performance
(e.g., round-trip time) and, in case of problems (e.g., when losses or delays are detected), promptly try alternative paths.
Therefore, the forwarding plane can be considered intelligent and adaptive: it can deal with short-term churns, while the routing protocol only deals with long-term topology changes.

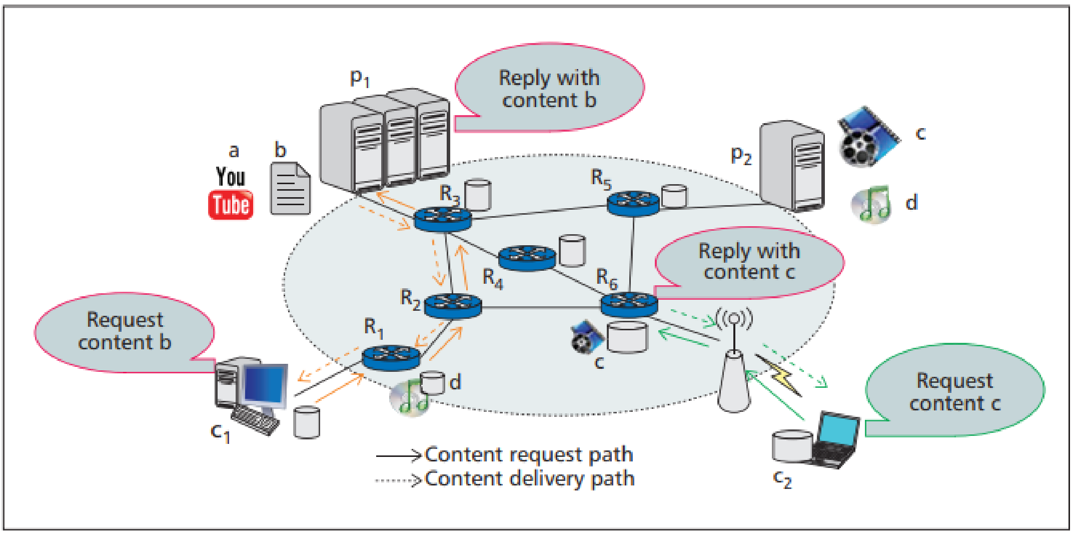

Figure 2. Content exchange in ICN: consumers request contents that can come from any source holding a copy of them (either the original provider or a caching node).

Using ICN for IOT

Main IOT requirements are:

- **Scalability**

  Feature: In the presence of an upcoming and increasing explosion of data/signalling packets generated by billions of connected devices. The forefront of typical IP-based content retrieval mechanisms (e.g., peer-to-peer, P2P, and content delivery networking, CDN) poses complex issues, such as suboptimal peer selection or their incapability to leverage in-network storage, in such scenarios.

  ICN Prospect: By offering name resolution at the network layer and forwarding content by its name, ICN also has the potential to reduce the signaling footprint in IoT deployments. Concretely, ICN nodes have the ability to identify requests for the same named information, avoiding the need to forward them differently on the same path. In addition, content becomes cached in traversing nodes, allowing requests to be satisfied by the first available copy, preventing source over-querying and supporting connectionless scenarios. Finally, ICN allows data to be transmitted to multiple consumers by using native anycasting and multicasting.
  However, the utilization of these mechanisms in IoT environments also has the potential to raise scalability issues of their own, under debate by the ICN community [2]. Concretely, ICN name-based mechanisms are made available regardless of the content location, which can limit different scenarios. Considerations on extending information naming to also identify devices can actually draw solutions that reduce the applicability scope of ICN, as it would be trying to mimic the host-based behavior of TCP/IP. Moreover, the amount of content names is orders of magnitude larger than the number of hosts connected to the current Internet, meaning that the routing and naming capabilities of ICN face a much more difficult task when compared to the current global routing and Domain Name Service (DNS) resolution services.

- **Quality of Service**

  Feature: Due to the high heterogeneity of IoT use cases, quality of service (QoS) requirements can be very different. For instance, sensing requires the exchange of typically small data, either in an event triggered (e.g., an alarm) or periodical (e.g., traffic monitoring) manner. Some sensing data require timely reception (e.g., in case of an alarm), while others may tolerate longer delivery delays (e.g., home temperature monitoring). Some IoT applications also account for data freshness needs, for example, when consumers are interested in the latest instance of a constantly upgraded content (e.g., a hospital needs updated vital signs of a remotely monitored patient) vs. an available older copy in a nearby cache point.

