CLAIMS

WHAT IS CLAIMED IS:

1. A method operational in a relay node, comprising:

configuring the relay node to operate between a first access node and a first mobile node by relaying traffic between the first access node and the first mobile node, where

a first communication interface of the relay node is adapted to communicate with the first access node, the relay node appearing as a second mobile node to the first access node, and

a second communication interface adapted to communicate with the first mobile node, the relay node appearing as a second access node to the first mobile node;

sending a device authentication message to enable device authentication of the relay node; and

sending a subscriber authentication message to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over a communication network.

2. The method of claim 1, further comprising:

obtaining access to the communication network upon successful subscriber authentication and device authentication.

3. The method of claim 1, further comprising:

receiving a service grant message granting access to the communication network upon successful subscriber authentication and device authentication; and

receiving a service denied message denying access to the communication network upon unsuccessful subscriber authentication or device authentication.

4. The method of claim 1, wherein the device authentication message and the subscriber authentication message are sent concurrently as a single authentication message.

5. The method of claim 1, wherein the first communication interface implements a different over-the-air communication protocol than the second communication interface.

6. The method of claim 1, wherein device authentication is performed using at least one of a device identifier or device key unique to the relay node and stored in a secure, non-removable storage device within the relay node.

7. The method of claim 6, wherein the device identifier is at least one of an International Mobile Equipment Identity (IMEI) for the relay node, an access node module within the relay node, or a mobile node module within the relay node.

8. The method of claim 1, wherein the first communication interface is part of a mobile access module adapted to operate as an enhanced Node B for a Long Term Evolution-compliant network.

9. The method of claim 1, wherein the first communication interface is part of a mobile node module of the relay node and the second communication interface is part of an access node module of the relay node.

10. The method of claim 1, wherein subscriber authentication is subsequently repeated more frequently than device authentication.

11. The method of claim 1, further comprising:

configuring the relay node to translate traffic of a first packet type received over the first communication interface to a second packet type for transmission over the second communication interface; and

configuring the relay node to translate traffic of the second packet type received over the second communication interface to the first packet type for transmission over the first communication interface.

12. The method of claim 1, further comprising:

configuring the relay node to translate data traffic transmissions between the first communication interface and the second communication interface from a first signal type to a second signal type.

13. The method of claim 1, wherein a subscriber identifier or key used in subscriber authentication is pre-associated with a device type, and subscriber authentication is successful only if the device authentication identifies the same device type.

14. A relay node, comprising:

a first communication interface adapted to communicate with a first access node, the relay node appearing as a second mobile node to the first access node;

a second communication interface adapted to communicate with a first mobile node, the relay node appearing as a second access node to the first mobile node; and

a processing circuit coupled to the first communication interface and the second communication interface, the processing circuit adapted to:

relay traffic between the first access node and the first mobile node,

send a device authentication message to enable device authentication of the relay node, and

send a subscriber authentication message to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over a communication network.

15. The relay node of claim 14, wherein the processing circuit is further adapted to:

obtain access to the communication network upon successful subscriber authentication and device authentication.

16. The relay node of claim 14, wherein the processing circuit is further adapted to:

receive a service grant message granting access to the communication network upon successful subscriber authentication and device authentication; and

receive a service denied message denying access to the communication network upon unsuccessful subscriber authentication or device authentication.

17. The relay node of claim 14, further comprising:

a non-removable secure storage device coupled to the processing circuit, the non-removable secure storage device storing at least one of a device identifier or key unique to the relay node and used for device authentication.

18. The relay node of claim 17, wherein the device identifier is at least one of an International Mobile Equipment Identity (IMEI) for the relay node, an access node module within the relay node, or a mobile node module within the relay node.

19. The relay node of claim 14, wherein the first communication interface implements a different over-the-air communication protocol than the second communication interface.

20. The relay node of claim 14, further comprising:

a mobile node module including the first communication interface and a non-removable storage device for storing one or more mobile node identifiers and/or keys used for device authentication.

21. The relay node of claim 14, further comprising:

an access node module including the second communication interface and a non-removable storage device for storing one or more access node identifiers and/or keys used for device authentication.

