March 2022

METHOD TO SECURELY AUTO-RECOVER THE STRANDED MESH ROUTER IN SOFTWARE-DEFINED WIRELESS MESH NETWORK DEPLOYMENTS

NIRANJAN M M

METHOD TO SECURELY AUTO-RECOVER THE STRANDED MESH ROUTER IN SOFTWARE-DEFINED WIRELESS MESH NETWORK DEPLOYMENTS

AUTHOR:
NIRANJAN M M

ABSTRACT

Software-Defined Wireless Mesh Network (SDWMN) deployments are considered as a viable option to provide wireless coverage for a vast area. SDWMN is combination of Software-Defined Networking (SDN) and Wireless Mesh Network (WMN). Backbone of a WMN is made up of dedicated wireless nodes called Mesh Routers (MRs). These MRs can be freely organised into any network topology and communicate with each other using protocols such as DSR, OLSR etc., to find optimised path and hence to achieve higher performance. However, potential isolated (disconnected) MRs are the major obstacles to achieve high performance. Due to dynamic nature of network topology and link or node failures, some MRs (known as island/stranded/isolated MRs) may fail to find available paths to the SDN Controller. One of the pain points commonly heard is debugging and recovering such stranded MR in WMN deployments. The techniques presented herein propose method to detect stranded MR, connecting to it through alternate secure path, diagnose and auto-recover. The proposed method intelligently locates, securely connect, and recover stranded MRs automatically without manual intervention.

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 centralised 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). These MRs can be freely organised into any network topology and communicate with each other using protocols such as DSR (Dynamic Source Routing), Optimised Link State Routing (OLSR) etc., to find optimised path and hence to achieve higher performance.

However, potential isolated (disconnected) MRs are the major obstacles to achieve high performance. Due to dynamic nature of network topology and link or node failures, some MRs (known as island/stranded/isolated MRs) may fail to find available paths to the SDN Controller. Depending on specific topologies and failure probabilities, the proportion of stranded MRs may not be negligible.

One of the pain points commonly heard is debugging and recovering stranded MR in WMN deployments. As the connectivity is lost, IT engineers must physically reach the place of MR where it is deployed and connect to console, debug, and recover. This is often very time-consuming process and expensive method. With the advent of WiFi-6, new and dense deployments will grow prominently. This further increase challenges in debugging and recovering stranded MRs.

Wireless Network Data Analytics would help in identifying that there is some problem in the network based on the statistics and one of the reasons of the problem could be when MR get stranded, but it doesn't provide ways to recover from the problem.

Following are some of the scenarios where MR shall get stranded:

- No L3 (Layer-3/Network) reachability from SDN Controller, but network path exists.
- Loss of back-haul (Ethernet or Wireless) connectivity.
- MR with wrong configuration and/or with corrupted configuration.
- MR connectivity failure due to certificate issues (invalid, expiry etc.,)

Currently, there are very few ways to connect to the MR and debug the issues.

- Connecting to MR console physically.
- SSH/Telnet to MR through back-haul. We need to have IP address of the MR.
- Enabling debugs on the SDN Controller and/or MR.

Above debugging capabilities are not feasible when MR is already stranded. Also, some of the scenarios requires manual intervention to recover even if there is a connectivity to the MR.

The techniques presented herein propose method to detect stranded MR, connecting to it through alternate secure path, diagnose and auto-recover. The proposed method intelligently locates, securely connect, and recover stranded MRs automatically without manual intervention. With this method to locate and auto-recovery, we are providing self-healing wireless network which is obvious requirement for 11ax as number of wireless devices increased exponentially as well as throughputs are multi-folded. This method also includes auto-configuration of new out-of-the box MR by placing into the existing deployment, which could help in network automation. Whenever new MR deployed into the existing Wireless Mesh Network, neighbouring MRs would detect this new MR and report to the SDN Controller, which later would use the similar method as that of auto-recovery of stranded MR. The techniques presented herein providers auto-recovery of the stranded MR starting with detection of stranded MR, reporting stranded MR to the SDN controller, providing connectivity to the stranded MR and recover back the stranded MR to the SDN wireless mesh network.
Every step of auto-recovery could lead to security vulnerabilities i.e.,

