dAuth: A Resilient Authentication Architecture for Federated Private Cellular Networks

Matthew Johnson*
matt9j@cs.washington.edu

Sudheesh Singanamalla*
sudheesh@cs.washington.edu

Nick Durand*
durandn@cs.washington.edu

Esther Jang
infrared@cs.washington.edu

Spencer Sevilla
sevilla@cs.washington.edu

Kurtis Heimerl
kheimerl@cs.washington.edu

University of Washington
Seattle, WA, USA

Abstract

We present dAuth, an approach to device authentication in private cellular networks which refactors the responsibilities of authentication to enable multiple small private cellular networks to federate together to provide a more reliable and resilient service than could be achieved on their own. dAuth is designed to be backwards compatible with off-the-shelf 4G and 5G cellular devices and can be incrementally deployed today. It uses cryptographic secret sharing and a division of concerns between sensitive data stored with backup networks and non-sensitive public directory data to securely scale authentication across multiple redundant nodes operating among different and untrusted organizations. Specifically, it allows a collection of pre-configured backup networks to authenticate users on behalf of their home network while the home network is unavailable. We evaluate dAuth's performance with production equipment from an active federated community network, finding that it is able to work with existing systems. We follow this with an evaluation using a simulated 5G RAN and find that it performs comparably to a standalone cloud-based 5G core at low load, and outperforms a centralized core at high load due to its innate load-sharing properties.

CCS Concepts

• **Networks** → **Mobile networks**; **Network security**; Network mobility; *Network structure*; • **Applied computing**; • **Security and privacy** → *Authentication*; **Network security**;

Keywords

LTE, 5G, authentication, cellular networks, secret sharing, community networks

ACM Reference Format:
Matthew Johnson, Sudheesh Singanamalla, Nick Durand, Esther Jang, Spencer Sevilla, Kurtis Heimerl. 2024. dAuth: A Resilient Authentication Architecture for Federated Private Cellular Networks. In *ACM SIGCOMM 2024 Conference (ACM SIGCOMM '24), August 4–8, 2024, Sydney, NSW, Australia.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3651890.3672263

*Work done while at the University of Washington

ACM SIGCOMM '24, August 4–8, 2024, Sydney, NSW, Australia

ACM ISBN 979-8-4007-0614-1/24/08
https://doi.org/10.1145/3651890.3672263

1 Introduction

Private cellular networks, logically discrete cellular networks operated by small organizations such as factories, universities [15], or libraries [13], are expected to grow massively over the next five years, with Grand View Research predicting a compound annual growth rate of 51.3% through 2030 [47]. Despite this expected growth, critical elements of how these systems will be deployed remain unclear; will they simply be extensions of existing carrier networks (known as Public Network Integrated Non-Public Networks), or will some of them operate autonomously – providing connectivity without incumbent participation (known as Standalone Non-public Networks)? Historical trends argue for centralization, with existing mobile operators reaping the benefits.

In this work, we explore how to design private networks for a more distributed and equitable future. Researchers have proposed that community-based networks (CNs) could help to bridge the internet usage gap, both by providing access to new areas by changing the economic balance of providing connectivity [48], and by allowing locally engaged organizations to reach sub-populations excluded by traditional networking systems and structures [11]. In particular, community-based CNs offer affordances well-suited to bridging access gaps, including wide-area coverage [23] serving many users [53], and indoor coverage to reach people outside of traditional public access locations [12].

However, despite significant technology shifts, including new licensing regimes for spectrum (e.g., CBRS) and production-grade open-source core networks, various challenges remain in enabling small local organizations to independently deploy and operate cellular networks. Notably, the design of the network authentication process limits the utility of standalone private networks, requiring each edge network to either register each user or rely on the roaming process to authenticate with the a new user's home network. Furthermore, existing core network architectures require the core network to be highly available and reachable (discussed in §2.2), which drives small networks to use managed core networks provisioned by a traditional telecom provider (Telco) or cloud provider. Yet, this outsourcing approach removes the agency of the local networks, requires users to put their trust in an external entity, and results in coupling that harms resiliency in the face of central service outages. Notable recent events events such as the Rogers

communication outage in Canada (due to network misconfigurations [56]) and AT&Ts multi-day South-East outage (due to an explosion [58]) brought millions of users offline.

In this work, we propose a design that instead takes advantage of the independent operations of private network operators to provide robust and resilient connectivity to end-users despite individual operator unreliability. We imagine a diverse collection of local institutions, grounded on physical-world relationships and hosting their systems in both local and cloud servers, would serve as the anchor for their local users. Unlike the traditional cellular architecture, our design allows the network to more gracefully tolerate transient unavailability of its individual components, making it feasible for smaller organizations to operate networks themselves.

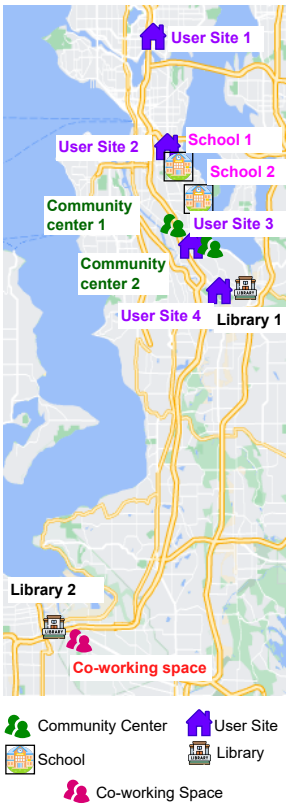


Figure 1: A map of the Seattle Community Network.

Specifically, we define a community-based federated trust model that allows organic scaling of a wide-area network deployment with only incremental trust between partner organizations. We then build an authentication and authorization scheme using this model for granting access on a serving network (even when the user's home network is offline). Unlike traditional roaming, which requires explicit partnerships and agreements between telecoms, we introduce an additional layer of abstraction which removes the need for explicitly setting up these relationships – allowing our system to scale with minimal overhead. Our design, dAuth, remains compatible with off-the-shelf devices (UEs) to take advantage of the robust existing handset install and repair base (and avoid kafkaesque cellular standardization).

We develop a prototype of dAuth, evaluate its performance, and demonstrate its compatibility and technical feasibility with a testbed deployment in partnership with the Seattle Community Network (SCN), a regional federation of community cellular networks deployed in an urban area in the United States. We evaluate our system's performance against a centrally hosted "cloud core" and a non-roaming "edge core" private network. In addition to allowing for organic decentralized growth of federated mobile access networks, we believe that the benefits of our proposed architecture go beyond this use case, offering opportunities to design more resilient cellular networks.

Host Org.	Backhaul Fiber Provider	Availability
Co-working space	University Campus	99.021%
School 1	Lumen	98.998%
Community Center 1	Lumen	95.815%
Library 1	Lumen	91.821%
School 2	University Hospital	89.562%
Community Center 2	Lumen	87.171%
Library 2	University Campus	N/A

Table 1: Deployed LTE sites in the Seattle Community Network. Uptime has been largely determined by equipment failures and upstream ISP misconfigurations. No sites have "3 nines" of availability (< 8 hours and 47 minutes of yearly downtime). Library 2 has yet to launch due to construction.

2 Background & Context

Our work is situated at the intersection of work on community-based networks and cellular networks. In this section we provide background context for both of these domains.

2.1 Community Networks

Community networks (CNs) are physical instantiations of networks built, owned, and operated by the community the serve. There are a huge diversity of CNs – as diverse as the varied communities they come from.

The designs in this project were motivated by experiences working with SCN, a network founded to connect marginalized populations who have not been able to, do not want to, or could not afford services from traditional providers.

SCN has a strong organizational mandate to empower local users and seeks to de-mystify Internet infrastructure through co-ownership. SCN currently has 11 deployed sites (7 Private LTE and 4 WiFi) with a variety of partners including 2 public libraries, the local school district, 2 community centers, 4 Tiny House Villages (user sites), and a hackerspace. The sites are diverse and have a variety of backhaul connections from various ISPs. Table 1 lists the 7 LTE site details. Importantly, all sites are maintained and operated by volunteers or available staff at each partnering host organization and see a range of uptimes which are individually insufficient for traditional high-reliability cellular network services.

2.2 Cellular Networks

This work focuses on cellular networking technologies, which are heavily standardized and have a specific set of roles and functions divided between the "Radio Access Network" (RAN), the actual radio basestations providing access across the network, and the "Core Network" (Core), the set of more centralized systems connecting together the RAN elements. The cellular network architecture evolved in the context of wide-area telecommunications services and core network functions are responsible for city or region-scale sets of resources operated by a professional "mobile network operator" (operator/MNO) commonly of national scale.

Cellular networks have standardized interfaces for "roaming", the ability to use a device from one operator's network via another operator's network [1]. In cellular roaming, the "visited" or "serving" network communicates back to the "home" network to authenticate the users' identity. The home network completes the Authentication and Key Agreement (AKA) with the UE based on the secret key held by the operator and the users' SIM card. At the

conclusion of the AKA procedure the serving network is provided a key to communicate with the UE and the user can be confident that their home network has approved of the operations of the visited network they are communicating with. There are many variations of roaming architectures between operators, and in some cases the users' traffic is tunneled all the way back to their home network for policy enforcement and billing [34].

2.3 LTE & 5G Networks

Starting with 4G-LTE (3GPP Release 8+) and continuing with 5G (3GPP Release 15+), modern cellular networks have moved to a design where packet-switched IP services are used to provide both plain data and QoS-enhanced voice/video and emergency services to end users over a common substrate.

Partly due to the ease of IP interconnect and partly due to the availability of new hardware in lightly-licensed regimes like CBRS or general secondary use [4], researchers have explored smaller and more standalone deployments of cellular networks for community connectivity over a town-scale area from a single tower [25, 30, 53]. These networks have either operated independently in a standalone mode, with no roaming capability, or relied on a third-party service to hold user keys and serve as a broker for authentication [33].

Network Authentication: One may immediately ask, if we want users to be able to roam onto many different network, *'Why not just replicate the user credentials across every node?'*. While this would allow for users to move between networks, it would create unacceptable security concerns due to the reveal of secret keys. While most higher-level user traffic is end-to-end encrypted on modern mobile devices, users are still vulnerable if connected to a compromised cellular access network. In addition to attacks such as blackholing, or redirecting the encrypted user traffic, a fully authenticated mobile network has much more control over the user's device than in more distributed standards like WiFi.

Along one dimension, the RAN has tight control over the UE radio and can cause it to tune to different frequencies and transmit at different power levels, potentially turning the UE into an unwitting jammer or scanner, and draining its battery. Along another, in LTE (which a 5G network can commonly downgrade to) the network also has the ability to craft and intercept SMS messages from arbitrary numbers, creating spam or malicious phishing messages from sensitive trusted numbers. Additionally, the cellular standards allow an authenticated RAN to query sensitive information from the UE baseband like hardware identifiers (e.g., IMEI) or the user's current location (e.g., E-CID). Even at the application layer, the RAN provides timing and coarse location data which can be spoofed and consumed by a phone's operating system and/or applications leading to timing attacks. Unlike prior works, the importance of a non-malicious serving network drives dAuth to not dismiss link authentication [53].

3 Design Elements

As discussed in 2.1, the primary purpose of dAuth is to allow a wider variety of smaller anchor community organizations to control and operate mobile private access networks in a municipality-scale federation. Given our experience with SCN, we expect these organizations to vary widely in their technical capacity, interest, and resilience. Given this, the overarching technical design goal of dAuth is to **enable an organizationally heterogeneous network**, including low-technical capacity and even potentially malicious actors.

