March 2022

EFFICIENT DISTRIBUTION OF ROGUE INFORMATION IN SOFTWARE DEFINED WIRELESS NETWORKS

Niranjan M M

EFFICIENT DISTRIBUTION OF ROGUE INFORMATION IN SOFTWARE DEFINED WIRELESS NETWORKS

AUTHOR:
Niranjan M M

ABSTRACT

Rogue Access Points (RAPs) are unauthorized devices connected to a network, providing unauthorized wireless access to one or more clients. Rogue Access Points (RAPs) produce security vulnerabilities in networks by circumventing inherent security mechanisms. Detection of Rogue APs is a challenge for network administrator. There are techniques for detecting Rogue APs from the network with the help of neighbouring legitimate APs and facilitated by SDN Controller. Once Rogue APs are detected, the rogue information needs to be propagated across the APs and Controllers in the deployment, to take actions such as containment of Rogue APs and connected Rogue Clients, blocking legitimate clients from connecting to SSID broadcasted by those Rogue APs, to verify if client is roaming from legitimate APs etc., There are existing techniques to distribute rogue database across APs and SDN Controllers periodically or on detection, but none of the existing methods consider optimal and efficient way of sharing rogue information. The technique presented herein propose method to have distributed way of sharing rogue information considering network efficiency and performance.

DETAILED DESCRIPTION

Rogue Access Points (RAPs) are unauthorized devices connected to a network, providing unauthorized wireless access to one or more clients. Such devices pose significant security risk to organizations, since they provide a convenient means for hackers and insiders to hide malicious or unsanctioned activities in industry, government, and enterprise network deployments. Same is applicable to Software-Defined Wireless Network (SDWN) deployments, where-in these Rogue APs (aka unauthorized/malicious APs) may induce security vulnerabilities (expose the network to unwanted access) and may degrade the network performance.

Detection of Rogue AP is a challenge for network administrator. Undetected Rogue APs are serious threats which may steal sensitive information from the network. There are techniques for detecting Rogue APs from the network with the help of neighbouring legitimate APs and facilitated by SDN Controller. Once Rogue AP is detected, SDN Controller keeps the rogue information in the rogue database. This database is used to take actions such as containment of Rogue APs and connected Rogue Clients, blocking legitimate clients from connecting to SSID broadcasted by those Rogue APs, to verify if client is roaming from legitimate APs etc., Hence rogue database need to be replicated/synced across APs and even across Controllers in Cluster deployments to avoid computational effort in re-detection of Rogue APs and Rogue Clients which are already detected by legitimate APs. Propagating the rogue database to all the legitimate APs is required for multiple reasons:

- To detect and mitigate Rogue Clients (i.e., clients who are connected to Rogue APs). Mitigation is also called as containment.
- To block client roams if they are re-associating from the Rogue APs.
- Due to dynamic nature of Wireless networks, all the APs in the deployment may need to detect Rogues (APs and Clients) periodically. If rogue is already identified by legitimate AP or SDN Controller, then the rogue information should be propagated as early as possible to avoid re-computation of rogue AP detection at each legitimate AP of a particular deployment.
- Detecting Rogue APs may take a while, in-between legitimate clients may get associated to the Rogue APs (with broadcasting same SSID as that of legitimate AP or using different authentications scheme as that of legitimate SSID etc.,). Hence if any of the legitimate AP already detected the Rogue AP, may need to propagate this rogue information as early as possible to avoid such scenarios.

Currently there are methods to sync/replicate/distribute rogue database across APs and SDN Controllers periodically or on detection, but it would not be optimal to do as the number of APs in the deployment could range from hundreds to thousands in numbers. The replication (distribution) of the whole rogue database is not an amicable solution especially for wireless mesh network deployments when the scale of APs is ranging from hundreds to thousands and more. The replication complexity and subsequent update (add/deletion of an entry) would obviously consume

more resource and time. Along with replication complexity, the propagation of rogue AP information from the AP who detected it as Rogue and to the SDN Controller and later to all other APs would require more time and may cause security breach (i.e., legitimate clients may join to impersonated SSID of Rogue/Malicious AP etc.,) by the time other APs come to know about the presence of Rogue APs. Did not encounter any method which would do distributed way of sharing rogue information in the network.

