Datanet: Enabling Seamless, Metered and Trusted Internet Connectivity without Subscriptions

Madhumitha Harishankar*, Jinhang Zuo*, Sriram Venkateswaran Iyer†, Patrick Tague*, Carlee Joe-Wong*
*ECE Dept., Carnegie Mellon University
{mharisha, jzuo, tague, cjoewong}@andrew.cmu.edu
†Flipkart
sriramv.iyer@flipkart.com

***Abstract*—Relying on dedicated contracts with specific network operators for Internet access significantly limits connectivity options for devices. As new usecases for internet access emerge, e.g., with the Internet of Things in smart-cities, managing such individual contracts for each deployed device with varying data needs is prohibitively cumbersome and highly expensive. In this work, we enable contract-less connectivity between end-devices and access points/networks that have no a-priori trust relationship. Our core insight is that exchange of services and payments can be *trustlessly* enforced by distributed ledger technologies; the credentials that blockchains use for account management can also be used for TLS-based authentication in networks. However, the blockchain's ability to enforce transaction rules is limited by the extent to which the underlying exchange of services is digitally trackable, which is susceptible to manipulation in this case. Requiring blockchain-integrated trusted hardware at the access points for bandwidth metering significantly hinders adoption; even software modifications required at the access points to process blockchain-based auth and payments incur practical deployment and scalability challenges. In designing *Datanet*, we address these challenges and enable seamless and incentivized connectivity between unknown end-devices and APs, using existing standards that allow for interoperability with current and future networks, and without significant overhead for client devices.**

I. Introduction

Devices in the Internet of Things (IoT) may have widely different network requirements and be deployed at locations without dedicated Internet access, like city streets. Current approaches to IoT connectivity require device owners to manage individual data contracts and pay separate monthly fees for each IoT device on a given network [1], [2]. Managing such contracts with a LoRaWAN or NB-IoT provider for each device in dense IoT installations, however, is expensive, scales poorly, and may be a bottleneck for realizing large-scale deployments, e.g., in smart cities. These devices vary considerably in their data needs, which also makes different connectivity models appropriate for different devices. For example, a camera continuously sending a video stream and a temperature sensor sending a single measurement every hour upload varying quantities of data at varying frequencies and qualities-of-service (QoS). Providing for these diverse needs will become even more challenging as IoT deployments grow.

This work was supported in part by the NSF grant CNS-1751075. We thank NSF for the support.

The overhead of provisioning dedicated contracts for each device may accelerate as 5G networks are more widely installed: such networks are expected to include dense deployments of multiple access points of different radio access technologies [3], [4], potentially with different operators, making it even more difficult to pre-specify contracts for individual IoT devices on each nearby operator. In this work, we develop an incentive-compatible mechanism that *unlocks* closed networks for end-devices to connect to, *without requiring any a-priori identity or trust association between these networks and devices*. Called *Datanet*, our system allows end-devices to seamlessly and securely connect to nearby closed networks that meet their needs and provide compensation for availed data services in real time, without relying on pre-established network-specific credentials like Subscriber Identification Modules (SIM)/ Pre-Shared Keys (PSK) or long-term payment contracts. As one of its key design goals, *Datanet* emphasizes *interoperability* with existing standards: it does not require firmware/hardware modifications in last-mile network equipment, and is hence compatible with any access network as long as EAP Transport Layer Security (EAP-TLS) authentication mechanism is supported (e.g. WPA-2 Enterprise WiFi and 5G-AKA').

Our Contributions. *Datanet* relies on three core insights to address *identity, trust, scalability, deployability and metering challenges* that arise in facilitating seamless and incentive-compatible connectivity between unknown devices and networks. First, we realize that **users' blockchain credentials can serve as their non-custodial identity across networks**, and access points (APs) can validate unknown users' payment ability by analyzing their records in tamper-proof and public decentralized ledgers. However, this requires significant AP hardware and software modification to integrate with the blockchain, which poses steep deployment challenges; further, this requires users to forecast APs they may connect with and lock up sufficient funds on the blockchain in escrow accounts with each (i.e. for making frequent off-chain micropayments for incremental units of service provided by the AP [5], [6], [7]), which is highly unscalable and practically limits the usefulness of such systems. Here, our second core insight is to use the remote Authentication, Authorization and Accounting (AAA) mechanism widely employed by cellular networks and