3.1 Key design goals

This high-level goal breaks down along three major axes: (1) **Tolerate Failures:** Tolerate temporary failure of a subset of nodes without losing liveness or safety of the overall system. (2) **Tolerate Malicious Nodes:** Tolerate the presence of malicious nodes outside the users' home network without compromising the users' security. (3) **Compatibility:** The system must work in both cloud and edge cores [52] and interoperate with existing off-the-shelf hardware built for standardized 4G and 5G networks and without requiring dAuth-specific upgrades.

3.1.1 ***Tolerate Failures*** To lower the threshold to include organizations in the federation with a wide-range of networking experience and technical sophistication, the overall federation must be resilient to (relatively) small hiccups in operation of any particular organization's network. This reduces the operational burden on individual anchor institutions and allows for operational shortcuts like planned maintenance windows and system reboots with minimal disruptions. Specifically dAuth should allow a user to gain access through an alternative serving network in the federation even when the user's home network core is temporarily unavailable. We parameterize our prototype around the expectation of home network outages lasting a day.

3.1.2 ***Tolerate Malicious Nodes*** Driven by our desire to increase the number of operators by lowering the trust barrier to entry, dAuth needs to tolerate a subset of malicious nodes in the federation. It is even possible that previously trusted nodes could become malicious due to compromise. As a federation of organizations running networks, a *threshold* for malicious behavior or mis-configurations is agreed upon and configured in the dAuth ecosystem, forming the requirements for cryptographic secret sharing. While we assume any user can trust their own home network, dAuth should provide a way to prevent a user from attaching to untrusted serving networks and tolerate the compromise of a subset of backup networks while providing strong accountability guarantees to serving networks about the users and their home network – critical for compliance and billing.

3.1.3 ***Compatibility*** Fundamentally, this research is a form of action research [7] and this technology is being developed to enable SCN to provide connectivity to low-income and unhoused people in our home region. Deploying our solution into production will require flexibility in deployment environments given the diversity of operators and the economies of scale of the existing cellular equipment ecosystem with a design that can be realized with unmodified off-the-shelf user device hardware built for standards-compliant 4G and 5G networks.

In 4G-LTE there was only a single authentication scheme (4G-AKA) required for user devices, and while 5G does specify additional optional support for the IEEE Extensible Authentication Protocol (EAP), the only authentication all devices are required to support is 5G-AKA [3]. 5G AKA is very similar to 4G AKA, with an additional round of confirmation that the user is present in the serving network

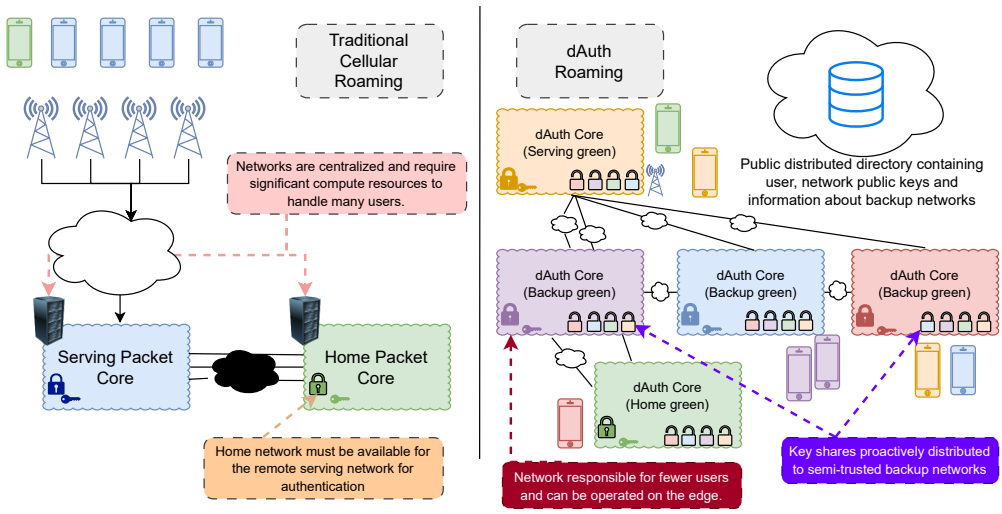


Figure 2: The high-level design of dAuth versus traditional cellular roaming. dAuth factors some non-sensitive information into a distributed public directory service, and allows home networks to proactively distribute shares of key material to backup networks to improve resiliency in a semi-trusted environment.

before exchanging the session key. In order to support the broadest number of devices possible, we have designed dAuth to look exactly like 4G/5G AKA from the basestation and handset's perspectives. We do assume that the core network functions (in software) can be modified at will and the user's SIM card is issued and managed by their trusted *home* network operator.

3.2 Threat Model

dAuth assumes the same threat model of a traditional cellular network: your home network is completely trusted and other providers are not. This can be seen in authentication, where critical key information (K_i) is stored on the SIM card, which is manufactured and distributed by the operator. Roaming similarly works in this way, with intermediate serving providers having business agreements with various networks simply forwarding packets between users and home networks to conduct authentication.

This model is assumed primarily for backwards compatibility (see 3.1) and not correctness. While cellular systems clearly operate successfully at scale with such a setup, there are numerous known attack vectors including physical attacks such as ThinSIMs[45], interconnect attacks at the SS7 layer [26], and social attacks such as SIM swaps [31]. As far as we know, such attacks are perpendicular to our goals in this work and solutions should be compatible when developed.

dAuth additionally assumes the capability for adversaries to perform denial of service attacks on the home network of the user and other federated entities within the failure tolerance threshold preventing the ability to complete 4G/5G AKA procedures in traditional roaming context.

3.3 Refactoring Auth For Trust at Scale

In order to allow dAuth to scale, the system design distinguishes between non-sensitive public information, such as public keys and subscriber network mapping, from sensitive personal information like when and where the user has authenticated and which traffic they send. dAuth factors out the non-sensitive global information to allow the use of a traditional large distributed directory like a verifiable key directory, DNS, or a distributed ledger [55]. These directories can scale up publicly with very low overhead.

dAuth leaves the sensitive information about authenticating the particular user and making authorization decisions for that user onto a particular serving network to a much smaller set of trusted entities. These entities communicate directly, limiting the exposure of the user's more sensitive telemetry to only the nodes participating in the current authentication. While authentication information is split across multiple backup networks, the fan-out of information from each home network is limited to a constant factor (at most 31 in the current design). This constant factor, independent of the total number of networks, allows the overall system to scale naturally with the increase in participating networks.

Federated Trust Model: Decentralized and federated systems allow users to limit the scope of who they trust with their information. With dAuth, users can establish a real-world relationship with an organization they trust. This trusted organization is the user's *home* network, and serves to anchor their identity in the wider dAuth ecosystem. The dAuth home network fulfills the role of a traditional operator home network, holding the user's AKA derived secret key, generating authentication vectors, and serves as an anchor for user identity when roaming onto a different network.

Our desire to enable resiliency in the face of home network failure is at odds though with the interactive authentication between the home HSS/AUSF and the serving network in traditional 3GPP standardized cellular roaming. To navigate this tension, we define a third intermediate level of trust in between the home network and the untrusted serving network, the *backup* network. In our trust model, a set of semi-trusted backup networks can cooperate with a dAuth serving network to complete the interactive portion of 4G/5G-AKA during home network unavailability, without ever

having access to the user's symmetric key or the derived secrets. Additionally, unlike a traditional 3GPP home network, dAuth backup network grants are *revokable*, allowing the user or the user's home network to remove trust from a backup network through a secure revocation procedure.

3.4 System Components

Each operator deploying dAuth in their core network generates a public-private key pair (SK, PK) used for cryptographically signing messages. The public keys (PK) are shared with other operators in the federation. In dAuth, the public keys of each network is shared using a *directory* with no controlling organization allowing for existing verifiable key directory schemes [14, 35], or hierarchical approaches such as DNS with DNSSEC usage to be used. The directory is distributed allowing the discovery and verifiable identification of the public key PK_n associated with a specific network operator, while also allowing operators to verifiably share information about subscribers and their home network operator mappings through cryptographic signatures. Each network publishes signed information about their backup networks and are assumed to change rarely.

3.5 Specific Protocol Components

dAuth– at its core, leverages the existing standards for providing privacy to user identifiers and bi-directional authentication between the network and the user device. The inherent replay resistance and the determinism of *sequence numbers* from the SIM identifiers enable dAuth to pre-compute authentication vectors which are shared with other participating networks in the federation. Additionally, parts of the authentication vector are split and shared among the backup networks configured by the home network using a cryptographic *key sharing* techniques such as Shamir secrets.

3.5.1 ***Sequence Number Handling:*** In 4G and 5G AKA, there is a sequence number (SQN) associated with each authentication attempt to prevent replay attacks against the symmetric ciphers used in the network. The SIM is responsible for storing a record of the used sequence numbers and ensuring that no sequence numbers are ever repeated. The 3GPP recommends an implementation in TS 33.102:Annex C [2] where the SQN tracks the greatest sequence number seen across 32 independent slices and invalidates the usage of prior SQN values in the a given slice. dAuth takes advantage of this behavior to allocate independent authentication vectors (AUTN) – containing the SQN, Message Authentication Code (MAC) and related authentication management fields (AMFs), to each backup network that do not have to be synchronized across the backup networks at authentication time, lowering coordination overhead between the networks. It also takes advantage of the ability for new sequence number to supersede older issued sequence numbers within a slice to allow the home network additional control to revoke published AUTH tuples containing the AUTN, a hashed expected response to check `H(XRES)`, and an intermediate derived key $K_{asme/seaf}$ from backups at a later time. See 4.3 for details on the revocation procedure, and Appendix B for more general information on SIM card behavior.

3.5.2 ***Key Shares:*** The dAuth protocol leverages threshold-protected key shares to provide resistance against a subset of compromised backup networks. The key shares are constructed with Shamir secret sharing [54], originally described by Adi Shamir in 1979. The shares are constructed together by the home network, and then split up among the different backup networks as part of key share dissemination.

Shamir secret sharing provides the guarantee that if M or more of N total shares are combined, the original secret ($K_{asme/seaf}$) can be losslessly recovered. If fewer than M shares are available, no information is leaked about the underlying secret. We leave the threshold M configurable on a per-network basis, since there is a tradeoff in the robustness of the level of protection provided by a high threshold against the performance and availability of the network when some backup networks are slow to respond or unreliably online.

Shamir secret sharing also does not inherently provide a way to validate a received share is valid, and is subject to tampering if a node contributes a malformed share. There are extensions to Shamir sharing that do provide validation at the expense of extra overhead [18, 41], but we use simple Shamir sharing in dAuth because the shares are always part of larger signed messages transmitted by the home network. The usage of a schemes such as Feldmans verifiable secret sharing provides validity guarantees for each share with a minimal cryptographic overhead [18].

Acronym	Definition
SIM	Subscriber Identity Module
IMSI/SUPI	Subscriber Identifier
SUCI/GUTI	Concealed/Temporary Subscriber Identifier
SQN	Sequence Number
AUTN	Authentication Vector
MAC	Message Authentication Code
AMF	Authentication Management Field
$K_{asme/seaf}$	Shared key after key agreement used to derive radio (AS) and network encryption (NAS) keys
XRES	Expected Response

4 Operation

In this section we detail the design of a basic scheme which allows mutual authentication, and then extend this scheme to allow the user to continue to authenticate when the home network is down for an extended multi-hour period.

