Datanet: Enabling Seamless, Metered and Trusted Last-Mile Connectivity without Subscriptions

Madhumitha Harishankar, Jinhang Zuo, Sriram V. Iyer, Patrick Tague, Carlee Joe-Wong
Carnegie Mellon University, Flipkart

Problem

Limitations of relying on trusted ISPs with long-term subscriptions for last-mile network connectivity:

- **Managing per-device data contracts** and **requiring deployment of new infrastructure for internet connectivity** poses significant overhead for realizing the IoT (e.g. smart-cities)
- End-device **restricted** to accessing ISP-enabled networks or known/open access points (AP) only
- **No seamless way** for closed networks to monetize underutilized resources by authenticating unknown devices and enforcing payments

Our Goal

- Enable devices to **seamlessly and securely connect** with closed last-mile networks with **no a-priori identity or trust relationship**.
- Enable closed networks to connect with unknown devices and enforce payments, **without requiring hardware or firmware modification**.
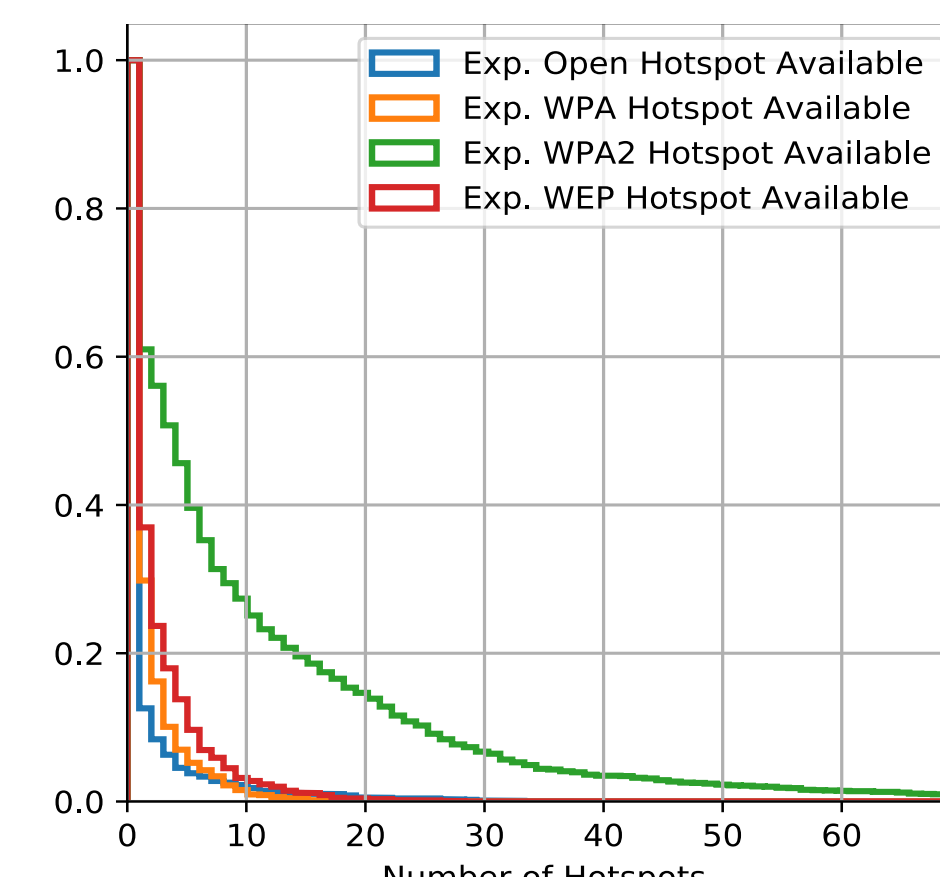
Potential Impact

