November 27, 2018

PROVIDING REFERENCE CLIENT PERSPECTIVE FOR ENHANCED RADIO FREQUENCY AND ASSURANCE FUNCTION

Indermeet Gandhi

Min Se Kim

Taranpreet Kohli

Gal Katz

PROVIDING REFERENCE CLIENT PERSPECTIVE FOR ENHANCED RADIO FREQUENCY AND ASSURANCE FUNCTION

AUTHORS:
Indermeet Gandhi
Min Se Kim
Taranpreet Kohli
Gal Katz

ABSTRACT

Techniques are described through which a sensor can provide a client Radio Frequency (RF) perspective to a wireless infrastructure. This enables establishing ultimate close-loop telemetry data for root cause analysis on Wi-Fi® problems through an assurance engine. Exchange methods and enhanced measurement reports provide a client perspective of the ever-changing RF conditions autonomously or on-demand basis to the wireless infrastructure.

DETAILED DESCRIPTION

Years ago, wireless networks were limited to conference rooms and public areas for convenience. Today, Wireless Local Area Networks (WLANs) are not only the standard part of enterprise networks for the entire facility, but they are even more critical as many companies are also migrating from Ethernet to a complete wireless-only infrastructure.

As these wireless networks grow especially in remote facilities where Information Technology (IT) professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues, ideally before the users notice connectivity degradation.

Wireless assurance typically relies on collecting information about a network and then using this information to interpret the performance of the wireless clients on the Wireless LAN (WLAN). Until now, collecting information was possible from the WLAN infrastructure perspective, which is a limited view of the actual WLAN performance because they do not have the client's view. Assurance tools that rely on infrastructure components have only a partial, and skewed/asymmetric view of the actual WLAN performance.

Until now, certain wireless sensors have been utilized to only run synthetic tests (e.g., onboarding, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), etc.) and report back the synthetic results to an assurance engine.

Techniques described herein enhance wireless sensor reports of the client Radio Frequency (RF) views to the wireless infrastructure and assurance engine. This enhances the Radio Resource Management (RRM) function in the wireless infrastructure (which has until now mostly relied on Access Point (AP) – to – AP Neighbor Discovery Protocol (NDP) message exchanges and often misses the client RF perspective which is asymmetric in nature) and improves the analytics on the assurance engine.

Several mechanisms and embodiments are provided through which a sensor may exchange a client RF perspective to the wireless infrastructure.

1. In one scenario, the 802.11k beacon report is sent to the wireless infrastructure (unsolicited) after performing an association process.

2. In another embodiment, the sensor sends an unsolicited 802.11k beacon report to the wireless infrastructure at regular intervals without requests from the AP. This may be based on timer configuration or when there is a change in RF degradation such as increased transmission packet retries or packet loss (the AP does not have this complete view), rapid data rate changes, or changes in Received Signal Strength Indication (RSSI) / signal strength.

As per Institute of Electrical and Electronics Engineers (IEEE) standards, a 802.11k beacon report is sent in response to a 802.11k beacon request. In the real world, not all clients implement 802.11k behavior. In this step, the sensor as a client autonomously sends the beacon/RF scan report whenever there is a change in RF degradation. Thus, the 802.11k frame is used to provide the client RF perspective autonomously to the wireless infrastructure.

3. In another embodiment, the sensor sends an (user defined) enhanced beacon report as a transparent container over the wired link (almost all sensor customer deployments use a wired backhaul to report test results bypassing wireless infrastructure) directly to the assurance engine. This may be solicited by an assurance engine (wired link) or wireless infrastructure at regular intervals, or unsolicited. The assurance engine uses the

enhanced beacon report to provide a view of client's scan report to the network administrator. The assurance engine exchanges the enhanced beacon (RF scan) report with an RRM function of the wireless infrastructure (cloud or on-premise). Thus, in this embodiment, enhanced beacon/scan reports are provided to the RRM function without the use of the wireless RF. In one variant, the enhanced beacon report reports Basic Service Set (BSS) color of the neighbor APs to the WLAN infrastructure through a vendor specific Information Element (IE). Knowing the Down Link (DL) RSSI level as seen from the sensor helps the AP to understand the asymmetric nature of the link and predict the DL RSSI observed at the other clients (not supporting beacon reports) in proximity to the sensor and feedback to the RRM.

Thus, the 802.11k beacon report is enhanced to include the BSS color of the neighboring APs. Additional information (as generated in embodiments 6 and 10 below) may be carried as RF scan reports to the wireless infrastructure. This information is additional to 802.11 standards and hence the alternative channel is optionally mentioned as wired or any other medium.

4. In another embodiment, on-demand proprietary RF scan report is carried as data packets over the wireless infrastructure. The assurance engine then exchanges the proprietary RF scan report with the RRM function of the wireless infrastructure (cloud or on-premise). This does not require any enhancements to 802.11 protocols.