4.1 dAuth in Traditional Roaming

When the home network is online, dAuth functions similarly to standard 5G roaming but with special handling of the authentication sequence number to not interfere with existing generated backup authentication vectors (see 3.5.1). The authentication process starts once the UE synchronizes its radio with the serving network and sends an `AttachRequest` message containing the user identifier in the form of an IMSI/SUPI, SUCI, or GUTI depending on the previous connection state. If the ID is an IMSI/SUPI the serving network queries the public directory service to look up the user's home network [1]. Recall that the public directory does not change

[1] This is the primary change to the standard roaming message flow; in a traditional architecture the serving network uses SS7 signalling with the user's MNC/MCC to route the authentication messages.

often, so it can be implemented as a widely distributed system with relatively low latency like DNS. Cellular networks traditionally perform such discovery through SS7 signaling. If the ID is a SUCI, the home network ID is directly embedded in the message. If the ID is a GUTI, the serving network receives a pointer to the prior serving network it can contact for the user's identity and home network. If this contact fails, the serving network can request that the UE provide a long-lived identifier and receive an IMSI/SUPI or SUCI. The home network receives the request for the authentication vector corresponding to the ID and returns the ⟨AUTH, H(XRES)⟩ to the requesting core network who then only forwards the AUTH information in an `AuthRequest` message to the user. The user device validates the information, generates a response which is sent to the network core, and validated establishing the shared agreed session key. Appendix 8 details these message flows.

Regardless of which ID lookup path is taken, once the user's home network identity is established, the serving network opens a direct connection to the home network and requests to begin authentication which generates a one-time-use authentication vector challenge forwarded to the UE.

4.2 dAuth Backup Authentication Scheme

The core innovation in dAuth is handling network failures using a novel authentication caching scheme. When the home network is not online, dAuth nodes can seemlessly fall back to the backup scheme. It has three phases: key material dissemination (while the home network is online), backup authentication (while the home network is offline), and reporting (when the home network is online again). Appendix 9 details the message flows for this circumstance.

4.2.1 ***Key Material Dissemination:*** In this phase the home network generates a set of AKA authentication vectors, a hash of the expected response ($\mathbb{H}$(XRES)), and corresponding key shares for each user to be cached among backup networks. The vector sequence numbers are chosen carefully so each backup network's sequence numbers are in independent dimensions of the sequence number space. Once generated, the tuple containing the authentication vector, $\mathbb{H}$(XRES), and random salt (RAND) are serialized into a binary bundle, signed by the home network, and sent to a specific backup network. The corresponding *key shares* are also added to bundles with the hashed expected response (used as its index) and random salt value, and each key share bundle is also signed by the home network. The key share bundles are split up, with each being sent to a different backup network.

The backup network must generate N^2 key shares and N auth vectors to provide a single auth vector to all backup networks. In practice N is limited by the number of practical backup networks, the number of sequence number slices in commonly available SIM cards (32, with one reserved for the home network), and the limited number of subscribers in private networks, so the N^2 scaling is not an issue in practice since the maximum number of backups is limited to a relatively small constant factor. Additionally, if 5G ID encryption is used by the home network, the home network shares the ID decryption key with the backup networks. To address the increase in the storage overheads, a number of geographic optimizations by placing the requested data only on specific shards could reduce the storage overheads. The key shares for different users could be computed in parallel, and each backup network only receives their respective shares. We leave further storage optimizations for future work after the system scales to that degree.

4.2.2 ***Backup Authentication:*** Backup authentication occurs between the set of backup networks and a serving network when the subscriber home network is unavailable. As presented in Algorithm 1, after determining the user's home network via the same procedure as basic auth or via the directory service, the serving network identifies backup networks elected by the home network from the directory. It then opens a secure connection to the closest or a randomly chosen backup network, requests the authentication vector by sending the user ID (IMSI/SUPI or SUCI – decrypted by the backup network), and validates the signed response.

After validating the request received from the serving network, the backup network looks up the sequential authentication vector for that user, and returns the home network signed authentication vector bundle to the serving network. The serving network then validates the home network's signature, and forwards the authentication vector to the UE. Upon reception the UE validates the vector as in the basic AKA scheme and returns its response (RES) to the serving network which can then validate the response against its received expected hash ($\mathbb{H}$(XRES)) confirming UE validity.

The serving network then creates and signs a bundle of hashed response, and the received response from the UE that is the preimage for the hash in an effort to prove that the UE was indeed present at the serving network, and is forwarded to *all* backup networks requesting associated key shares.

Upon receiving the key request from the serving network, the backup networks validate the serving network signature and the hash preimage. If valid, each looks up the key share it has stored. The backups store the received bundle from the serving network in persistent storage to report a *proof of consumption* to the home network once it is back online. Each backup then forwards its key share bundle to the serving network, which after receiving and validating enough bundles to meet the network's configured threshold assembles the session key $K_{\text{seaf}/\text{asme}}$ completing the authentication.

4.2.3 ***Event Reporting:*** Once the home network is online, the backup networks report authentication events to the home network and request new auth material to replace used vectors and shares. This triggers the home network to update any backup networks that were not part of the authentication event to replace their now obsolete key shares. The home network is also able to validate if there is any inconsistency between backup network reports, and potentially stop trusting particular backup networks or serving networks involved with inconsistent authentication attempts.

4.3 Revoking a Backup Network

dAuth allows the home network to revoke a backup network's ability to authenticate a user in the future in the event a backup network is compromised or becomes untrustworthy. The backup network's auth vectors are revoked by initiating a special authentication within the revoked network's sequence number slice at a value greater than the greatest sequence number ever disseminated to the now-revoked network. If the user is currently attached to a serving network, the home network contacts the serving network directly and requests the network perform a network-initiated reauthentication immediately. The serving network returns the UE's

Algorithm 1 Authentication using Backup Networks

SETUP:
$\mathcal{U} \leftarrow$ User Device containing symmetric key K_i
$\mathcal{S} \leftarrow$ Serving Network, managing key pair $(\text{SK}_{\mathcal{S}}, \text{PK}_{\mathcal{S}})$
$\mathcal{B} \leftarrow$ Backup Network for $\mathcal{S}$ with $(\text{SK}_{\mathcal{B}}, \text{PK}_{\mathcal{B}})$
$\mathcal{H} \leftarrow$ Subscriber Home Network
$\mathcal{D} \leftarrow$ Distributed Directory containing
  Network Key Directory $\langle \mathcal{S} | \mathcal{H} | \mathcal{B} : \text{PK} \rangle$
  Home configured Backup networks $\langle \mathcal{H} : \{\mathcal{B}_i, \mathcal{B}_j \cdots\} \rangle$
$\sigma \leftarrow$ Signature covering the message contents

AUTHENTICATION PROCEDURE:
$\mathcal{U} \rightarrow \mathcal{S}$: `AttachRequest` $(\mathcal{U}_{\text{IMSI}})$
$\mathcal{S} \rightarrow \mathcal{D}$: `GetNetwork`$(\mathcal{U}_{\text{IMSI}})$
$\mathcal{D} \rightarrow \mathcal{S} : \mathcal{H}$
$\mathcal{S} \rightarrow \mathcal{D}$: `GetBackupNetworks`$(\mathcal{H})$
$\mathcal{D} \rightarrow \mathcal{S} : (\mathcal{B}_i, \text{PK}_{\mathcal{B}_i})\ \forall\ i \in 0 \ldots N$
$\mathcal{S} \rightarrow \mathcal{B}_r$: `GetAuthVector`$(\mathcal{U}_{\text{IMSI}})$, $r \xleftarrow{\$} \{B_i, \cdots\}$
$\mathcal{B}_r \rightarrow \mathcal{S} : \langle \text{AUTN}, \mathbb{H}(\text{XRES}) \rangle$
$\mathcal{S} \rightarrow \mathcal{U}$: AUTN
$\mathcal{U}$ performs VERIFY(AUTN, K_i) **or** `ABORT`
$\mathcal{U} \rightarrow \mathcal{S}$: RES $s.t.$ RES $\leftarrow$ `ComputeRES`(AUTN, SQN, K_i)
$\mathcal{S}$: **`AssertEqual`**$(\mathbb{H}(\text{XRES}), \mathbb{H}(\text{RES}))$
$\mathcal{S} \rightarrow$ Shuffle$(\mathcal{B}_i \in \{\mathcal{B}_0, \mathcal{B}_1, \cdots\})$[: Threshold] :
  `Verify(GetKeyShare`$(\mathbb{H}(\text{XRES}), \text{RES}), \sigma, \text{PK}_{\mathcal{B}_i})$
$\{\mathcal{B}_0, \mathcal{B}_1, \cdots\} \rightarrow \mathcal{S}$: [**Share**$(K_{\text{seaf/asme}})_i, \cdots]$
$\mathcal{S} : K_{\text{seaf/asme}} \leftarrow$ `CombineShares`(**Share**$(K_{\text{seaf/asme}})_i, \cdots)$
$\mathcal{S} \rightarrow \mathcal{U}$: `Attach Accept, Set SecurityMode`$(K_{\text{seaf/asme}})$
$\mathcal{U} \rightarrow \mathcal{S}$: **`AssertEqual`**$(\mathcal{U}_{K_{\text{seaf/asme}}}, \mathcal{S}_{K_{\text{seaf/asme}}})$
Authentication Complete.

authentication response to prove it completed the handshake. The home network then notifies the remaining backups to delete the obsolete key shares.

Due to the replay resistance provided by the SIM's sequence number, the key shares with the revoked sequences are automatically invalidated and never accepted for authentication by the UE. If the user is not currently attached, the home network sends a "flood vector" request to all remaining backup networks, providing the vector and key shares to be used for the next auth for the user instead of the backup's usual series of vectors. This alone does not guarantee that the user will not initiate an authentication with the now-revoked backup. At the same time, the home network instructs all backup networks to invalidate and delete their key shares corresponding to the vectors given to the deleted backup network. Even if the now-revoked network were to be selected by a serving network and provide its auth tuple, as long as N − threshold of the backup networks have received the revocation notice, the untrusted backup will be unable to receive threshold number of key shares to reconstruct the keys needed to complete the authentication.

5 Implementation

We developed a proof-of-concept open-source prototype of the dAuth system consisting of three components to demonstrate its feasibility and evaluate performance. We implement (1) A dAuth service daemon running on each edge-core, responsible for tracking state relevant to each particular network and interfacing with the local core network, the directory service, or other dAuth instances. (2) A modified version of the Open5GS core network stack interfacing with the dAuth instances, and (3) A public centralized directory service for initial prototype testing and discovery.

5.1 dAuth Service

The dAuth daemon is implemented as an asynchronous Rust-based gRPC server with the Tonic gRPC framework. All messages to the server are serialized as *protobuf* messages which are supported by a wide variety of programming languages and are designed to be interoperable. The service provides three endpoints, a `LocalAuth` endpoint to interface with the edge-core, a `BackupNetwork` endpoint to provide key shares and accept authentication proofs when a backup, and a `HomeNetwork` endpoint to distribute key shares to backup networks and accept asynchronously reported authentication proofs. The `BackupNetwork` and `HomeNetwork` endpoints communicate with other network's instances of the dAuth service. It uses SQLite to store persistent state (user keys and sequence numbers associated with the subscriber for its home network users, and delegated authentication information when performing the role of a backup network to a different home network). Each backup network stores authentication events and reports them to the home network while also periodically polling the home network for uptime.

While only a proof of concept and not heavily tuned or optimized, our implementation does include 3 notable optimizations: (1) the ability to cache and re-use gRPC connections between the dAuth instances (2) local in-memory caching of directory information, (3) ability to race concurrent requests to multiple backup networks when obtaining authentication vectors and key shares when required to assemble the key $K_{\text{seaf/asme}}$ We find these optimizations significantly improved the performance of the network, particularly for repeat requests as would be expected for a network operating in a local area with a set of consistent users.

5.2 Modified Open5GS Network Core

We integrate dAuth services with Open5GS instances, although it should be portable to other core network implementations. Open5GS is written in C/C++, and we use Google's open-source C++ gRPC client implementation to communicate with the dAuth service using the same protobuf messages compiled into C++. We modified the AUSF, the function responsible for authentication in 5G, to query the dAuth services via the `LocalAuth` endpoint for new authentications for 5G connections, and similarly the MME to query the `LocalAuth` endpoint for 4G connections. Our implementation allows the AUSF and MME to concurrently answer other queries while waiting for a response from dAuth.

