Packet Loss in wireless networks:

This can be due to multitude of reasons. However, the first immediate checkpoint should be SNR, RSSI and operating frequency/co-channel interference. A wifi-analyzer can almost take you near to the solution.

Wireless router location - Check whether the wireless router is centrally located within areas requiring coverage. Ensure to avoid coverage holes with proper overlapping of coverage areas. Ensure to avoid buildings in-between to reduce interference. Also, note that there is a relation between the distance and data rate for a user. The the nearer the user, the higher the data rate because of reduced path loss (because this in-turn increases the SNR).

Type of Antenna - An isotropic antenna provides coverage area in the form a sphere. Dipole antenna provides coverage area in the form of doughnut. There are also various directional antennas. Beware that the omni-directional antenna can lead to hidden node problem in case of large cell size. Antenna with focused beam can be helpful. Multi-sector directional antenna can give high capacity, range. The type of antenna, its location and antenna gain determines the radio transmission range and the coverage area.

Communication channel / Operating frequency - Presence of other AP's operating in the same frequency in the same radio coverage area can cause interference. In such cases, the operating channel and channel separation should be changed accordingly to reduce interference if there are only 802.11 devices nearby.

Power level - The higher power level can increase the range but if there are nearby AP's, it can lead to interference. For higher capacity, AP's might be close together, in such cases low power level is preferred to reduce interference.

Other devices - Interference can also be introduced by non-802.11 devices like microwave ovens, bluetooth, cordless phones etc.. In such cases, it is better to remove those devices or shield it to avoid interference.

Packet loss in terms of burst also seems to suggest that the stack is not able to handle bursty traffic and its traffic shaping policy may be to simply drop such bursty packets. Double check if such traffic burst is generated.

NACK not reaching the server : Again, this can be due to the transmission media related issues that can cause the NACK to be dropped over the air. In case if the NACK has reached the host but not the server application/un-handled, then it can be due to the architecture of the server or stack related OS configuration.

Typical steps for analysing packet loss scenarios

- Check the firewall settings, OS configurations, router configurations and network hardware capabilities/ configs (throughput capability, operation mode), intermediate node config/ capabilities(MTU, routing/forwarding table)
- On the wireless path, check location of AP, operating range(frequency), channel separation, SNR ,RSSI, antenna type/gain, coverage holes, distance from AP, presence of other 802.11 devices & non-802.11 devices in coverage area.
- Check packet statistics on all input & output points of the various nodes & interfaces
- Check packet statistics on all input & output points in applications/protocol layers
- Repeated tests to identify the pattern of the packet loss with various combinations of throughput, packet size, duration of run, different applications, different payload sizes, different number of pkts, power level, AP location, channel... is also a way to determine the area of problem.

Source: Karthik Balaguru - StackOverflow