- Detection of stranded MR: This may be vulnerable if malicious device can act as stranded MR and try to advertise "Recovery SSID" and can cause DoS attack.
- Reporting stranded MR to the SDN Controller: This may be vulnerable if neighbour MRs report the malicious device which acts as stranded MR, to the SDN Controller and can cause performance degradation.
- Providing connectivity to the stranded MR: Here, both stranded MR and neighbour MR should establish trust before establishing connectivity.
- Recover back the stranded MR: Here, stranded MR should validate the trustworthiness of the SDN Controller before applying config and/or image sent by the SDN Controller.

For providing trustworthiness among SDN Wireless Mesh Network elements which includes stranded MR, SDN Controller and Neighbour MRs, attestation method is used to validate the Proof of Integrity of the device. Any Mesh Router accepting a new connection from an unknown Mesh Router can be a security vulnerability. Generally, an authentication mechanism is recommended, but it is not sufficient, hence we need trustworthiness in place which is achieved through attestation method.
The proposal adds attestation information to the messages between stranded MR, neighbour MRs and SDN Controller as an extension that embeds:
- Hardware Fingerprint - Derived from SUDI or similar.
- Software - OS, BIOS, kernel, Version, application binaries/libraries etc.,
- Platform Information - PCR (Platform Config Registers), time-ticks, signature.

Stranded MR, Neighbour MRs and SDN Controller will use this information against the device fingerprint and Known Good Values (KGV), to verify whether the peer is trustworthy or not.

Depending on the outcome of the verification, the stranded MR, neighbour MR and SDN Controller can decide, whether connectivity to the remote device should be considered or not. Hence, all the steps of auto-recovery are incorporated with trustworthiness among SDWMN elements using above attestation method.

- Messages from stranded MR to the neighbour MRs are accompanied with attestation information which includes hardware fingerprint, software information, counters/time-ticks etc., which would be validated by the neighbour MR before acting upon it.
- Messages from the neighbour MR to the stranded MR are also accompanied with attestation information, so that stranded MR is sure that he is being auto recovered by the trusted neighbour MR.
- Messages from the SDN Controller to the stranded MR also carry attestation information, so that stranded MR is auto recovered with trusted SDN Controller.

There are mainly three phases in auto-recovery of stranded MR, which includes, Detect, Connect and Recover as described below:

- Detect:
    - MR upon getting stranded, will start beaconing pre-defined "Recovery SSID" (with capability as 0x01) with vendor specific "Correct Me" IE containing reason code. Beaconing would be on all available channels/bands to notify neighbour MRs.
    - Stranded MR sends the attestation information as mentioned above along with the vendor specific "Correct Me" IE in beacon packets.
    - Neighbour MRs on receiving these beacons, verifies the trustworthiness of the stranded MR using attestation information and updates SDN Controller with the details (including error reason code) of stranded MR in the network along with their own parameter’s aka "RSSI", "Platform Type" and "Current Load". SDN Controller would update the stranded MR information in the cache.
    - SDN Controller selects a best neighbour, based on the algorithm considering parameters/factors "RSSI", "Platform Type" and "Current Load" to assist the stranded MR.
- Connect:
    - SDN Controller instructs the elected best neighbouring MR, to beacon security enabled hidden "Recovery SSID" (with capability as 0x02).
    - On receiving these beacons from neighbouring MR, the stranded MR triggers client state machine and stops its beaconing with "Correct Me" IE. At this stage "Stranded MR" will act as wireless client and associate to "Recovery SSID" of neighbour MR.
    - Neighbour MR would verify the trustworthiness of the stranded MR using attestation information before allowing connection from it.
    - The "Recovery SSID" shall support various security mechanisms in the order of EAP-TLS (certificates are flashed to the MR during Manufacturing), PSK, MAC filtering.
    - Either local DHCP server on MR or SDN Controller will assist stranded MR to get the IP address and it will further move to RUN state.
    - Once the stranded MR connects, secure end-to-end connection is established.
- Recover:
    - Just to recap, when MR is stranded, it run the self-diagnostics to identify the possible issue and update the error reason code. Stranded MR will include this error reason code along with attestation information in the "Recovery SSID" beacons part of vendor specific "Correct Me" IE. Neighbouring MRs uses attestation information to validate trustworthiness of the stranded MR and if

verification is successful, it updates SDN Controller with stranded MR information including error reason code. Based on the error reason code, SDN Controller will attempt to recover the stranded MR via already elected best neighbour MR.