5.3 Directory Service

We also implement a simple directory service with Rust and the Tonic gRPC server. This directory stores its information in SQLite and contains functions to query and update network public keys, service addresses for discovery, and users to network, and home to backup networks mappings.

6 Evaluation

To evaluate dAuth's feasibility, we tested its performance across 4 scenarios informed by our experience working with SCN. We explore how dAuth performance scales as the security parameters of the system change and load increases in each of the four scenarios, comparing dAuth to both a local "edge-core" which does not allow roaming, and a cloud-based centralized core emulating a traditional network deployment. We used Open5GS v2.4.7 for all core network instantiations (both on the edge and in the cloud) to avoid confounds from performance optimization of a particular core network stack.

6.1 Test Network

Our test network consists of 12 nodes containing heterogeneous processors, memory, and disk configurations matching the diversity of machines deployed in production by community networks (see Appendix C). Two machines are actual nodes in SCN open to experimental services. Four nodes are cloud machines at four different major cloud providers, three nodes are low-power edge computers deployed on residential cable Internet connections, and the last three nodes are in a university lab with a high-quality Internet backbone.

Due to the presence of NAT on some connections and to mitigate risks of deploying our prototype software on the SCN network nodes, we used Tailscale [42] to establish a mesh VPN between all endpoints for testing and evaluation. We characterized the overhead caused by the Tailscale VPN, and identified a fixed latency penalty of ~3ms RTT and a throughput penalty of <10% compared to not using the VPN.

6.2 Physical Testing

To validate dAuth's ability to interface with COTS UE equipment, we integrated it with production hardware loaned from SCN. The physical testbed RAN used a Baicells Nova 233 CBRS eNodeB with 20MHz of bandwidth and a CBRS-compatible TDD duplex mode, deployed in a university lab. We conducted two types of physical tests – a compatibility test using an off-the-shelf phone and SIM, and performance tests, with an instrumented software-defined UE to precisely measure authentication timing.

6.2.1 ***Physical Compatibility Testing:*** For the compatibility test, we used an unmodified Google Pixel 4 running Android 12 as the UE with an off-the-shelf SIM conforming to the TS 33.102:Annex C standard [2]. We tested all 3 configurations of dAuth, including local authentication to the home network, roaming authentication to the home network, and backup authentication when the home network was offline. In all cases the UE was able to successfully connect.

We also validated that the UE was unable to connect if fewer than the key share threshold of the backup networks approved the authentication request from the serving network and that authentication attempts were promptly reported to the home network when it returned online.

6.2.2 ***Physical Performance Testing:*** With the correctness, compatibility and functionality of dAuth evaluated, we evaluate performance of dAuth using srsRAN UE – a software-defined UE implementation that can operate with common SDRs like the Ettus USRP [19]. We started with the latest released version 22_04, and instrumented it to capture fine-grained timing measurements during the *attach* and *authentication* process. We use a USRP B210 as the SDR controlled by srsRAN. Our USRP did not have a functioning GPSDO and suffered from clock instability, so 39 of 1986 samples (1.96%) were excluded from further analysis due to synchronization loss during the authentication process. Since this SDR-based system is not approved for the CBRS bands, tests were performed in an RF-isolated environment.

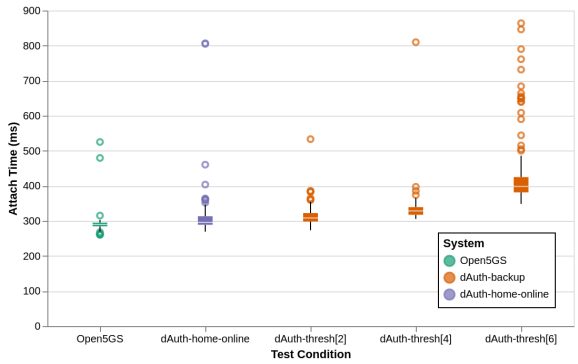
During each test, the srsUE continuously attached and detached from the test core network and recorded each attach duration. The LTE and 5G protocols include optimizations for re-attachment, so to accurately test the performance of a new UE to the dAuth network, we additionally modified srsUE to discard its connection state context and always attach from scratch in every iteration. For each test we collected at least 250 attach samples, and repeated this process with an edge deployment of modified Open5GS, and variable dAuth modes. First, when the home network is online, then configuring dAuth to use 6 backup networks in SCN while varying the key share thresholds (excluding the four cloud-based test networks and two UERANSIM host nodes) as shown in Figure 3. Overall dAuth performed well, adding ≤50ms of additional latency for the backup authentication process when the authentication threshold was low as shown in Figure 3a. At the highest threshold, the authentication process was limited by the least performant node, a low-powered atom-based device with a relatively high latency backhaul connection. dAuth with a low threshold achieves comparable performance to traditional authentication with Open5GS instances as shown in Figure 3b.

6.3 Simulated Large-scale Auth Testing

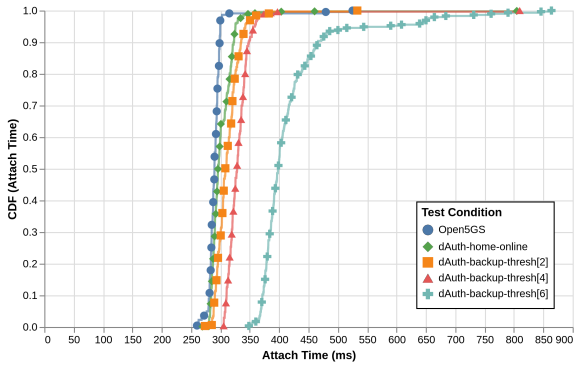
While srsUE allows us to make precise authentication measurements, we are unable to generate more than one authentication at a time. To test the scaling performance of dAuth, we used the UERANSIM open-source 5G-RAN emulator (v3.2.4) to generate a configurable number of authentication events in each test [20]. UERANSIM has both a gNB and UE component, and simulates connection overhead and the full 5G connection state machine to appear to the core network as a fully-functional 5G RAN. We modified the UE component to record a high-precision timestamp when it starts, and completes the connection process. We then launch new UEs at a regular interval for each load level to simulate new users entering and authenticating to the network, possibly overlapping, and analyze the recorded timestamps to determine the connection latency experienced.

6.3.1 ***Connection Scenarios:*** We identified four scenarios of interest for evaluating dAuth– representing different styles of private network endpoints we observe deployed in SCN.

(1) An "edge core" deployment on an embedded computer at a site with high-quality Internet access. This corresponds to the majority of sites in SCN. For dAuth tests in this scenario we configure the RAN emulator to be attached to the serving network directly and communicate with other dAuth instances via the backhaul connection. For Open5GS tests in this scenario we run a local instance of Open5GS on the edge with no roaming support, emulating a private 5G network.



(a) BoxPlots of Attach Times Across dAuth Test Conditions: dAuth adds a small but acceptable amount of additional latency when resorting to backup networks. All cases include rare outliers when packets must be retransmitted and/or inter-function connections established.



(b) CDF of Attach Times Across dAuth Test Conditions. dAuth is competitive with Open5GS when the home network is online with a low backup threshold. As the backup threshold increases, the serving network must wait for responses from straggling backup nodes before it can proceed.

Figure 3: The authentication performance of dAuth vs. Open5GS with an off-the-shelf Baicells eNodeB and srsUE when a single UE continuously attaches.

(2) An "edge core" deployment on an embedded computer at a site with residential-quality Internet (asymmetric, higher latency, typically cable. dAuth and Open5GS are configured as in (1).
(3) A managed "cloud core" deployment at a site with high-quality Internet, representing an approachable turnkey deployment solution for less technical organizations. For dAuth tests in this scenario we configure the RAN emulator to attach to a serving network hosted in the closest datacenter of the 4 providers in the test network. For Open5GS tests we run Open5GS in the cloud, emulating a cloud provider or operator's hosted core network.
(4) A managed "cloud core" deployment with residential Internet. dAuth and Open5GS are configured as in (3).

6.3.2 ***General Performance:*** Overall our dAuth prototype performed well relative to the baseline of Open5GS, and shows that the inter-site roaming and backup authentication capabilities provided by the dAuth architecture do not significantly impair overall performance.

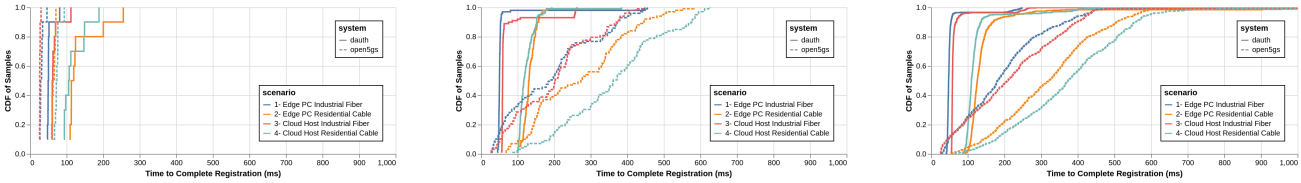
Evaluating Impact of Core and Back-haul Types: In our first test we compare the latency of dAuth when a home network is available to a standalone Open5GS core in the settings of the various scenarios described in §6.3.1. Results are shown in Figure 4 comparing dAuth to Open5GS with varying load levels. Our results indicate that the core networks deployed at the "edge" on a high-quality Internet back-haul link (blue lines), out-perform the traditional cloud hosted core networks with similar Internet connectivity (red line) and are consistent across both dAuth and Open5GS. The additional overhead of dAuth relative to the standalone core is noticeable but acceptable in a privately deployed cellular network at low load levels. At higher load levels (increased registrations) dAuth actually outperforms the standalone Open5GS core and is able to maintain relatively consistent performance due to load-distribution across machines.

dAuth Based vs Traditional Roaming Authentication: In our second general performance test we explored how dAuth behaves when operating in the backup network mode. The ability to authenticate when the home network is offline is a new capability relative to existing cores and comes with additional communication and cryptographic overhead, so we expected performance to degrade. We do see that overall the backup mode is slower than both standalone Open5GS and dAuth in the home mode at low load levels. As load increases in dAuth each serving network has to communicate with multiple backup networks for each authentication, so there is less gain from load sharing across the network and performance degrades similarly to the centralized core. In Figure 5, we compare dAuth's backup mode with traditional roaming in Open5GS instances where the core networks incur a 5ms RTT latency between the serving network and the subscriber home network. We observe that dAuth in backup mode still marginally outperforms Open5GS at higher load (Fig. 5b, 5c), due to load sharing. This leads us to believe that as the number of participating nodes grows larger than the number of backups, the load will reach a steady state per node while the total network capacity can continue to scale. Additionally, the dAuth instance maintains persistent long term connections which are re-used between dAuth service instances compared to Open5GS instances performing on-demand network connections over the S6a/N12 interfaces.

Overall our dAuth prototype performed well relative to the baseline Open5GS, and shows that the additional capabilities for inter-site roaming and backup authentication provided by the dAuth architecture in-fact improve authentication latencies under high network load conditions but are marginally worse in lower network load conditions.

