May 2022

LAWFUL INTERCEPT IN MULTI-PROVIDER 5G DEPLOYMENTS USING HOLOCHAIN

Niranjan M M

Nagaraj Kenchaiah

LAWFUL INTERCEPT IN MULTI-PROVIDER 5G DEPLOYMENTS USING HOLOCHAIN

AUTHORS:
Niranjan M M
Nagaraj Kenchaiah

ABSTRACT

Since Third Generation Partnership Project (3GPP) fifth generation (5G) wireless technology enables the potential for billions of connected network devices, a secure and scalable lawful intercept (LI) capability is needed across the mobile core. Although LI for third generation (3G) and fourth generation (4G) networks is a well-known concept, new challenges are posed with respect to the implementation of an LI capability in a 5G network, particularly when such a network employs a Control and User Plane Separation (CUPS) architecture. Also, in a 4G network and in a Long-Term Evolution (LTE) environment a user plane and a control plane are located within a data center making it easier to implement a LI capability. In a 5G network, the user plane is moving closer to a gNodeB (gNB) and hence implementing a LI capability will be challenging. To address these types of challenges, techniques are presented herein that support the use of a Holochain to provide a LI capability across multi-provider 5G deployments. Aspects of the presented techniques improve the security, scalability, and automation of a LI capability across the 5G core. Further aspects of the presented techniques help prevent the abuse of or the unlawful use of a LI (by, for example, individuals looking to make political, monetary, or business gains) through the use of Holochain validation rules whereby an abuse of power in a government agency or a service provider may be controlled and monitored (e.g., the tracking and monitoring of an interception may be completely audited to ensure that only properly authorized personnel are granted access to the data streams).

DETAILED DESCRIPTION

As an initial matter, it will be helpful to confirm the meaning of a number of terms that appear in the narrative that is presented below. Specifically:

Term	Meaning
Court of Justice	An authority that delivers the authorization to perform a lawful interception.
Happ	Holochain Lawful Intercept Application.
LEA	Law Enforcement Agency. An authority that intends to carry out a lawful interception on a user, a list of users, a service, or a list of services.
LI	Lawful Intercept.

Since Third Generation Partnership Project (3GPP) fifth generation (5G) wireless technology enables the potential for billions of connected network devices, a secure and scalable LI capability is needed across the mobile core. Although LI for third generation (3G) and fourth generation (4G) networks is a well-known concept, new challenges are posed with respect to the implementation of an LI capability in a 5G network, particularly when such a network employs a Control and User Plane Separation (CUPS) architecture. Also, in a 4G network and in a Long-Term Evolution (LTE) environment a user plane and a control plane are located within a data center making it easier to implement a LI capability. In a 5G network, a user plane is moving closer to a gNodeB (gNB) and hence implementing a LI capability will be challenging (as will be described next).

As defined in Section 12.9.2 (LI Architecture with CUPS) of the 3GPP Technical Specification (TS) 33.107, to accomplish a LI a user plane (UP) function duplicates the UP packets of the traffic that is to be intercepted (which is identified by the packet detection rules), as instructed by a control plane (CP) function, and then sends the duplicated UP packets to the Split X3 LI Interworking Function (SX3LIF) over the X3u reference point. The CP function also provides the forwarding action rules to the UP function which enables the UP function to determine how to send the duplicated UP packets over the X3u reference point to the SX3LIF. The CP function provides the intercept control information (such as a correlation identifier, a target identity, and intercepted packet identification rules) to the SX3LIF over the X3c reference point. The SX3LIF receives the UP packets from the UP function (over the X3u reference point), associates the UP packets to the target interception based on the intercept-related information that it received from the CP function (over the

X3c reference point), and then delivers the Content of Communication (CC) to Delivery Function 3 (DF3) over the X3 reference point.

In short, a CP function needs to define and share a range of information across a UP function, an SX3LIF, etc. Such information includes packet detection rules, forwarding action rules, and intercepted packet identification rules.