ICN Prospect: ICN has the potential to improve the quality of content retrieval and manage different QoS demands. The native support of in-network caching, anycasting, and multicasting all together contributes to speed up data retrieval and reduce traffic congestion. Moreover, every ICN design is able to perform advanced and efficient forwarding mechanisms. For instance, architectures with LRS may leverage knowledge of the network topology to compute optimal delivery paths (e.g., PURSUIT). Vice versa, architectures with NBR may leverage the adaptive forwarding capability to react to early signs of network problems (e.g., NDN).

- **Security**

Feature: Enabling security services in IoT is fundamental, since most IoT applications have the potential to affect our personal daily lives, and are not deployed in isolation but are exposed to external controls on the Internet.

ICN Prospect: By offering security support at the network layer, ICN facilitates content sharing between nodes since data authentication and integrity can be verified locally, removing the need for trusting in intermediary nodes. In addition, by securing the content itself, ICN can restrict data access to a specific user or a group of users.

- **Energy Efficiency**

Feature: Resource-constrained IoT devices have severe limitations on power and computing capabilities, as well as on networking functionalities. Most embedded devices spend a great part of their lifetime in sleep mode and only awake when they need to exchange data. Therefore, energy-efficient operation design is crucial for any IoT networking solution.

Current energy efficiency approaches are not handled at the network layer, being targeted at the medium access control (MAC) layer or above the transport layer. For example, the Constrained Application Protocol (CoAP) from CoRE provides a web framework realized through a subset of Representational State Transfer (REST) primitives. By running over UDP, it provides a lightweight transport solution with no connection establishment phase and small overhead. However, CoAP targets a limited class of applications (i.e., manipulation of simple resources) and requires devices to support a full web stack implementation, which might be prohibitive for different devices. Moreover, strategies such as header compression done in 6LoWPAN can imprint processing requirements over low-powered devices.

ICN Prospect: The receiver-driven communication model of ICN, coupled with any-casting and in-network caching, can help retrieve contents even in constrained networks with low duty-cycle providers. In fact, a request can be satisfied by another node, holding a copy of the data, when the producer is in doze/sleeping mode. Furthermore, distributed caching may avoid massive data access to constrained devices, thus saving energy resources. Native multicasting also matches the goal of reducing the amount of traffic and interactions with energy-constrained nodes.

- **Mobility**

Feature: Mobility support is a key requirement, for example, when IoT devices move aboard vehicles or are carried by humans.
IP mobility management solutions (e.g., Mobile IP) have been under continuous research, especially due to the explosion of mobile terminals. However, they have been commonly associated with scalability problems, leading to more efficient solutions (e.g., distributed mobility management), which have yet to reach adoption by mobile operators. In any case, the validity of such approaches in IoT scenarios has yet to be proved.

ICN Prospect: ICN supports consumer mobility: when a consumer relocates, it can simply re-issue any unsatisfied request/subscription and be served by a different node. Moreover, ICN natively supports host multi-homing, so content requests or data delivery can use any of the interfaces (or even all simultaneously) available at the device. In general, producer mobility entails additional signalling in ICN: it requires updates in intermediate forwarders (in the NBR case) or in entities managing name resolution. Such procedures may generate delays and disruption periods; however, any-casting, in-network caching, and multi-homing may greatly help in coping with the issue.

- **Heterogeneity**

Feature: IoT is expected to be a highly heterogeneous environment, with a rich variety of devices, technologies, and services involving different stakeholders and manufacturers. The Internet will be traversed by huge amounts of IoT data generated by networked devices with widely different traffic characteristics.
This implies added challenges to network providers regarding infrastructure planning, considering that the full extent of upcoming global IoT traffic is still unknown. Despite the flexibility of the narrow-waist design of IP and its ability to maximize interoperability, it becomes complex to apply common network functionality to the explosive number of technologies involved in the upcoming IoT.

