Claims

We claim:

1. A method of transmitting data packets securely through a cloud, the data packets comprising digital data, the digital data comprising a series of data segments, the cloud comprising a network of media nodes, the media nodes being hosted on servers, each of the media nodes receiving data packets from other media nodes in the network and transmitting data packets to other media nodes in the network, the method comprising:

storing shared secrets in a first media node or in a server associated with the first media node, the shared secrets comprising a list of concealment algorithms;

storing the shared secrets in a second media node or in a server associated with the second media node;

causing the first media node to perform a first concealment operation on a data packet in accordance with one or more of the concealment algorithms on the list of concealment algorithms to conceal at least a portion of the content of the data packet, the one or more concealment algorithms used by the first media node in performing the first concealment operation being selected in accordance with a dynamic state;

causing the first media node to transmit the data packet or constituent sub-packets of the data packet to the second media node, along with a digital representation of the dynamic state used by the first media node in performing the first concealment operation on the data packet;

causing the second media node to perform an inverse of the first concealment operation so as to recreate the data packet in the form that the data packet existed before the first media node performed the first concealment operation on the data packet, using the one or more concealment algorithms and the dynamic state used by the first media node in performing the first concealment operation on the data packet.

2. The method of Claim 1 wherein the shared secrets comprise a seed generator for generating a seed comprising a digital value representing the dynamic state, an algorithm used by the seed generator, a hidden number generator for using a seed to generate a hidden number, an algorithm used by the hidden number generator, zone information and algorithm shuffling processes.

3. The method of Claim 1 wherein the dynamic state used by the first media node comprises a time at which the first media node performs the first concealment operation on the data packet.

4. The method of Claim 1 wherein the dynamic state used by the first media node comprises a media node number, a network identification, a GPS location, a counter for incrementing a random number each time a packet traverses a media node in the network, or an algorithm for selecting a concealment algorithm based on a parametric value derived form data contained within the data packet.

5. The method of Claim 1 wherein the first media node uses the dynamic state as an input variable in executing at least one of the concealment algorithms.

6. The method of Claim 1 wherein the first concealment operation comprises at least one technique selected from the group consisting of:

scrambling the data packet by changing an order of at least some of the data segments in the data packet in accordance with a scrambling algorithm;

encrypting the data packet by encrypting at least some of the data in the data packet in accordance with an encryption algorithm;

splitting the data packet into at least two sub-packets in accordance with a splitting algorithm;

mixing the data packet by combining the data packet with at least one other data packet in accordance with a mixing algorithm; and

adding junk data to and/or removing junk data from the data packet in accordance with at least one junk data algorithm.

7. The method of Claim 1 wherein an address of the second media node used by the first media node to transmit the data packet or constituent sub-packets to the second media node is chosen by another server not hosting the first media node

8. The method of Claim 1 wherein causing the first media node to transmit the data packet or constituent sub-packets to the second media node comprises causing the first media node to transmit the data packet or constituent sub-packets through at least one intermediary media node en route to the second media node, wherein the at least one intermediate node does not change the digital data in the data packet except to update a destination address for a next hop of the data packet or constituent sub-packets.

9. The method of Claim 8 wherein an address of the at least one intermediate media node used by the first media node to transmit the data packet or constituent sub-packets to the at least one intermediary media node is chosen by another server not hosting the first media node

10. The method of Claim 1 wherein the first media node comprises a gateway node, the gateway node being connected to a client device via a last mile connection.

11. The method of Claim 1 comprising causing the second media node to perform a second concealment operation on the data packet, the second concealment operation comprising at least one technique selected from the group consisting of:

scrambling the data packet by changing an order of at least some of the data segments in the data packet in accordance with a second scrambling algorithm and a dynamic state;

encrypting the data packet by encrypting at least some of the data in the data packet in accordance with a second encryption algorithm and a dynamic state;

splitting the data packet into at least two sub-packets in accordance with a second splitting algorithm and a dynamic state;

mixing the data packet by combining the data packet with at least one other data packet in accordance with a second mixing algorithm and a dynamic state; and

adding junk data to and/or removing junk data from the data packet in accordance with at least one second junk data algorithm and a dynamic state,

wherein the second concealment operation is different from the first concealment operation.

12. The method of Claim 11 wherein the dynamic state used by the second media node comprises a time at which the second media node performs the second concealment operation on the data packet.

13. The method of Claim 11 wherein the second media node uses the dynamic state as an input variable in executing at least one of the second scrambling algorithms, second encryption algorithms, second splitting algorithms, second mixing algorithms and second junk algorithms.

