March 2022

SECURE METHOD TO DISCOVER MESH ROUTERS IN SOFTWARE-DEFINED WIRELESS MESH NETWORKS

Niranjan M M

SECURE METHOD TO DISCOVER MESH ROUTERS IN SOFTWARE-DEFINED WIRELESS MESH NETWORKS

AUTHOR:
Niranjan M M

ABSTRACT

The combination of Software-Defined Networking (SDN) and Wireless Mesh Network (WMN) is challenging due to the different natures of both concepts. SDN describes networks with homogeneous, static and centralised controlled topologies. In contrast, a WMN is characterised by a dynamic and distributed network control, and adds new challenges with respect to time-critical operation. However, SDN and WMN are both associated with decreasing the operational costs for communication networks which is especially beneficial for internet provisioning in rural areas. Due to dynamic nature of the topology in SDWMN deployments, Mesh Router (MR) discovery is a challenge. The techniques presented herein propose method to de-centralise the MR discovery in SDWMN deployments without compromising on authentication and security aspects. Using this technique, adding, and removing of MR would be easy, secure, and automated, it also provides faster convergence of MR discovery.

DETAILED DESCRIPTION

Software-Defined Wireless Mesh Network (SDWMN) deployments are considered as a viable option to provide wireless coverage for a vast area, such as community-wide or city-wide. SDWMN is combination of Software-Defined Networking (SDN) and Wireless Mesh Network (WMN). In other words, it consists of Centralized SDN Controller and Wireless Mesh Network. Wireless Mesh Network (WMN) is a multi-hop radio network whose nodes are IP routers with one or more wireless interfaces, typically based on IEEE 802.11 Wi-Fi technologies. Backbone of a WMN is made up of dedicated wireless nodes called Mesh Routers (MRs). Traditional Software-Defined Networking describes networks with homogenous, static, and centralized controlled topologies. In contrast, a WMN is characterized by a dynamic and distributed network control with Mesh Routers forming the backbone of such networks. Due to dynamic nature of the topology in SDWMN deployments, Mesh Router discovery is a challenge. There are techniques which uses

centralized method to discover the nodes where each node register with the centralized entity (like service registry) which maintains list of registered nodes.

In centralised methods, the control channel between MR and SDN Controller could be in-band or out-of-band. In case of in-band, same wireless interface is used for both control and data channel and they are differentiated by using different SSID. In case of out-of-band, control channel is completely separated from the data channel and there could be dedicated wired connectivity for the control channel. Both methods are having their own advantages and disadvantages. Out-of-band channel deployments are more expensive due to the presence of alternative path for the control traffic, but MR node discovery is relatively easy by using existing LLDP based topology discovery protocols and control channel connection is over OpenFlow (OF) protocol. In-band channel deployments are less expensive, but node discovery and establishing control channel with the SDN Controller is complex i.e., for the centralized method to discover the nodes in case of in-band channel deployments, following are the pre-requisites.

- Before the SDN control channel connection can be established, a SDWMN interface of the MR needs to connect to one of its already connected neighbour MR or the SDN controller itself.
- MR node can be discovered only if its neighbour MR in the higher hierarchy is already discovered by the SDN Controller and control channel connection is established (it is of mesh tree structure with SDN Controller being root).

Considering the disadvantages of centrally managed methods, we need a way to de-centralize Mesh Router discovery in SDWMN deployments without compromising on authentication and security aspects. As SDWMN are probably on public (few could be private) deployments, it is extremely important to ensure the participating MRs are authentic and trusted. We need authentic and trusted mechanism to avoid malicious nodes (to avoid attacks such as Denial-of-Service, man-in-the-middle attacks, route poisoning etc.,) being added to the WMN deployments and once they are added, it is difficult to identify and remove from the deployments.

