ICN SUITABILITY FOR THE INTERNET OF THINGS

Nicholas Clark

C4I & Cyber Center, George Mason University, Fairfax, VA 22032, USA

ABSTRACT

The Internet of Things (IoT) refers to the billions of hardware devices that connect to the internet around the world. Mobility support, interoperability, scalability, and security are critical challenges for the Internet of Things (IoT). Recent research shows that Information-Centric Networking (ICN) is an emerging paradigm as an alternative Future Internet architecture that has the potential to solve these problems holistically. The central premise behind ICN is a fundamental change from host-centric based communications to content-centric with name-driven networking primitives that natively support multicast, mobility, and content-oriented security. However, there remain challenges in securing the ICN-IoT. This document describes the deficiencies of existing Internet, an ICN architecture, the characteristics that make it well-suited for the IoT, then summarizes a proposed architecture for securely instantiating devices into edge networks.

KEYWORDS

Internet of Things, IoT, Information-Centric Networking, ICN, Networking

1. INTRODUCTION

Many of the current problems with the Internet are a natural consequence of its architecture, which was designed to address communication needs in a time when the network was needed for sharing resources that were expensive and finite, such as mainframe computers. In the beginning, the Internet's essential function was to forward packets among a small number of machines that remained stationary with well-defined trust relationships. The fundamental design principles of the Internet made it very simple to link new networks and facilitated rapid growth. Concurrent to that growth, there were extraordinary innovations in the services and applications able to run on it, and in the development of technologies below the network layer that have emerged. This can be traced to the hourglass-shaped architecture (shown in Figure 1) into which the Internet stack has evolved and the Internet Protocol (IP) network layer forms its waist (Akhshabi et al, 2011).

Figure 1. Incomplete illustration of the hourglass Internet architecture

Over time, the growth of the Internet and the introduction of new applications to meet emerging needs gave rise to new requirements not met by the existing architecture, such as security, trust, mobility support, scalable content distribution, etc. A cycle of functional patches was introduced to address these new requirements that continue today. Whenever the Internet faces a new challenge, new patches are added to (at least partially) solve the problems. At the same time, many current and emerging requirements still cannot be addressed adequately by the existing Internet.

According to the Cisco Visual Networking Index forecast, video traffic will compromise 82% of global Internet traffic by 2022 (Cisco, 2017). The majority of this traffic is currently served to end-users via content delivery networks (CDNs), which are essentially application-layer overlays that cache content on servers near the network edge in order to reduce core network traffic and latency. Cisco expects that by 2022, 71 percent of all Internet traffic will be carried through CDNs (Cisco, 2017). CDNs represent the best current practice to manage this rapid growth. However, they require substantial infrastructure investment, are often application and provider-specific. Despite the benefits to scalability that CDNs have thus far provided, the current host-centric paradigm will not continue to scale with the rapid proliferation of mobile devices and the IoT coupled with the rapidly growing volume of video traffic.

Many of these pressing challenges are deeply rooted in the early design decisions of the Internet and may not be entirely solvable without a fundamental rethinking of its architecture. Many of the security problems relate to the Internet's weak notions of identity, such as the ease of spoofing everything from IP addresses to domain names, email addresses, and routing information. Mobility is challenging to handle because IP addresses are hierarchical and tightly coupled with the scalability of routing protocols. Breaking this coupling may require a new relationship between naming, addressing, and routing (Rexford, Dovrolis, 2010). These issues bring into question whether the approach of continuing to patch over existing patches is the best way to continue or whether a new clean-slate or green-field architectural approach might be needed. Towards this purpose, several research communities have formed, having identified architectural limitations in the current Internet, are working towards the development of new architectures and paradigms for a Future Internet (Pan et al, 2011).

2. INFORMATION-CENTRIC NETWORKING

Information-Centric Networking (ICN) has emerged as one promising candidate for the architecture of the Future Internet. ICN is rooted in the fact that the Internet is increasingly used for the dissemination of information (content distribution) rather than point to point communication between end hosts. An ICN architecture aspires to better reflect the current and future needs better than the existing one by meeting the demands for highly scalable and efficient distribution of content. In an ICN, the networking paradigm is switched from host-centric, where all requests for information are made to a host identified by its IP address(es), to a content-centric one, which decouples named data objects from the hosts that serve them. By naming information at the network layer, ICN favors the deployment of in-network caching and multicast mechanisms, allowing data to be delivered more efficiently and timely to requesting users.