14. The method of Claim 1 wherein the server associated with the first media node comprises a first DMZ server and the server associated with the second media node comprises a second DMZ server, and wherein the shared secrets are stored in the first and second DMZ servers, the first and second DMZ servers being isolated from the network such that none of

media nodes in the network, including the first and second media nodes, has access to the shared secrets.

15. The method of Claim 14 comprising:

causing the first DMZ server to select the one or more concealment algorithms from the shared secrets in accordance with the dynamic state and to instruct the first media node to perform the first concealment operation on the data packet by using the one or more concealment algorithms;

causing the first DMZ server to-generate a seed, the seed comprising a disguised digital value generated from the dynamic state used by the first DMZ server to select the one or more concealment algorithms from the shared secrets; and

causing the seed to be delivered to the second DMZ server.

16. The method of Claim 15 wherein causing the seed to be delivered to the second DMZ server comprises causing the first DMZ server to transmit the seed to the first media node, causing the first media node to transmit the seed to the second media node, and causing the second media node to transmit the seed to the second DMZ server.

17. The method of Claim 15 wherein causing the seed to be delivered to the second DMZ server comprises causing the first DMZ server to transmit the seed to a signaling server and causing the signaling server to transmit the seed to the second DMZ server.

18. The method of Claim 15 comprising causing the second DMZ server to use the seed to identify the one or more concealment algorithms used by the first media node in performing the first concealment operation on the data packet and to instruct the second media node to perform an inverse of the first concealment operation on the data packet.

19. The method of Claim 15 wherein causing the second media node to perform a second concealment operation on the data packet comprises causing the second DMZ server to select one or more second concealment algorithms from the shared secrets in accordance with the dynamic state and to instruct the second media node to perform the second concealment operation on the data packet by using the one or more second concealment algorithms.

20. The method of Claim 19 wherein the state used by the second DMZ server comprises a time at which the second DMZ server selects the one or more second concealment algorithms from the shared secrets.

21. The method of Claim 1 wherein the first and second media nodes are located in a first zone of the cloud and wherein the cloud comprises a second zone, the second zone comprising a plurality of media nodes, the method comprising:

storing a second set of shared secrets in media nodes in the second zone or in servers associated with the media nodes associated with media nodes in the second zone, the second set of shared secrets comprising a second list of concealment algorithms, the second list of concealment algorithms being different from the list of concealment algorithms in the shared secrets; and

using the second set of shared secrets to select concealment algorithms to be used by media nodes in the second zone to perform concealment operations on the data packets as the data packets pass through media nodes in the second zone.

22. The method of Claim 21 wherein the cloud comprises a bridge media node located in both the first and second zones, the bridge media node performing an inverse of concealment operations on data packets arriving from media nodes in the first zone in accordance with the shared secrets and performing concealment operations on data packets destined for media nodes in the second zone in accordance with the second set of shared secrets.

23. The method of Claim 1 wherein the cloud comprises a gateway node, the gateway node being connected to a client device via a last mile connection, the method comprising storing the shared secrets and a second set of shared secrets in the gateway node or in a server associated with the gateway node and storing the second set of shared secrets in the client device, the second set of shared secrets comprising a second list of concealment algorithms different from the list of concealment algorithms in the shared secrets and comprising a plurality of algorithms selected from the group consisting of:

scrambling algorithms;

encryption algorithms;

splitting algorithms;

mixing algorithms; and

junk data insertion and/or removal algorithms.

24. The method of Claim 23 comprising:

causing the client device to perform a second concealment operation on a second data packet in accordance with one or more of the algorithms on the second list of

concealment algorithms, the one or more algorithms used by the client device in performing the second concealment operation being selected in accordance with a dynamic state; and

causing the client device to transmit the second data packet or constituent sub-packets of the second data packet to the gateway node, along with a digital representation of the dynamic state used by the client device in performing the second concealment operation on the second data packet.

25. The method of Claim 24 comprising causing the gateway node to perform an inverse of the second concealment operation so as to recreate the second data packet in the form that the second data packet existed before the client device performed the second concealment operation on the second data packet, using one or more of the algorithms on the second list of concealment algorithms and the dynamic state used by the client device in performing the second concealment operation on the second data packet.

26. The method of Claim 25 wherein the server associated with the gateway node comprises a gateway DMZ server, the method comprising:

storing the shared secrets and the second set of shared secrets in the gateway DMZ server; and

causing the client device to generate a seed and causing the seed to be delivered to the gateway DMZ server, the seed comprising a digital representation of the dynamic state used by the client device in performing the second concealment operation on the second data packet.

