

ABSTRACT

BLUETOOTH LOW ENERGY (BLE) ADVERTISING PACKET SECURITY

Secure pairing of computing devices, such as a field tool and a battery-powered device (BPD), may include generating by the BPD a challenge message including a randomly-generated challenge, and receiving at the field tool a challenge message from the BPD via a Bluetooth low-energy (BLE) advertisement message. The challenge message can include a randomly-generated challenge and can be issued in a scannable undirected advertising message. The challenge key can be calculated via a secure hash algorithm (SHA) to obtain a response solution. The response solution can be sent by the field tool to the advertising device in response to the challenge message. The response solution can be verified by the BPD using a cryptographic message authentication code such as an HMAC, and the BPD sends a confirmation message to the field tool indicating that the response solution is verified as correct.

FIG. 5