enterprise WiFi solutions. Cloud-based AAA servers can be easily modified to **integrate with the blockchain and perform EAP-TLS authentication to validate users' presented blockchain credentials** and authorize their access to last-mile networks. Anyone can host such a AAA service, and we refer to them as *Datanet* operators; instead of depositing their funds in escrow accounts with each individual AP, **end-users can then establish escrows with a limited number of *Datanet* operators and access any AP that utilizes one of these operators**. A simple configuration change to the AP suffices to offload these operations to the external AAA server, without hardware or software changes.

Finally, though decentralized ledger technologies can often act as a proxy for trusted intermediaries (e.g. displacing the role of Internet Service Providers or ISPs in our case), their ability to enforce and adjudicate interactions between the end-device and the access point depends on *the device data usage being digitally tracked in a tamper-proof manner*. Such **trusted metering**, however, is challenging to achieve in these situations without dedicated trusted hardware; indeed, solutions [8] requiring dedicated last-mile hardware that provides trusted metering of data sessions have seen slow adoption. The predominant micropayment model [5], [6], [7] alluded to earlier has been a workaround for this, where trusted metering is foregone but the loss incurred from failure to pay or failure to provide data services is capped: at most one round of *incremental* payment or service is wasted if the other party fails to provide the corresponding service or payment. But even so, a metering mechanism of *some* granularity is required to facilitate even the simplest QoS agreements/resource-use contracts essential for most applications, and to form a basis for discerning between unreliable and reliable access points and users. To enable tamper-proof monitoring of exchanged data services **without custom trusted hardware at APs**, we design a novel solution based on **trusted execution environments**, which are widely available in mobile phones and expected to be deployed in IoT devices [9].

We first present related work in Section II. We then analyze two publicly available datasets in Section III to demonstrate *Datanet*'s potential impact on IoT device connectivity and end-user data access. Section IV elaborates on *Datanet*'s design. In Section V, we present preliminary findings from our experimental evaluation of *Datanet* that demonstrates its low overhead and practicality, and conclude in Section VI.

II. Related Work

Blockchain's potential in displacing the role of centralized ISPs in the device-AP association process has received attention recently. Althea [10] facilitates an incentivized wireless mesh network (with possible gateway to the Internet) by providing Raspberry-Pis running specialized routing and pricing software, which users can plug into their off-the-shelf routers. Althea users make cryptocurrency micropayments to APs to pay incrementally for their data forwarding services, using pre-established payment channels with each router they connect to. Orchid [5] also has similar requirements to facilitate device access to a previously unknown router; however, it requires routers to be reflashed with special-purpose software. Helium [11] creates a wireless mesh network of proprietary LongFi hotspots that eventually have internet backhaul. These LongFi networks are expected to serve IoT devices and to be deployed by end-users. These protocols thus require APs to install special-purpose hardware or software to accept and validate micropayments that users send over pairwise user-AP channels, posing significant adoption barriers. Further, the pairwise payment channel model incurs significant scalability challenges for the networking context, where users may choose between tens to hundreds of APs a day to connect with and must first establish a payment channel with sufficient funds with each AP they transact with.

III. Potential *Datanet* Impact

Impact on IoT Devices. To assess potential connectivity benefits afforded to IoT devices due to *Datanet*, we consider the Array of Things project [12], which currently has a smart-city testbed of 126 IoT devices deployed in the city of Chicago. With *Datanet*, WiFi-capable IoT devices can utilize any *Datanet*-enabled WiFi access point that is in range for transmitting their sensed data to external servers for processing. Any WiFi AP can join *Datanet* as long as the AP supports authenticating with EAP-TLS (e.g. if the AP supports WPA-Enterprise as most do, changing its AAA server to a *Datanet* operator is a one-click setting change). Using crowdsourced information about WiFi hotspots in the area obtained from WiGLE [13], we correlate the location of each device in the testbed with WiFi APs in transmission range, categorized by the authentication mechanism used by the AP. We consider APs within a $0 - 50$m radius of the IoT device, based on previous studies on how the WiFi RSSI decays with distance from the WiFi AP [14].