ICN Prospect: Standardized ICN naming schemes for IoT would allow abstracting services and contents in order to hide the heterogeneity in underlying networks and devices, and facilitate interoperability among different players. For example, ICN naming has the potential to allow entities to request content by its name, independent of the type of service that provides and transports it from the source — message queuing telemetry transport (MQTT), CoAP, and Advanced Message Queuing Protocol (AMQP). Furthermore, by decoupling consumers and producers and delivering self-consistent data packets, ICN can interconnect information, devices, and services under heterogeneous network scenarios.

Challenges and Opportunities based on ICN protocols

- ### Naming

An ICN naming scheme for IoT should be highly expressive and customizable, and it should expose service (e.g., sensing and action) and data features.

Hierarchical names have been mainly considered in the literature to support such properties.The basic idea is to define a hierarchy of name components that identify the IoT application (e.g., building management system, energy control) and the attributes that describe the related contents and services.

Similarly, in the case of actuation applications, commands/management parameters can be provided as named components.

Flat names are typically obtained through hash algorithms applied to (already existing) contents and can hardly be

assigned to dynamic IoT contents that are not yet published.

Differently, hierarchical names facilitate the request of dynamic contents that are generated on demand (e.g., a parameter measured by a sensor), provided that naming conventions have been specified during the system configuration/setup.

Through the hierarchy of name components, a simple versioning system can be deployed to manage those cases where a producer constantly updates the content value, like the temperature in a room

However, hierarchical names are subject to length constraints, for instance, to fit the maximum payload size of some protocols such as ZigBee.

By sharing a common name prefix for multiple contents services, hierarchical names scale better than flat names, since they facilitate the definition of name aggregation rules in the FIB, which is critical for big data. This implies that IoT applications operating in the same domain and handling information/ services with global scopes should be designed by developers

with common (shared) name-prefixes. In ICN deployments dealing with Internet contents, name prefixes are usually related to the top-level and second-level domain names that identify websites and their contents; for example, the prefix youtube.com is associated with every Youtube video.

- **Security**

ICN security mechanisms that consider the unique features of IoT applications and device limitations must be defined. First, some IoT applications require queries from consumers to be authenticated; for example, an actuator will executean action, such as turning-on/off appliances, only if this is required by a trusted authorized entity. Currently, ICN security mechanisms are only applied over data packets and do not support request authentication. Second, IoT devices with low processing and memory capabilities hardly use resource-intensive public key cryptography.Specific lightweight solutions for encryption and authentication become fundamental for resource-constrained devices.

In this context, symmetric cryptography can be useful . The disadvantage lies in the inflexibility with respect to key management, as it requires pre-distribution of keys. A good tradeoff between complexity and resource saving can be obtained by elliptic curve cryptography, the prevalent public key scheme currently considered for small devices.

Generally, ICN security functions for IoT must be flexible in the selection of cryptographic techniques, since there is no one-size-fits-all solution; the most appropriate one shall be chosen.

- **Caching**

In-network caching acquires special significance in IoT domains. On one hand, caching is generally beneficial because it speeds up data retrieval and increases its availability. On the other hand, caching and related replacement operations can be quite expensive in terms of both processing and energy consumption. Therefore, a first question is whether caching should be enabled in any IoT device or only in powerful nodes.

A simple design choice would forbid constrained devices to cache contents , but in caching proved to be highly beneficial even when enabled in IoT nodes with small storage capacity. In fact, it reduces the number of (lossy) hops toward the producer by limiting the network load and the overall energy consumption. In addition, caching is viable since data generated by IoT. Overall, IoT data can be cached in network routers and resource-constrained devices by implementing caching decision and replacement policies that account for the peculiarities ofIoT traffic, for example, compatibly with freshness requirements and device capabilities (e.g., residual battery level and storage).

In addition, ICN may resort to off-path caching (according to which caching points are along alternative paths) to alleviate the load on constrained IoT devices and proactively distribute contents in specific locations (e.g., the cloud) by preventing data redundancy at the cost of additional overhead for cache management.

- **Discovery and Delivery**

Name-based routing and lookup-based resolution systems offered by ICN for content discovery may suit specific IoT scenarios, mainly depending on the content characteristics (e.g., popularity, dynamic generation) and network features (e.g.,infrastructureless vs. infrastructured).