Array of Things testbed of 126 IoT devices in Chicago
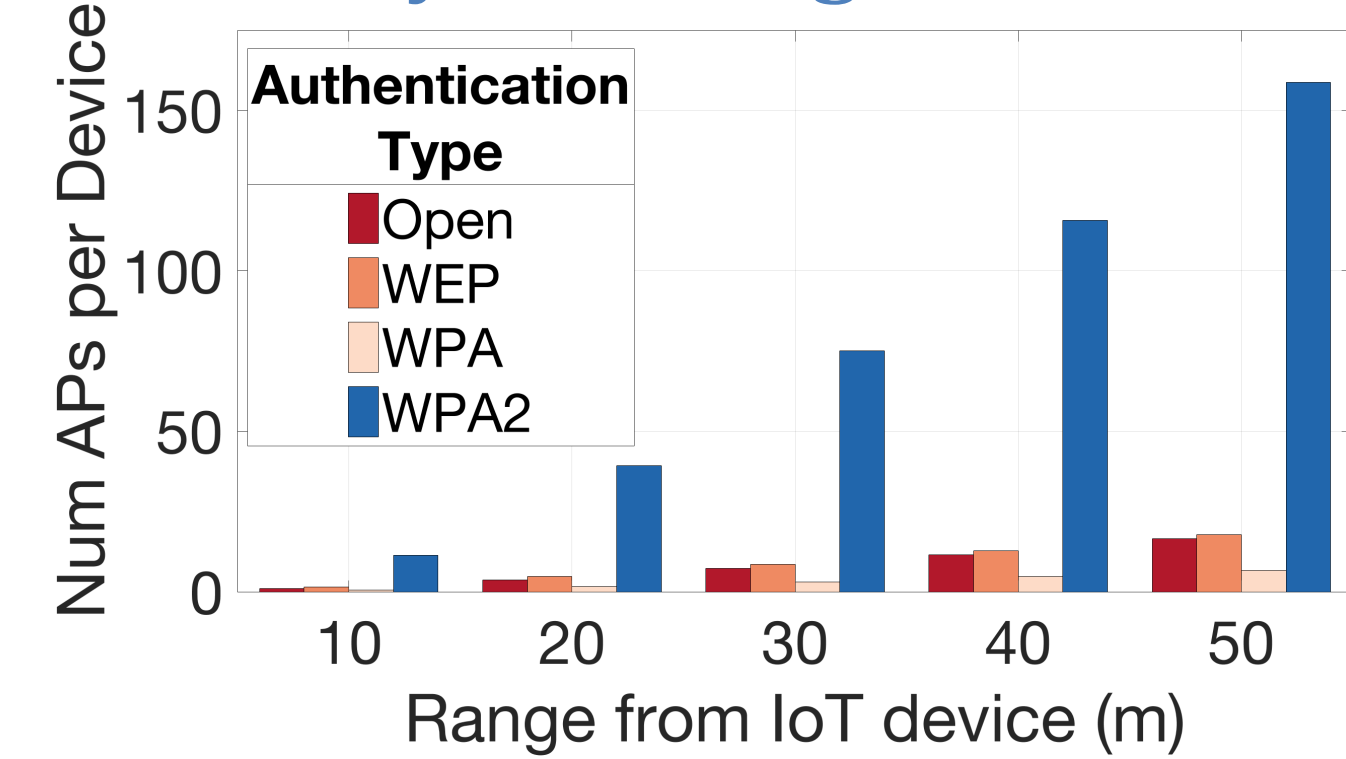
Even within a range of 10m, ~12 closed Datanet-compatible WiFi access points (i.e. WPA/WPA2) are available on average to each device.

LifeMap mobility dataset (fine-grained location tracking of 12 students for 7 months in Seoul, South Korea)

Reverse CDF of estimated number of accessible APs within a 30m range of each location, categorized by encryption used. 20% prob. of at least 15 closed APs vs 5% prob. of atleast 5 open APs per location