As shown in Figure 1a, an IoT device in this testbed, on average, can reach approximately 14 hotspots (omitting APs whose employed security suite is unknown) even within a conservative range of 10m that presumably yields strong signal strength. Only 1 of these APs is open on average, while approximately 12 of the 13 closed APs use the WPA1 or WPA2 security suite (hence capable of supporting WPAx-Enterprise standard for remote AAA-based EAP-TLS authentication), which make them candidate *Datanet* APs. Upon widening the acceptable transmission range to 50m, the fraction of open hotspots does not exceed 10%, while the number of closed WPAx networks increases over tenfold. With *Datanet*, these private hotspots can become candidate Internet gateways for IoT devices, and be compensated for the occasional data transport services they provide.

Impact on End-user Devices. Smartphone users may also consider cheaper data plans with lower data limits if *Datanet* APs are widespread and provide a contract-less means of data access at more competitive rates. To quantify this hypothesized gain from *Datanet*, we verify whether a dense deployment of currently inaccessible closed APs exists around locations that users typically visit based on their regular mobility patterns.

For this evaluation, we utilize fine-grained mobility traces collected using the LifeMap mobility learning system [15], [16], which tracks the locations of eight students in Seoul, South Korea once every two minutes for two months. Prior analysis [15], [16] on this dataset shows that students are stationary 85% of the time, indicating that they would likely maintain stable connectivity even with short-range WiFi networks if they were to use *Datanet*. Some participants also made occasional trips outside South Korea. *Datanet* users who make such visits can particularly benefit from *Datanet* by avoiding the high international or roaming fees typical of most cellular data plans. For each unique location in this dataset, we retrieve information about WiFi hotspots found nearby from WiGLE and estimate the average number of accessible APs for different transmission ranges, accounting for user localization errors specified in the mobility trace.

Figures 1b and 1c depict reverse CDFs of mean hotspot availability corresponding respectively to 10m and 30m radius from each user location. There is $< 5\%$ chance of a user encountering an open hotspot within a 10m radius, compared to a 35% likelihood of finding a closed WPAx hotspot in that range and even a 10% chance of encountering upto five WPA2 hotspots. Even after expanding the radius to 30m, there are significantly fewer open hotspots than private ones. There is a 20% probability of encountering atleast 15 closed hotspots in a given location while only a 5% chance of encountering atleast five open hotspots. Finally, we account for time spent in each location. Figure 1d shows the average count of each type of router accessible within different transmission distances from users' locations, weighted by the time users spent in that location. A typical user is within range of $2-17$ closed WPA2 hotspots at any given time, while very few open routers are deployed. *Datanet*-enabled opportunities to utilize these private hotspots thus significantly increase end-user connectivity options.

Impact on Access Points. We next demonstrate that private routers have sufficient idle capacity to serve additional users through *Datanet*. We analyze the hourly bandwidth utilization of 1,200 home routers from the Measuring Broadband America initiative [17], collected on October 2017. Figure 2a shows a mean network utilization of at most 2 Mbps across routers for all days observed, including peak evening hours. With typical home network capacity of $40-75$ Mbps [18], over 90% of this capacity is unused. Though closed routers in corporate environments may be more heavily utilized, this analysis nevertheless indicates that many private APs would be able to monetize their additional capacity with *Datanet*.

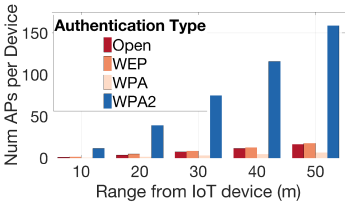
To measure these APs' incentive to join *Datanet*, we correlate government-provided population densities for Seoul, South Korea [19] with the APs for which they are in transmission range. The population data partitions Seoul's total area of 605sq. km. into 19153 regions, and provides hourly measures of the number of people in each region. From the WiGLE database, we find approximately 650000 APs with unique MAC IDs in Seoul. Approximately 88% of the APs support WPAx encryption, while 6% of them are open. Most of Seoul lies within 50m of at least one AP (Figure 2b).

