March 2022

MULTIPLE PROVIDER SDN PROVISIONING USING HOLOCHAIN TECHNOLOGY

NIRANJAN M M

MULTIPLE PROVIDER SDN PROVISIONING USING HOLOCHAIN TECHNOLOGY

AUTHOR:
NIRANJAN M M

ABSTRACT

Typically, SDN controller manage network devices (Router, Switches, Servers etc.,) within given service provider or enterprise domains. These controllers are either deployed centrally or distributed across provider network to provide redundancy, however the scope of network devices they manage are limited within operator's domain. Many service providers want to launch end-to-end fully automated enterprise services extending across other service providers. They may deploy SDN controllers to program and manage configuration within their own networks; however, coordination of provisioning services in another provider network is either manual or extremely difficult. The techniques presented herein propose method which enables securing end-to-end services in multiple provider SDN deployments using service and flow-based security policies. These services and security policies are based on a variety of attributes such as parameters associated with SDN controllers and devices/switches, context information such as location and routing information, and services accessed in SDN as well as security attributes associated with the controllers and switches in different domains. In short, call these as "Policy Attributes", which are significant for securing end to end services in multiple provider SDN deployments. With the techniques presented herein, SDN controllers in multiple provider deployments will be able to securely exchange provisioning configurations, policy parameters, request and share resources based on the access control policies without compromising on privacy.

DETAILED DESCRIPTION

Typically, SDN controller manage network devices (Router, Switches, Servers etc.,) within given service provider or enterprise domains. These controllers are either deployed centrally or distributed across provider network to provide redundancy, however the scope of network devices they manage are limited within operator's domain. New enterprise services e.g., L2/L3 VPN, EVPN, 5G network slicing etc., are likely to extend beyond one operator's domain. Hence, for providing global services, they might involve many operators across geographies involving different carriers.

Many service providers want to launch end-to-end fully automated enterprise services extending across other service providers. They may deploy SDN controllers to program and manage configuration within their own networks; however, coordination of provisioning services in another provider network is either manual or extremely difficult. The deployment of enterprise services across different service provider is not automated due to lack of SDN controllers' integration.

Even if some techniques provide secure mechanism for an SDN controller from one operator to communicate and pass configuration/policy parameters to SDN controller of another operator, but they lack providing policy-based access control along with privacy, when extending services across multiple service providers.

The techniques presented herein propose method which enables securing end-to-end services in multiple provider SDN deployments using service and flow-based security policies. These services and security policies are based on a variety of attributes such as parameters associated with SDN controllers and devices/switches, context information such as location and routing information, and services accessed in SDN as well as security attributes associated with the controllers and switches in different domains. In short, call these as "Policy Attributes", which are significant for securing end to end services in multiple provider SDN deployments.

As per this method, each SDN Controller (Peer-1) acts as a Holochain node and consider passing provisioning parameters to another SDN controller (Peer-2) (via the Holochain network) as a "transaction" (let us say T1), which gets recorded in the ledger of both the peers. Holochain technology make sure, the transaction T1 is passed over the encrypted channel, tamper-proof (not modified, not repeated) and authentic. And validation rules setup between Peer-1 and Peer-2 makes sure, access control along with privacy is maintained so that any other SDN controller (let us say, Peer-3) will not be able to know what all the services and security policies are used between Peer-1 and Peer-2. Validation Rules are defined as per the "Policy Attributes".

In this method, each service provider has SDN controllers and number of devices (Switches/Routers/WLC) managed by those SDN controllers. SDN controllers are enabled with Holochain functionality. Validation rules are setup according to service and security policies defined, also called as "Policy Attributes". Holochain will have validation rules and would be the first entry in the local hash-chain. Same validation rules are used between the peers (SDN Controllers) which provides sort of access control and privacy. Validation rules govern who are all allowed to join a network and see its data. In other words, validation rules make sure only allowed user/node can join the Holochain network and see its data. Validation rules can be used to validate the structured data, upper/lower bounds of numbers, string lengths, non-empty fields, or correctly formatted content. Validation rules can make sure transactions are legitimate. Here only validation rules require global consensus compared to Blockchain where every transaction need global consensus. With these validation rules as the foundation, each peer keeps an immutable record (transaction) of their own actions on a local hash-chain. Each hash-chain entry (record/transaction) is cryptographically signed to prove authorship and ensure accountability. Transactions are mutually counter signed by both the peers (here, SDN Controllers). They can audit each other's chains before agreeing to the transaction. Holochain DHT confirm the provenance of every piece of data (transaction), validate the signature of its author and make sure it is already committed to their local hash-chain. Mutually signed published transaction on the Holochain DHT makes tamper-proof.
With this method, SDN controllers in multiple provider deployments will be able to securely exchange provisioning configurations, policy parameters, request and share resources based on the access control policies without compromising on privacy.