However, the standards do not define any method or protocol for the sharing of that information across 5G entities. Accordingly, techniques are presented herein that support a distributed method for sharing LI information across different 5G entities using a distributed ledger.

While the LI use case for 5G is known in the literature, it does not consider the important aspects of security and scalability.

Regarding security, the known use case does not address an unauthorized disclosure. For example, a compromised LI function may be activated or initiated without being triggered by a 5G operator, a compromised LI function may provide a LEA with information about users that do not belong to the declared list in an authorization, a compromised LI function may deliver information to an external attacker, and a compromised LI function may continue delivering information even after the end of the designated period in an authorization. Additionally, the known use case does not address disruption. For example, a compromised LI function may impact the quality of a given service. Finally, the known use case does not address deception. For example, a compromised LI function may deliver to a LEA fake information (e.g., services to which a user is subscribed (i.e., slices)) about the suspected user.

Concerning scalability, the known use case does not address LI across multiple service providers and does not explain the handling of LI with respect to a 5G CUPS architecture.

While there are known solutions that support a LI capability for 3G and 4G deployments, there are no solutions for providing a secure and scalable LI capability across 5G service providers. Consequently, techniques are presented herein that address the security, scalability, and privacy aspects of a LI capability in 5G multi-provider deployments.

As noted previously, the implementation of a LI capability in a 5G CUPS architecture faces many challenges with respect to providing complete scalable solution which works across multiple service providers and across multiple countries. Additionally, existing LI methods face many challenges with respect to security and scalability. Consequently, a LI method is needed that satisfies a number of requirements.

A first requirement encompasses scalability. For example, the LI capability should work across multiple service providers. Additionally, the capability should work with a 5G CUPS architecture. A second requirement encompasses transparency. For example, a LI, when activated, should not be detectable. A third party (e.g., through observation) or a user (e.g., through quality of service) should not notice any change when an LI function is activated. A third requirement encompasses confidentiality. For example, only concerned entities (i.e., the 5G operator LI service and a LEA) should have access to the list of the wiretapped. A fourth requirement encompasses dependability and reliability. For example, a 5G operator should be able to provide a high level of assurance regarding the validity of any collected information. A fifth requirement encompasses security. For example, only the 5G operator should be able to activate a LI to obviate fraudulent interceptions. Additionally, information that is delivered by a LI must be provably trustworthy.

The techniques presented herein support a method which satisfies the above LI requirements. Aspects of the presented techniques employ a Holochain to provide a LI capability across multi-provider 5G deployments (as will be described and illustrated later in the instant narrative). Importantly, the presented techniques improve the security, scalability, and automation of LI across the 5G core.

Additionally, the presented techniques help prevent the abuse of or the unlawful use of a LI (by, for example, individuals looking to make political, monetary, or business gains) through the use of Holochain validation rules. Through such rules an abuse of power in a government agency or a service provider may be controlled and monitored (e.g., the tracking and monitoring of an interception may be completely audited to ensure that only properly authorized personnel are granted access to the data streams).

Before beginning a detailed discussion of the techniques presented herein, it will be helpful to briefly describe three of the capabilities that the presented techniques leverage – i.e., Holochain technology, a Distributed Hash Table (DHT), and the Gossip protocol.

First, Holochain technology addresses various of the drawbacks with blockchain technology and employs a fully distributed means for data sharing and access, holographic data storage, and secure peer-to-peer network communication (i.e., there is no centralized server, there are no ledgers, and there are no intermediaries such as miners).

A Holochain integrates a number of technologies to achieve the features that were described above including hash-chains (that provide data integrity that cannot be changed and which maintain the order of transactions based on the time sequence on each node), digital signatures (whereby messages and validation confirmations are signed cryptographically to ensure authorship, origin, and accountability with any re-signing of transactions or interactions between any parties leading to a rejection and the "locking" of a chain), and a DHT (that utilizes cryptographic hashes for content-addressable storage and validates same with hash-chains and a digital signature before storing a transaction on the DHT).