With *Datanet*, closed APs may seamlessly connect to and serve any interested user. We thus aim to estimate the number of such users for each AP. We pick a representative day from the population density traces and conservatively consider users within a short 10m transmission range. For each closed AP, we estimate the potential number of users it may serve each hour by multiplying the population density in the AP's region for that hour by the transmission coverage area. Figure 2c shows the resulting mean and standard deviation across the APs, indicating that they could serve over 10 additional users for at least 10 of the busiest hours of the day. Figure 2d further weights this potential benefit by users' typical daily data usage, which is estimated from smartphone usage measurements collected from 20 users over 10 days. Factoring this in, a closed router may serve several hundred megabytes of additional network traffic on average at some hours of the day.

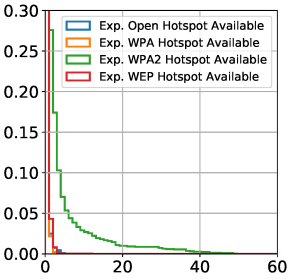
IV. *Datanet* Design

Figure 3 illustrates *Datanet*'s core components and the typical end-device flow in *Datanet*. We define the *Datanet* **smart-contract** on a public and permission-less blockchain. The contract implements a payment protocol that facilitates large volumes of frequent off-chain device-AP payments through intermediary *Datanet* operators. Several scalable off-chain cryptocurrency payment mechanisms have been proposed that may be used here, for e.g. Lightning-style payment hubs, custodial payment hubs, and PayPlace [20]; further discussion about these payment protocols is out of scope here.

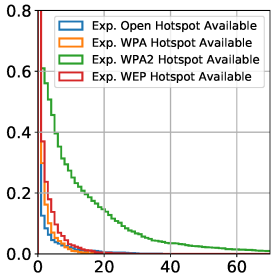
The user of an end-device (smartphone, IoT device, etc.) first queries the *Datanet* contract for a list of registered *Datanet* operators, i.e. their public keys and any other associated identifiers (step 1 in Figure 3). Indeed, *Datanet* operators are required to register with the contract to be able to function as intermediaries in the device-AP payment flow. The user then registers their public key with the *Datanet* contract (step 2 in Figure 3) by depositing some value of cryptocurrency that they can later spend off-chain for data connectivity services availed through *Datanet* access points. Users also specify an initial split of this deposit amount between *Datanet* operators of their choice. They may later move their unspent funds from one operator to the other using challenge-timeout exit games [21]. For instance, once a user submits a request to the contract to move a portion of their deposited funds from one operator to the other, the contract initiates a wait period during which the originating operator can challenge this transfer by providing proof (i.e. a micropayment cryptographically signed by the user) that the user has already spent the referenced funds. If the transfer is proven to be invalid, it is cancelled by the contract and the user potentially penalized; otherwise, the transfer finishes when the wait period times out. Similar to prior work, we denote the cryptocurrency denomination by ₵ (e.g. ETH/BTC/other ERC-20 tokens). The registering user's details (public key, amount deposited) are broadcasted by the contract (similar to Ethereum events) and received by subscribed *Datanet* operators (steps 3-4).



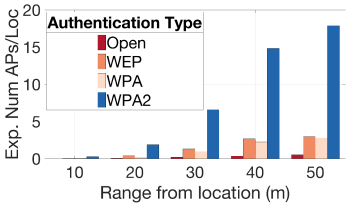
(a) Approximately 12 closed *Datanet*-compatible WiFi access points are available on average to each deployed IoT device in the testbed, even within 10m.



(b) Reverse CDF (zoomed in) of number of WiFi APs within 10m of each location.

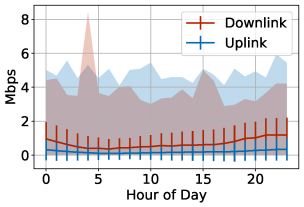


(c) Reverse CDF (zoomed in) of number of WiFi APs within 30m of each location.

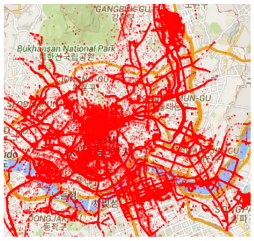


(d) Estimated average number of accessible WiFi routers across all locations, weighted by duration spent in that location and categorized by supported encryption type.

