Ground Truth MQTT

1. Formal verification of the implementation of the MQTT protocol in IoT devices (2017)

Sr.#	Properties
1	Where a flag bit is marked as “Reserved” it is reserved for future use and MUST be set to the value listed.
2	After a Network Connection is established by a Client to a Server, the first packet sent from the Client to the Server MUST be a CONNECT packet.
3	The Server MUST process a second CONNECT packet sent from a Client as a Protocol Error and close the Network Connection.
4	The protocol name MUST be the UTF-8 String "MQTT". If the Server does not want to accept the CONNECT, and wishes to reveal that it is an MQTT Server it MAY send a CONNACK packet with Reason Code of 0x84 (Unsupported Protocol Version), and then it MUST close the Network Connection.
5	If the Keep Alive value is non-zero and the Server does not receive an MQTT Control Packet from the Client within one and a half times the Keep Alive time period, it MUST close the Network Connection to the Client as if the network had failed.
6	A PUBLISH Packet MUST NOT have both QoS bits set to 1 [MQTT-3.3.1-4]. If a Server or Client receives a PUBLISH packet which has both QoS bits set to 1 it is a Malformed Packet. Use DISCONNECT with Reason Code 0x81 (Malformed Packet).
7	Bits 3,2,1 and 0 of the Fixed Header in the PUBREL packet are reserved and MUST be set to 0,0,1 and 0 respectively. The Server MUST treat any other value as malformed and close the Network Connection.
8	Bits 3,2,1 and 0 of the Fixed Header of the SUBSCRIBE packet are reserved and MUST be set to 0,0,1 and 0 respectively. The Server MUST treat any other value as malformed and close the Network Connection.
9	The Server MUST treat a SUBSCRIBE packet as malformed if any of Reserved bits in the Payload are non-zero.
10	The Server MUST send a PINGRESP packet in response to a PINGREQ packet.

2. MPInspector: A Systematic and Automatic Approach for Evaluating the Security of IoT Messaging Protocols (2021)

Sr.#	Properties
1	The ClientID MUST be used by Clients and by Servers to identify state that they hold relating to this MQTT Session between the Client and the Server.
2	The ClientID MUST be present and is the first field in the CONNECT packet Payload.
3	The ClientID MUST be a UTF-8 Encoded String.
4	The Server MUST allow ClientID’s which are between 1 and 23 UTF-8 encoded bytes in length, and that 910 contain only the characters.
5	A Server MAY allow a Client to supply a ClientID that has a length of zero bytes, however if it does so the Server MUST treat this as a special case and assign a unique ClientID to that Client.

6	It MUST then process the CONNECT packet as if the Client had provided that unique ClientID, and MUST return the Assigned Client Identifier in the CONNACK packet.
7	If the Server rejects the ClientID it MAY respond to the CONNECT packet with a CONNACK using Reason Code 0x85 (Client Identifier not valid) as described in section 4.13 Handling errors, and then it MUST close the Network Connection.
8	If the User Name Flag is set to 1, the User Name is the next field in the Payload. The User Name MUST be a UTF-8 Encoded String.
9	The receiver of a PUBLISH Packet MUST respond with the packet as determined by the QoS in the PUBLISH Packet.
10	In this case the Server 1730 MUST deliver the message to the Client respecting the maximum QoS of all the matching subscriptions.
11	If the Client specified a Subscription Identifier for any of the overlapping subscriptions the Server MUST send those Subscription Identifiers in the message which is published as the result of the subscriptions.
12	If the Server sends a single copy of the message it MUST include in the PUBLISH packet the Subscription Identifiers for all matching subscriptions which have a Subscription Identifiers, their order is not significant.
13	If the Server sends multiple PUBLISH packets it MUST send, in each of them, the Subscription Identifier of the matching subscription if it has a Subscription Identifier.
14	A PUBLISH packet sent from a Client to a Server MUST NOT contain a Subscription Identifier.
15	The Client MUST NOT send more than Receive Maximum QoS 1 and QoS 2 PUBLISH packets for which it has not received PUBACK, PUBCOMP, or PUBREC with a Reason Code of 128 or greater from the Server.
16	The Client MUST NOT delay the sending of any packets other than PUBLISH packets due to having sent Receive Maximum PUBLISH packets without receiving acknowledgements for them.
17	The Server MUST NOT send more than Receive Maximum QoS 1 and QoS 2 PUBLISH packets for which it has not received PUBACK, PUBCOMP, or PUBREC with a Reason Code of 128 or greater from the Client.
18	The Server MUST NOT delay the sending of any packets other than PUBLISH packets due to having sent Receive Maximum PUBLISH packets without receiving acknowledgements for them.
19	The Server MUST NOT send this property if it would increase the size of the CONNACK packet beyond the Maximum Packet Size specified by the Client.
20	The Server MUST send all User Properties unaltered in a PUBLISH packet when forwarding the Application Message to a Client. The Server MUST maintain the order of User Properties when forwarding the Application Message.
21	The sender MUST NOT send this property if it would increase the size of the PUBACK packet beyond the Maximum Packet Size specified by the receiver.
22	The sender MUST NOT send this property if it would increase the size of the PUBREL packet beyond the Maximum Packet Size specified by the receiver.

23	The sender MUST NOT send this property if it would increase the size of the PUBCOMP packet beyond the Maximum Packet Size specified by the receiver.
24	The Topic Filters MUST be a UTF-8 Encoded String. Each Payload MUST contain at least one Topic Filter and Subscription Options pair.
25	The sender MUST NOT send this property if it would increase the size of the DISCONNECT packet beyond the Maximum Packet Size specified by the receiver.
26	The sender MUST NOT send this property if it would increase the size of the AUTH packet beyond the Maximum Packet Size specified by the receiver.
27	The Response Topic MUST be a UTF-8 Encoded String.
28	The Response Topic MUST NOT contain wildcard characters.
29	The Server MUST send the Response Topic unaltered to all subscribers receiving the Application Message.
30	The Server MUST send the Correlation Data unaltered to all subscribers receiving the Application Message.