Named Data Networking of Things and Example Application "Flow"

Zhehao Wang, Jeff Burke

***Abstract*—Many emerging IoT approaches depend on cloud services to facilitate interoperation of devices and services within them, even when the primary need for communication is local in scope, as in many "smart home" applictions. While such designs offer a convenient way to implement IoT applications using today's TCP/IP Internet architecture, they also introduce dependencies between applications and Internet connectivity that are unnecessary and often brittle. This paper uses the design of an IoT-enabled home entertainment experience to demonstrate how the Named Data Networking (NDN) architecture enables cloud-independent IoT applications. It does so by enabling local trust management and rendezvous, which play a foundational role in realizing other IoT services. By employing application-defined naming rather than host-based addressing at the network layer, and securing data directly, NDN enables straightforward and robust implementation of these two core functions for IoT networks with or without cloud connectivity. At the same time, NDN-based IoT designs can also employ cloud services to complement local system capabilities. After describing the motivation, design, and preliminary generalization of the driver application, the paper concludes with a brief comparison with how it would be achieved using two popular IoT frameworks, Amazon's AWS IoT service and the Apple HomeKit framework.**

I. Flow: a Home Entertainment Experience over NDN

In this section, we describe the design of Flow, a home entertainment experience that leverages NDN to realize a cloud-independent, IoT-supported application. We conclude by summarizing the components of a generalized NDN-IoT framework developed based on this design. Flow is a prototype of a multi-user "exploration game", in which participants navigate and interact with a virtual world rendered in a game engine using a combination of inputs:

1) *Indoor positioning*: participants' positions in physical space, detected by indoor positioning (person tracking), modify the virtual landscape;
2) *Wearable sensing*: participants directly control orientation of the environment's virtual camera using gyroscopes connected to microcontrollers, which can be worn or carried;
3) *Mobile phone interface*: participants interact with the virtual environment through controls on their smartphone, for example to share social media images in the virtual environment.

In addition to various types of IoT devices and the game engine, the system on which Flow is built also includes an *authentication server* (AS) that performs local trust management. The AS can be implemented as an app on the owner's smartphone, or a service daemon on a dedicated control hub (e.g., the home router).

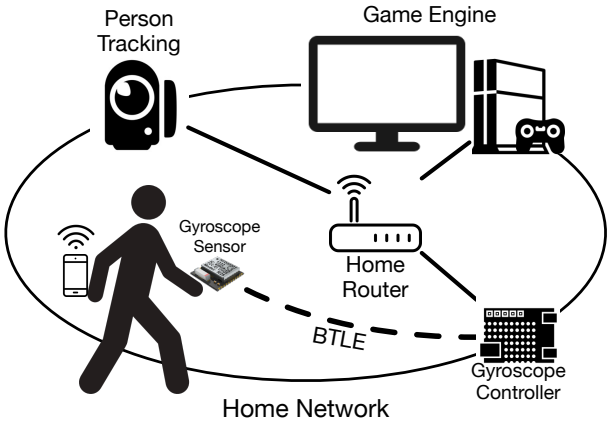

Fig. 1: Typical deployment of the Flow home entertainment experience.

Figure 1 shows a typical deployment scenario of Flow in a home network. NDN interconnectivity between different components is supported over Ethernet and Wi-Fi, through the home Wi-Fi router in a hub-and-spoke topology.

Sensor devices with limited networking capability (e.g., the gyroscope in Fig. 1) may be bridged via a helper device. We assume all devices can reach each other over NDN, which is trivial in a hub-and-spoke topology.[1]

A. Naming and Identity

In Flow, data from the IoT *things* used by the application are named using three namespaces:

- *Application namespace*: a local namespace for publishing and accessing application data, e.g., gyroscope readings needed to control the environment;
- *Device namespace:* a local namespace for publishing device identity certificates and metadata;[2]
- *Manufacturer namespace*: a global namespace created by the IoT device vendors and for trust bootstrapping.

Fig. 2 shows an example of the Flow namespace. In addition to these three namespaces which names devices, things and their data, note the *discovery* branch under the local root prefix,

[1]A routing protocol may be required if a sensor mesh topology is deployed inside the home network.

[2]Device metadata could include information about devices and their capabilities as well as bindings to application names.