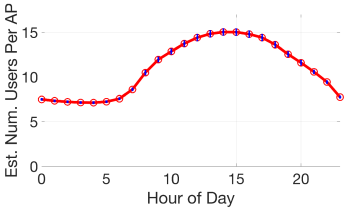
Fig. 1: We depict statistics for the number of accessible hotspots for each unique location in the LifeMap mobility dataset [15].



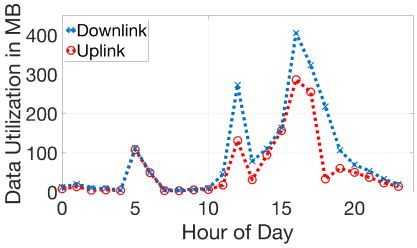
(a) The mean downlink and uplink utilization for home routers do not exceed 2Mbps.



(b) Locations within 50m range of WiFi APs in Seoul.



(c) Potential number of users, on average, that a closed WiFi AP in Seoul may connect to within 10m range, based on region density for each hour of day.



(d) Mean additional downlink and uplink utilization at closed WiFi APs from potential *Datanet* end-devices, by hour of day.

Fig. 2: Depicting (a) underutilization of typical home routers, and (b,c, d) potential benefit to private APs in Seoul by serving data needs of devices accessible through *Datanet*.

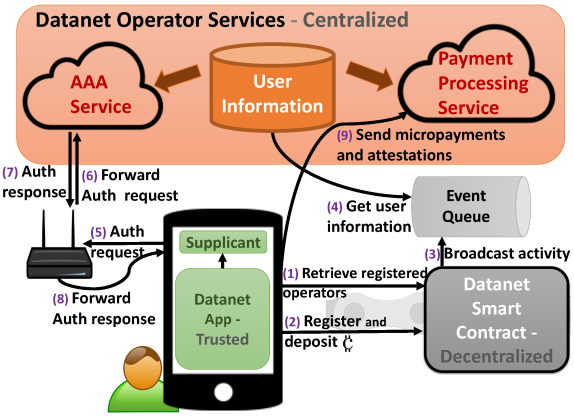


Fig. 3: We illustrate *Datanet*'s core components and interactions for an end-device to onboard and avail *Datanet* APs.

An **access point** onboards onto the *Datanet* system (i.e. can serve unknown users in return for remuneration) simply by associating with a *Datanet* operator of its choice, i.e. directing its auth module (e.g. that usually defaults to WPA-Personal for home WiFi routers) to the chosen operator's remote AAA service, configurable via the administration interface for WPAx routers. We note that a WiFi AP may continue to provision WPA-Personal authentication for home users, if needed, using a separate isolated SSID. 3GPP networks are ubiquitously configured to utilize their respective operator's AAA services for SIM-based authentication today; to support connections from unknown users with *Datanet*, they simply need to associate with a *Datanet* operator to perform the requisite EAP-TLS authentication. For instance, the cellular network operator may themselves function as a *Datanet* operator by implementing the appropriate blockchain-based functionality or utilize an available *Datanet* operator for performing authentication and payment processing of unrecognized users.

A *Datanet* **operator** hosts cloud applications for (1) performing AAA functions that specify whether an AP should accept connection requests from untrusted end-devices, and (2) processing micro-payments received in real time from end-devices connected to APs that use the operator's AAA service. Specifically, *Datanet* AAA servers receive the connecting end-users' blockchain credentials through the EAP-TLS authentication standard, and verify whether a) the presented credentials are correct (i.e. the user is the owner of the claimed public-key), 2) the public-key has been registered on the *Datanet* smart-contract, and 3) the user has non-zero deposited funds with this operator and the unspent portion of these funds exceeds some minimum threshold set by the operator. The EAP-TLS authentication succeeds if these checks are met; the AP can then commence a data-session with the user. This allows for a seamless connectivity experience as end-devices and WiFi hotspots almost ubiquitously support the EAP-TLS standard; with 5G, even cellular networks are expected to support EAP-TLS through the EAP-AKA' standard. We note that the authority signing the end-user's certificate is irrelevant since the *Datanet* smart-contract on the blockchain specifies public-keys of valid end-users. Since end-devices retrieve the list of *Datanet* operators from the blockchain (step 1 in

Figure 3), they can verify whether the presented AAA server's credentials belong to a valid *Datanet* operator during the EAP-TLS handshake.