Design
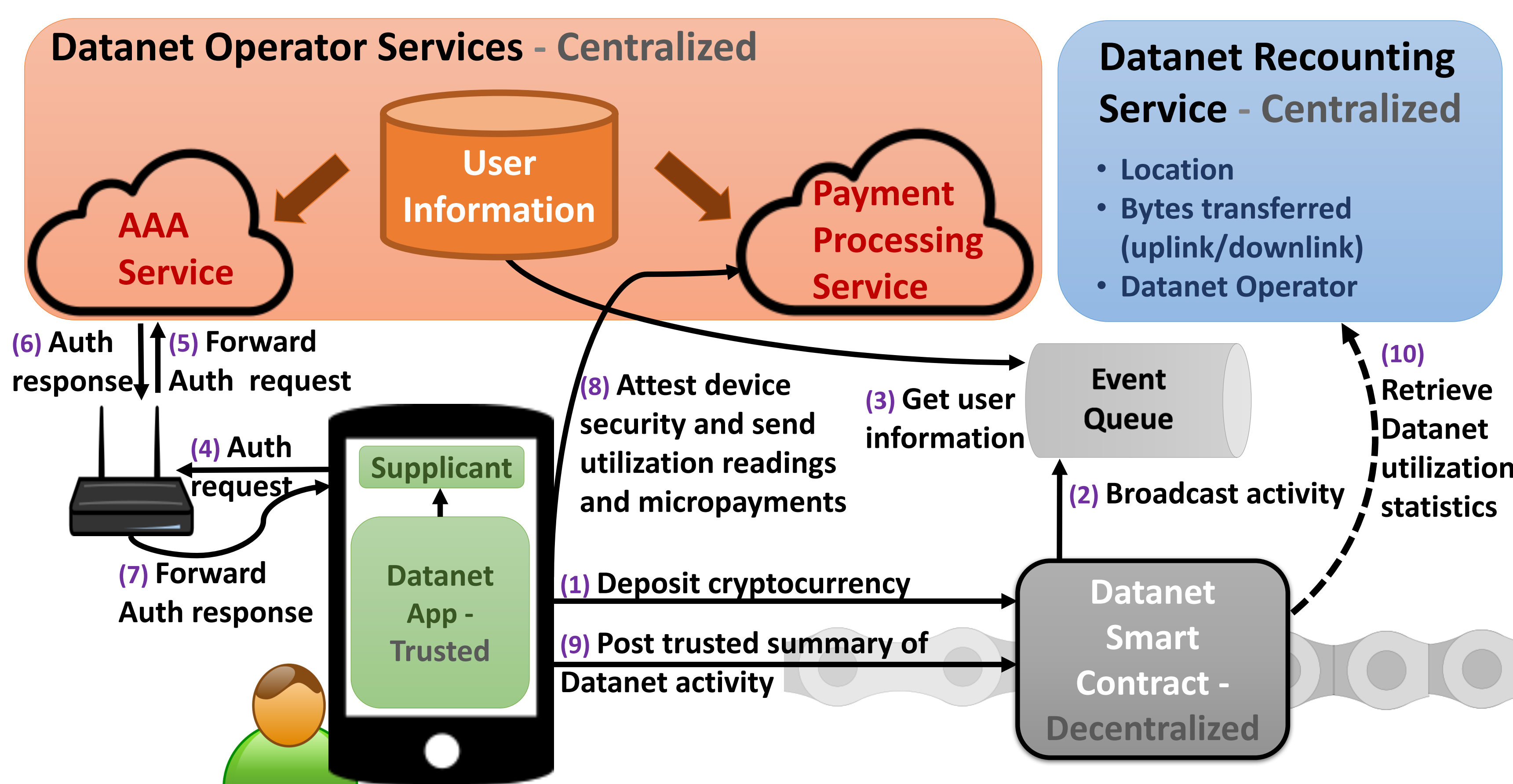
Key Insights

- Leverage blockchain PKI credentials to authenticate device into network using EAP-TLS and remote AAA servers
  - *Enables non-custodial identity management*
  - *Allows the use of existing standards for auth*
  - *Does not require AP modification for blockchain-based auth*
- AAA servers run by Datanet operators who receive micropayments for incremental bandwidth consumption from connected client devices and relay these payments to APs using the PayPlace protocol