The techniques presented herein use Hyperledger to discover MRs in the SDWMN deployments. Hyperledger is a permissioned blockchain framework that provides privacy and confidentiality required especially for these types of deployments. This is also termed as private blockchain. In SDWMN deployment, the Endorser functionality of Hyperledger would be done by the Mesh Routers and Consenter functionality would be done by the SDN Controller. SDN

Controller acts as a Blockchain Provider (BP). Optionally BP functionality may run on a trusted entity outside the SDN deployment as well, which might be useful when SDN controller does not have support for Blockchain. Using Hyperledger we are making sure, only authenticated MRs would have access to the permissioned ledger. And Hyperledger would help in logical separation from different operator domain (in other words, avoid false positives of discovering MRs of neighbour SDWMN deployment).

Authentication using secure credentials would not be sufficient, we need to verify the trustworthiness and integrity of the MRs before adding to the Hyperledger. Hyperledger is made available to all the MRs in the deployment, so that all MRs can learn the MR being discovered and may use this information to authenticate and further communicate with each other to form the Wireless Mesh backbone.

Phase-1 of Discovery:

Before adding MR to the Hyper Ledger, trustworthiness of the MR is validated using Attestation method as below:

(Let us say, MR-1 is MR being discovered and MR-2 is its neighbour MR)

1. MR-1 being discovered, will first connect to the neighbour MR-2 over wireless interface.
2. MR-1 sends "Add Me" message to neighbour MR along with Attestation Information.
3. Attestation Information from MR-1 would carry, Hardware Fingerprint, Software information, Counters, time-ticks, signature etc.,
4. Neighbour MR-2 would validate Proof of Integrity using Attestation Information sent by the MR-1.
5. Once validation is successful, neighbour MR-2 adds MR-1 to the Hyperledger.

At the end of the discovery, all MRs would be added to the Hyperledger and same is available with the SDN Controller to establish secure control channel connection with each discovered MR.

Phase-2 of Discovery:

Before initiating the secure control channel connection with the discovered MRs, SDN controller being Blockchain Provider (BP), also ensure the freshness of Proof of Integrity of all the MRs using following mechanism:

To attest the MR, Blockchain Provider (BP) retrieves the Public Attestation Identity Key PK_AIK_MR and sends a "nonce" to the target MR.

1. The target MR answers with a quote that contains this "nonce" and its current Platform Configuration Registers (PCR) values that are stored inside the local TPM of the target MR.
2. This quote is signed by the Private Attestation Identity Key SK_AIK_MR of the target MR to ensure the integrity of the response.
3. After the receipt of the payload from the target MR, BP compare the "nonce" to check the freshness of attestation and if this matches the expected value, compare the received PCR values with a library of trusted MR configurations.

The techniques presented is explained in detail as below:

1. All the MRs in the SDWMN deployment are enabled with Hyperledger functionality.
2. MRs will have the Endorser and SDN Controller will have the Consenter functionalities of Hyperledger and manages the hyper ledger.
3. MRs in the Software Defined Wireless Mesh Network are authenticated using secure credentials.
4. Along with authentication, trustworthiness of the MR is established using attestation method as explained above in "Phase-1 of Discovery".
5. MRs validate each-other and are added as legitimate blockchain entities in the hyper ledger.
6. At the end of Phase-1 of Discovery, BP will have list of all the MRs registered with the hyper ledger.
7. Along with Attestation of MRs, freshness of Proof of Integrity is validated by the SDN Controller as explained above in "Phase-2 of Discovery".
8. BP also help with accounting; lawful intercept and they maintain immutable records.
9. Markle tree hash algorithms (double SHA-256) are used for generation of public keys for enhanced security and enterprise consensus algorithms such as Proof of elapsed time (PoET) or Practical Byzantine Fault Tolerance (PBFT) are used to synchronise database among all MRs in the SDWMN deployments.
10. Permission ledger is used to allow only authenticated and trusted MRs to participate and share the information.

Figure-1 depicts Mesh Router Discovery using Hyperledger in SDWMN deployments.