An end-user who has registered with the *Datanet* contract and has sufficient unspent funds deposited with *Datanet* operators, can then seamlessly access *Datanet*-enabled APs. *Discovering* these access points is easiest if they can beacon *Datanet* support; Hotspot 2.0 frames support signalling details like associated *Datanet* operator, price charged by the access point, QoS capabilities, and others. For APs that do not yet support Hotspot 2.0, *Datanet* operators may be queried off-band to retrieve details of surrounding *Datanet* APs. AP-specific information can always be signalled at the application layer by the corresponding *Datanet* operator after an end-device establishes a successful connection to the AP.

An **end-device** initiates association by sending an EAP-TLS authentication request to a *Datanet* AP using its blockchain credentials (step 5) that is forwarded to the corresponding operator's AAA service (step 6). Note that once a successful handshake is established with the end-device (steps 7-8), *the ensuing session between the end-device and the AP is encrypted at the PHY-layer (as per the remote EAP-TLS standard)*. Once the session is established, the *Datanet* application installed on the device initiates periodic micropayments to the operator identified in the handshake (step 9). For instance, if the advertised charge of the AP is .001¢ per minute, the *Datanet* application makes an incremental micropayment of .001¢ every minute. The remote payment processing service performs continuous authorization of connected users, ensuring that each received micropayment is valid (i.e. correctly signed with the user's blockchain credentials). Processing micropayments remotely through the operator's cloud services allows APs to use *Datanet* without requiring special-purpose software to handle these. If an active user misses consecutive payments or their unspent funds with the operator gets depleted, the payment service notifies the AAA server, which issues a well-defined disconnect command (e.g. CoA in RADIUS [22]) to the AP that terminates the user's session. If, on the other hand, the user finds the AP's service quality poor, the user may halt micropayments. Through this mechanism, untrusting APs and end-devices engage in incentive-compatible data sessions with negligible loss.

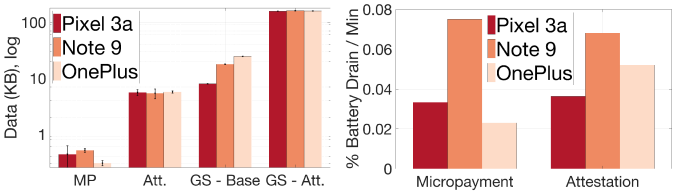
However, more reasonable payment structures likely include some measure of the data service rendered in exchange for micropayments. For instance, the AP may wish to charge .004¢ per MB of data transferred; in this case, the micropayment amount that the operator receives every minute varies based on the amount of data transferred between device and AP. To correctly detect user's underpayment and issue a connection termination command to the AP, the operator must then be able to compare the received payments to the services provided. Such remote monitoring of the device-AP data session requires tamper-proof metering of the session. Running traffic monitoring software on the end-device's Trusted Execution Environment (TEE) and reporting the recorded incremental network utilization to the operator would be a straightforward solution. However, popular mobile and embedded operating systems do not typically support running third-party software in their TEE (e.g. ARM TrustZone [23]). Hence, we instead design the *Datanet* application that runs on the end-device to be *trusted* (as in Figure 3), require that the end-device itself be uncompromised, and subsequently incorporate network traffic monitoring capability into the application.

Ensuring that the *Datanet* application is *trusted* is done by open-sourcing the codebase and explicitly relating this code to the executable available in App Stores (e.g. Google Play Store's APK) through certified compilation techniques (e.g. [24]) and publicly auditable Continuous Integration servers. For every time period that the application issues a micropayment for a usage-based payment structure, it also reports measured data usage statistics to the operator. To trust the reported readings, the operator must be able to verify that they have been generated by the (trusted) *Datanet* application running on an untampered device. We utilize TEE-enabled remote attestation services for this. In Android phones, for instance, we can avail Google's `SafetyNet` Attestation API [25]; when reporting the measured utilization values, the *Datanet* application also makes a call to the SafetyNet API and sends the signed response it receives to the operator. The response identifies the calling application, timestamp, and an indication of any known current integrity issues in the device (e.g. root capabilities that invalidate OS trust). If the timestamp matches current time, the stated package name of the calling application matches the trusted *Datanet* application, no integrity issues are indicated, and the signature on the attestation has been generated by the trusted third party (Google, in this case), then the operator considers the reported utilization as accurate. Trusted utilization readings can similarly be obtained in other OS as well. For instance, for IoT devices that may run on ARM boards like the Raspberry Pi, the *Datanet* application can be executed as a Trusted Application in OP-TEE, and remote kernel-integrity attestation services [26] along with Linux IMA and Secure Boot utilized to validate that the device has not been tampered with.