  - *Overcomes prohibitive capital requirements typically imposed on consumers and intermediaries by PCNs*
  - *Does not require AP modification to process micropayments*
- Datanet operators enforce payments based on *trusted* utilization readings relayed by client devices
  - *Enabled by remote attestation techniques that verify device security and code being executed*
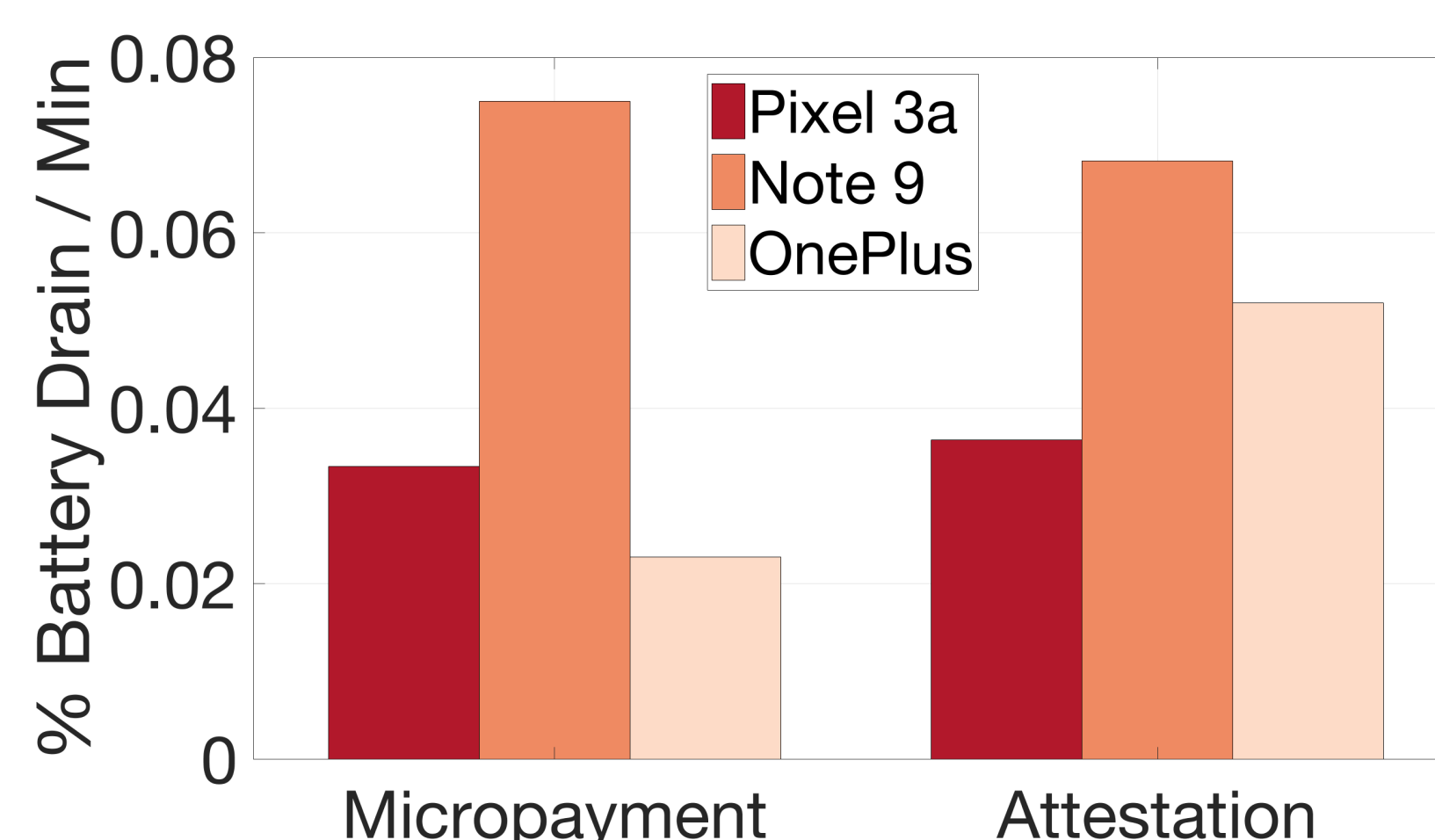
Evaluation