In short, blockchain technology has a number of drawbacks and limitations including scalability (as data needs to be replicated on all of the blockchain nodes and is also limited by the number of transactions), a longer convergence time, the addition of transactions to the blockchain (e.g., on Ethereum it takes approximately ten minutes to add a transaction to the blockchain), and the need for the time (i.e., a clock) to be synchronized among the blockchain nodes as a timestamp is part of a transaction and is used during the merging of ledgers.

A Holochain overcomes the above blockchain limitations and supports fully distributed peer-to-peer computing.

A Holochain also has a robust security system and is safe from malicious attacks. This is achieved by implementing three cryptographic technologies, namely digital signatures (to provide authenticity and ownership of the data), hash-chains (to provide data integrity and ordering based on a time sequence), and a DHT (to provide decentralized data storage so that it may be hosted by outside communities from a centralized authority system).

Additionally, Holochain is an open source framework, it is being positioned as an alternative to blockchain, it is agent-centric (i.e., it is modelled from the user perspective) compared to blockchain which is data-dependent, it avoids keeping a global consensus (by

using an agent system where each agent maintains a private fork), and it solves the scalability problems of blockchain by using a DHT. Further, the decentralized application (dApp) on a Holochain is called a Happ. The different Happs are empowered by the Holochain runtime, with each user (i.e., node) running their own copy of the backend code, controlling their identity, and storing their own private and public data. The users (i.e., Happ instances) communicate with each other directly over an encrypted peer-to-peer network.

It is important to note that in the above discussion the terms data, information, transaction, event, message and packet are used interchangeably.

Second, in a generic DHT the nodes coordinate among themselves to balance and store data in the network without any central coordinating party. DHTs are both fault tolerant and resilient when key-value pairs are replicated. DHTs require that information be evenly distributed across the network. To achieve this goal, the concept of consistent hashing is used. A key is passed through a hash algorithm that serves as a randomization function. This ensures that each node in the network has an equal chance of being chosen to store the key-value pair.

DHTs enable key-value pair storage and retrieval across many machines. The only validation rules they have concern the hash of the data itself to confirm that what is obtained is what was intended. They have no other means to confirm the authenticity, provenance, timelines, or integrity of data sources.

For a Holochain variant of a DHT, by embedding validation rules as a condition for the propagation of data, a Holochain DHT keeps its data bound to signed source chains. This can provide similar consistency and rule enforcement as blockchain ledgers asynchronously, so bottlenecks of immediate consensus become a thing of the past.

A Holochain DHT leverages the signed source chains to ensure the tamperproof immutability of data, as well as cryptographic signatures to verify data origins and provenance. A Holochain DHT also emulates aspects of a graph database by enabling a node to connect links to other hashes in the DHT that are tagged with semantic markers. This helps solve the problem of finding the hashes that are to be retrieved from the DHT.

Third, the Gossip protocol is the Holochain protocol that is used by many peer-to-peer networks to rapidly propagate data. Each node has knowledge of a few other nodes,

the few other nodes have knowledge of several more nodes, and so forth. Whenever any node receives a message, they broadcast it to some or all of their peers. Data propagates slowly at first, then spreads at an exponential rate. Nodes in a Holochain network share entries, metadata, neighborhood health, and peer addresses via the Gossip protocol.

Figure 1, below, presents elements of an exemplary arrangement according to aspects of the techniques presented herein and reflective of the above discussion.