- For config related errors: SDN Controller shall send relevant configs.
- For image related errors: SDN Controller shall send the suitable image.
- SDN Controller shall push appropriate configs/image along with attestation information to the stranded MR via elected best neighbour MR.
- Stranded MR validate the trustworthiness of the SDN Controller before updating the received config/image. It saves and restarts itself to attempt network re-join.
- If all the above attempts to recovery of stranded MR fails, elected neighbour MR shall update SDN Controller for taking appropriate action.
- Stranded MR allows SSH connection as an alternate mechanism for remote access and further debugging.

Figure-1 depicts the over-all flow of auto-recovering the stranded Mesh Router in SDWMN deployments. The steps from (1) to (8) are mentioned along with the description in-line with the flow diagram.

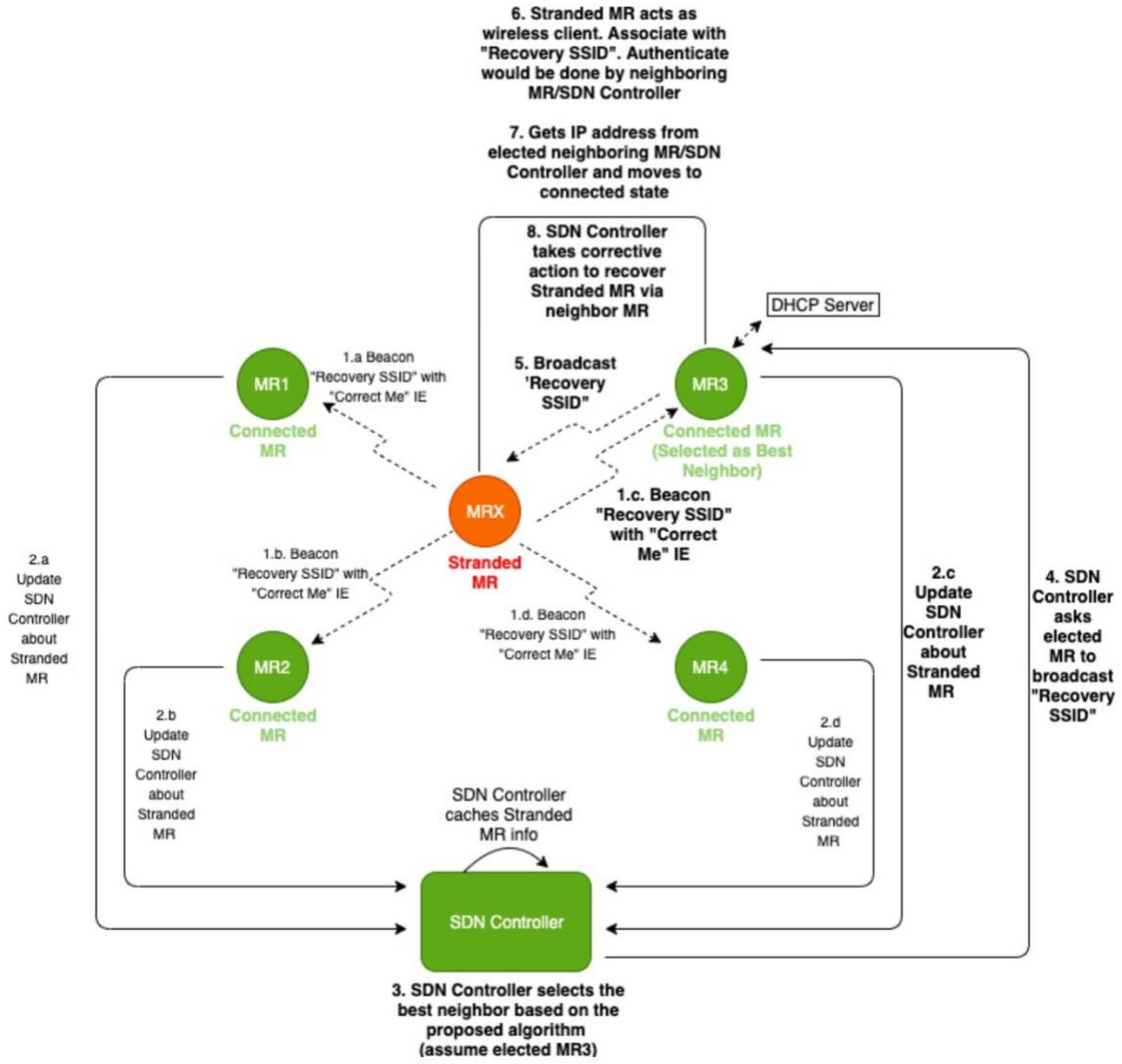

Figure-1

Figure-2 shows the sequence of steps involved in auto-recovery of stranded Mesh Router in SDWMN deployments.

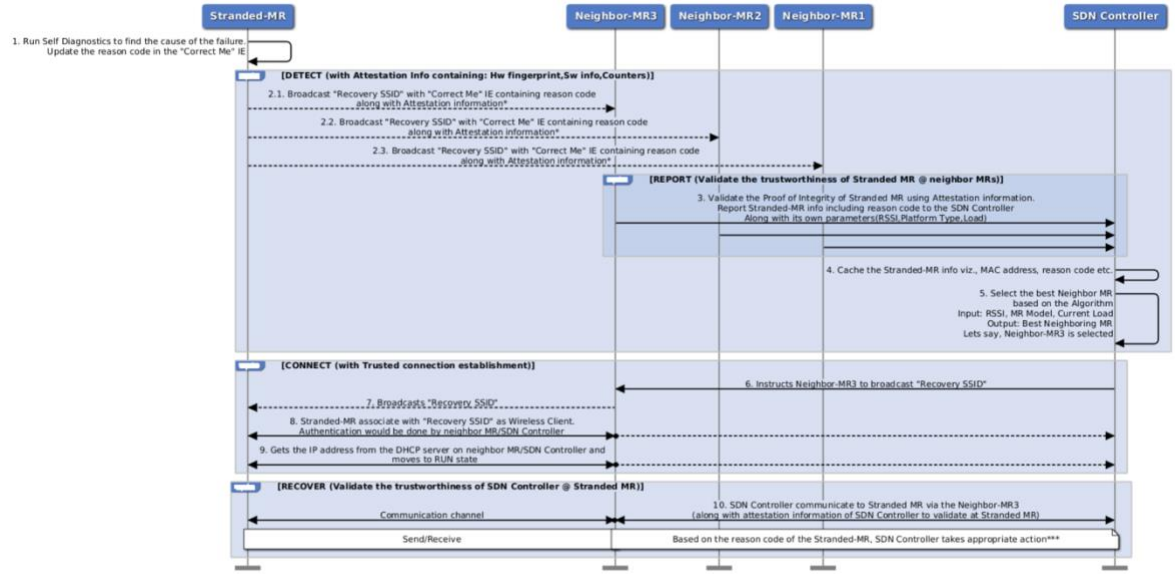

Figure-2

The techniques presented herein provides method to intelligently detect and recover a stranded MR. Moreover, this method establishes trust between stranded MR, neighbouring MR and SDN Controller before any of the auto-recovery phases. Additionally, to avoid malicious/rogue clients acting as stranded MR and connecting to the neighbour MR selected by the SDN Controller, only stranded MRs known by SDN Controller (i.e., previous connection history, MR mac-address filter table etc.,) would only be allowed to associate as wireless client to the neighbour MR.