Current vs. Proposed State
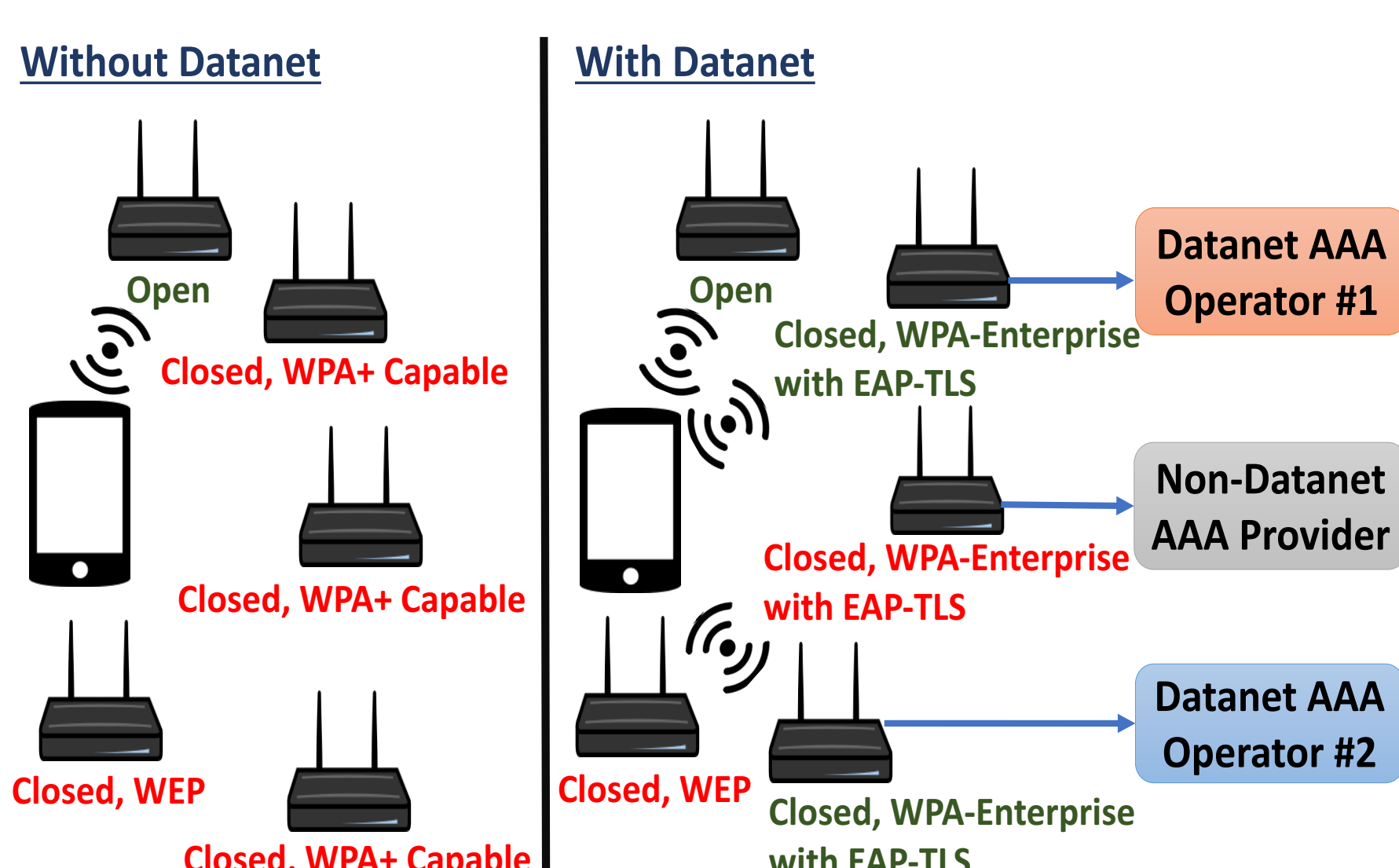