individually addressed robust management frames and group addressed management frames.

SUMMARY

[0004a] In a first aspect, the present disclosure provides a transmitting multi-link device (MLD) comprising: circuitry, which in operation, constructs an Additional Authentication Data (AAD) and a Nonce and encapsulates a plaintext MAC protocol data unit (MPDU), the AAD and the Nonce to generate an encapsulated MPDU, wherein the AAD includes an Address 1 (A1) field to which a recipient MLD's MLD medium access control (MAC) address is set, and an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set, and wherein the Nonce includes an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set; and a transmitter, which in operation, transmits the encapsulated MPDU to the recipient MLD on a first link.

[0004b] In a second aspect, the present disclosure provides a communication method for a transmitting multi-link device (MLD), the communication method comprising: constructing an Additional Authentication Data (AAD) and a Nonce; encapsulating a plaintext MAC protocol data unit (MPDU), the AAD and the Nonce to generate an encapsulated MPDU, wherein the AAD includes an Address 1 (A1) field to which a recipient MLD's MLD medium access control (MAC) address is set, and an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set, and wherein the Nonce includes an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set; and transmitting the encapsulated MPDU to the recipient MLD on a first link.

[0005] One non-limiting and exemplary embodiment facilitates providing a first multi-link device (MLD) configured to operate with a first plurality of affiliated stations, comprising: circuitry, which in operation, sets up a robust security network association (RSNA) with a second MLD that is configured to operate with a second plurality of affiliated STAs, wherein two or more links have been established between STAs of the first plurality of affiliated STAs and corresponding STAs of the second plurality of affiliated STAs, wherein the circuitry constructs an Additional Authentication Data (AAD) and a Nonce that are used for cryptographical encapsulation of a MAC protocol data unit (MPDU) to form an encapsulated MPDU, wherein the AAD includes an Address 1 (A1) field, an Address 2 (A2) field, an Address 3 (A3) field and a Sequence Control (SC) field, and the Nonce includes an A2 field, wherein the SC field of the AAD is based on a SC field of the MPDU, and a transmitter, which in operation, transmits the encapsulated MPDU to the second MLD on a first link as an initial transmission, and upon failure of the initial transmission, retransmits the encapsulated MPDU on a second link without reperforming the cryptographical encapsulation.

[0006] Another non-limiting and exemplary embodiment facilitates providing a method for retransmission of a MPDU in a multi-link communication, comprising: setting up, at a first MLD, a robust security network association (RSNA) with a second MLD that is configured to operate with a second plurality of affiliated STAs, wherein two or more links have been established between STAs of the first plurality of affiliated STAs and corresponding STAs of the second plurality of affiliated STAs; constructing

CLAIMS

1. A transmitting multi-link device (MLD) comprising:

circuitry, which in operation, constructs an Additional Authentication Data (AAD) and a Nonce and encapsulates a plaintext MAC protocol data unit (MPDU), the AAD and the Nonce to generate an encapsulated MPDU, wherein the AAD includes an Address 1 (A1) field to which a recipient MLD's MLD medium access control (MAC) address is set, and an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set, and wherein the Nonce includes an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set; and

a transmitter, which in operation, transmits the encapsulated MPDU to the recipient MLD on a first link.

2. The transmitting MLD according to claim 1, wherein if the transmission of the encapsulated MPDU is unsuccessful on the first link, the transmitter retransmits the encapsulated MPDU on another link without encapsulating the MPDU with a new packet number (PN).

3. The transmitting MLD according to claim 2, wherein the Nonce includes a PN field and a PN that is set in the PN field is not refreshed for retransmission of the encapsulated MPDU on the another link.

4. The transmitting MLD according to claim 1, comprising a first plurality of affiliated STAs that are capable of establishing one or more links with a second plurality of affiliated STAs associated with the recipient MLD, wherein the MLD

MAC address in the A1 field is different from a MAC address of any one of the second plurality of affiliated STAs and the MLD MAC address in the A2 field is different from a MAC address of any one of the first plurality of affiliated STAs.

5. The transmitting MLD according to claim 1, wherein

a MAC header of the MPDU comprises a legacy Address 1 (legacy A1) field to which a MAC address of a receiving STA is set and a legacy Address 2 (legacy A2) field to which a MAC address of a transmitting STA is set; and

the MLD MAC address in the A1 field of the AAD is different from the MAC address that is set in the legacy A1 field and the MLD MAC address in the A2 field of the AAD and the Nonce is different from the MAC address that is in the legacy A2 field.

6. The transmitting MLD according to claim 3, wherein the settings of the A1 and A2 fields are indicated in one of a Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) Header field or a Galois/Counter Mode Protocol (GCMP) Header field of the encapsulated MPDU.

7. The transmitting MLD according to claim 1, wherein a packet number (PN) in a PN field in the Nonce is incremented to obtain a fresh PN for each MPDU.

8. The transmitting MLD according to claim 1, wherein one of a Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) or a Galois Counter Mode Protocol (GCMP) is used to cryptographically protect the MPDU.

9. The transmitting MLD according to claim 1, wherein the control circuity, in operation, maintains a single packet number (PN) space for a plurality of links.

10. A communication method for a transmitting multi-link device (MLD), the communication method comprising:

constructing an Additional Authentication Data (AAD) and a Nonce;

encapsulating a plaintext MAC protocol data unit (MPDU), the AAD and the Nonce to generate an encapsulated MPDU, wherein the AAD includes an Address 1 (A1) field to which a recipient MLD's MLD medium access control (MAC) address is set, and an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set, and wherein the Nonce includes an Address 2 (A2) field to which the transmitting MLD's MLD MAC address is set; and

transmitting the encapsulated MPDU to the recipient MLD on a first link.

11. The communication method according to claim 10, wherein if the transmission of the encapsulated MPDU is unsuccessful on the first link, the communication method including: retransmitting the encapsulated MPDU on another link without encapsulating the MPDU with a new packet number (PN).

12. The communication method according to claim 11, wherein the Nonce includes a PN field and a PN that is set in the PN field is not refreshed for retransmission of the encapsulated MPDU on the another link.

13. The communication method according to claim 10, the transmitting MLD comprising a first plurality of affiliated STAs that are capable of establishing one or

more links with a second plurality of affiliated STAs associated with the recipient MLD, wherein the recipient MLD's MLD MAC address in the A1 field is different from a MAC address of one of the second plurality of affiliated STAs and the transmitting MLD's MAC address is different from a MAC address of one of the first plurality of affiliated STAs.

14. The communication method according to claim 10, wherein

a MAC header of the MPDU comprises a legacy Address 1 (legacy A1) field to which a MAC address of a receiving STA is set and a legacy Address 2 (legacy A2) field to which a MAC address of a transmitting STA is set; and

the MLD MAC address in the A1 field of the AAD is different from the MAC address that is set in the legacy A1 field and the MLD MAC address in the A2 field of the AAD and the Nonce is different from the MAC address that is in the legacy A2 field.

15. The communication method according to claim 10, wherein the settings of the A1 and A2 fields are indicated in one of a Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) Header field or a Galois Counter Mode Protocol (GCMP) Header field of the encapsulated MPDU.

16. The communication method according to claim 9, wherein a packet number (PN) in a PN field in the Nonce is incremented to obtain a fresh PN for each MPDU.

17. The communication method according to claim 10, wherein one of a Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) or a

Galois Counter Mode Protocol (GCMP) is used to cryptographically protect the MPDU.

18. The communication method according to claim 10, comprising maintaining a single packet number (PN) space for a plurality of links.