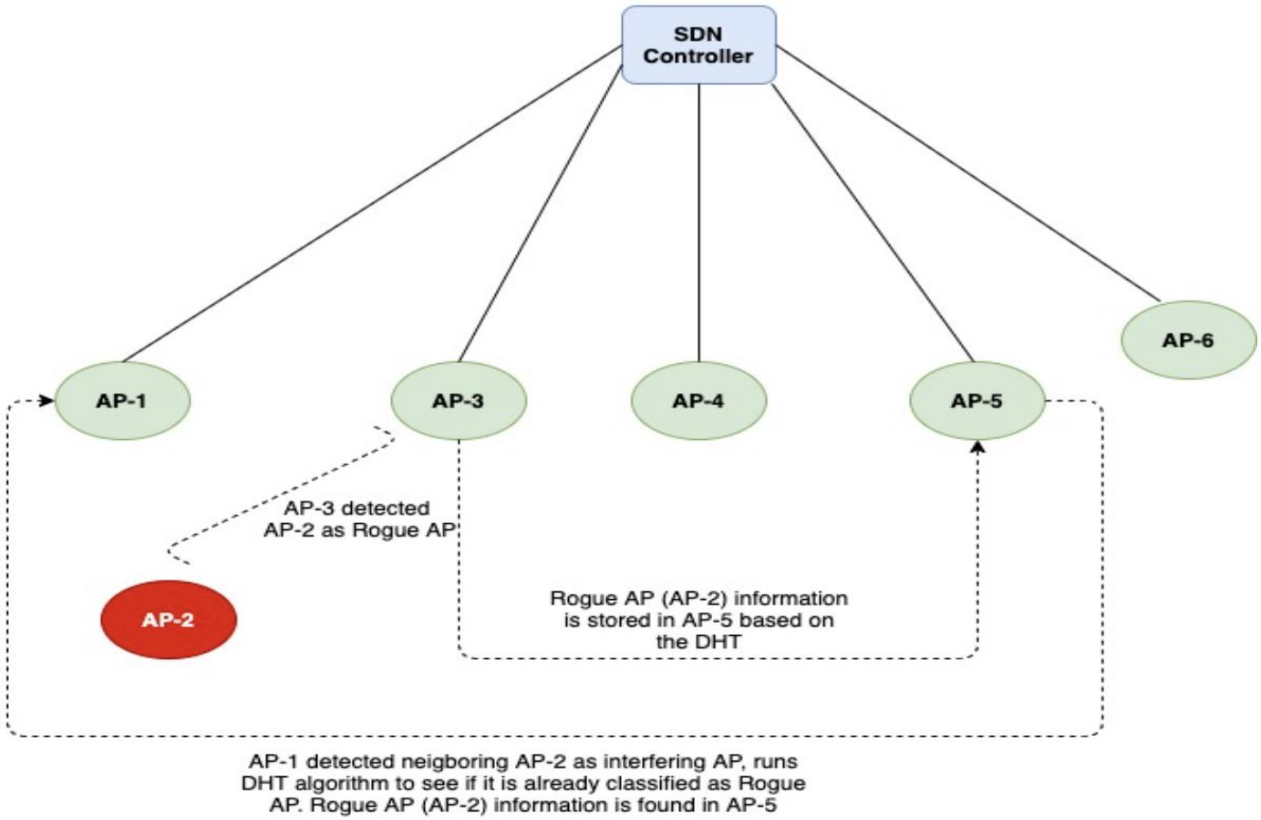
The technique presented herein propose method to have distributed way of sharing rogue information considering network efficiency and performance. Once Rogue AP is detected, store the entry for that Rogue AP in one of the legitimate APs by using DHT technique i.e., with the concept of consistent hashing with "Key" as "MAC address of Rogue AP" passed through a hashing algorithm that serves as a randomisation function. This ensures that each legitimate AP in the network has an equal chance of being chosen to store the <Key, Value> pair. Further if any of the neighbouring AP found to be interfering or having interfering SSIDs etc., then legitimate AP investigate this distributed database using "key" as "MAC address of the neighbouring AP" to see if that AP is already detected as Rogue by any other legitimate AP in the deployment. If it already detected as Rogue, then no need to run complex algorithms to detect the same. The idea here is, whenever Rogue AP is detected by a legitimate AP, identify the right legitimate AP to store the entry for detected Rogue using DTH (which uses consistent hashing) based on MAC address of Rogue AP as "Key" to store <Key, Value> pair. Here "Value" would be the details about the rogue AP viz., classification type, type of threat, detected on the LAN, type of containment etc., Same method is used later by other legitimate APs before running complex algorithm to detect any of the neighbour AP as Rogue. This method is applicable for storing Rogue Clients with "Key" as "MAC address of Rogue Client". Considering the cluster deployment, the DHT runs over all the APs connected under the Master Controller, so that the database is distributed equally across all legitimate APs in the deployment.