5. In one embodiment, the AP advertises its support for the enhanced beacon/scan reports through vendor specific IE in the beacon or probe response. In this particular alternative, dedicated sensors respond with an on-demand, unsolicited beacon/RF scan report through any suitable means (e.g., those described in connection with embodiments 2-4) if the vendor specific IE is present in the beacon or probe response.

The standards need not be substituted. Rather, an additional bit/subfield/IE may be provide so that the sensor can differentiate wireless infrastructures on a vendor basis and communicate the enhanced RF scan reports only with a specific vendor wireless infrastructure.

6. In this embodiment, the dedicated sensor sends transmission packet retries and packet loss statistics through vendor specific IEs in a station (STA) statistics report or

alternatively in action frames to a wireless infrastructure or as a transparent container to a digital network architecture.

7. In this scenario, the AP compares the channel utilization which it broadcast (BSS load) with the channel load/utilization as seen by the sensor (client view - not ceiling) and returned to the AP on demand (channel load report). This in turn helps to make better judgement of channel utilization.

8. In this embodiment, a dedicated sensor is configured to run an Internet Protocol (IP) Service Level Agreement (SLA) test against the AP acting as the IP SLA responder and provide over-the-air jitter, latency, and packet loss results to the digital network architecture / RRM function. For example, IP SLA testing may be automatically triggered upon excessive packet loss from a neighboring client and validate the source of excess packet loss (network or server). IP SLA testing may be used to validate and optimize RRM configuration. If the sensor is experiencing high jitter/delay or packet loss from the client perspective. RRM may leverage IP SLA test results to augment a Transmit Power Control (TPC) / Dynamic Channel Assignment (DCA) decision.

9. In this scenario, a Citizens Broadband Radio Service (CBRS) / 5G capable sensor may send the detailed beacon/scan report inside a transparent container over Resource Reservation Control (RRC) signaling to the infrastructure. The RRM function co-located with the converged CBRS/Wi-Fi® AP uses it to improve Coverage Hole Detection (CHD) and align AP channel and color. An alternate channel provides RF scan report to the wireless infrastructure given the APs are getting ready to provide CBRS capability.

10. In further enhancements, the sensor is configured to perform the following techniques:

10a. The sensor is used to derive airtime utilization using edge analytics. Currently, an AP-based view provides per-radio level utilization but does not provide visibility into Service Set Identifier (SSID) level. A sensor with promiscuous mode radio will capture raw Wi-Fi packets and provide air time consumption for each Basic SSID (BSSID) and ESSID through sensor-based, Packet Capture (PCAP) analytics. PCAP may be automatically (or manually) triggered by the digital network architecture for issues or on-demand and assess and analyze RF anomaly behaviors and generate RF issue with PCAP at the edge. PCAP is heavily weighted and expensive data from a telemetry and WAN perspective so leveraging edge analytics from the sensor is most optimal approach.

This allows actual consumption and provides an estimated view on over-the-air capacity. These analytics also include the impact of management/control frame from enterprise SSIDs as well as the neighboring AP. The sensor analyzes the actual duration of each frame and calculates air time per BSSID.

10b. Sensor reported packet loss per Modulation and Coding Scheme (MCS) is used for network capacity assessment. The sensor runs a series of multiple pilot data frames per each MCS and reports the number of packet loss and average latency per MCS. This may identify the optimal data rate per sensor location that can be used to identify network capacity.

10c. Location calibration probing may be performed using burst, periodic probe requests. A digital network architecture may be used to program sensor location calibration mode. Once the sensor gets configured for location calibration mode, the sensor sends a series of broadcast probe requests to all channels which may be used as RF location calibration probes. This uses automated, system triggered calibration. Moreover, the sensor is orchestrated to send multiple, burst probe packets. Hence, accurate data may be obtained for calibration purposes.

10d. A dynamic AP heatmap may be generated through the sensor's neighbor AP RSSI / Signal to Noise Ratio (SNR). In this embodiment, the sensor embeds AP RSSI and SNR in a sensor heartbeat message to the digital network architecture center, which is sent at regular intervals. Sensor location is leveraged to visualize an AP heatmap with actual RF propagation using reported AP RSSI/SNR/Datarate.

A packet retry distribution is obtained across all MCSs in a coordinated fashion. As the exact location of the sensor and type of radio is known, optimal data rate per location may be identified using a sensor, which is the reference client. Using synthetic traffic, a statistical distribution of packet loss per MCS may be obtained over specific coordination of location. Hence, the optimal data rate per area and feedback to RRM may be evaluated.

Thus, a series of techniques, some leveraging the 802.11k standards, is provided in an enhanced way. Methods are introduced to generate the RF scan reports at the sensor and triggers to transport them to the wireless infrastructure.

In summary, techniques are described through which a sensor can provide a client RF perspective to a wireless infrastructure. This enables establishing ultimate close-loop telemetry data for root cause analysis on Wi-Fi problems through an assurance engine. Exchange methods and enhanced measurement reports provide a client perspective of the ever-changing RF conditions autonomously or on-demand basis to the wireless infrastructure.