The named data networking (NDN) project (Zhang et al, 2009) is one ICN architecture that offers capabilities that are useful to the IoT. In the NDN model, there are chunks of data known as content objects that make up the thin waist in place of the one in Figure 1. Each content object has a unique name, similar to a uniform resource locator. Naming in NDN uses a hierarchically structure but otherwise arbitrary data identifiers. The content linked to a name is usually considered immutable. To retrieve the desired content object, an interest packet is sent by the requestor to the network. The interest packet must contain at least the name of the desired content object, but it can also include a signature to verify the identity of the requestor. The network retrieves the suitable content object and delivers it back to the requestor in a data packet. The data packet must contain the name, its content, and the signature of the publisher, which allows the requestor to verify the authenticity and integrity of the content object.

The NDN network includes content routers (CR) that maintain three data structures: pending interest table (PIT), forwarding information base (FIB), and content store (CS). These tables determine the forwarding procedures for interest and data packets. When an interest packet is received, the CR first looks in its CS for a match. The CS is a cache of data packets indexed by names. When a match is found in the CS, then the data is served, and the request is considered satisfied. If there is no match, then the PIT is checked. The PIT shows if a previous interest for the same name has already been forwarded and remains unsatisfied. If there is a PIT entry, the CR doesn't need to forward the interest again. It will instead add the identifier of the face (interface) the interest was received on to that PIT record. If there isn't a PIT entry, then the CR consults the FIB, which utilizes a configurable forwarding strategy to identify which face to which it should forward the interest and update the PIT with a new record that the interest was forwarded. Data packets are typically forwarded along the reverse path contained in the corresponding PIT entries. When a CR receives a data packet, it checks its

PIT to determine which faces to which it should be forwarded. The PIT record is removed after the data is forwarded, and depending on the caching policies, the data packet may be added into the CS so to satisfy future requests.

2.1 ICN+IoT

The IoT is an emerging paradigm that promises to interconnect billions of heterogeneous devices and the Internet. Still, it is facing the challenge of building an infrastructure able to scale and cope with its dynamic environment. The core premise of ICN lies in the name-based routing that enables users to retrieve data objects by names irrespective of their locations. It follows that ICN is well suited for IoT applications, where users consume data generated from IoTs without maintaining secure connections to them. The basic request/response style APIs used in ICN enables developers to build IoT applications simply and efficiently.

The proliferation of low-cost sensing and actuator devices combined with the advancement in wireless communications technologies and the desire to connect and integrate these devices on a global scale has led to the rise of the IoT, which introduces new risks and challenges. As most IoT devices will be limited in their memory, processing, or energy resources, IETF working groups have proposed a suite of protocols and open IP-based standards to support IoT-like environments that support these constrained devices. Standards like 6LoWPAN, RPL, and CoAP are designed to support IP-based IoT solutions. However, there remain open challenges in deploying IP-based IoT solutions on a large scale (Ghodsi et al, 2013). IP-based solutions require a rigid application and device requirements based on the host-centric IP paradigm. The use of IP addresses implies requirements for an additional resolution system to translate application-level requests, such as in URLs, into IP addresses, connection-oriented end-to-end security, and additional protocols to enable mobility support. The ICN paradigm has been proposed (Ghodsi et al, 2013) as a well-suited alternative to IP based networking for the IoT.

In an ICN, data is delocalized and does not need to be retrieved via end-to-end transport streams. Rather, hop-wise replication and in-network caching support content dissemination in a way that is well suited to the IoT because it relaxes the demand for constant continued connectivity. ICNs have several attributes that make them well suited to the IoT. In particular, many of the most common communication patterns used in the IoT, such as scheduled and on-request data retrieval, are easily accommodated in an ICN and could benefit from a cache-assisted, hop-by-hop replication system (Arshad et al, 2018).

An ICN-IoT could reduce the network layers and subsume network, transport, and basic application logic. An ICN approach to IoT might offer opportunities to efficiently factorize core functionalities, such as caching and buffering for error control; reduce the complexity of autoconfiguration mechanisms as compared to those used in a layered protocol stack; and achieve a reduced memory and storage footprint compared to IP based standards and protocols, such as IPv6, 6LoWPAN, and RPL. Some research (Baccelli et al, 2014) has validated the applicability of an ICN in the IoT experimentally and demonstrated that it has advantages over IP-based technologies in terms of energy consumption and memory footprint. However, a number of issues remain related to security and scalability. ICNs are an active research area with several working groups, such as the IRTF's Information-Centric Networking Research Group (ICNRG) and NIST's Information-Centric Networking Program.