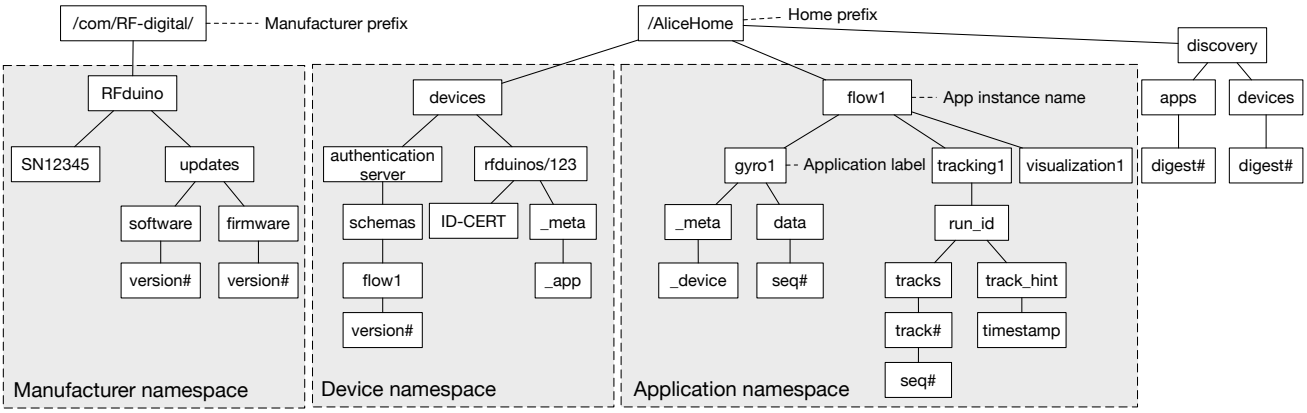

Fig. 2: Example namespace within the home environment where Flow is deployed.

which is used for device rendezvous and for application prefix discovery. Details of its functionality are described later.

The device and application namespaces both have as their root a home prefix that is either context-dependent (e.g., "`/AliceHome`" as in Fig. 2) or globally reachable (e.g., "`/att/ucla/dorm1/301`").

The application namespace starts with a unique instance name (e.g., "`/AliceHome/flow1`") created by the application at installation. Data produced by each component is named under an application label configured by the developer (e.g. "`/AliceHome/flow1/tracking1`"). The application label also contains a metadata subtree containing the device name that serves this data (e.g. "`/AliceHome/flow1/tracking1/_meta/_device`").

Devices publish their local identity certificates under the device namespace (e.g., "`/AliceHome/devices`"). They also publish metadata (profile) information in the "`_meta/_app`" branch under the device identity prefix to list the application data prefixes they are publishing under. The device namespace of an AS also contains the trust schema of currently active applications. Schema and trust relationship details are described later in this section.

The manufacturer namespace falls under vendor-specific prefixes that are independent from the home network's local prefix. We envision that manufacturers will have globally unique names for their products used during bootstrapping, over-the-air updates, and similar processes. Manufacturers publish their own certificates under this globally unique prefix so that the devices can authenticate the data coming from the vendors such as software/firmware updates and service notifications.[3] In the research example of Flow, all devices are configured with vendor-provided identity names and profiles in their initial provisioning, before being connected to the home network. These are used for device onboarding.

B. Trust Management

Flow demonstrates a multi-step process for trusting new devices in a home IoT network and enabling their data to be used in an application. First, a device is assigned a device-level name and added to the trust hierarchy for things in the home. Then, it is configured with one or more application-level names for its data, and these names are added to application trust hierarchies. Finally, the device is configured to respond to requests in application namespaces.

The authentication server acts as the trust anchor. It can be coordinated with but does not depend on a remote cloud services. While the devices and users may have public identities outside the home environment, they all need to obtain local identities that are certified by the AS before they can start interacting with other local entities.[4]

The process of establishing a trust relationship between a new device and the home through the AS is similar to the Bluetooth pairing process. To bootstrap a new device, the user—or a configuration application on his/her behalf—provides a shared secret and a local device name. The shared secret may be a device barcode, identity communicated by NFC, or simply a PIN number. The AS sends a command Interest to the device, signed using a key derived from the shared secret, to ask that it generate a public/private key pair associated with the device's new name on the local network. The device replies with a Data packet containing an identity certificate request, also signed by the shared secret. The AS generates the identity certificate based on this request. The device, now part of the trust hierarchy, can advertise its services or participate in an application over the local network. This process is illustrated in Fig. 3. If the device has been issued a public identity certificate by its vendor, the AS may optionally authenticate its public identity, e.g., by asking the device to sign an AS-generated challenge.