These trusted utilization readings can also be used to assess different APs' and end-devices' reliability, potentially leading to a *reputation system* that informs users' decisions to connect with specific APs and vice-versa. Note that WiFi access points are increasingly equipped with Trusted Platform Module that provide attestation capabilities as well. Such APs can also send their own trusted measurements for computing ground truth.

V. Preliminary Evaluation

To assess the overhead on end-devices in *Datanet*, we implement a functional prototype. A *Datanet* operator is setup on AWS cloud, with a FreeRADIUS instance providing the blockchain-based AAA services. We setup a test blockchain network using Ganache including a smart-contract for coordinating user balances and payment transactions. We use an off-the-shelf UniFi AC Pro AP for processing *Datanet* connection requests from end-devices, configured to use the FreeRADIUS AAA cloud instance. We develop the *Datanet* application



(a) Data consumed per micropayment/attestation call, in KB - log scale

(b) Battery drain per minute for micropayment and attestation operations.

Fig. 4: (a) Network traffic and (b) battery drain from performing attestation and micropayment every minute for 5 hours.

on the Android OS; Google's SafetyNet API [25] is used for remote attestation of measured utilization readings, and `secp256k1` curve (used in Ethereum) is used for generating user keys. We run the *Datanet* application on three devices – Google Pixel 3a, Samsung Galaxy Note 9 and OnePlus 7 Pro. Attestation and micropayment calls are separately repeated every minute at each device for upto 5 hours.

We use Android's `BatteryHistorian` and `BatteryProfiler` tools [27] to infer the overhead of these operations in terms of network traffic and the resulting battery drain. Sending a micropayment to the *Datanet* operator's payment service consumes less than 500 bytes on average while sending the attestation command response over the network incurs approximately 10KB. For the attestation call inspecting the call trace revealed that hidden Google Play processes were invoked, which may transfer additional information over the network to Google's server. As Figure 4a shows, the typical network traffic generated by Google Services is around 10KB/minute (GS-Base) but increases to 100KB/minute when the attestation call is performed every minute (GS-Att), indicating a 100KB overhead per `SafetyNet` API call. As seen in Figure 4b, the battery drains at a rate of $.04 - .08\%$ per minute, across attestation and micropayment, indicating *no significant increase in battery consumption* from these operations.

VI. Conclusion

In this work, we propose *Datanet* to enable seamless and incentive-compatible connectivity between end-devices and access points without any prior subscriptions, using trustless blockchain-federated identity management and payments. We employ remote AAA servers to perform this blockchain-based authentication, thereby avoiding any hardware or even software modification at access points (which otherwise would considerably impede adoption). We utilize the well-defined and ubiquitously adopted EAP-TLS authentication standard that results in encrypted PHY-layer sessions between devices and APs. To enable practically useful payment models like usage-based payments, we design a novel use of trusted execution environments that are available for performing device integrity checks and attestations in mobile OS, to provide tamper-proof network utilization metering without specialized hardware support. We demonstrate *Datanet*'s potential benefit to IoT devices and end-users and preliminary evaluation shows that *Datanet* incurs little overhead in client devices.

References

[1] D.-K. Electronics, "IoT Cellular Data Plans," 2020. [Online]. Available: https://www.digikey.com/en/resources/iot-resource-center/iot-cellular-data-plans

[2] T-Mobile, "Network pricing for the Internet of Things," 2020. [Online]. Available: https://www.t-mobile.com/business/iot/pricing

[3] S. Andreev, V. Petrov, M. Dohler, and H. Yanikomeroglu, "Future of ultra-dense networks beyond 5g: harnessing heterogeneous moving cells," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 86–92, 2019.