22. The relay node of claim 14, wherein the processing circuit is further adapted to:

translate data traffic transmissions between the first communication interface and the second communication interface from a first signal type to a second signal type.

23. A relay node, comprising:

means for communicating with a first access node, the relay node appearing as a second mobile node to the first access node;

means for communicating with a first mobile node, the relay node appearing as a second access node to the first mobile node;

means for relaying traffic between the first access node to the first mobile node;

means for sending a device authentication message to enable device authentication of the relay node, and

means for sending a subscriber authentication message to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over a communication network.

24. The relay node of claim 23, further comprising:

means for obtaining access to the communication network upon successful subscriber authentication and device authentication.

25. The relay node of claim 23, further comprising:

means for securely and non-removably storing at least one of a device identifier or key.

26. The relay node of claim 23, further comprising:

means for translating data traffic transmissions between the first communication interface and the second communication interface from a first signal type to a second signal type.

27. A processor-readable medium comprising one or more instructions operational on a relay node adapted to operate between a first mobile node and a first access node, which when executed by a processing circuit, causes the processing circuit to:

communicate with a first access node via a first communication interface, the relay node appearing as a second mobile node to the first access node;

communicate with a first mobile node via a second communication interface, the relay node appearing as a second access node to the first mobile node;

relay traffic between the first access node and the first mobile node; and

send a device authentication message to enable device authentication of the relay node, and

send a subscriber authentication message to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber

authentication in determining whether the relay node can obtain communication service over a communication network.

28. The processor-readable medium of claim 23, comprising one or more instructions which when executed by a processing circuit, causes the processing circuit to:

obtain access to the communication network upon successful subscriber authentication and device authentication.

29. A method operational in a network authentication entity, comprising:

receiving a device authentication message originated by a relay node that operates between a first mobile node and a first access node;

performing device authentication based on one or more device identifiers or keys associated with the relay node, an access node module of the relay node, or a mobile node module of the relay node;

receiving a subscriber authentication message originated by the relay node;

performing subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node; and

sending a message granting the relay node access to the communication network upon successful subscriber authentication and device authentication.

30. The method of claim 29, further comprising:

sending a message denying the relay node access to the communication network upon unsuccessful subscriber authentication or device authentication.

31. The method of claim 29, further comprising:

sending a first message to the relay node to initiate device authentication; and

sending a second message to the relay node to initiate subscriber authentication.

32. The method of claim 29, wherein a subscriber identifier or key used in subscriber authentication is pre-associated with a device type, and subscriber authentication is successful only the device authentication identifies the same device type.

33. The method of claim 29, wherein device authentication is performed by a device authentication node while subscriber authentication is performed by a subscriber authentication node.

34. The method of claim 29, wherein the device authentication message and the subscriber authentication message are received concurrently as a single authentication message.

35. An authentication entity, comprising:

a communication interface adapted to communicate with a relay node over a communication network;

a processing circuit coupled to the communication interface, the processing circuit adapted to:

receive a device authentication message originated by the relay node that operates between a first mobile node and a first access node;

perform device authentication based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

receive a subscriber authentication message originated by the relay node;

performing subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node; and

send a message granting the relay node access to the communication network upon successful subscriber authentication and device authentication.

36. The authentication entity of claim 35, wherein the processing circuit is further adapted to:

sending a message denying the relay node access to the communication network upon unsuccessful subscriber authentication or device authentication.

37. The authentication entity of claim 36, further comprising:

a device authentication node to perform device authentication; and

a subscriber authentication node to perform subscriber authentication.

38. An authentication entity, comprising:

means for receiving a device authentication message originated by a relay node that operates between a first mobile node and a first access node;

means for performing device authentication based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

means for receiving a subscriber authentication message originated by the relay node;

means for performing subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node; and

means for sending a message granting the relay node access to the communication network upon successful subscriber authentication and device authentication.