Applications like Flow are "installed" in a similar way to devices, with the AS signing both identity certificates and trust schema for the application. The application's trust schema expresses *what devices identities are authorized to publish*

[3]Reachability of data in this prefix is not addressed here but can be accomplished through encapsulation supported by the home router, for example.

[4]The public identities may be used to assist the onboarding process, but will not be required for local communication once the initial configuration has finished. For example, a new user can authenticate with the AS using her public identity (e.g., OpenID or Google/Facebook account) before creating her local identity that is used solely by the home environment.

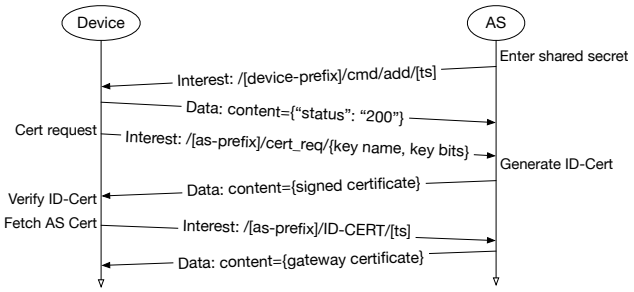

Fig. 3: Bootstrap trust relationship for new device.

under what application prefixes and is published as a normal Data object on the local NDN network. For example, in Fig. 2 "`flow1`" is a specific Flow instance and "`schema`" branch contains the trust schema of this instance. The schema name includes a monotonic version number at the end, so when there is a change in the schema a newer version is published. The technical details of how to specify a trust schema are described in [1].

When a device that produces data is installed, it sends a command Interest to the AS that includes the application prefix it intends to publish under and its own local identity. If the request to publish data in the home network is granted, the AS will update the trust schema with the authentication rules for data published by this device. The rule binds a device identity with the application prefixes it's authorized to publish under.[5] Schematized trust enables fine-grained control over what devices can publish what data for which application instances. Consumer devices fetch the latest trust schema over the network via NDN and follow the rules to authenticate the data packets published in the network. The producer authorization process, as well as an example of the resulting trust relationship, is shown in Fig. 4, in which the AS signs a device identity, and the device signs a piece of application data it publishes.

C. Rendezvous

Flow also demonstrates a name-based, distributed rendezvous mechanism for devices and applications to discover each other over NDN. As described in the previous section, The key idea is to synchronize the set of device and application names (called the *rendezvous dataset*) across nodes in the network that are interested in learning about them. The synchronization process utilizes the decentralized and serverless ChronoSync [2] protocol to effectively synchronize prefixes of active devices under the home entertainment "`/AliceHome/discovery/devices`" namespace.

Name discovery is performed independently on each device by lookups in the local copy of the rendezvous dataset. Once an application obtains the name prefix of the target device or application, the devices can follow the namespace

[5]This binding addresses potential collision in application labels–for example, by default the AS does not authorize a second device to publish under an application namespace claimed by another.

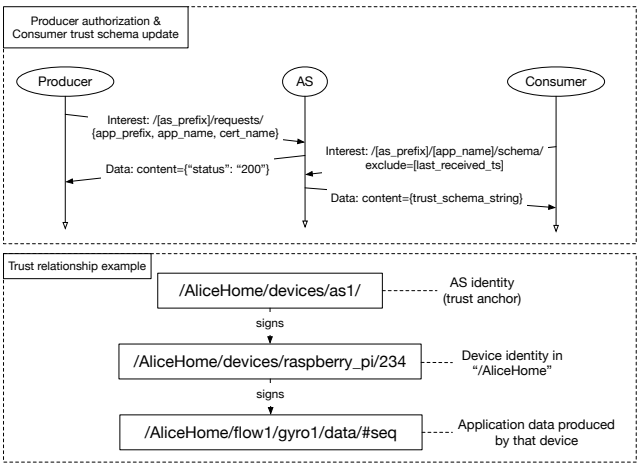

Fig. 4: Schematized trust between producers and consumers.

structure described in I-A to construct Interests for fetching the certificates and metadata, which will bootstrap high-level service communication.