The downside of deploying NBR is mainly related to the growth of the FIB size and routing updates in the case of a huge number of names, and the overhead of maintaining the soft-state. However, name-prefix aggregation can successfully cope with such challenges, together with adaptive forwarding.

In summary, NBR and LRS solutions may complement each other. Hence, by leveraging cloud computing, multi-level DHT, name-prefix aggregation and adaptive forwarding, an effective discovery and delivery platform can be provided with the potential to scale even for a huge number of IoT resources.

- **Morphing**

ICN node does not (and should not) provide any data transformation (aggregation, filtering, etc.), because it should be kept outside the ICN domain to reduce inside complexity and function overloading. Notwithstanding, even if not explicitly mentioned among the ICN core principles,

ICN could enable lightweight in-network data manipulation (we call it morphing) at intermediate nodes, by embedding semantics awareness at the networking layer.

The motivations for data morphing are manifold and particularly strong for IoT. First, there is a high abundance of raw data in the network, but consumers are likely to want to receive manipulated data. Second, morphing greatly simplifies data post-processing for those applications that either operate on aggregated data or need a complete knowledge base without information loss. Third, filtering/aggregating data helps to improve the scalability in content retrieval and reduce the network and device resource usage.

Hierarchical names could facilitate data aggregation and enable intermediate nodes to track and process packets, while meeting latency and accuracy demands. The requester could explicitly ask to retrieve aggregated data, allowing the network to select the best nodes providing them.

Otherwise, more powerful nodes perform such tasks in a transparent way for the consumers (e.g., a concentrator replies to the utility company with aggregated energy consumption data from multiple users). Morphing would be expected only at carefully selected locations in order to trade off between effectiveness and computational resource demands.

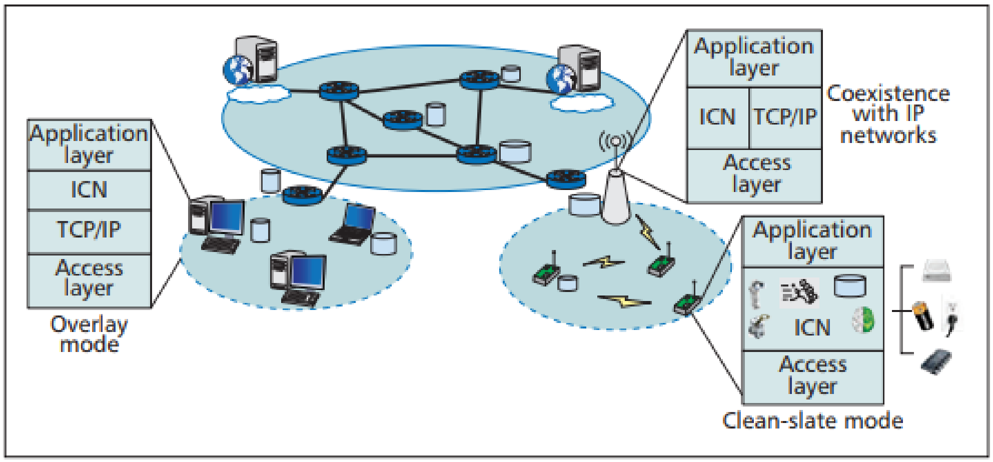

Figure 3. Main deployment options.

Conclusion

ICN solutions can be deployed as overlay over the existing IP infrastructure, or as clean-slate implementation directly over access layer technologies to replace IP. Overlay solutions are discouraged due to their complexity and the overhead for overlay management and encapsulation inside IP protocols. This is also inadvisable for resource-constrained devices, representing a high percentage of IoT objects. A clean-slate solution can easily be deployed where there is no need to communicate with IP-based nodes (e.g., in isolated vehicular environments) or to maintain backward compatibility, but it raises concerns when global access and connectivity are required. A most likely short-term design would allow coexistence with IP-based technologies. Similarities between ICN hierarchical names and URIs of web resources could facilitate such coexistence. The translation between them may be implemented easily in the node (e.g., a smart home gateway) interfacing ICN islands and the rest of the Internet. In conclusion, we can state that ICN holds promise as a candidate networking solution for IoT.

THANK YOU!!!