27. The method of Claim 26 comprising causing the gateway DMZ server to use the seed transmitted by the client device to identify the one or more algorithms on the second list of concealment algorithms used by the client device in performing the second concealment operation on the second data packet and to instruct the gateway node to perform the inverse of the second concealment operation on the second data packet by using the one or more algorithms on the second list of concealment algorithms.

28. The method of Claim 27 comprising:

causing the gateway DMZ server to select at least one third concealment algorithm from the shared secrets in accordance with the dynamic state and to instruct the

gateway node to perform a third concealment operation on the second data packet by using the at least one third concealment algorithm; and

causing the gateway node to send the second data packet to a third media node in the network.

29. The method of Claim 1 comprising periodically changing the shared secrets by changing the list of concealment algorithms.

30. The method of Claim 1 comprising routing the data packet through at least one intermediate media node between the first and second media nodes.

31. The method of Claim 30 comprising routing the data packet through a plurality of intermediate media nodes between the first and second media nodes and rescrambling and/ or re-encrypting the data packet in at least some of the intermediate nodes, wherein a scrambling algorithm and/or encryption algorithm used to scramble and/or encrypt the data packet in each of the intermediate media nodes in which the data packet is rescrambled and/or re-encrypted is different from a scrambling algorithm and/or encryption algorithm used to scramble the data packet in every other intermediate media node in which the data packet is rescrambled and/or re-encrypted.

32. The method of Claim 1 wherein the first concealment operation comprises splitting the data packet into at least two sub-packets, the at least two sub-packets comprising a first sub-packet and a second sub-packet, the method comprising routing the first sub-packet through a first series of intermediate media nodes between the first media node and the second media node, routing the second sub-packet through a second series of intermediate media nodes between the first media node and the second media node, and mixing the first and second sub-packets in the second media node.

33. The method of Claim 32 wherein the first series of intermediate media nodes does not comprise any media node that is comprised within the second series of intermediate media nodes.

34. The method of Claim 33 wherein the first series of intermediate media nodes comprises at least one media node that is comprised within the second series of intermediate media nodes and at least one media node that is not comprised within the second series of intermediate media nodes.

35. The method of Claim 1 comprising:

providing a first client device, the first client device being in communication with an entry gateway node in the network via a first mile connection;

providing a second client device, the second client device being in communication with an exit gateway node in the network via a last mile connection;

providing one or more signaling servers;

causing the first client device to transmit an address of the second client device to a signaling server;

causing the signaling server to develop a network routing plan defining the route of a data packet from the first client device to the second client device through the network; and

causing the signaling server to send a command and control packet to media nodes designated in the network routing plan, each command and control packet informing a media node designated in the network routing plan where to send an incoming data packet identified by a specific identifying tag and what tag to apply to the data packet before sending the data packet to next media node in the network routing plan.

36. The method of Claim 35 wherein the signaling server stores a network node list, the network node list comprising a list of active media nodes and client devices and the address of each of the active media nodes and client devices, the method comprising:

causing the first client device to initiate a communication with the second client device by transmitting to the signaling server an identity of the second client device and a request for an address of the second client device; and

causing the signaling server to pass the address of second client device to the first client device.

37 The method of Claim 36 wherein in developing a network routing plan the signaling server considers propagation delays between media nodes on the network node list in order to reduce a transit time of a data packet through the network.

38. The method of Claim 35 comprising:

providing one or more name servers, the one or more name servers storing a network node list, the network node list comprising a list of active media nodes and client devices and addresses of the active media nodes and client devices;

causing the first client device to initiate a communication with the second client device by transmitting to a name server an identity of the second client device and a request for an address of the second client device; and

causing the name server to pass the address of second client device to the first client device.

39. The method of Claim 35 wherein at least one of the command and control packets instructs a media node on the network routing plan to split or mix an incoming data packet and instructs the media node where to send the mixed data packet or, if the data packet is split, where to send each of the sub-packets.

40. The method of Claim 35 wherein the network routing plan specifies an entry gateway node linking the first client device to the network via a first-mile connection and an exit gateway node linking the second client device to the network via a last-mile connection, and wherein none of the media nodes in the network other than the entry gateway node knows the address of the first client device and none of the media nodes in the network other than the exit gateway node knows the address of the second client device.

41. The method of Claim 35 comprising causing the first client device to scramble and/or encrypt the data packet and to transmit security credentials to the second client device, the security credentials enabling the second client device to unscramble and/or decrypt the data packet so as to recreate the data packet prior to the scrambling and/or encrypting by the first client device.