[4] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5g and future mobile networks: mobility, resource management, and challenges," *IEEE communications magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[5] J. S. Cannell, J. Sheek, J. Freeman, G. Hazel, J. Rodriguez-Mueller, E. Hou, and B. J. Fox, "Orchid: A Decentralized Network Routing Market," Orchid Labs, Tech. Rep., 2019. [Online]. Available: https://www.orchid.com/assets/whitepaper/whitepaper.pdf

[6] R. Radhakrishnan, G. S. Ramachandran, and B. Krishnamachari, "SDPP: Streaming Data Payment Protocol for Data Economy," in *2019 ICBC*. IEEE, 2019, pp. 17–18.

[7] D. Chen, Z. Zhang, A. Krishnan, and B. Krishnamachari, "Payflow: Micropayments for bandwidth reservations in software defined networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops*. IEEE, 2019, pp. 26–31.

[8] "Ammbr whitepaper," Ammbr Foundation, Tech. Rep., 2018. [Online]. Available: https://ammbr.com/docs/2018/11/Ammbr_Whitepaper.pdf

[9] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: an enhanced, trusted execution environment for industrial IoT edge devices," *IEEE Internet Computing*, vol. 21, no. 1, pp. 40–47, 2017.

[10] J. Tremback, J. Kilpatrick, D. Simpier, and B. Wang, "Althea whitepaper," Hawk Networks, Tech. Rep., 2019. [Online]. Available: https://althea.net/whitepaper

[11] A. Haleem, A. Allen, A. Thompson, M. Nijdam, and R. Garg, "Helium: A Decentralized Wireless Network," Helium Systems Inc., Tech. Rep. [Online]. Available: http://whitepaper.helium.com/

[12] "Array of things." [Online]. Available: https://arrayofthings.github.io/

[13] WIGLE, "Wigle.net," 2020. [Online]. Available: https://wigle.net/

[14] A. Valenzano, D. Mana, C. Borean, and A. Servetti, "Mapping wifi measurements on openstreetmap data for wireless street coverage analysis," in *FOSS4G Conference Proceedings*, vol. 16, no. 1, 2016, p. 5.

[15] J. Chon and H. Cha, "Lifemap: A smartphone-based context provider for location-based services," *IEEE Pervasive Computing*, 2011.

[16] Y. Chon, H. Shin, E. Talipov, and H. Cha, "Evaluating mobility models for temporal prediction with high-granularity mobility data," in *2012 IEEE PerCom*. IEEE, 2012, pp. 206–212.

[17] SamKnows, "Measuring Broadband America," 2017. [Online]. Available: https://www.measuringbroadbandamerica.com/

[18] S. Intelligence, "Speedtest global index," 2020. [Online]. Available: https://www.speedtest.net/global-index

[19] Seoul Metropolitan City Office, "Seoul Living Population," 2020. [Online]. Available: http://data.seoul.go.kr/dataVisual/seoul/seoulLivingPopulation.do

[20] M. Harishankar, D.-G. Akestoridis, S. V. Iyer, A. Laszka, C. Joe-Wong, and P. Tague, "Payplace: Secure and flexible operator-mediated payments in blockchain marketplaces at scale," *arXiv preprint arXiv:2003.06197*, 2020.

[21] "Minimum viable plasma," https://ethresear.ch/t/minimal-viable-plasma/426, accessed: 2019-12-07.

[22] Network Working Group, "Dynamic authorization extensions to Remote Authentication Dial In User Service (RADIUS)," RFC 5176, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5176

[23] K. Ying, A. Ahlawat, B. Alsharifi, Y. Jiang, P. Thavai, and W. Du, "Truz-droid: Integrating trustzone with mobile operating system," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, 2018, pp. 14–27.

[24] X. Rival, "Symbolic transfer function-based approaches to certified compilation," *ACM SIGPLAN Notices*, vol. 39, no. 1, pp. 1–13, 2004.

[25] Android Developer, "Safetynet attestation api," 2020. [Online]. Available: https://developer.android.com/training/safetynet/attestation

[26] S. Han and J.-H. Park, "Shadow-box v2: The practical and omnipotent sandbox for arm," 2018, slideshow at Blackhat Asia 2018.

[27] "Profile battery usage," 2020. [Online]. Available: https://developer.android.com/topic/performance/power/setup-battery-historian