The techniques presented herein is explained in detail as below:

1. All the APs and centralised SDN controller would be having DHT functionality.
2. Legitimate APs co-ordinate with the centralised controller to detect Rogue APs in the deployment.
3. Once rogue AP is detected, store the Rogue AP information in one or more legitimate APs using DHT with "Key" as "MAC address of Rogue AP".

4. DHT would help in having distributed rogue database across all legitimate APs and SDN Controllers in the deployment.
5. At a later point of time, when legitimate AP found any of its neighbouring AP interfering or having interfering SSIDs etc., then legitimate AP investigate the distributed rogue database with "Key" as "MAC address of the neighbouring AP".
6. If neighbouring AP found in the distributed rogue database, then it considered as Rogue AP and would skip running detection algorithms further and avoid re-computational effort.

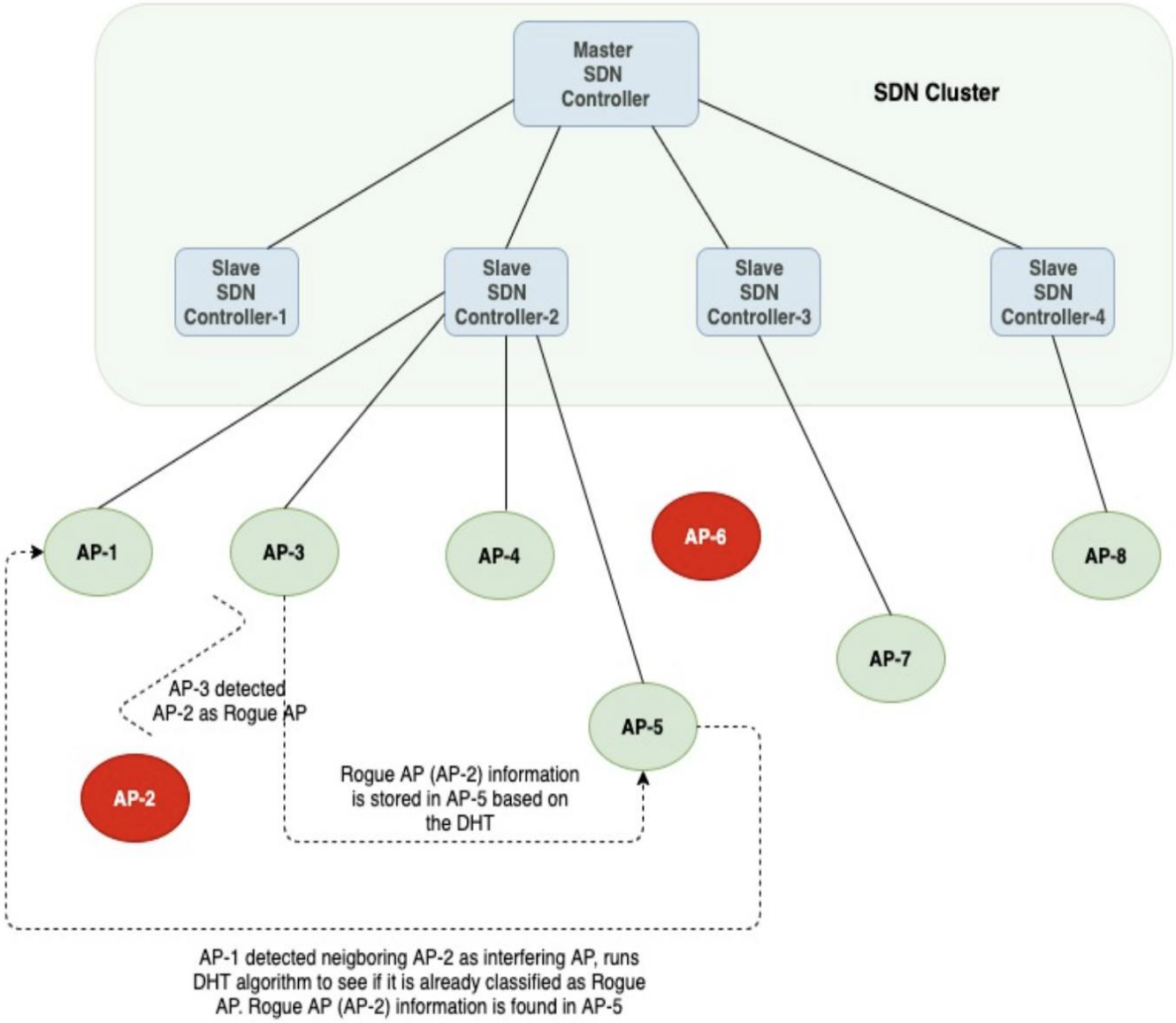
The Figure-1 depicts the Software Defined Wireless Network deployment with centralised SDN Controller with legitimate Access Points. Legitimate Access Points detect Rogue using existing methods and distribute the rogue information using DHT.



Here,
1. AP-1, AP-3, AP-4, AP-5 and AP-6 are Legitimate APs
2. AP-2 is the Rogue APs (marked as Red)
3. AP-3 detects AP-2 as Rogue AP
4. Stores Rogue AP (AP-2) information in AP-5 using DHT