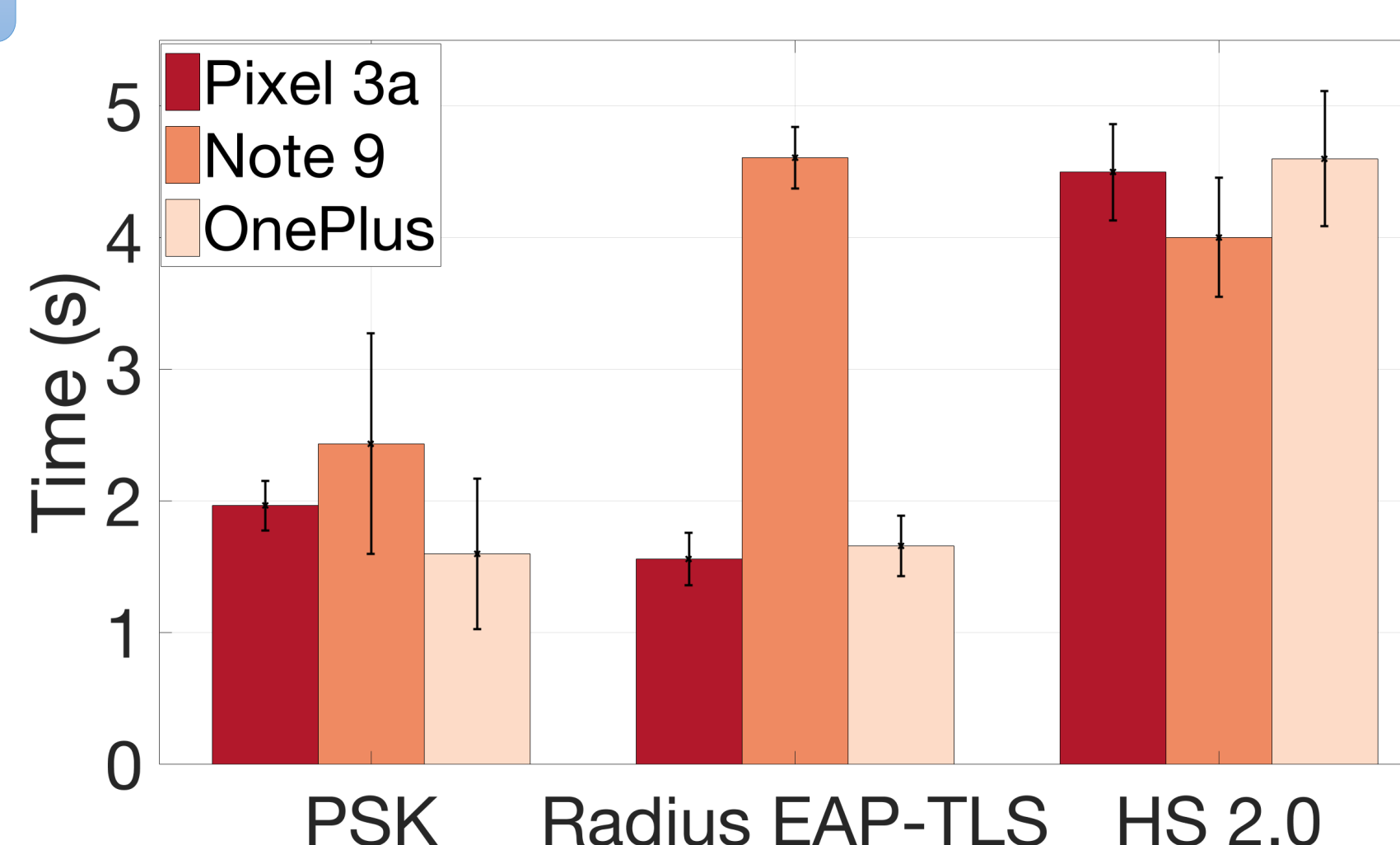

