

ABSTRACT

BLUETOOTH PAIRING SYSTEM, METHOD, AND APPARATUS

Two Bluetooth enabled devices may communicate over a secure link provided they share the same link key which is used to mutual authentication and generation of encryption keys. A method for generating a link key is described which includes storing a partial link key in the device. A link key may then be generated when the associated secret key is provided to the device. This approach may be used in a bonding method in which a first device stores a link key, and a second device stores the associated partial link key. A system for providing link keys to a plurality of devices includes storing link keys in a first set of devices. The first set may be divided into several groups based on the stored link keys being associated with the same partial link key. A second set of devices store the set of all partial link keys and their associated group identifier. Bonding is performed by providing the group identifier and secret key associated with a device from the first set to a device in the second set. A secure system for remotely monitoring the status of a device using bonded Bluetooth devices is also described.

Figure 1B