Figure-1 describes the high-level architecture of SDN Controllers in Multi-Provider deployment using Holochain Technology.

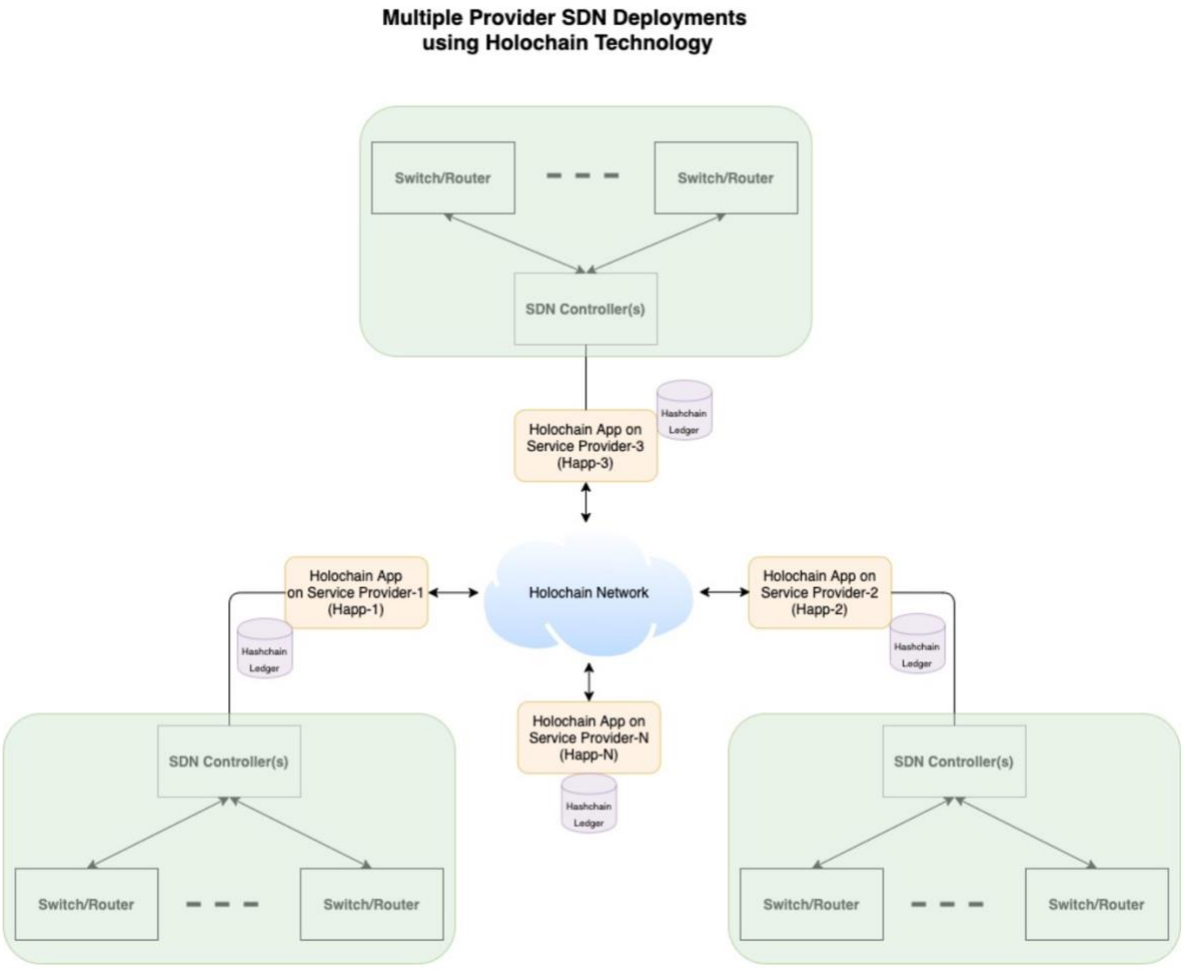

Figure-1

Let us consider, Peer-1 wants to exchange provisioning configurations and policy parameters with the Peer-2 (Let us say, as Transaction T1).