With Datanet, end-devices can access any hotspot that supports EAP-TLS and uses a Datanet operator for remote auth.
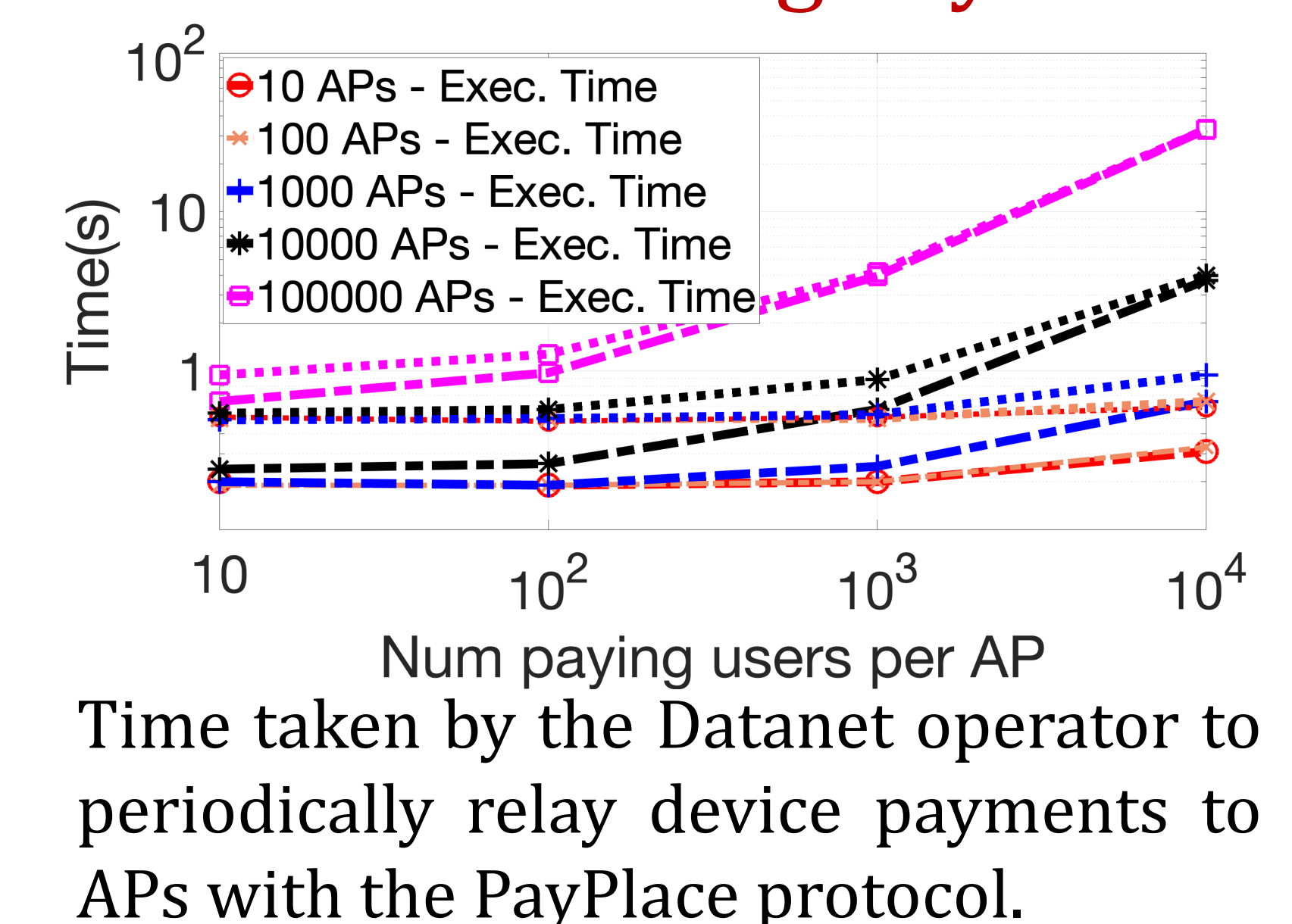
Overhead of Datanet