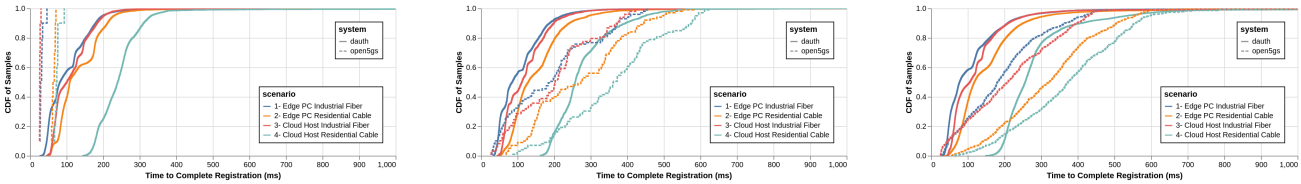
6.4 Impact of Security Parameters

The level of security given by dAuth is directly related to the threshold of collaborating backups required to reconstruct the key from the key shares. The system is more resistant to collusion as the threshold increases, but at high thresholds serving networks must wait for many responses before proceeding with authentication. Similarly, the total number of backup networks also impacts performance – interrelated with the threshold. A wide gap between



(a) 20 registrations per minute (b) 200 registrations per minute (c) 1000 registrations per minute

Figure 4: Attach latency of dAuth to a nearby home network vs Open5GS in a nearby (~5ms RTT) datacenter region. At low load the inter-core communication for dAuth advantages Open5GS (lower latency dashed lines), but with increased load dAuth spreads processing across multiple machines outperforming Open5GS (solid lines). The physical proximity of the edge compared to the cloud to the user results in lower latencies for edge core networks under comparable network conditions.



(a) 20 registrations per minute (b) 200 registrations per minute (c) 1000 registrations per minute

Figure 5: Attach latency of dAuth with 8 random backup networks vs Open5GS in a nearby (~5ms RTT) datacenter. At medium and high load, dAuth outperforms the centralized cloud core on slower edge hardware, particularly over a slower residential Internet connection (notice inverted orange and teal lines compared to Figure 4). For multiple samples at each load dAuth is reconfigured with 8 random backups and a key threshold of 4.

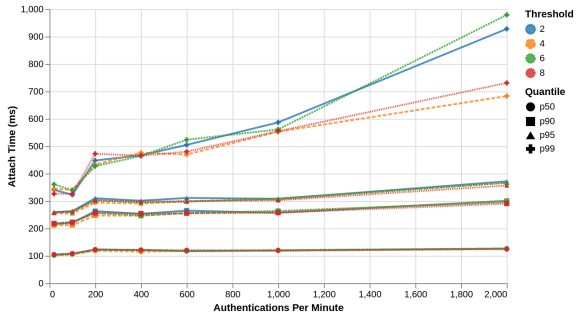


Figure 6: The authentication latency at different load levels for different key share thresholds, with backup network size of 8. Under load there is no consistent relationship between the threshold and relative performance, median or tail.

the number of backups and the threshold gives the most flexibility to the serving network, but adding additional backup networks requires trusting them to not collude and adds additional message overhead (since messages will be concurrently sent to all available backups during authentication through backups).

For a single UE, Figure 3 shows how the latency increases as the threshold is increased given a fixed set of available backup networks (rightmost 3 box plots). In the many UE case though, the threshold does not have a consistent impact on latency or throughput, indicating the bottleneck at higher load is elsewhere in the system. Figure 6 shows the latency performance at varying load levels and thresholds with a fixed total number of backup networks.

While the threshold alone does not significantly change performance under simulated load, increasing the total number of backups does have a measurable impact as load increases. In particular, the system saturates and tail latency degrades for a threshold level as the number of backups decreases. The backups are queried in parallel for both initial authentication vectors and key material, but only the key material requires a threshold response, so having more backup networks allows more opportunities for the auth vector to be received quickly. While the RAN and UE are processing the auth vector and preparing the RES, gRPC connections are still being established to the lagging backup networks and all backup networks can proactively read key shares into memory, making the key share query following receipt of the RES from the RAN much faster due to connection re-use.

7 Discussion

7.1 Cloud-Only Networks

As discussed in 3.1 and evaluated in 6.3, we consider both cloud and edge deployments of dAuth. We note that cloud hosting dAuth does not fundamentally resolve the reliability issues as outages also include factors such as configuration, payment, migration, and routing. Similarly, there are extensive benefits to edge-core architectures for marginalized communities [52] (such as rural areas or sovereign networks) that we'd like to support. Moreover, many of these organizations fundamentally want to own their own network and not just a relabeled MNVO-like structure. Given this, we'd like to re-emphasize that enabling organizational distribution is a key goal of dAuth, as we anticipate a future world where some small private network operators (and their customers) would benefit more

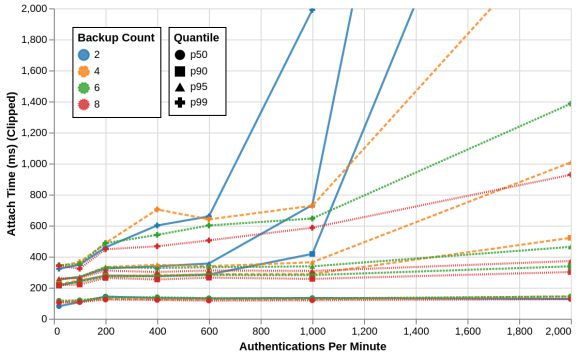


Figure 7: The authentication latency at different load levels for different numbers of configured backup networks, key share threshold of 2, clipped for scale (see Appendix E). Tail latency degrades as the number of backup networks decreases and fewer nodes are available for load balancing.

from federation than simply offloading their network operation (and revenue) onto traditional MNOs.

As such, even a cloud-only dAuth federation will have to be *distributed*, with multiple organizations running their instances separately across different accounts/nodes, and distributed systems should still be resilient to intermittent node failures in that context. Lastly, the degree of resilience (number of backup cores required for reconstruction of the key) is a network configuration variable that can be tuned up or down based on performance and safety considerations.

7.2 Why not eliminate the home network?

The main benefit of dAuth is that the home network does not need to be online for a UE to authenticate to a serving network. This opens up an interesting possibility of actually eliminating the home network entirely and implementing the home network functionality on the user's device itself. In this mode the secret key would only exist on the user's device and would be used to generate auth tuples and key shares then proactively distributed across the backup networks. After the UE is initially bootstrapped to provide its own keys to a set of backup networks, the UE itself has all of the data necessary to act as a home network with only one user. This would raise challenges in provisioning enough network IDs for every user, and for the initial trust between the serving network and the user device but could be surmounted by aggregating multiple UEs together into a virtual pseudonetwork, while still keeping the secret keys only ever present on the UE and establishing an incentive driven mechanism for initial serving network connectivity – such as a micropayment. Theoretically, the home network could destroy the symmetric key associated with the user SIM identity after issuing the maximum permissible number of authentication vectors associated with the one-time SQN numbers in the SIM card and behave as a serving network requesting and assembling key shares from the backup networks to complete user authentication trading-off latency to improved security and preventing potential compromise of sensitive key material.

7.3 Long Term Home Network Outages

We note that, if the home network is out for an extended period of time, the precomputed key shares could be used up by a client, creating a form of a denial of service attack preventing any further authentications. While technically possible, the overall amount of user communication that a single vector allows for is a network-configurable variable that should be tuned to match network expectations. In addition, these variables could be changed dynamically, such as during an outage, to increase uptime without leaking any new information. Similarly, the number of pre-generated vectors is another configuration and a large number could be pre-produced if such an attack or outage was expected. However, the drawback of such an approach is that changes to the secret recovery thresholds require the revocation and re-issuance of all the key shares resulting in increased communication overheads.

7.4 Future Work

This work raises implications for how to design fallback to allow connectivity when networks inevitably fail, even within the status quo of a few large networks. In particular we hope to dive into the nuances of how to better handle the SUCI key and do a more thorough and formal analysis of how reputation could be managed and correct behavior incentivize in a production dAuth network.

Handover: We also think there is interesting work to be done in applying the same ideas from dAuth to explore how to perform handover between small networks in our envisioned federation. Allowing for performant and secure inter-organizational handover likely requires additional changes to the cellular standards that were out of scope for dAuth, but solving it would make a large-scale dAuth system much more performant and suitable for more rapid mobility scenarios.

Spectrum sensing and coordination: As the utilization of Citizens Broadband Radio Service (CBRS) and other unlicensed spectrum increases enabling such federated cellular networks, there is also an opportunity to reduce the dependency on centralized spectrum access systems (SAS) to manage radio resource usage. The existing network of federated nodes improves reliability, fairness, and trustworthiness of the SAS [59].

Billing and Charging: Though this work is couched in the context of CNs that provide free Internet, we recognize that not all federations will do that. Fortunately, the dAuth architecture is well suited to a simple billing model where the home network charges users for the generation of authentication tokens. As these are reported when used by serving networks, operators ensure that users receive Internet access and that revenue can be shared with serving networks. d-Cellular [6] is an interesting work building in this direction by resolving network usage auditing in a similarly distributed fashion.

8 Related Work

8.1 Community Networks

dAuth is motivated in part by the wider body of work building and characterizing community networks (CNs), networks owned and operated by users in a collaborative way. CNs have been viewed as a promising mechanism for increasing access among rural and disadvantaged populations [43, 49]. They come in as many diverse

forms as there are communities to host them, ranging from large urban areas [29, 44] to small rural sites [21], in the global north [8, 44] and global south [24, 32] and employ a variety of organizational structures such as user-to-user meshes or community-oriented structures [9, 16, 17, 36, 53]. Examples of operational CNs include Guifi.net [10], Digital Tribal Village [50], and TakNet [32]. In dAuth, we take advantage of the natural decorrelation that occurs in decentralized CNs with multiple owning and operating organizations, different supporting infrastructure and motivate our assumptions by this existing body of work.

A notable thread inside of CN research is on community *cellular* networks; focused on using cellular infrastructure (rather than WiFi), often because of its better wide-area properties. Most existing Cellular CN research has focused on the challenges of building and deploying in a single network context [22, 30, 52], focusing on rural access and coverage. Building from this work, dAuth positions itself as a community-appropriate cellular technology targeting a different operational point envisioning multiple coexisting operators bringing additional challenges and the need to deploy authentication protocols in a different trust model.

8.2 Shared Cellular

Other research explores different models for shared cellular networks. Hasan et al. developed Community Cellular Manager (CCM), a system which allows an anchor MNO to leverage federation with community cellular network more easily than permitted by existing 3GPP protocols [21]. Its architecture accounts for backhaul unreliability by pushing core network functions to the edge like dAuth, but assumes a setting where either nodes are trusted and authentication information can be shared directly with the edge nodes, or they are not and the authentication information must remain with the anchor operator. Some of the original authors of CCM went on to work on Magma, a 4G/5G-capable distributed core network with a similar high-level architecture [57]. Neither CCM nor Magma directly address the challenge of safely distributing security information across edge nodes when edge nodes cannot be independently trusted. dAuth addresses this problem directly, and the techniques developed for dAuth could be applied in other federated network architectures. d-Cellular [6] is a recent exciting work that explores network measurement and accounting in distributed cellular networks, which could greatly ease outstanding issues across billing and performance in dAuth.

8.3 Core Reliability and Performance

Beyond community networks, general reliability in cellular networks has received considerable attention from the networking community. Skycore sought to build a reliable UAV-based network and arrived at an architecture where each UAV runs its own core network stack at the edge, similar to CCM, Magma, CoLTE, and dAuth, while implementing pre-computation and distribution of security information to lower USAV processing overheads [39]. dAuth builds on this work in a very different operational domain adding additional guarantees to safeguard the pre-computed authentication information in the event of node compromise.

Much attention has also focused on possibilities for refactoring and redesigning monolithic cellular core networks for increased performance, both in terms of scalability, latency, and throughput [38, 40]. Qazi et al. proposed re-architecting the protocols between core network components for better state locality [46], and Mohammadkhan et al. redesigned the division of concerns between core network components to improve performance [37]. While these systems improve reliability and performance within an single network, none of them address the risk inherent in single-operator systems. By allowing for collaboration between multiple organizations, dAuth provides an additional layer of resiliency and decorrelation, which could theoretically be combined with proposed intra-operator architectures in future work.