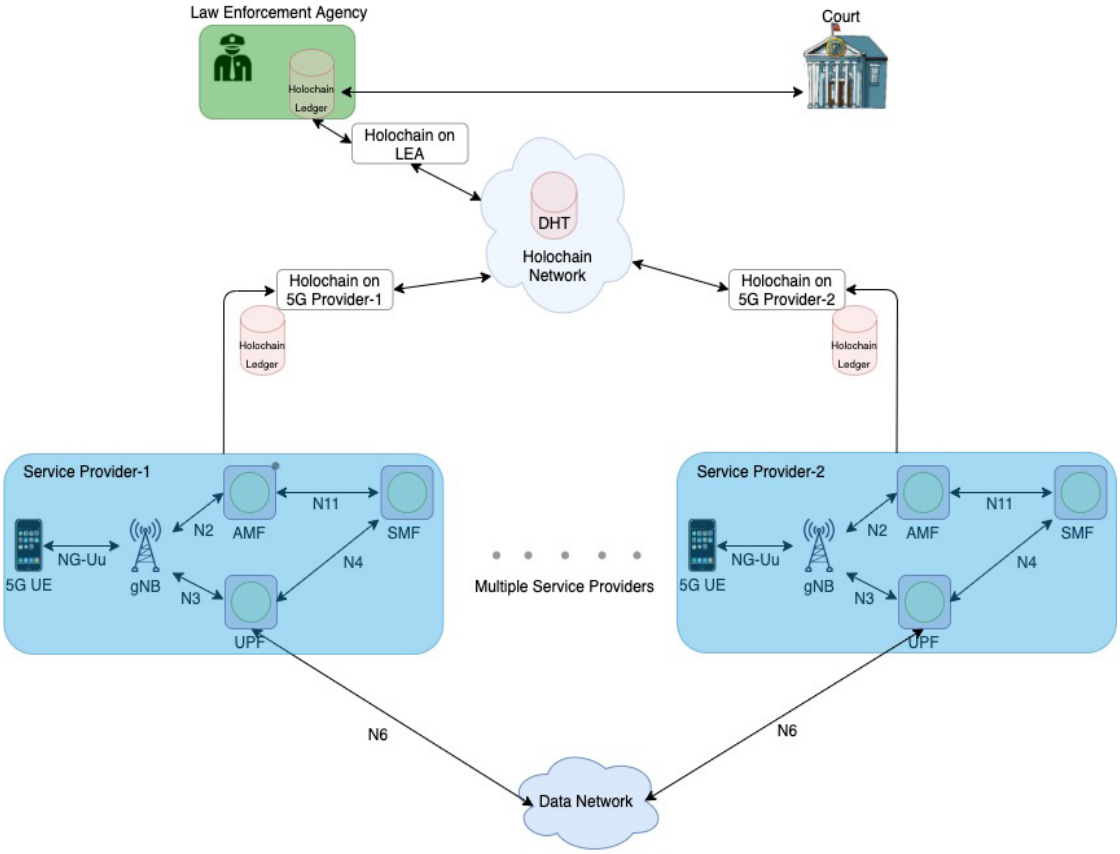

Figure 1: Exemplary Arrangement

As depicted in Figure 1, above, a LEA may receive a court order or a warrant indicating that a LI is to be performed. Such an artifact may request that the LEA allow a judge or a court administrator to enter the details of the mobile device that is associated with the LI. Following the receipt of such a request, the LEA may allow access to the judge or the court administrator so that they may add a transaction (containing the details of the mobile device) to a Holochain.

The judge or the court administrator may employ a secure Holochain LI application to enter into a Holochain a transaction with all of the essential data (e.g., the details of a particular mobile device or a set of mobile devices) that is needed to perform the LI.

Access to the Holochain LI application (i.e., a Happ) may employ multifactor authentication (such as, for example, two-form authentication). This, in turn, may provide a digital form of a court order so that the LI process may be fully automated.

The Holochain LI application (i.e., a Happ) may communicate with a mediation server or device to translate the mobile device details into a user equipment (UE) identity (e.g., an international mobile subscriber identity (IMSI), an International Mobile Equipment Identity (IMEI), etc.). Further, a Happ may add the details of the mobile device (such as IMSI, IMEI, etc.) as transaction T to the Holochain DHT.

Once the new LI transaction is added to the Holochain DHT, the 5G service providers are ready to stream the activities of a mobile device or phone number to the LEA location.

