March 2022

5G NETWORK DEPLOYMENTS WITH DE-CENTRALISATION OF POLICIES AND CONFIGURATIONS

NIRANJAN M M

5G NETWORK DEPLOYMENTS WITH DE-CENTRALISATION OF POLICIES AND CONFIGURATIONS

ABSTRACT

5G network deployment comprises of multiple AMFs, SMFs, UPFs, gNodeBs etc., intended to provide collaborative services such as network slicing, session management, roaming, load balancing etc.,. These 5G network deployments being large, configuring individual AMFs, SMFs etc., in such large system is difficult. Presented herein are techniques to incorporate 5G network deployments with authenticated distributed ledger to securely store the configuration and subsequent configuration changes (keep only changes from the previous one, using dictionary method: key-value pair to identify the difference), so that AMF configuration can be shared across AMF Set or AMF Region. Further, access to the ledger is based on different criteria such that configurations can be shared with-in or across AMF Regions.

DETAILED DESCRIPTION

5G network deployment comprises of multiple AMFs (identified using Globally Unique AMF Identifier [GUAMI]), SMFs, UPFs, gNodeBs etc., intended to provide collaborative services such as network slicing (eg., URLLC, eMBB), session management, roaming, load balancing etc.,. AMF configurations are being done through centralised management system (e.g., RAN EMS). AMF configuration mainly includes PLMN identifier, NSSAI (slice ID, slice type information) along with configurations required to communicate with SMF, NSSF, PCF etc., Also AMF typically queries the 5G Service-Based Architecture's Network Repository Function (NRF) to discover and select available SMF instances. SMF configurations are done through SMF Operations (Ops) Center. SMF configuration mainly includes the NRF profile data configuration, the externally visible IP addresses and ports etc., In addition, need to configure other elements of 5G deployment for the whole network to be up and functional.

These 5G network deployments being large, configuring individual AMFs, SMFs etc., in such large system is difficult. Also AMFs should be horizontally as well as vertically scalable to handle the massive UE scale. For horizontal scaling, AMFs would run multiple UEMgr processes (to handle UE state machine and database) based on the resource availability. For vertical scaling, AMFs (on an appliance or virtual or containerised instance) would form cluster with role as Master and Slave. One of the AMF would be elected as Master using consensus algorithm. Master is the point of contact for all configurations, policies, image management, config backup and recovery, load balancing of UEs across Slave devices.

The 5G core network will contain multiple logically separated network slices. Each slice has a specific network topology, network function, and resource allocation model. If manual configuration is used for network planning and deployment, operators' O&M system will potentially face a huge number of significant challenges and also manual configurations will significantly increase OPEX.

As such, there is a need for a mechanism to incorporate secure and optimised techniques to distribute configurations in 5G network deployment and also as part of this technique we should track who, what and when a configuration change occurred. In addition, mechanism should address issue with new AMF addition, replacement due to hardware failure and allowing the cluster to self-configure the new AMF without the need for external 3rd party systems.

The techniques presented herein propose to incorporate 5G network deployments with authenticated distributed ledger (private blockchain) to securely store the configuration and subsequent configuration changes (keep only changes from the previous one, using dictionary method: key-value pair to identify the difference), so that AMF configurations can be shared across AMF Set or AMF Region. Further, access to the ledger is based on different criteria such that configurations can be shared with-in or across AMF Regions.

The AMFs in the AMF Region form a group to construct a private blockchain. Then all configuration actions are stored in the created private blockchain (also called as HyperLedger). This would allow an accurate tracking of how, what and when the configurations are changed. The distributed nature of HyperLedger remove the need to store the whole configuration on the centralised server. In case of centralised method, they need to have high availability to handle failure cases (i.e., apart from storing on the centralised server, need to take backup outside the deployment as well).

Most of the devices has Plug and Play (PnP) agent integrated into it, and is applicable even to AMF/SMF in the 5G deployment, which plays a role in the initial configuration of the devices. PnP server would be running on the device configuration management system (viz., it could be RAN EMS or a cluster master) run a lightweight blockchain client to update device configuration changes and record the information about the changes in authenticated HyperLedger which is distributed across the 5G deployment. PnP agent (aka PnP Client) running on the devices (viz., AMF/SMF) would also run lightweight blockchain client to fetch configuration from the HyperLedger.

Advantages of using PnP agent is that it is already there in most of the devices, so requires less adoption issue and it works with configuration management system (running PnP Server) to extract or push any configuration changes to the devices.

PnP agent is well integrated with device security framework for initial on-boarding. This can be leveraged for securing blockchain client certificate information in the device. Devices can use ACT2 chip which is a tamper-proof HW chip used for storing the certificates. Blockchain client running on the AMF/SMF authenticates itself using SUDI certificate (viz., signed with Root CA) stored in the ACT2 chip to prevent malicious devices from writing to the blockchain or even reading from the blockchain which is a requirement to use

Authenticated HyperLedger. In case of virtual/container instances, similar security is provided by vTPM (or virtual Trusted Anchor Module [vTAM]).

The following steps illustrate the technique presented to de-centralisation of policies and configurations in 5G deployments:

- Consider 5G deployment comprises of multiple AMF Regions which in-turn have multiple AMF Sets.
- All the AMFs register with the private blockchain with specific services which they are interested, so that they can access the authenticated HyperLedger provided for that service.
- HyperLedger is a permission blockchain framework that provides privacy and confidentiality.
- All configurations are done on the configuration management system (RAN EMS or an AMF cluster master) run a lightweight blockchain client to update device configuration changes and record the information about the changes in authenticated HyperLedger.
- All the AMFs would fetch configurations/policies/slice information from the Authenticated HyperLedger by running lightweight blockchain client.
- Same thing holds good for other 5G network elements such as SFM/PCF etc.,
- For adding new AMF to the AMF Region (or AMF cluster): Only after authenticating with the private/permissive blockchain, access is allowed to the HyperLedger to get initial config as well as sub-sequent “config diff” as per the registered service and apply all configuration in-order.
- For Return Merchandise Authorization (RMA) of AMF: New AMF authenticates using SUDI certificate (stored in TPM/vTPM) and register required service(s) with the private blockchain and get all relevant configuration based on the registered service and apply.

The techniques presented herein have several advantages, includes:

- Distributed secure storage of the configurations.
- Storing only the modified config changes in the Blockchain.
- Avoids having one-to-one secure communication channel between AMF and device management device (e.g., RAN EMS or cluster master) for sharing the configuration.
- Easy to track individual changes done and by whom.
- Authenticated way of accessing private Blockchain using device specific SUDI certificate stored in the ACT2 chip. Hence prevent malicious devices from writing to the blockchain or even reading from the blockchain.
- Isolated networks from the internet are unable to take advantage of

enterprise PnP. Also isolated networks require 3rd party software for configuration backup to be deployed, which means a customer that has multiple isolated networks would need multiple of those configuration backup systems. The customer has to be concerned with storage and managing of these 3rd party systems. If the blockchain can be distributed among devices, then storage is built-in and automatically supports isolated networks. Also having individual configuration changes in time will allow a customer or TAC Engineer to better debug when an issue has occurred.

- Efficient way to handle failure scenarios in High Availability and Cluster deployments.

The techniques presented herein can be used to share configuration and policies among AMFs in the AMF Region in an optimized way. In addition, the techniques presented herein can be used to share configuration and policies in AMF cluster deployments. In general, the techniques can be used for any configuration and policy management of 5G network deployments.