8.4 Alternative Authentication Schemes

Researchers have explored flexible alternative authentication schemes for cellular networks. DLTE is a network architecture based on publicly releasing the symmetric keys for all SIMs, effectively removing authentication protections and relying on over-the-top services for security via VPN connections or TLS [27]. Schmitt et al. propose using the same SIM credentials for all users in the network to preserve anonymity at the link-layer while remaining relatively anonymous [51]. Both of these approaches are backwards-compatible with the existing device ecosystem but, by relinquishing control over the connection between the UE and the basestation, leave the user vulnerable to attacks abusing the basestation's trust. dAuth provides additional guarantees to the user that the serving network is trusted by their home organization.

In Cellbricks, Luo et al. outline a vision like ours, where small organizations join together into a federated cellular network [33]. Unlike dAuth, their approach relies on a centralized online data broker validating user credentials (and so vulnerable to an outage), and requires modifying the baseband of the user device to use asymmetric cryptography similar to dHSS proposed by Jover et al. with a coordinating blockchain [28]. In contrast to these works, dAuth maintains compatibility with standard 3GPP cryptography.

9 Conclusion

Our system, dAuth, enables real-world deployment of small cellular networks with standards-compliant Commercial Off The Shelf (COTS) UEs widely available today. We take advantage of the details of the battle-tested AKA authentication scheme to allow networks to proactively share authentication material to allow redundancy in the case of local failure and share the load of authentication across multiple nodes through natural sharding of user state.

Ethics

This work raises no ethical concerns. With widespread implementation and usage, dAuth enables users of home networks imposing active service restrictions to seek unrestricted services with other serving networks – circumventing censorship.

Acknowledgments

This research was funded by the National Science Foundation (Award# 2423770) as well as by the Public Interest Technology University Network (PIT-UN). We thank the users and volunteers at SCN for their assistance in the incredibly large amount of non-research tasks needed for a project of this scale.

References

[1] 3GPP. 2020. TS-22-011:Service Accessibility (3GPP TS 22.011 Version 16.5.0 Release 16).

[2] 3GPP. 2020. TS-33-102: Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture.

[3] 3GPP. 2020. TS-33-501: Security Architecture and Procedures for 5G System.

[4] APC News. 2020. What's New on the Spectrum? "Let's Make Sure We Can Use It for What Is Needed": A Conversation with Peter Bloom from Rhizomatica | Association for Progressive Communications. https://www.apc.org/en/news/whats-new-spectrum-lets-make-sure-we-can-use-it-what-needed-conversation-peter-bloom.

[5] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. *DNS Security Introduction and Requirements.* Technical Report RFC4033. RFC Editor. RFC4033 pages. https://doi.org/10.17487/rfc4033

[6] Serhat Arslan, Ali Abedi, and Sachin Katti. 2023. d-Cellular: Trust-Free Connectivity in Decentralized Cellular Networks. In *2023 IEEE Future Networks World Forum (FNWF)*. IEEE, IEEE, Baltimore, MD, USA, 1–6. https://doi.org/10.1109/FNWF58287.2023.10520508

[7] David E Avison, Francis Lau, Michael D Myers, and Peter Axel Nielsen. 1999. Action research. *Commun. ACM* 42, 1 (1999), 94–97.

[8] Roger Baig, Lluís Dalmau, Ramon Roca, Leandro Navarro, Felix Freitag, and Arjuna Sathiaseelan. 2016. Making Community Networks Economically Sustainable, the Guifi.Net Experience. In *Proceedings of the 2016 Workshop on Global Access to the Internet for All (GAIA '16)*. ACM, New York, NY, USA, 31–36. https://doi.org/10.1145/2940157.2940163

[9] Roger Baig, Ramon Roca, Felix Freitag, and Leandro Navarro. 2015. Guifi.Net, a Crowdsourced Network Infrastructure Held in Common. *Computer Networks* 90 (Oct. 2015), 150–165. https://doi.org/10.1016/j.comnet.2015.07.009

[10] Roger Baig, Ramon Roca, Leandro Navarro, and Felix Freitag. 2015. Guifi.Net: A Network Infrastructure Commons. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development (ICTD '15)*. Association for Computing Machinery, Singapore, Singapore, 1–4. https://doi.org/10.1145/2737856.2737900

[11] Luca Belli, Bruno de Souza Ramos, Panayotis Antoniadis, Virginie Aubrée, Roger Baig Viñas, Aris Dadoukis, Paolo Dini, Mélanie Dulong de Rosnay, Nicolas Echániz, Kurtis Heimerl, Matthew Johnson, Pathirat Kosakanchit, Florencia López Pezé, Steven Mansour, Stavroula Maglavera, Jens Martignoni, John Mavridis, Sascha Meinrath, Leandro Navarro, Harris Niavis, Ramon Roca i Tió, Spencer Sevilla, and Félix Tréguer. 2018. *The Community Network Manual : How to Build the Internet Yourself.* FGV Direito Rio, Paris, France.

[12] Nicola J. Bidwell. 2020. Women and the Sustainability of Rural Community Networks in the Global South. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development (ICTD2020)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3392561.3394649

[13] Celona. 2022. New York Public Library and Celona Partner to Shrink the Digital Divide. https://www.celona.io/resources/celona-at-nypl.

[14] Melissa Chase, Apoorvaa Deshpande, Esha Ghosh, and Harjasleen Malvai. 2019. SEEMless: Secure End-to-End Encrypted Messaging with Less</> Trust. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 1639–1656. https://doi.org/10.1145/3319535.3363202

[15] Michael Cooney. 2022. Duke University to test private LTE/5G network using CBRS spectrum. https://www.networkworld.com/article/970984/duke-university-to-test-private-lte5g-network-using-cbrs-spectrum.html.

[16] Stefano Crabu and Paolo Magaudda. 2018. Bottom-up Infrastructures: Aligning Politics and Technology in Building a Wireless Community Network. *Computer Supported Cooperative Work (CSCW)* 27, 2 (April 2018), 149–176. https://doi.org/10.1007/s10606-017-9301-1

[17] Michaelanne Dye, David Nemer, Neha Kumar, and Amy S. Bruckman. 2019. If It Rains, Ask Grandma to Disconnect the Nano: Maintenance & Care in Havana's StreetNet. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 187:1–187:27. https://doi.org/10.1145/3359289

[18] Paul Feldman. 1987. A Practical Scheme for Non-Interactive Verifiable Secret Sharing. In *28th Annual Symposium on Foundations of Computer Science (Sfcs 1987)*. IEEE, Los Angeles, CA, USA, 427–438. https://doi.org/10.1109/SFCS.1987.4

[19] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Doug J. Leith. 2016. srsLTE: an open-source platform for LTE evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization* (New York City, New York) *(WiNTECH '16)*. Association for Computing Machinery, New York, NY, USA, 25–32. https://doi.org/10.1145/2980159.2980163

[20] Ali Güngör. 2022. Aligungr/UERANSIM.

[21] Shaddi Hasan, Mary Claire Barela, Matthew Johnson, Eric Brewer, and Kurtis Heimerl. 2019. Scaling Community Cellular Networks with CommunityCellularManager. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19) (NSDI'19)*. USENIX Association, Boston, MA, USA, 735–750. https://doi.org/10.5555/3323234.3323294

[22] Kurtis Heimerl, Shaddi Hasan, Kashif Ali, Eric Brewer, and Tapan Parikh. 2013. Local, Sustainable, Small-scale Cellular Networks. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers - Volume 1 (ICTD '13)*. ACM, New York, NY, USA, 2–12. https://doi.org/10.1145/2516604.2516616

[23] Kurtis Heimerl, Shaddi Hasan, Kashif Ali, Tapan Parikh, and Eric Brewer. 2015. A Longitudinal Study of Local, Sustainable, Small-Scale Cellular Networks. *Information Technologies & International Development* 11, 1 (2015), 20.

[24] Calvin Artemies G. Hilario, Mary Claire Barela, Mar Francis D. De Guzman, Rizza T. Loquias, Ramon Vann Cleff B. Raro, Jean Jay J. Quitayen, and Joel Joseph S. Marciano. 2020. LokaLTE: 600 MHz Community LTE Networks for Rural Areas in the Philippines. In *2020 IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE, Seattle, WA, USA, 1–8. https://doi.org/10.1109/GHTC46280.2020.9342849

[25] Raynell A. Inojosa, Philip A. Martinez, Ramon Vann Cleff B. Raro, Riza Carmela M. Pineda, Jerome Dylan S. Villamater, Kenneth Rey L. Sumalinog, Maria Aya Lei P. Banzuela, Kerry C. Hiponia, Kieth Joshua M. Manato, and Peter Antonio B. Banzon. 2022. Towards the Development and Deployment of Community LTE Networks in Rural Areas. In *2022 International Conference for Advancement in Technology (ICONAT)*. IEEE, Goa, India, 1–6. https://doi.org/10.1109/ICONAT53423.2022.9725850

[26] Kristoffer Jensen, Thanh Van Do, Hai Thanh Nguyen, and Andre Arnes. 2016. Better protection of SS7 networks with machine learning. In *2016 6th International Conference on IT Convergence and Security (ICITCS)*. IEEE, IEEE, Prague, Czech Republic, 1–7. https://doi.org/10.1109/ICITCS.2016.7740315

[27] Matthew Johnson, Spencer Sevilla, Esther Jang, and Kurtis Heimerl. 2018. dLTE: Building a More WiFi-like Cellular Network: (Instead of the Other Way Around). In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks (HotNets '18)*. ACM, New York, NY, USA, 8–14. https://doi.org/10.1145/3286062.3286064

[28] R. P. Jover and J. Lackey. 2016. dHSS - Distributed Peer-to-Peer Implementation of the LTE HSS Based on the Bitcoin/Namecoin Architecture. In *2016 IEEE International Conference on Communications Workshops (ICC)*. IEEE, Kuala Lumpur, Malaysia, 354–359. https://doi.org/10.1109/ICCW.2016.7503813

[29] Anne Kadet. 2019. New York City Neighbors Build Cheaper Way to Connect to Web. *Wall Street Journal* US Metro Money (6 Aug. 2019), 1–1.

[30] Mohamed M. Kassem, Mahesh K. Marina, and Bozidar Radunovic. 2018. DIY Model for Mobile Network Deployment: A Step Towards 5G for All. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS '18)*. Association for Computing Machinery, Menlo Park and San Jose, CA, USA, 1–5. https://doi.org/10.1145/3209811.3212703

[31] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. 2020. An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Boston, MA, USA, 61–79.

[32] Adisorn Lertsinsrubtavee, Liang Wang, Arjuna Sathiaseelan, Jon Crowcroft, Nunthaphat Weshsuwannarugs, Apinun Tunpan, and Kanchana Kanchanasut. 2015. Understanding Internet Usage and Network Locality in a Rural Community Wireless Mesh Network. In *Proceedings of the Asian Internet Engineering Conference (AINTEC '15)*. Association for Computing Machinery, Bangkok, Thailand, 17–24. https://doi.org/10.1145/2837030.2837033

[33] Zhihong Luo, Silvery Fu, Mark Theis, Shaddi Hasan, Sylvia Ratnasamy, and Scott Shenker. 2021. Democratizing Cellular Access with CellBricks. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference (SIGCOMM '21)*. Association for Computing Machinery, New York, NY, USA, 626–640. https://doi.org/10.1145/3452296.3473336

[34] Anna Maria Mandalari, Andra Lutu, Ana Custura, Ali Safari Khatouni, Özgü Alay, Marcelo Bagnulo, Vaibhav Bajpai, Anna Brunstrom, Jörg Ott, Marco Mellia, and Gorry Fairhurst. 2018. Experience: Implications of Roaming in Europe. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. ACM, New York, NY, USA, 179–189. https://doi.org/10.1145/3241539.3241577

[35] Marcela S. Melara, Aaron Blankstein, Joseph Bonneau, Edward W. Felten, and Michael J. Freedman. 2015. {CONIKS}: Bringing Key Transparency to End Users. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. USENIX, Washington D.C., USA, 383–398.