39. A processor-readable medium comprising one or more instructions operational on an authentication entity operating within a core communication network, which when executed by a processing circuit, causes the processing circuit to:

receive a device authentication message originated by a relay node that operates between a first mobile node and a first access node;

perform device authentication based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

receive a subscriber authentication message originated by the relay node;

perform subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node; and

send a message granting the relay node access to the communication network upon successful subscriber authentication and device authentication.

CLAIMS

1. A method operational in a relay node, comprising:

configuring the relay node to operate between a first access node and a first mobile node by relaying traffic between the first access node and the first mobile node, the first access node equipped to provide access to a communications network, where

a first communication interface of the relay node is adapted to communicate with the first access node utilizing a first signaling protocol, the relay node appearing as a second mobile node to the first access node, and

a second communication interface adapted to communicate with the first mobile node utilizing a second signaling protocol, the relay node appearing as a second access node to the first mobile node;

sending a device authentication message from the relay node to the first access node to enable device authentication of the relay node; and

sending a subscriber authentication message from the relay node to the first access node to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain service over the communication network accessed via the first access node and wherein the relay node is granted access to communicate with the communications network upon both successful subscriber authentication and successful device authentication.

2. The method of claim **1**, further comprising:

obtaining access to the communication network upon receiving signals from the access node indicating that successful subscriber authentication and device authentication has been granted.

3. The method of claim **1**, further comprising:

receiving a service grant message from the access node granting access to the communication network upon successful subscriber authentication and device authentication; and

receiving a service denied message from the access node denying access to the communication network upon unsuccessful subscriber authentication or device authentication.

4. The method of claim **1**, wherein the device authentication message and the subscriber authentication message are sent concurrently from the relay node to the access node as a single authentication message.

5. The method of claim **1**, wherein the first communication interface uses over-the-air signaling to communicate with the first access node.

6. The method of claim **1**, wherein device authentication is performed using at least one of a device identifier or a device key unique to the relay node and stored in a secure, non-removable storage device within the relay node.

7. The method of claim **6**, wherein the device identifier is at least one of an International Mobile Equipment Identity (IMEI) for the relay node, an access node module within the relay node, or a mobile node module within the relay node.

8. The method of claim **1**, wherein the first communication interface is part of a mobile access module adapted to operate as an enhanced Node B for a Long Term Evolution-compliant network.

9. The method of claim **1**, wherein the first communication interface is part of a mobile node module of the relay node and the second communication interface is part of an access node module of the relay node.

10. The method of claim **1**, wherein subscriber authentication is subsequently repeated more frequently than device authentication.

11. The method of claim **1**, further comprising:

configuring the relay node to translate traffic of a first packet type received over the first communication interface to a second packet type for transmission over the second communication interface to the mobile node; and

configuring the relay node to translate traffic of the second packet type received over the second communication interface to the first packet type for transmission over the first communication interface to the access node.

12. The method of claim **1**, further comprising:

configuring the relay node to translate data traffic transmissions between the first communication interface and the second communication interface from a first signal type associated with the first signaling protocol to a second signal type associated with the second signaling protocol.

13. The method of claim **1**, wherein one or more of a subscriber identifier or a key used in subscriber authentication is pre-associated with a device type, and subscriber authentication is successful if the device authentication identifies the same device type.

14. The method of claim **1** wherein the first and second signaling protocols are the same.

15. The method of claim **1** wherein the first and second signaling protocols are Evolved Universal Terrestrial Access (E-UTRA) protocols.

16. The method of claim **1** wherein the first and second signaling protocols are different over-the-air communication protocols.

17. The method of claim **1** wherein the relay node appears as a user equipment (UE) to the first access node.

18. The method of claim **1** wherein the relay node appears as an enhanced Node B (eNB) to the first mobile node.

19. A relay node, comprising:

a first communication interface adapted to communicate with a first access node utilizing a first signaling protocol, the relay node appearing as a second mobile node to the first access node, the first access node equipped to provide access to a communications network;

a second communication interface adapted to communicate with a first mobile node utilizing a second signaling protocol, the relay node appearing as a second access node to the first mobile node; and

a processing circuit coupled to the first communication interface and the second communication interface, the processing circuit adapted to:

relay traffic between the first access node and the first mobile node,

send a device authentication message from the relay node to the first access node via the first communication interface to enable device authentication of the relay node, and

send a subscriber authentication message from the relay node to the first access node via the first communication

interface to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over the communication network accessed via the first access node and wherein the relay node is granted access to communicate with the communications network upon both successful subscriber authentication and successful device authentication.