Micropayments and attestation operations do not result in significant increase in battery drain. Performed once every minute for 5 hours.
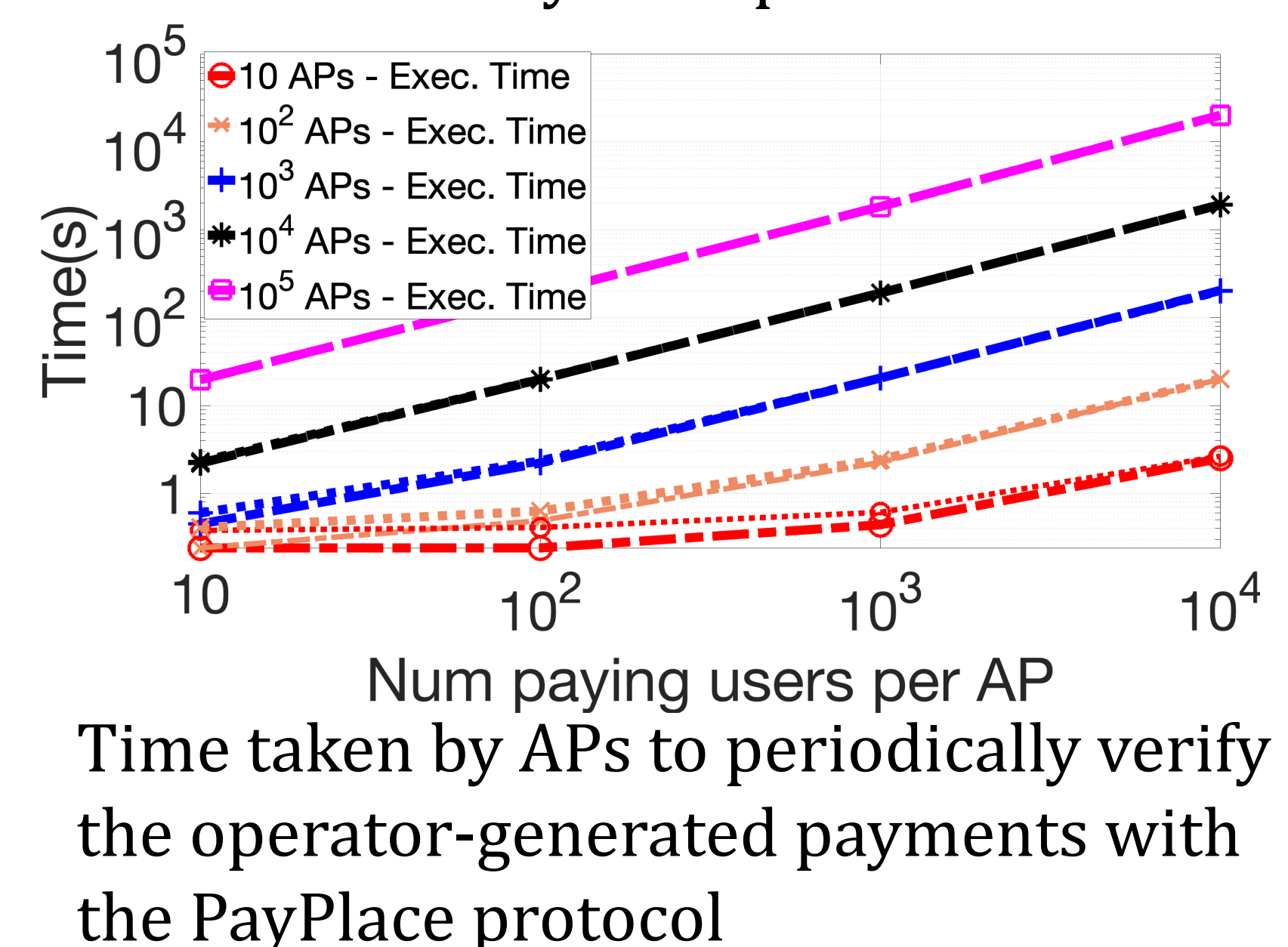

Latencies in connecting to a Datanet-enabled AP is seen to be equivalent to connecting with a PSK or to a Hotspot 2.0 enabled EAP-TTLS AP.

Overhead of Processing Payments

Time taken by the Datanet operator to periodically relay device payments to APs with the PayPlace protocol.

Time taken by APs to periodically verify the operator-generated payments with the PayPlace protocol