[36] Panagiota Micholia, Merkouris Karaliopoulos, Iordanis Koutsopoulos, Leandro Navarro, Roger Baig Vias, Dimitris Boucas, Maria Michalis, and Panayotis Antoniadis. 2018. Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions. *IEEE Communications Surveys Tutorials* 20, 4 (2018), 3581–3606. https://doi.org/10.1109/COMST.2018.2817686

[37] Ali Mohammadkhan, K. K. Ramakrishnan, and Vivek A. Jain. 2020. CleanG—Improving the Architecture and Protocols for Future Cellular Networks With NFV. *IEEE/ACM Transactions on Networking* 28, 6 (Dec. 2020), 2559–2572. https://doi.org/10.1109/TNET.2020.3015946

[38] Mehrdad Moradi, Yikai Lin, Z. Morley Mao, Subhabrata Sen, and Oliver Spatscheck. 2018. SoftBox: A Customizable, Low-Latency, and Scalable 5G Core Network Architecture. *IEEE Journal on Selected Areas in Communications* 36, 3

(March 2018), 438–456. https://doi.org/10.1109/JSAC.2018.2815429
[39] Mehrdad Moradi, Karthikeyan Sundaresan, Eugene Chai, Sampath Rangarajan, and Z. Morley Mao. 2018. SkyCore: Moving Core to the Edge for Untethered and Reliable UAV-based LTE Networks. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. ACM, New York, NY, USA, 35–49. https://doi.org/10.1145/3241539.3241549
[40] Mehrdad Moradi, Wenfei Wu, Li Erran Li, and Zhuoqing Morley Mao. 2014. SoftMoW: Recursive and Reconfigurable Cellular WAN Architecture. In *Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies (CoNEXT '14)*. Association for Computing Machinery, New York, NY, USA, 377–390. https://doi.org/10.1145/2674005.2674981
[41] Torben Pryds Pedersen. 1992. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Advances in Cryptology — CRYPTO '91 (Lecture Notes in Computer Science)*, Joan Feigenbaum (Ed.). Springer, Berlin, Heidelberg, 129–140. https://doi.org/10.1007/3-540-46766-1_9
[42] Avery Pennarun. 2020. How Tailscale Works. https://tailscale.com/blog/how-tailscale-works/.
[43] A. Pentland, R. Fletcher, and A. Hasson. 2004. DakNet: Rethinking Connectivity in Developing Nations. *Computer* 37, 1 (Jan. 2004), 78–83. https://doi.org/10.1109/MC.2004.1260729
[44] Gregers Petersen. 2014. Freifunk: When Technology and Politics Assemble into Subversion. In *Subversion, Conversion, Development: Cross-Cultural Knowledge Exchange and the Politics of Design*. The MIT Press, Boston, MA, USA, 39–56.
[45] Rowan Phipps, Shrirang Mare, Peter Ney, Jennifer Webster, and Kurtis Heimerl. 2018. ThinSIM-based Attacks on Mobile Money Systems. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (Menlo Park and San Jose, CA, USA) *(COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 23, 11 pages. https://doi.org/10.1145/3209811.3209817
[46] Zafar Ayyub Qazi, Melvin Walls, Aurojit Panda, Vyas Sekar, Sylvia Ratnasamy, and Scott Shenker. 2017. A High Performance Packet Core for Next Generation Cellular Networks. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM '17)*. ACM, New York, NY, USA, 348–361. https://doi.org/10.1145/3098822.3098848
[47] Grand View Research. 2023. Private 5G Network Market Size & Trends. https://www.grandviewresearch.com/industry-analysis/private-5g-network-market.
[48] Carlos Rey-Moreno. 2017. *Supporting the Creation and Scalability of Affordable Access Solutions: Understanding Community Networks in Africa* (first ed.). Internet Society, Galerie Jean-Malbuisson 15, CH–1204 Geneva, Switzerland.
[49] Carlos Rey-Moreno, Anriette Esterhuysen, Mike Jensen, Peter Bloom, Erick Huerta, and Steve Song. 2017. Can the Unconnected Connect Themselves? Towards an Action Research Agenda for Local Access Networks. In *Community Networks: The Internet by the People, for the People*, Luca Belli (Ed.). FGV Direito Rio, Geneva, Switzerland, 103–118.
[50] Christian Sandvig. 2012. Connection at Ewiiaapaayp Mountain: Indigenous Internet Infrastructure. In *Race After the Internet*. Routledge, New York, 168–200.
[51] Paul Schmitt and Barath Raghavan. 2021. Pretty Good Phone Privacy. In *30th USENIX Security Symposium (USENIX Security 21)*. Usenix, Vancouver, B.C., Canada, 1737–1754. arXiv:2009.09035
[52] Spencer Sevilla. 2018. CoLTE: The Community LTE Project. UW ICTD Lab.
[53] Spencer Sevilla, Matthew Johnson, Pat Kosakanchit, Jenny Liang, and Kurtis Heimerl. 2019. Experiences: Design, Implementation, and Deployment of CoLTE, a Community LTE Solution. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19)*. Association for Computing Machinery, Los Cabos, Mexico, 1–16. https://doi.org/10.1145/3300061.3345446
[54] Adi Shamir. 1979. How to Share a Secret. *Commun. ACM* 22, 11 (Nov. 1979), 612–613. https://doi.org/10.1145/359168.359176
[55] Sudheesh Singanamalla, Apurv Mehra, Nishanth Chandran, Himanshi Lohchab, Seshanuradha Chava, Asit Kadayan, Sunil Bajpai, Kurtis Heimerl, Richard Anderson, and Satya Lokam. 2022. Telechain: Bridging telecom policy and blockchain practice. In *ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies (COMPASS)*. Association for Computing Machinery, New York, NY, USA, 280–299.
[56] Internet Research Team. 2022. Rogers Outage Analysis: July 8, 2022. https://www.thousandeyes.com/blog/rogers-outage-analysis-july-8-2022.
[57] The Magma Authors. 2022. About Magma. https://magmacore.org/about-magma/.
[58] Mariah Timms. 2020. AT&T Outage: Internet, 911 Disrupted, Planes Grounded after Nashville Explosion. Get the Latest Updates. *The Tennessean* Local (Dec. 2020), 1.
[59] Yang Xiao, Shanghao Shi, Wenjing Lou, Chonggang Wang, Xu Li, Ning Zhang, Y Thomas Hou, and Jeffrey H Reed. 2022. Decentralized spectrum access system: Vision, challenges, and a blockchain solution. *IEEE Wireless Communications* 29, 1 (2022), 220–228.

Appendix

We provide the following appendices which are supporting material that clarify the terminologies, details about SIM card functionality, information about test networks and message flow diagrams supporting the protocols in the paper. The appendices are supporting material that have not been peer-reviewed.

A System Entities

User Equipment (UE) The user's off-the-shelf device.

SIM The user's SIM card, issued by the user's home network.
It can be customized but must maintain compatibility with the UE baseband interface.
The SIM holds K_i^u, the user's milenage key, $\langle SQN \rangle^u$, the user's vector of used SQN values, SQN_{max}^u, and the user's current identity $GUTI^u$

Home Network The user's home network, which in \dauth is run by a small community network at a single community organization. Runs the dAuth service, and optionally fulfills the role of a serving network for this user, or a backup network or serving network for other users. It holds the signing key Sk_h for its published Pk_h, and key material for all of its users $(K_{i,u}, SQN[v \forall v \in SIM]) \forall u \in HNet$

Serving Network (Snet) An off-the-shelf Radio Access Network with a customized software-defined core network and dAuth service, providing coverage to the user when away from the home network. The SNet holds a private signing key Sk_s corresponding to its published public key Pk_s.

Backup Network(s) A set of networks semi-trusted by the home network to collectively hold single-use key material for the user. The backup network holds a signing key Sk_b corresponding to published Pk_b, a set of assigned auth vectors for each backed up user $(AUTH, H_1(HRes^*), RAND)_{i,n}$, and the key shares corresponding to auth vectors held by other backups $Share(Res, K_{seaf/asme})_{H_1(HRes^*),i,n}$

Directory Visible to all participants, and can be based on existing verifiable public key directory schemes [14, 35], or a hierarchy like DNSSEC [5]. All information in the directory is public information with no controlling organization. The directory contains Pk_n and an address for each Network. It also contains a mapping from user to home network for each user, and a set of backup networks for each home network.
Entries in the directory are signed by their respective parties, and are assumed to change rarely.

B SIM Details

The sequence number, or sqn, is a component of the authentication process that prevents re-authentication using old authentication data.

When considering sqn as a single monotonically increasing value, determining a valid sqn number could be done by choosing any sqn larger than what has already been used. However, SIM cards can maintain a set of independent sqns by dividing the range of possible sqn values into a fixed number of 'slices'. Each slice is the set of all numbers that share the same modulo:

$$\text{slice} = \text{sqn}\%\text{number of total slices}$$

The 3GPP specifies an informative implementation suggestion in TS 33.102 [2] where the SIM card maintains counters for *each slice*. Consider a SIM card that maintains 32 slices. For slice 1 out of 32 (zero indexed), the slice counter would keep track of sqns 1, 33, 65, and so on. Table 2 below shows this breakdown:

SIM Slices				
%32 = 0	**%32 = 1**	**%32 = 2**	**...**	**%32 = 31**
0	1	2	...	31
32	33	34	...	63
64	65	66	...	95
...	...	...	...	...

Table 2: Table showing sequence of values from 0 and on, separated into slices

In the SIM Slices table 2, note that the counters operate independently. It is possible to use a smaller sqn following a larger sqn, provided that the smaller sqn is on a different slice and is the largest seen of that particular slice. For example, a sqn of 33 (slice 1) would be valid, while 64 (slice 0) would be invalid. Table 3 shows an example valid SIM state in the 3GPP informative implementation.

SIM Slices				
%32 = 0	**%32 = 1**	**%32 = 2**	**...**	**%32 = 31**
96	1	66	...	31

Table 3: Table showing an example valid state for internal SIM slice counters

C Test Network Details

Purpose	Location	Node Type	ISP	Processor	RAM	NIC	Disk
Test	SCN Library	Protectli	A	Intel Celeron J3160 @ 1.60GHz	8GB DDR3	1Gbps Intel	SATA3 SSD
Test	SCN Community Center	Quotom	A	Intel i5-4200U @ 1.60GHz	8GB DDR3	1Gbps Intel	SATA3 SSD
Test	Uni-Lab	Quotom	University	Intel Core i3-4005U @ 1.70GHz	8GB DDR3	1Gbps Intel	SATA3 SSD
Test	Cloud Azure US-West-2	F2s v2	Private	Intel Xeon 8370C 2cpu	4GB	?	"Premium" SSD
Test	Cloud AWS US-West-2	C6a.large	Private	AMD EPYC 7R13 Processor 2cpu	4GB	?	Cloud block storage
Test	Cloud Digital Ocean SF	CPU Droplet	Private	Intel Xeon 8168 CPU @ 2.70GHz 2 CPU	4GB	?	Attached SSD
Test	Cloud GCP US-Central-1	c2d standard2	Private	AMD EPYC 7B13 "Milan" 2 cpu	8GB	10Gbps vnic	Balanced persistent cloud storage
Test	Uni-Lab	Zotac	University	Intel Celeron N3160 @ 1.60GHz	8GB DDR3	1Gbps Real-tek	SATA2 HDD, 5400RPM
Test	Home A	Zotac	B	Intel Celeron N3160 @ 1.60GHz	8GB DDR3	1Gbps Real-tek	SATA3 SSD
Test	Home B	Zotac	C	Intel Celeron N3160 @ 1.60GHz	4GB DDR3	1Gbps Real-tek	SATA1 HDD, 5400RPM
RAN	Home A	Latitude e7470	B	Intel Core i7-6600U @ 2.60GHz	16GB DDR4	1Gbps Intel	SATA3 SSD
RAN	Uni-Lab	Dell Precision	University	Intel Core i7-4790 @ 3.60GHz	8GB DDR3	1Gbps Intel	SATA3 HDD 7200RPM

Table 4: Details of the nodes in the test network. All nodes are connected via a TailScale Mesh VPN and had direct accessability during the duration of tests. RAN nodes hosted UERANSIM and did not host a dAuth daemon at test time.