D. Generalizing IoT functionality in NDN

Through the design of Flow, we explored how to use NDN to provide the functionality discussed in section **??** without reliance on any cloud services, and generalized it in a framework called *NDN-IoT*, which provides the following features:

- *Identity, authentication and authorization*: each device in NDN-IoT possesses two identities: a manufacturer-given name used before and during device onboarding, and a local device name used afterwards. NDN-IoT implements mechanisms described in sections I-A and I-B for naming, data authentication and device authorization.
- *Rendezvous and resource discovery*: nodes in NDN-IoT find the name prefixes of other devices, applications and services in *discovery* namespace via distributed dataset synchronization, and then uses discovered names to fetch devices and applications data, or invoke services in the local system.
- *Device management*: NDN-IoT performs device onboarding and software updates in manufacturer namespace, and device monitoring in device namespace.
- *Application data messaging*: NDN-IoT provides application-level pub-sub under two types of namespace abstractions. The framework pipelines interest for data named in a *sequence number namespace* (e.g. "`/AliceHome/flow1/gyro1/data/[sequence_number]`"), or keeps outstanding interest for data named in a *timestamp namespace* (e.g. "`/AliceHome/devices/pc1/_status/[timestamp]`").
- *Gateways to external network and services*: the local IoT system can request data from the global Internet using their public names, meanwhile its local data can be made available to the public Internet by using a globally reachable name prefix, or having a gateway device

that uses data named under a globally reachable prefix to encapsulate data from the local system (e.g. "`/att/ucla/dorm1/301/flow1/gyro1/data/1`" → "`/AliceHome/flow1/gyro1/data/1`").

II. Implementation

We have implemented the NDN-IoT framework and a prototype of the Flow entertainment experience to verify the design introduced in the previous section. The implementation follows a modular structure and differentiates between the framework-level services that we believe are common to many home IoT systems and the functionality that supports Flow-specific application logic. This section describes details in both the framework and application components.

A. NDN-IoT framework

The NDN-IoT framework includes an implementation of the authentication server and a set of client libraries.

The AS functionality is implemented based on the team's previous work on NDN-pi (citation: ndn-pi TR). The framework provides a server implementation in Python, which we run on Raspbian platform in Flow application. Compared with the earlier work in NDN-pi, we added "application publishing authorization", and "application trust schema distribution" to the server implementation, to handle the construction and distribution of an application trust schema. The server implementation also updates the codebase to work with PyNDN2 2.0b4, with major updates to security module interface, including using CCL library's built-in public/private key storages. [6] Authentication clients are available in both Python and JavaScript in order to support application components running on Ubuntu, OSX, Raspbian, and browser (Chrome and Firefox) platforms. Compared with the earlier work in NDN-pi, this implementation added a port in JavaScript to support browser applications. The JavaScript port uses the library's IndexedDbIdentityStorage and IndexedDbPrivateKeyStorage for key storage (this means the key storage in browser is origin-based, thus in our installation the webpage that adds this "device" and the webpage that publishes application content should be hosted under the same origin). Recall that in NDN-pi the client device generates a device ID[7]. In browser application's case we generate a random string in IndexedDB if one doesn't already exist, to use as the device identification of the device that currently runs the browser.

The NDN-IoT client libraries are built on top of the NDN Common Client Libraries [3], and aims to provide abstractions to faciliate application development in a home environment. The client libraries are available in Python, C++, JavaScript and C#. They are organized into three major functional blocks:

Bootstrap follows the suggestion in section VI.B and VI.C of the IoTDI '16 paper, and helps with device and application identity setup. Its abstractions include:

1) KeyChain setup: given a device identity (and optionally an AS name), construct a KeyChain and set up the default device certificate name for this application instance. This KeyChain is later used for signing and verification of all application data.
2) Consumer setup: given an application prefix, the Bootstrap module keeps outstanding interest for the application's trust schema (add example), and updates the local copy whenever a later version is received and verified.[8]
3) Producer setup: given an application prefix, the Bootstrap module requests authorization from the AS to publish under that prefix by sending a command interest including this device's identity and the prefix it wants to publish for (add example). If the AS authorizes the request, it adds an entry stating to the application trust schema to reflect the updated trust relationship, and publishes a new version for all consumers to fetch.