At the LEA location referenced within the court order, a chosen law enforcement official may use the secure Holochain Lawful Intercept application (i.e., a Happ) and multifactor authentication to initiate the LI data streams be sent to that LEA location through an encrypted tunnel. The data may be decrypted for real-time listening, or it may be stored in a secure storage drive within the server that is hosting the Happ. The law enforcement official may log in to the Happ to retrieve recordings from the server (where they are stored in an encrypted form) for playback by using a time-line playback system.

Under the above approach, access to a LI data stream would be validated through the Holochain validation rules. Further, the Holochain may be externalized across service providers (e.g., all of the different 5G vendors may register their 5G network elements (such as, for example, an AMF) as part of the Holochain). Similarly, LEAs would also register their nodes across the 5G mobile core to gain access to the Holochain and, in turn, access to the LI data streams.

A court order (as described above) may contain a time limit on how long a LEA may record a mobile phone's data. The Holochain nodes at a 5G service provider will continue to stream the phone's LI data to the LEA office until a court order time limit has expired or until it is terminated by the judge at the original courthouse, at which point the

Holochain nodes at the 5G service provider will stop streaming the LI data to the LEA office.

Figure 2, below, illustrates elements of the above discussion according to aspects of the techniques presented herein.

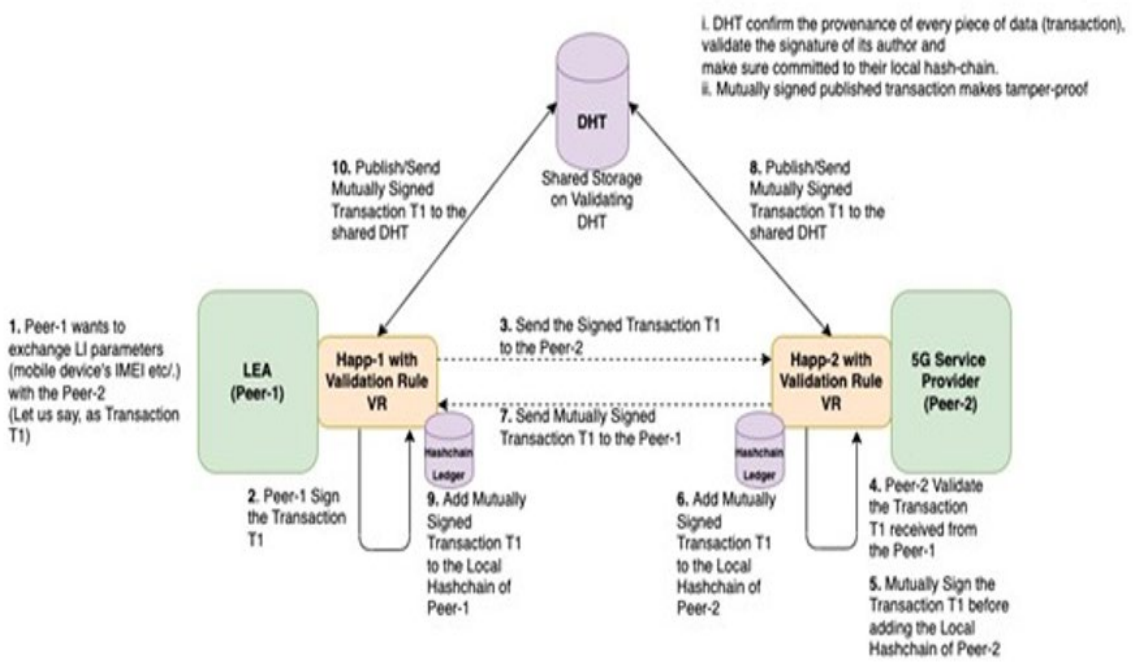

Figure 2: Transaction Exchange Between LEA and 5G Service Providers

Aspects of the techniques presented herein encompass global policing and validation rules. A global policy server may be used to provide flexibility and to support the management of various country interactions from within a LEA (where the policy controls that are to be enforced and implemented may be based on country regulations and determined by a phone number, a LEA_Provider_ID, and a SP_Provider_ID). This type of global expansion and flexibility may be seen in a multi-country implementation and will help with automation, completeness, and flexibility on a global scale.