D Message Flow Diagrams

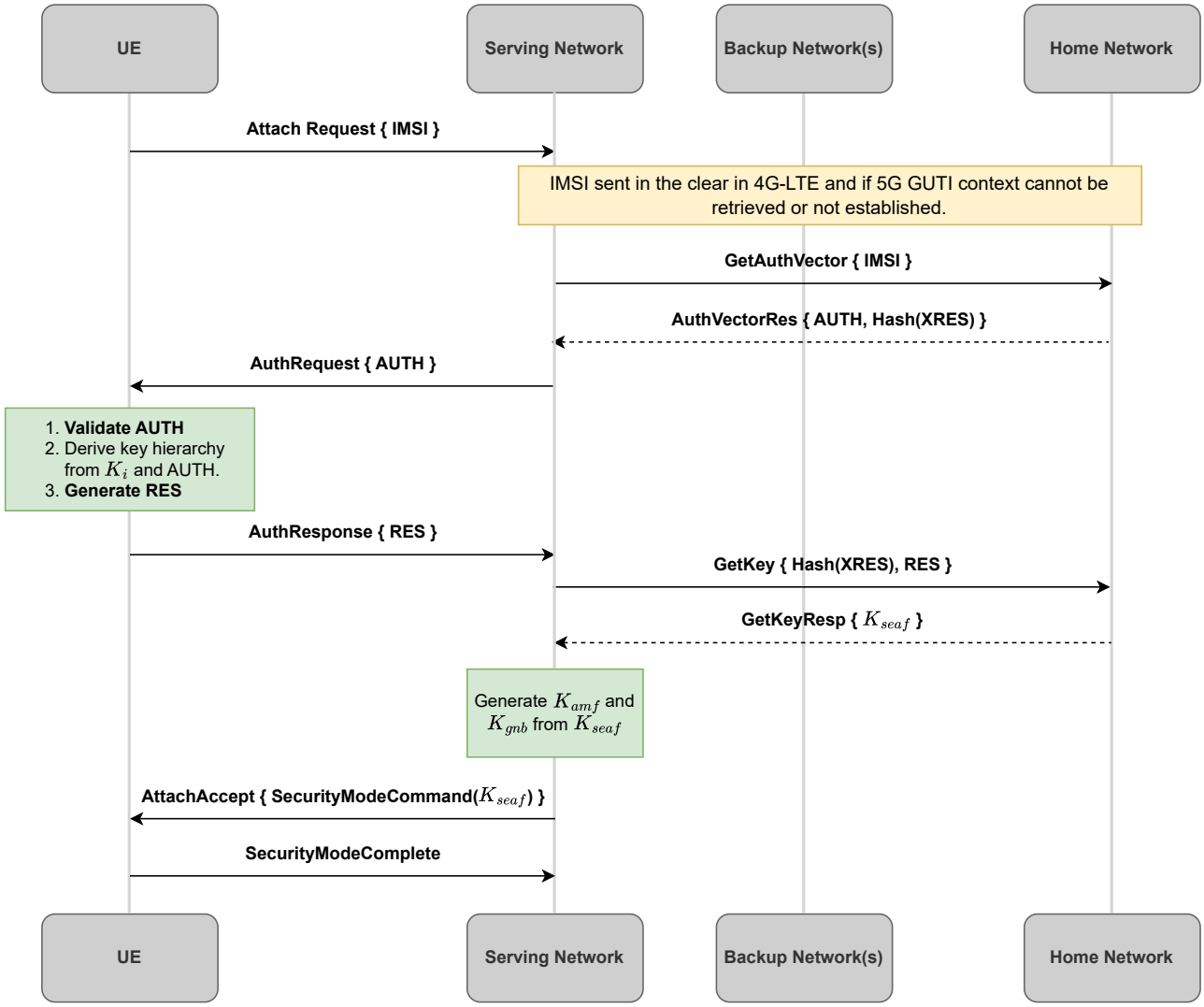


Figure 8: Basic authentication flow used between a serving network and the home network when the home network is available.

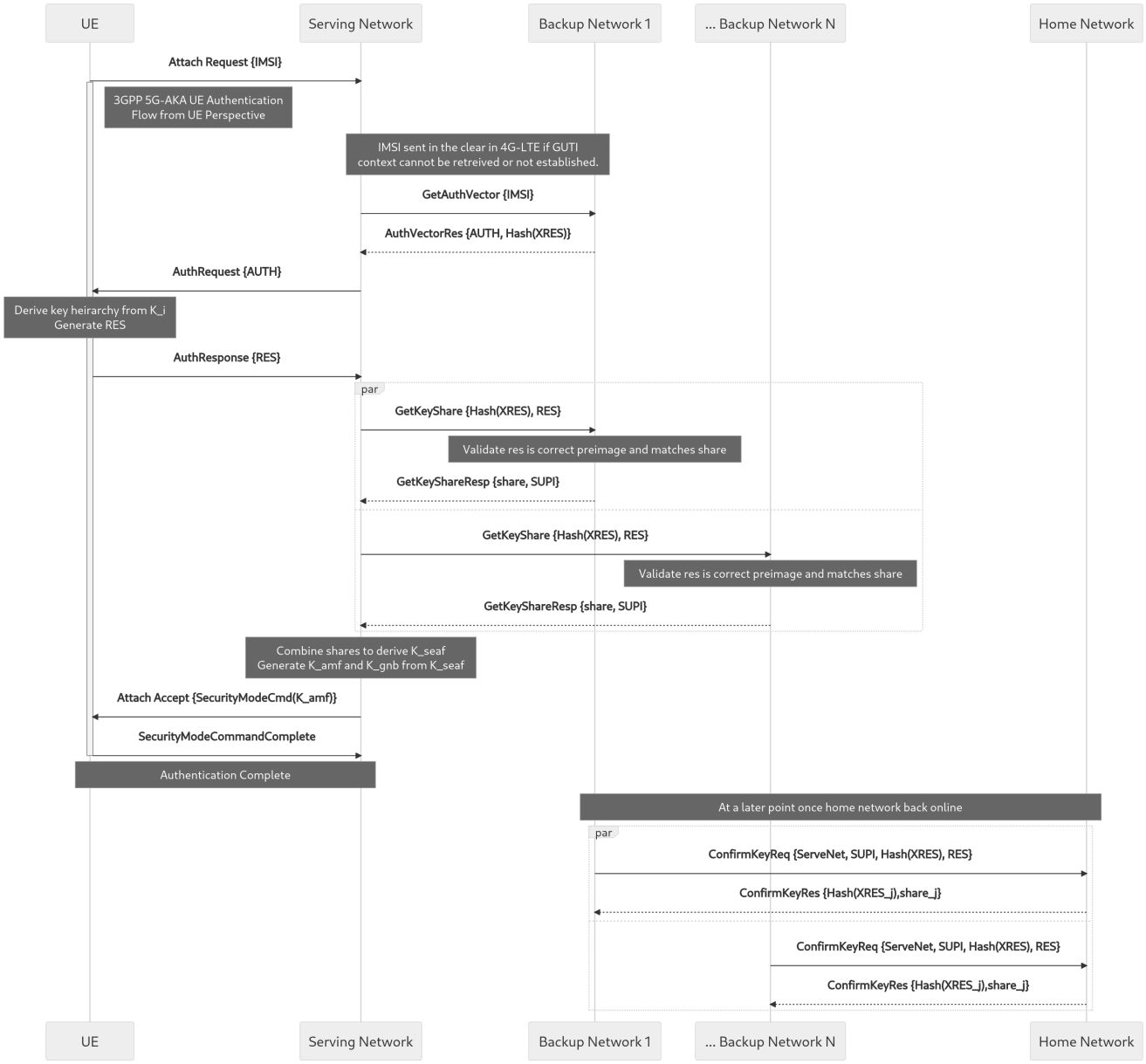


Figure 9: Message flow graph for Algorithm 1. dAuth authentication flow when the home network is offline. dAuth allows a (sub)set of backup networks to authenticate a user on behalf of the home network when the home network is unavailable. As long as one of the participating backup networks follows the protocol, the home network will receive confirmation of where the user was authenticated and can detect malicious or suspicious activity. Additionally, a serving network of insufficient reputation will not be able to establish radio control over the UE as long as one of the threshold backup networks faithfully enforces the user's trust preferences.

E Overflow Graphs

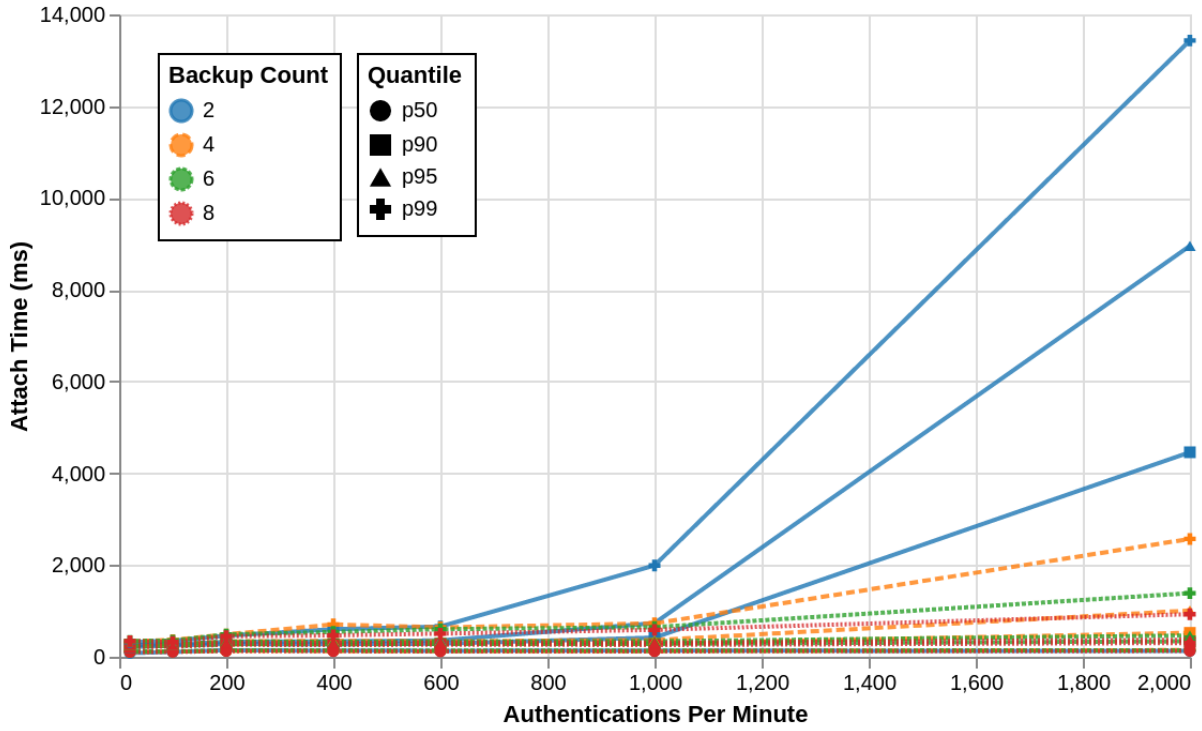


Figure 10: Performance vs. Backup Count, Full Graph