Wiki »

KITE

The **KITE protocol** allows building forwarding paths for prefixes using "authenticated" Interest-Data exchanges between a mobile producer (MP) and a trusted Rendezvous Server (RV).

An MP sends a **KITE request** (a signed Interest that follows a special naming convention), which is forwarded to the RV because the RV announces a prefix of the name. The KITE request leaves traces in the stateful forwarding plane (PIT entries), constructing a forwarding path for Data to be forwarded to the MP. The RV will verify the information carried in the KITE request (primarily the signature, and thus the term "authenticated Interest-Data exchange"), and respond with a **KITE acknowledgment**, a Data packet, for legitimate KITE requests. The KITE acknowledgment sent by the RV will trigger intermediate forwarders to save the reversed forwarding path for Data as Interest forwarding information, for a prefix specified by the name of the Interest-Data exchange.

KITE Request

A **KITE request** is essentially a signed Interest (http://named-data.net/doc/NDN-packet-spec/current/signed-interest.html) with extra information such as nonce and timestamp to for replay-attack prevention. A KITE request is signed and sent by an MP to be verified by an RV,

An Interest packet that satisfies the following requirements is a KITE request:

- Conforms to signed Interest specifications.
- With the trailing Interest signing name components removed, the remaining leading part of the name conforms to KITE request name specifications (see below).
- The ApplicationParameters contains the expiration period for the forwarding path (optional, details TBD).

KITE request name specifications:

- Starts with an **RV prefix**, i.e., a prefix announced by an RV.
- Followed by a **"32=KITE"** keyword name component.
- Followed by a **producer suffix**, i.e., one or more arbitrary name components. The concatenation of an RV prefix and a producer suffix in the same KITE request name is the **producer prefix** specified in this name. The forwarding path to be set up is for the producer prefix.
- End with two name components for replay-attack prevention: **timestamp** and **nonce**.

For example, for RV prefix = /RV, producer suffix = /Alice, thus making producer prefix /RV/Alice, the full name of the corresponding KITE request will be defined as:

```
/RV/32=KITE/Alice/<timestamp>/<random-value>/<any-number-of-trailing-name-components>

                \                        /\                                  /
                 ------------  -----------  -------------------  ------------------
                             \/                                \/
                for replay-attack prevention     components of Signed Interest
```

KITE Acknowledgment

A **KITE acknowledgment** is a Data packet sent by the RV for an Interest (a **KITE request**) that passes verification. A KITE request that passes the verification is supposed to be sent by the owner of the prefix for which the forwarding path is set up.

A Data packet that satisfies the following requirements is a KITE acknowledgement (note that a KITE acknowledgment is always generated in response to a KITE request):

- Has the same name with a KITE request.
- ContentType is 6 (KITE Acknowledgment).
- Carry a prefix announcement object as payload, and the "announced prefix" indicated by the PA object must be the same as the producer prefix specified in the name (refer to KITE request specifications for determining the producer prefix).
- The payload only consists of a prefix announcement object in data form, no other content.

由 Zhongda Xia 更新于 9 个月 之前 · 8 修订