

CLAIMS

1. A first multi-link device (MLD) configured to operate with a first plurality of affiliated STAs, 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 Address 2 (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.
2. The first MLD according to claim 1, wherein the A2 field of the AAD and the Nonce is set to a medium access control (MAC) address that identifies the first MLD, and wherein the A1 field of the AAD is set to a MAC address that identifies the second MLD.

3. The first MLD according to claim 1, wherein the A3 field of the AAD is set to a MAC address that identifies an Access Point (AP) MLD, wherein the AP MLD is the first or second MLD.

5 4. The first MLD according to claim 1, wherein the circuitry specifies in the MPDU settings of the A1, A2, A3 fields, the settings indicating whether, during cryptographical decapsulation of the retransmitted MPDU, the A1, A2, A3 fields are to be set to a MAC address that identifies the second MLD, a MAC address that identifies the first MLD and a MAC address that identifies an AP MLD respectively,
10 or the A1, A2, A3 fields are to be set to a MAC address of an affiliated STA of the second MLD, a MAC address of an affiliated STA of the first MLD and the MAC address that identifies the AP MLD respectively, or the A1, A2, A3 fields are to be set to A1, A2, A3 fields of the MPDU respectively, wherein the AP MLD is the first or second MLD.

15

5. The first MLD according to claim 3, wherein the settings of the A1, A2, A3 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.

20

6. The first MLD according to claim 1, wherein the A2 field of the AAD and the Nonce are set to an A2 field of the MPDU, and the A1 field of the AAD is set to an A1 field of the MPDU, wherein upon failure of the initial transmission, the circuitry further specifies in the retransmitted MPDU settings of the A1, A2, A3 fields, the
25 settings indicating whether, during cryptographical decapsulation of the

retransmitted MPDU, the A1, A2, A3 fields are to be set to MAC addresses of an affiliated STA of the second MLD and an affiliated STA of the first MLD respectively, or the A1, A2, A3 fields are to be set to the A1, A2, A3 fields of the retransmitted MPDU respectively.

5

7. The first MLD according to claim 1, wherein one of a CCMP or a GCMP is used to cryptographically protect the MPDU.

8. The first MLD according to claim 1, wherein the MPDU comprises identification information of the first and second MLDs, wherein the A2 field of the AAD and the Nonce is set to a MAC address that identifies the first MLD indicated in the identification information, and the A1 field of the AAD is set to a MAC address that identifies the second MLD indicated in the identification information.

9. A first multi-link device (MLD) configured to operate with a first plurality of affiliated STAs, 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, and

a receiver, which in operation, receives a cryptographically encapsulated MAC protocol data unit (MPDU) from the second MLD, wherein the circuitry constructs an Additional Authentication Data (AAD) and a Nonce that are used for cryptographic decapsulation of the received 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 Address 2 (A2) field, wherein the A2 field of the AAD and the Nonce may be set to either an A2 field of the MPDU or a medium access control (MAC) address that identifies the second
5 MLD or a MAC address of one of the second plurality of affiliated STAs, the A1 field of the AAD may be set to either an A1 field of the MPDU or a MAC address that identifies the first MLD or a MAC address of one of the first plurality of affiliated STAs, the A3 field of the AAD may be set to either an A3 field of the MPDU or a MAC address that identifies either the first or the second MLD that acts
10 as an access point MLD and the SC field of the AAD is based on a SC field of the MPDU.

10. The first MLD according to claim 9, wherein the circuitry cryptographically decapsulates the MPDU received from the second MLD, wherein the A2 field of the
15 AAD and the Nonce is set to the MAC address that identifies the second MLD, and the A1 field of the AAD is set to the MAC address that identifies the first MLD.

11. The first MLD according to claim 9, wherein the circuitry cryptographically decapsulates the received MPDU based on settings of the A1, A2, A3 fields
20 indicated in the MPDU, the settings indicating whether, during the cryptographical decapsulation, the A1, A2, A3 fields are to be set to the MAC address that identifies the first MLD, the MAC address that identifies the second MLD and a MAC address that identifies an AP MLD respectively, or the A1, A2, A3 fields are to be set to the
25 MAC address of an affiliated STA of the first MLD, the MAC address of an affiliated STA of the second MLD and the MAC address that identifies the AP MLD

respectively, or the A1, A2, A3 fields are to be set to the A1, A2, A3 fields of the MPDU respectively, wherein the AP MLD is the first or second MLD.

12. The first MLD according to claim 11, wherein the settings of the A1, A2, A3 fields are indicated in one of a CCMP Header or a GCMP Header of the MPDU received from the second MLD.

13. The first MLD according to claim 9, wherein the circuitry cryptographically decapsulates a first MPDU received from the second MLD by setting the A2 field of the AAD and the Nonce to the A2 field of the first MPDU, and the A1 field of the AAD to the A1 field of the first MPDU, wherein the first MPDU includes a Retry subfield that is set to 0; and wherein the circuitry cryptographically decapsulates a second MPDU received from the second MLD based on the settings of the A1, A2, A3 fields indicated in the second MPDU, the settings indicating whether, during the cryptographic decapsulation, the A1, A2, A3 fields are to be set to the MAC address of an affiliated STA of the first MLD, the MAC address of an affiliated STA of the second MLD and a MAC address that identifies an AP MLD respectively, or the A1, A2, A3 fields are to be set to A1, A2, A3 fields of the second MPDU respectively, wherein the second MPDU includes a Retry subfield that is set to 1, and wherein the AP MLD is the first or second MLD.

14. The first MLD according to claim 9, wherein one of a CCMP or a GCMP is used to cryptographically decapsulate the MPDU.

15. The first MLD according to claim 9, wherein the MPDU carries identification information of the first and second MLDs, wherein the circuitry cryptographically decapsulates the MPDU by setting the A2 field of the AAD and the Nonce to the MAC address that identifies the second MLD indicated in the MPDU, and by setting
5 the A1 field of the AAD to the MAC address that identifies the first MLD indicated in the MPDU.

16. A method for retransmission of a MPDU in a multi-link communication, comprising:
10 setting up, at a first MLD configured to operate with a first plurality of affiliated STAs, 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;
15 constructing an Additional Authentication Data (AAD) and a Nonce, wherein the AAD includes an Address 1 (A1) field, an Address 2 (A2) field, an Address 3 (A3) and a Sequence Control (SC) field, and the Nonce includes an Address 2 (A2) field, wherein the SC field of the AAD is based on a SC field of the MPDU;
cryptographically encapsulating the MPDU using the AAD and Nonce to form
20 an encapsulated MPDU;
transmitting the encapsulated MPDU from the first MLD to the second MLD on a first link as an initial transmission, and
retransmitting the encapsulated MPDU on a second link without reperforming the cryptographic encapsulation upon failure of the initial transmission.

25