A policy-driven engine on the LEA side may handle the legal enforcement of local rules and provide for policy enforcement across all of the countries to help the LEA be fully in compliance with legal standings.

The approach that was described above may be expanded to other LEAs around the world (such as, for example, the International Criminal Police Organization (ICPO, or Interpol) which would help increase the security by adding more nodes and allow for multi-country data stream tracking.

Consider a first illustrative example comprising the Narcotics Control Bureau (NCB) which is an Indian federal law enforcement and intelligence agency under the Ministry of Home Affairs. Under the example, the NCB wishes to track a data stream from a mobile device that was located inside or outside India. The NCB would start a Holochain to establish the request for a LI of the data for the designated phone number. The other LEAs and service providers that are interacted with would have to agree to the Holochain request and then would open the data stream to the NCB for the particular phoner number.

Consider a second illustrative example comprising the Research and Analysis Wing (RAW) which is the primary foreign intelligence agency of India that deals solely with the collection of data for the judicial courts. Under the example, the RAW wishes to trace a data stream from a mobile device. The RAW would start a Holochain to establish the request for a LI. Following agreement from the other LEAs and service providers, the data stream would open to the RAW for the particular phone number or set of mobile numbers.

The techniques presented herein may be further explicated with reference to a discussion, from a Holochain’s point of view, of the above-described processes.

Initially, a judge or court administrator may add a transaction to the Holochain ledger that is maintained by a LEA. Later, the LEA may perform peer-to-peer communication with every service provider that is being asked to perform a LI. The LEA may request that all of the 5G service providers perform a LI for a particular mobile device for a specific duration. For simplicity of exposition, this request may be referred to as transaction T (comprising a mobile device's number, an IMEI, an operator identifier, etc.).

A Happ that is running on the LEA creates and signs transaction T and adds it to the local hash-chain. The Happ would then publish the signed transaction T to the Holochain DHT. The Happ would also use the Gossip protocol to convey the request to all of the 5G service providers and also to the other LEAs.

Every 5G service provider will process the request that was received over the Gossip protocol and publish a signed notification response (saying that they can and will

perform the LI for the specific mobile device) to the Holochain DHT. Following such a notification, the source LEA (i.e., the initiator) knows whether the LI can be completed by the 5G service providers. Importantly, privacy regarding the LI is provided by the Happ having both generic validation rules for all of the LEAs or for a specific LEA (based on, for example, a region or country) and/or for the 5G service providers.

Application of the techniques presented herein offers a number of advantages. For example, aspects of the presented techniques support an on-demand LI capability in 5G core network deployments in an efficient, secure, and authentic manner while considering the important issue of privacy (as described in the latest instance of the General Data Protection Regulation (GDPR)). Further, under aspects of the presented techniques there is no centralized gathering of LI information, rather any LI information is gathered in a distributed manner.

While the narrative that was presented above employed Holochain technology, it is important to note that the techniques presented herein are not limited to just that technology and may, for example, employ any efficient distributed ledger method.

In summary, techniques have been presented herein that support the use of a Holochain to provide a LI capability across multi-provider 5G deployments. Aspects of the presented techniques improve the security, scalability, and automation of a LI capability across the 5G core. Further aspects of the presented techniques help prevent the abuse of or the unlawful use of a LI (by, for example, individuals looking to make political, monetary, or business gains) through the use of Holochain validation rules whereby an abuse of power in a government agency or a service provider may be controlled and monitored (e.g., the tracking and monitoring of an interception may be completely audited to ensure that only properly authorized personnel are granted access to the data streams).