20. The relay node of claim **19**, wherein the processing circuit is further adapted to:

obtain access to the communication network upon receiving signals from the access node indicating that successful subscriber authentication and device authentication has been granted.

21. The relay node of claim **19**, wherein the processing circuit is further adapted to:

receive a service grant message from the access node granting access to the communication network upon successful subscriber authentication and device authentication; and

receive a service denied message from the access node denying access to the communication network upon unsuccessful subscriber authentication or device authentication.

22. The relay node of claim **19**, further comprising:

a non-removable secure storage device coupled to the processing circuit, the non-removable secure storage device storing at least one of a device identifier or a key unique to the relay node and used for device authentication.

23. The relay node of claim **22**, wherein the device identifier is at least one of an International Mobile Equipment Identity (IMEI) for the relay node, an access node module within the relay node, or a mobile node module within the relay node.

24. The relay node of claim **19**, wherein the first communication interface uses over-the-air signaling to communicate with the first access node.

25. The relay node of claim **19**, further comprising:

a mobile node module including the first communication interface and a non-removable storage device for storing one or more mobile node identifiers and keys used for device authentication.

26. The relay node of claim **19**, further comprising:

an access node module including the second communication interface and a non-removable storage device for storing one or more access node identifiers and keys used for device authentication.

27. The relay node of claim **19**, wherein the processing circuit is further adapted to:

translate data traffic transmissions between the first communication interface and the second communication interface from a first signal type associated with the first signaling protocol to a second signal type associated with the second signaling protocol.

28. A relay node, comprising:

means for communicating with a first access node utilizing a first signaling protocol, the relay node appearing as a second mobile node to the first access node, the first access node equipped to provide access to a communications network;

means for communicating with a first mobile node utilizing a second signaling protocol, the relay node appearing as a second access node to the first mobile node;

means for relaying traffic between the first access node and the first mobile node;

means for sending a device authentication message from the relay node to the first access node to enable device authentication of the relay node; and

means for sending a subscriber authentication message from the relay node to the first access node to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over the communication network accessed via the first access node and wherein the relay node is granted access to communicate with the communications network upon both successful subscriber authentication and successful device authentication.

29. The relay node of claim **28**, further comprising:

means for obtaining access to the communication network upon receiving signals from the access node indicating that successful subscriber authentication and device authentication has been granted.

30. The relay node of claim **28**, further comprising:

means for securely and non-removably storing at least one of a device identifier or key.

31. The relay node of claim **28**, further comprising:

means for translating data traffic transmissions between a first communication interface and a second communication interface of the relay node, from a first signal type associated with the first signaling protocol to a second signal type associated with the second signaling protocol.

32. A non-transitory processor-readable storage medium comprising one or more instructions operational on a relay node adapted to operate between a first mobile node and a first access node, which when executed by a processing circuit, causes the processing circuit to:

communicate with a first access node via a first communication interface utilizing a first signaling protocol, the

relay node appearing as a second mobile node to the first access node, the first access node equipped to provide access to a communications network;

communicate with a first mobile node via a second communication interface utilizing a second signaling protocol, the relay node appearing as a second access node to the first mobile node;

relay traffic between the first access node and the first mobile node;

send a device authentication message from the relay node to the first access node via the first communication interface to enable device authentication of the relay node; and

send a subscriber authentication message from the relay node to the first access node via the first communication interface to enable subscriber authentication of the relay node, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over the communication network accessed via the first access node and wherein the relay node is granted access to communicate with the communications network upon both successful subscriber authentication and successful device authentication.

33. The non-transitory processor-readable storage medium of claim **32**, comprising one or more instructions which when executed by a processing circuit, causes the processing circuit to:

obtain access to the communication network upon receiving signals from the access node indicating that successful subscriber authentication and device authentication has been granted.