- Peer-1 Sign the Transaction T1 (using its Private Key SK).
- Peer-1 sends the Signed Transaction T1 to the Peer-2.
- Peer-2 Validate the Transaction T1 received from the Peer-1 (using Public Key PK of Peer-1).
- Peer-2 Sign the Transaction T1 before adding to the Local Hash-chain (now Mutually Signed).
- Peer-2 adds Mutually Signed Transaction T1 to its Local Hash-chain.
- Peer-2 sends Mutually Signed Transaction T1 to the Peer-1.
- Peer-2 Publish/Send Mutually Signed Transaction T1 to the shared DHT.
- Peer-1 adds Mutually Signed Transaction T1 to its Local Hash-chain.
- Peer-1 Publish/Send Mutually Signed Transaction T1 to the shared DHT.

Figure-2 describes the peer-to-peer communication between SDN providers using Holochain.

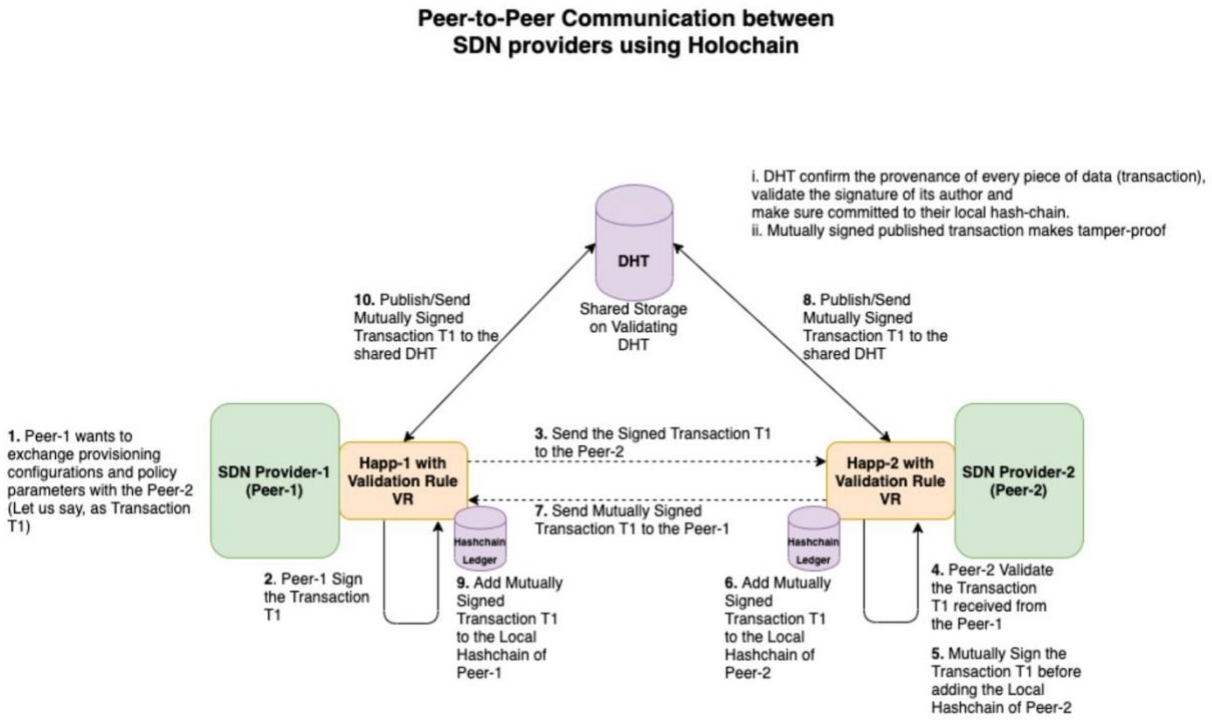

Figure-2

In summary, techniques described herein provide policy-based access control along with privacy for secure communication between SDN controllers in multiple service provider deployments. It is suitable for privacy sensitive scenarios, particularly, in the encryption system of industrial cloud, the policy attributes often involve business secrets of industrial enterprises. This method is very consistent with the security requirements of cloud storage. This method can be used in different enterprise services e.g., L2/L3 VPN, EVPN, 5G network slicing etc., as they are likely to extend beyond one operator's domain wherein maintaining privacy along with security is important aspect.