5. AP-1 detects interfering AP (AP-2) and uses DHT to fetch AP-2 information and found as Rogue

Figure-1

The Figure-2 depicts the Software Defined Wireless Network in Cluster deployment.



Here,
1. AP-1, AP-3, AP-4, AP-5, AP-7 and AP-8 are Legitimate APs
2. AP-2 and AP-6 are Rogue APs (marked as Red)
3. AP-3 detects AP-2 as Rogue AP
4. Stores Rogue AP (AP-2) information in AP-5 using DHT
5. AP-1 detects interfering AP (AP-2) and uses DHT to fetch AP-2 information and found as Rogue

Figure-2

The technique presented herein propose method such that, once Rogue AP is detected by any of the legitimate AP in the deployment, then same information is available/known by the other legitimate APs immediately. This method avoids running complex rogue detection algorithms whenever already detected Rogue AP trying to interfere with any of the legitimate APs. Moreover, this method avoids replicating rogue AP database across all legitimate APs and Controllers (Note here that, more than one controller is required in case of clustering deployments). Also, there is no multicast messaging to fetch the rogue AP database. Additionally, this method is highly scalable as number of Rogue APs detected does not increase the over-all memory requirement. The method can be used for any wireless network deployments and can be used wherever there is requirement of immediate replication of information across the devices in the larger deployments.