42. The method of Claim 41 wherein the security credentials are not sent to any media node in the network.

43. The method of Claim 1 comprising:

providing a first client device, the first client device being in communication with an entry gateway node in the network via a first mile connection;

providing a second client device, the second client device being in communication with an exit gateway node in the network via a last mile connection;

causing the first client device to transmit an address of the second client device to a third media node;

causing the third media node to develop a network routing plan defining the route of a data packet from the first client device to the second client device through the network; and

causing the third media node to send a command and control packet to media nodes designated in the network routing plan, each command and control packet informing a media node designated in the network routing plan where to send an incoming data packet identified by a specific identifying tag and what tag to apply to the data packet before sending the data packet to next media node in the network routing plan.

44. The method of Claim 43 wherein the third media node stores a network node list, the network node list comprising a list of active media nodes and client devices and the address of each of the active media nodes and client devices, the method comprising:

causing the first client device to initiate a communication with the second client device by transmitting to the third media node an identity of the second client device and a request for an address of the second client device; and

causing the third media node to pass the address of second client device to the first client device.

45. The method of Claim 43 wherein the third media node comprises an entry gateway node on the network routing plan.

46. A method of transmitting data packets securely from a first client device to a second client device through a cloud, the cloud comprising a network of media nodes, the media nodes being hosted on servers, each of the media nodes receiving data packets from other media nodes in the network and transmitting data packets to other media nodes in the network, the method comprising:

providing one or more signaling servers;

causing the first client device to transmit an address of the second client device to a signaling server;

causing the signaling server to develop a network routing plan defining the route of a data packet from the first client device to the second client device through the network; and

causing the signaling server to send a command and control packet to media nodes designated in the network routing plan, each command and control packet informing a media node designated in the network routing plan where to send an incoming data packet identified by a specific identifying tag and what tag to apply to the data packet before sending the data packet to next media node in the network routing plan.

47. The method of Claim 46 wherein the signaling server stores a network node list, the network node list comprising a list of active media nodes and client devices and the address of each of the active media nodes and client devices, the method comprising:

causing the first client device to initiate a communication with the second client device by transmitting to the signaling server an identity of the second client device and a request for an address of the second client device; and

causing the signaling server to pass the address of second client device to the first client device.

48. The method of Claim 47 wherein in developing a network routing plan the signaling server considers propagation delays between media nodes on the network node list in order to reduce a transit time of a data packet through the network.

49. The method of Claim 46 comprising:

providing one or more name servers, the one or more name servers storing a network node list, the network node list comprising a list of active media nodes and client devices and addresses of the active media nodes and client devices;

causing the first client device to initiate a communication with the second client device by transmitting to a name server an identity of the second client device and a request for an address of the second client device; and

causing the name server to pass the address of second client device to the first client device.

50. The method of Claim 46 wherein the network routing plan specifies an entry gateway node linking the first client device to the network via a first-mile connection and an exit gateway node linking the second client device to the network via a last-mile connection, and wherein none of the media nodes in the network other than the entry gateway node knows the

address of the first client device and none of the media nodes in the network other than the exit gateway node knows the address of the second client device.

51. A method of transmitting data packets securely from a first client device to a second client device through a cloud, the cloud comprising a network of media nodes, the media nodes being hosted on servers, each of the media nodes receiving data packets from other media nodes in the network and transmitting data packets to other media nodes in the network, the method comprising:

causing the first client device to transmit an address of the second client device to a first media node in the network;

causing the first media node to develop a network routing plan defining the route of a data packet from the first client device to the second client device through the network; and

causing the first media node to send a command and control packet to media nodes designated in the network routing plan, each command and control packet informing a media node designated in the network routing plan where to send an incoming data packet identified by a specific identifying tag and what tag to apply to the data packet before sending the data packet to next media node in the network routing plan.

52. The method of Claim 51 wherein the first media node stores a network node list, the network node list comprising a list of active media nodes and client devices and the address of each of the active media nodes and client devices, the method comprising:

causing the first client device to initiate a communication with the second client device by transmitting to the first media node an identity of the second client device and a request for an address of the second client device; and

causing the first media node to pass the address of second client device to the first client device.

53. The method of Claim 51 wherein the third media node comprises an entry gateway node on the network routing plan.

54. The method of Claim 51 wherein the network routing plan specifies an entry gateway node linking the first client device to the network via a first-mile connection and an exit gateway node linking the second client device to the network via a last-mile connection, and

wherein none of the media nodes in the network other than the entry gateway node knows the address of the first client device and none of the media nodes in the network other than the exit gateway node knows the address of the second client device.