Local Naming Service for Named Data Networking of Things

Yating Yang
School of Computer Science
Beijing Institute of Technology
yangyating@bit.edu.cn

Tian Song
School of Computer Science
Beijing Institute of Technology
songtian@bit.edu.cn

ABSTRACT

Resource-constrained IoT sensors deployed over NDN have to carry scalable and thus long names within length-limited packets for global use, which produces additional overhead in fragmentation and network traffic across layers. However, for a local IoT region, sensors normally offer relatively mono-service of sensing therefore the same prefix of names in a periodical manner. Based on this observation, we introduce a Local Naming Service (LNS) to convert name between specific long name and symbolic short one for support of both valid global communication and lightweight local transmission. LNS explores the potential of name conversion on the fly while preserving data authentication in NDN packets.

CCS CONCEPTS

• Networks → Naming and addressing; Ad hoc networks;

ACM Reference format:
https://doi.org/10.1145/3125719.3132104

1 INTRODUCTION

Naming is one of the most crucial and fundamental components for Named Data Network (NDN) [5] to build networking and steer packets. In order to efficiently relay packets in current diversified Internet of Things (IoT) applications, naming scheme is suggested to be a flexibly and scalably hierarchically manner [4], and consequently the IoT packets may have relatively long names for global networking. Nevertheless, the maximum transmission unit (MTU) of dominant IoT link layer protocol (i.e. IEEE 802.15.4) is only 127 bytes in length [2], which is much shorter than the one of Ethernet around 1500 bytes. Considering a simple and medium-size name /ndn/IoT/A-part/B-part/Temp, it takes up around 30 bytes. Given a NDN-IoT over 6LoWPAN [3] which is the common IoT standard via IPv6, although it compresses header into around 15 bytes, each packet handles 25-byte frame overhead, 21-byte link-layer security overhead and possible 30-or-more byte NDN names. Besides, each packet may have fields for timestamp and authentication, thus very few bytes are left. The limited content payload of packet may frequently trigger fragmentation mechanism, bringing in extra operations and bandwidth cost to divide and reassemble across layers. The cross-layer operations, even long names themselves and related maintenance of CS, PIT and FIB would impose severe costs in computing, storage and thus energy.

Name conversion and resolution can fundamentally mitigate the side effect of flexible naming scheme. For global NDN network, NDNS [1] provides a DNS-like lookup service for unreachable name by a top-down search for global NDN name resolution. For local IoT area, name conversion and resolution design has to address the following two issues: 1) availability: the network has been constructed by original names. Name conversion could break the original forwarding pattern, impairing communication ability. 2) security: a named packet including the name itself is authenticated as a signature by the provider, therefore name conversion may violate the authentication and security scheme.

2 LOCAL NAMING SERVICE

2.1 Observation

There is an important observation for the local IoT area that, a single sensor normally offers relatively mono-service of sensing temperature, humidity, voice, light, etc., in a periodical manner. For example, a sensor may periodically generate a temperature data with name of the prefix /ndn/IoT/A-part/B-part/Temp appending with the timestamps. There are just numerable service and data types in total for the surroundings of a sink node. Therefore, keeping long and global names in local transmission may cause waste for bandwidth and storage.

2.2 LNS Design

Based on this observation, we present a Local Naming Service (LNS) for lightweight transmission in a certain scope, which locally shortens long and complex names by replacing the specific content prefix with a short code. Considering the limitation of resources for end
sensors, we assign the pivot name conversion work to sink nodes which dominate end sensors in local area and bridge end sensors and global network. A sink makes name inter- conversion with two prefixes: long content prefix for external global network and short prefix code for lightweight transmission and maintenance in local IoT network. For simplicity, prefix code can be a hash value of the specific content prefix which the sensor wants to publish. Accordingly, the sink node will maintain a Prefix Code Table (PCT) for the matching relationships between original prefixes and short prefix codes. Each prefix code is attached with a valid time to restrict expiring services. If the sink doesn’t receive any packets with the registered prefix code during its valid time, it deletes the infrequent entry and cancels the corresponding local naming service. Since prefix part in names is shortened into a code in all the packets and tables in the local area, the network works on the basis of short prefix code with low cost both for transmission and storage.

Fig.1 demonstrates how LNS works. When a user requests a temperature data, it sends an Interest packet toward the sensor network. As a dominating node in local area, the sink bridges deployed sensors and external network. It checks PCT after receiving every packet. If the prefix of the packet has not been registered before, the sink node will forward the Interest as normal. Otherwise, it will make name conversion according to PCT, and then replaces the long prefix in the name with corresponding prefix code /0xA1B2 which will guide packets in local IoT network. When the sink node receives data with prefix code from the sensors, it will resolve the short name with PCT by replacing the code with original prefix, and then forward it toward external consumers.

2.3 Service Establishment

LNS is established on the demand of sensors and with the confirmation from sink node. Fig. 2 demonstrates how LNS is established between the sink and sensors. When a sensor wants to publish a new type of content and is willing to ask a local naming service for the prefix, it sends an Interest to the sink to request a prefix code according to its demand. After the sink receives the Interest of service request, it checks whether the prefix has been registered before. If the prefix is new and the sink has the ability to support the service, it generates a unique prefix code (i.e. hash value). Then the sink generates a Data, containing the prefix code, and records the matching relationship to the PCT. After that, the sink or sensor publishes the content with the short prefix code, depending on selected routing protocol. To this end, the service is established between the sensor and dominating sink node. Once the service is open, the local network will build communication on this local short prefix code, which means corresponding prefix parts in any packets and tables in certain scope are replaced with the short codes.

2.4 Security Support

This kind of naming service offers supports for existing security and trust scheme, because the sensor will make authentication and decryption with the original prefix. As Fig. 2 shows, when a sensor receives an Interest with short prefix code, before verifying the packet, it restores the name with original long prefix. Before the sensor loads the content to Data packet, it signs with original name, then converts the name with corresponding prefix code. Corresponding, the sink node will resolve the name and replace the short one with original prefix, before sending the Data packet to external network. The short prefix code only works in the certain scope between the sink and sensors, keeping original security scheme.

3 PRELIMINARY ANALYSIS

We make some preliminary analysis to show the potential of LNS. For a local area, we assume a normal name length as 30 bytes in average, and 100 bytes for network packets size. If we hash the name into 3 bytes name (assume one byte for ‘/’, the other two for prefix code, which can express more than 60k kinds of local attributes for data), it can reduce 90% name size and save more than 25% packets size. Furthermore, if we assume that more than 80% traffic in the local IoT can benefit from the local naming service, the PIT, CS, FIB table of local network nodes can save around 20% storage cost for communication maintenance with LNS, which is a promising saving for resource-constrained IoT environment.

4 CONCLUSIONS AND FUTURE WORK

In summary, we present a local naming service for NDN-IoT with name inter-conversion between specific name and short prefix code to support both valid global communication and lightweight local transmission.

This work is in early stage. With an observation of IoT traffic, we plan to explore a more efficient and fine-grained name conversion in a hierarchical manner, providing a reliable mapping of original prefixes into prefix codes. In addition, mobility support is one of our future concerns. Our next step is to design a more efficient local name inter-conversion scheme and deploy it in real IoT scenarios.

REFERENCES