2.2 ICN+IoT Security

In today's IoT, security is a fundamental need. IoT devices and applications often take data from our daily lives through the devices that surround us. Security in IP based networks is focused on securing information channels; whereas, ICNs perform all security mechanisms on the content itself. In NDN, each data packet is signed with the original provider's public key and then verified by any consumer in the network allowing the content to be both integrity-assured and authenticated. There remain a number of ongoing research challenges related to securing ICN-IoT.

An important issue in ICN-IoT security is how to securely authenticate and bootstrap new IoT devices into the. We present an overview of a work-in-progress architecture of an ICN-IoT that includes edge networks that may be smart homes or larger enclaves. This model is based on low overhead symmetric cryptography rather than computationally expensive asymmetric encryption. In this model, there are different types of nodes including device nodes (DN), coordinating nodes (CN), and connectors. DNs may be resource constrained in

memory or processing ability. Connectors serve as conduits to the wider internet. The coordinating nodes (CN) form a backbone network that interconnects with particular DN's to form subtrees or groups of subsidiary DN's. The CN and connector nodes are not considered to be resource constrained in this model. In addition to these, there is a network service provider known as a security provider (SP). New devices first discover their neighboring nodes, which are already authenticated and bootstrapped into the network topology. Neighbor devices can ask the SP device for the information required to authenticate new devices to the network. The new device sends an Init request, which is a broadcast forwarded interest packet, constituting a join request with a long PIT expiration and includes its hardware ID, a nonce and its current hop-distance from the CN. Neighbor DN's receiving the message will then relay the message, as a new Init Request, to its CN along with the auth parameter. The Init request is signed by the neighbor DN, giving allowance for the new DN to receive a route towards the CN. The SP completes the auth process and derives the security keys required for any future transmissions. It then replies with a network auth message that includes the new DN's next-hop neighbor and hop-distance, and CN to the neighbor DN, which then forward the reply to the new device after reverse-mapping it to satisfy the original Init Request. The processes of Init Request and Bootstrapping Request may be repeated multiple times to locate a shorter path to the AN. Furthermore, it might trigger subsequent discovery processes for other devices along the downstream path that the new device was added to, in order to adjust their hop-order in the hierarchical network. The result is the new device is initialized as part of tree and associated with a CN. This work will be presented in a future paper.

3. CONCLUSION

Deficiencies in the current internet architecture make it poorly suited for the rapidly increasing number of IoT devices and services. Existing research has shown that ICN's, such as the Named Data Network project are better suited to address these deficiencies; however, their remain issues to solve related to security. One issue is related to the initialization and bootstrapping of new devices and a brief intro to work in progress is introduced.

REFERENCES

- Akhshabi, S. et al. 2011. "The evolution of layered protocol stacks leads to an hourglass-shaped architecture," ACM SIGCOMM Computer Communication Review, vol. 41, no. 4, pp. 206–217
- Arshad, S. et al. 2018. "Recent Advances in Information-Centric Networking based Internet of Things (ICN-IoT)," pdfs.semanticscholar.org
- Baccelli, E. et al. 2014. Information centric networking in the IoT: experiments with NDN in the wild. New York, New York, USA: ACM, 2014, pp. 77–86.
- Chawla, M. et al. 2007, "A data-oriented (and beyond) network architecture", SIGCOMM'07. vol. 37, no. 4. New York, New York, USA: ACM, 2007, pp. 181–192.
- Cisco, 2017. Cisco Visual Networking Index: Forecast and Methodology 2017--2022.
- Dimitrov, V. and V. Koptchev. 2010. PSIRP project -- publish-subscribe internet routing paradigm: new ideas for future internet. New York, New York, USA: ACM, 2010, pp. 167–171.
- Ghods, A. et al. 2013. "Information-centric networking -- Ready for the real world? (Dagstuhl Seminar 12361)," Dagstuhl Reports, vol. 2, no. 9, p. 14.
- Jacobson, V. et al. 2009. "Networking named content," New York, New York, USA: ACM, 2009, pp. 1–12.
- Kutscher, E. D. et al. 2016. "Information-Centric Networking (ICN) Research Challenges," IETF RFC-7927
- Pan, J. et al. 2011. "A survey of the research on future internet architectures," IEEE Communications Magazine. Vol. 49, Issue 7.
- Rexford, J and Dovrolis, C. 2010. "Future Internet architecture: clean-slate versus evolutionary research," Communications of the ACM, vol. 53, no. 9, pp. 36–40
- Sheng, Z. et al. 2013. "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," ieeexplore.ieee.org.
- Zhang, L. et al. 2010. Named Data Networking (NDN) Project, Technical Report NDN-0001, Xerox Palo Alto Research Center-PARC, 2010.