Discovery uses a sync-based discovery different from suggested in section VI.B of the IoTDI '16 paper. (Protocol description)

Application-level pub/sub follows the suggestion in section VI.F of the IoTDI '16 paper, and provides the following abstractions:

1) Consumer for timestamp namespace (/prefix/[timestamp]): this consumer uses oustanding interest with range exclusion to ask for latest piece of data, and upon data retrieval and successful verification, updates the range exclusion with the received timestamp.
2) Consumer for sequence-number namespace (/prefix/[sequence-number]): this consumer pipelines interest for the next few sequence numbers, and upon data retrieval and successful verification, issues an interest for the sequence number after the last one in the pipeline.

(trust schema example) (discuss callback mechanisms?)

Compared with NDN-pi, the AS implementation made the following updates (insert details), and provided a similar functioning port in JavaScript.

B. Flow application components

In our prototype, each of the Flow application components is implemented as the following:

1) *Indoor positioning*: We use OpenPTrack,[9] a multi-camera person tracking system. The NDN producer for OpenPTrack[10] (written in C++) publishes the position of each person at a 30Hz rate, along with lower rate metadata about active tracks.

[6]We now use BasicIdentityStorage and FilePrivateKeyStorage for key storage, and ConfigPolicyManager for data verification, whereas the old implementation, developed at a time when PyNDN security library module was evolving, used custom derived classes (for example, IotPrivateKeyStorage).

[7]The server uses this ID to construct the initial "add device" interest name. This ID was implemented as the CPU serial of a Raspberry Pi.

[8]The application trust schema may evolve over time, when new device names are added and authorized to publish under certain application prefixes

[9]http://openptrack.org/about/

[10]https://github.com/OpenPTrack/ndn-opt/

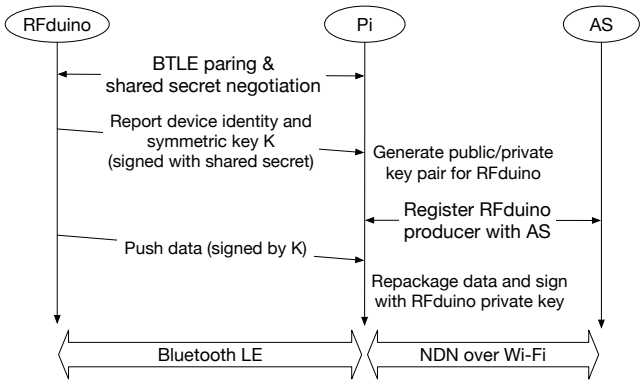

Fig. 5: RFduino data publishing with assistance of Raspberry Pi controller

2) *Wearable sensing*: We use an RFduino 22301 with gyroscope MPU6050 attached to provide virtual camera control. The RFduino cannot perform asynchronous signing operations quickly enough, so we introduced a Raspberry Pi controller as a gateway for bridging RFduino to the NDN home network. The data exchanged between RFduino and Raspberry Pi is signed with a shared secret key negotiated after Bluetooth pairing. The Raspberry Pi generates a public/private key pair on behalf of the RFduino to be associated with the RFduino's device identity. The RFduino runs a minimum NDN producer, implemented with the ndn-cpp-lite library[11], which generates data at roughly 2Hz rate. When new data is generated, the RFduino pushes the data (signed by the pre-negotiated shared secret) to the Raspberry Pi controller over the Bluetooth LE channel. The controller receives the data, repackages the data and signs the data using RFduino's private key, and then publishes the data on the home network. The RFduino data publishing process is shown in Fig. 5.
3) *Mobile phone interface*: We employ an Android phone that loads a control webpage (written in JavaScript) in a mobile browser to interact with the virtual environment. The phone sends out two types of command Interests: the first one matches an OpenPTrack track ID with that of the mobile, and the second one drops an image onto the virtual environment where the user's avatar is standing. ID matching is introduced so that the visualization knows the location of the user's avatar (identified by a track ID) when an image drop command Interest is issued by the same user (identified by the mobile's ID).
4) *Visualization*: We use the Unity3D[12] game engine for visualization. The game engine runs C# NDN data consumers that receive person tracking and virtual camera control data, and a producer that receives image dropping command Interests from the mobile web interface.

The implementation for both NDN-IoT framework and Flow application are available online.[13] We installed two instances of the Flow application testbed at UCLA and Huawei. Fig. 6 shows a diagram of the system and its message flows after all devices are bootstrapped with an AS, which in our installation is another Raspberry Pi.