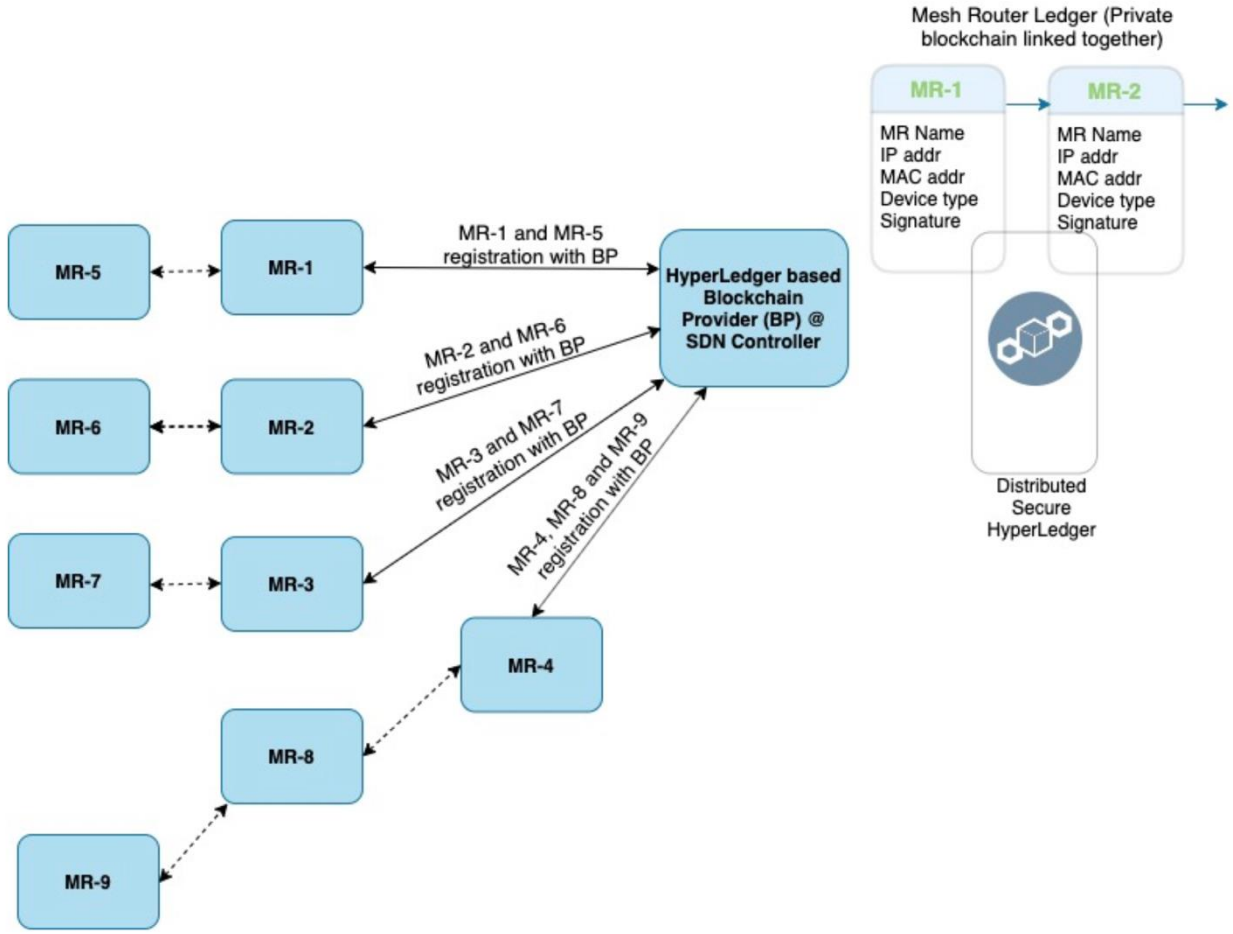

Figure-1

The techniques presented herein is very much required in public rural Software-Defined Wireless Mesh Network deployments. In general, the proposal is applicable for generic Wireless Mesh Network deployments where MR need to be discovered without having centralised entity. Using this method adding and removing of MR would be easy, secure, and automated, also provides faster convergence of MR discovery.