34. A method operational in a network authentication entity of a communication network, comprising:

receiving a device authentication message originated by a relay node that operates between a first mobile node and a first access node, wherein the relay node is configured to communicate between the first mobile node and the first access node utilizing first and second signaling protocols, respectively, and wherein the first access node is equipped to provide access to a communications network;

performing device authentication based on one or more device identifiers or keys associated with the relay node, an access node module of the relay node, or a mobile node module of the relay node;

receiving a subscriber authentication message originated by the relay node;

performing subscriber authentication of the relay node based on one or more subscriber identifiers or keys associated with the relay node; and

sending a message granting the relay node access to the communication network upon both successful subscriber authentication and device authentication, wherein the device authentication is bound to the subscriber authentication in determining whether the relay node can obtain communication service over the communication network.

35. The method of claim **34**, further comprising:

sending a message to the relay node denying the relay node access to the communication network upon one or more of unsuccessful subscriber authentication or device authentication.

36. The method of claim **34**, further comprising:

sending a first message to the relay node to initiate device authentication; and

sending a second message to the relay node to initiate subscriber authentication.

37. The method of claim **34**, wherein one or more of a subscriber identifier or key used in subscriber authentication is pre-associated with a device type, and subscriber authentication is successful if the device authentication identifies the same device type.

38. The method of claim **34**, wherein device authentication is performed by a device authentication node while subscriber authentication is performed by a subscriber authentication node.

39. The method of claim **34**, wherein the device authentication message and the subscriber authentication message are received concurrently as a single authentication message.

40. An authentication entity, comprising:

a communication interface adapted to communicate with a relay node over a communication network;

a processing circuit coupled to the communication interface, the processing circuit adapted to:

receive a device authentication message originated by the relay node that operates between a first mobile node and a first access node, wherein the relay node is configured to communicate with the first mobile node and the first access node utilizing first and second signaling protocols, respectively, and wherein the first access node is equipped to provide access to the communications network from the relay node;

perform device authentication of the relay node based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

receive a subscriber authentication message originated by the relay node;

performing subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node wherein device authentication is bound to subscriber authentication in determining whether the relay node can obtain service over the communication network; and

send a message granting the relay node access to the communication network upon both successful subscriber authentication and device authentication.

41. The authentication entity of claim **40**, wherein the processing circuit is further adapted to:

send a message denying the relay node access to the communication network upon one or more of unsuccessful subscriber authentication or device authentication.

42. The authentication entity of claim **41**, further comprising:

a device authentication node to perform device authentication; and

a subscriber authentication node to perform subscriber authentication.

43. An authentication entity of a communication network, comprising:

means for receiving a device authentication message originated by a relay node that operates between a first mobile node and a first access node, wherein the relay node is configured to communicate with the first mobile node utilizing a first signaling protocol and with the first access node utilizing a second signaling protocol;

means for performing device authentication based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

means for receiving a subscriber authentication message originated by the relay node;

means for performing subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node wherein device authentication is bound to subscriber authentication in determining whether the relay node can obtain service over the communication network; and

means for sending a message granting the relay node access to the communication network upon both successful subscriber authentication and device authentication.

44. A non-transitory processor-readable storage medium comprising one or more instructions operational on an authentication entity operating within a core communication network, which when executed by a processing circuit, causes the processing circuit to:

receive a device authentication message originated by a relay node that operates between a first mobile node and a first access node, wherein the relay node is configured to communicate with the first mobile node utilizing a first signaling protocol and with the first access node utilizing a second signaling protocol;

perform device authentication based on one or more device identifiers or keys associated with the relay node, an access node component of the relay node, or a mobile node component of the relay node;

receive a subscriber authentication message originated by the relay node;

perform subscriber authentication based on one or more subscriber identifiers or keys associated with the relay node wherein device authentication is bound to subscriber authentication in determining whether the relay node can obtain service over the communication network; and

send a message granting the relay node access to the communication network upon both successful subscriber authentication and device authentication.