REFERENCES

[1] Y. Yu, A. Afanasyev, D. Clark, k. claffy, V. Jacobson, and L. Zhang, "Schematizing Trust in Named Data Networking," in *Proceedings of the 2nd ACM International Conference on Information-Centric Networking (ICN)*, 2015, pp. 177–186.
[2] Z. Zhu and A. Afanasyev, "Let's ChronoSync: Decentralized Dataset State Synchronization in Named Data Networking," in *Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP)*, Oct 2013, pp. 1–10.
[3] J. Thompson and J. Burke, "NDN Common Client Libraries," NDN Project, Tech. Rep. NDN-0024, Revision 1, sep 2014.

[11]https://github.com/named-data/ndn-cpp/
[12]https://unity3d.com
[13]https://github.com/remap/ndn-flow

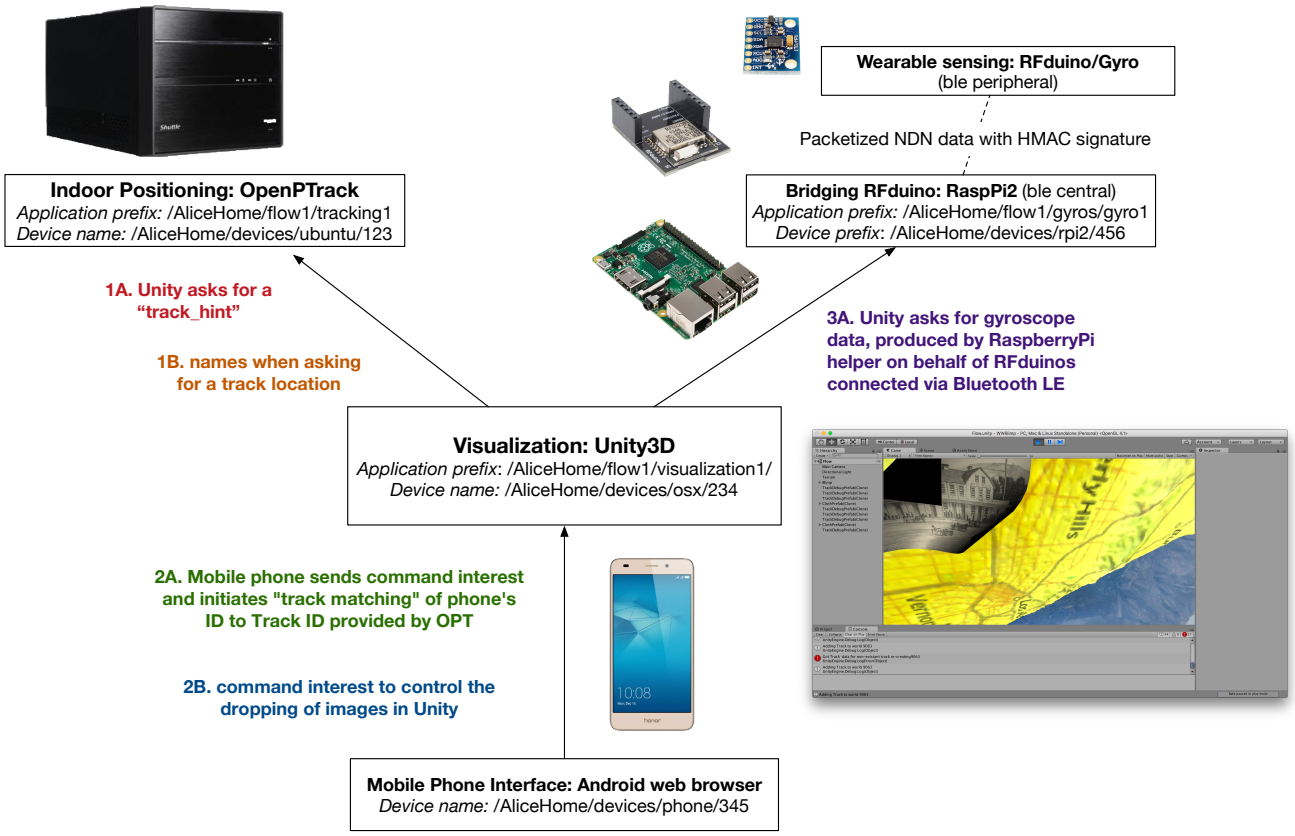

Fig. 6: Application components and message flows in Flow