CLAIMS

1. A method of transmitting packets containing digital data through a cloud, each of the packets comprising a plurality of data segments, the cloud comprising a network of undifferentiated metamorphic nodes, said nodes being hosted on servers or communication devices, the method comprising:

causing an undifferentiated metamorphic node to transform into a first task node;

causing said first task node to receive packets from other task nodes in the cloud;

causing said first task node, after receiving packets from other task nodes, to transmit packets to other task nodes in the cloud, whereby the packets transmitted by said first task node comprise at least a portion of data segments of packets previously received by said first task node;

causing said first task node to perform at least one of the following concealment methods:

scrambling an incoming packet by changing an order of the data segments in the incoming packet in accordance with a scrambling algorithm, said scrambling algorithm being created in accordance with a first state;

encrypting the incoming packet in accordance with an encryption algorithm and an encryption key, said encryption algorithm and said encryption key being created in accordance with said first state; and

causing said first task node to transform back into an undifferentiated metamorphic node after said first task node transmits said packets to said other task nodes.

2. The method of Claim 1 further comprising:

causing said first task node to both scramble and encrypt the incoming packet to produce an encrypted scrambled packet.

3. The method of Claim 2 further comprising:

causing said first task node to transmit the encrypted scrambled packet to a second task node;

causing the second task node to decrypt the encrypted scrambled packet using said algorithm and encryption key in accordance with said first state to recover the scrambled packet;

causing the second task node to encrypt the scrambled packet in accordance with an algorithm and encryption key created in accordance with a second state so as to produce a second encrypted scrambled packet;

causing the second task node to transmit the second encrypted scrambled packet to a third task node;

repeating in other task nodes the process of decrypting an incoming scrambled packet using a prior state to recover a scrambled packet and then re-encrypting the packet with a new state to generate a newly encrypted scrambled packet;

decrypting for a final time an incoming encrypted scrambled packet in a last task node using security credentials in accordance with a prior state in accordance with which the packet was encrypted to recover a scrambled packet; and

unscrambling the incoming packet in the last task node so as to recreate said packet prior to said scrambling in said first task node.

4. The method of Claim 2 wherein said scrambling algorithm is determined by a value of a state, a time, a geographic zone or a combination thereof.

5. The method of Claim 1 further comprising:

causing said first task node to perform a series of concealment operations on data in the packet, said concealment operations comprising scrambling, encryption, and insertion of junk data into the packet;

causing the first task node to transmit the packet on which said concealment operations have been performed to a second task node; and

causing the second task node to perform the inverse of said concealment operations on the packet, said inverse comprising descrambling, decryption, and removal of junk data and being performing in the reserve of the order in which said concealment operations were performed in the first task node,

wherein each of the concealment operations and the inverse of the concealment operations is performed in accordance with an algorithm, key or other security credential, said algorithm, key or other security credential being determined by a value of a state, a time at which said concealment operations were performed in said first task node, a geographic zone or a combination thereof.

6. The method of Claim 5 wherein the first task node accesses the algorithm, key or other security credential from a diffuse data cloud of disaggregated data.

7. The method of Claim 1 wherein a packet is routed through the cloud using the following sequence of steps:

a caller edge device provides an undifferentiated metamorphic node with an address of a callee edge device;

the metamorphic node transforms into an authority node;

the authority node develops a route for the packet through the cloud, the route comprising metamorphic nodes on the route, and informs each of metamorphic nodes on the route tasks to be performed in routing the packet through the cloud;

the authority node transforms back into an undifferentiated metamorphic node;

upon receiving the tasks to be performed from the authority node, each of the metamorphic nodes on the route transforms into a task node; and

after performing the tasks in routing the packet through the cloud, each of the task nodes transforms back into an undifferentiated metamorphic node.

8. The method of Claim 7 wherein a task node receives from the authority node no addresses of nodes on the route other than an address of a next node on the route.

9. The method of Claim 7 wherein, after a task node transforms back into an undifferentiated metamorphic node, no record of the tasks performed by the task node is retained in the undifferentiated metamorphic node into which the task node transforms.

10. The method of Claim 7 wherein, after the authority node transforms back into an undifferentiated metamorphic node, no record of nodes on the route is retained in the undifferentiated metamorphic node into which the authority node transforms.

11. The method of Claim 7 wherein the authority node develops a route for the packet through the cloud by using network propagation delay maps.

12. The method of Claim 7 wherein:

in developing a route for the packet through the cloud the authority node contacts an undifferentiated metamorphic node with a request for addresses of undifferentiated nodes on the route;

the undifferentiated metamorphic node contacted by the authority node transforms into a name server node;

the name server node obtains the requested addresses of undifferentiated metamorphic nodes on the route from a diffuse data cloud and delivers the requested addresses to the authority node; and

the name server node transforms back into an undifferentiated metamorphic node.

13. The method of Claim 7 wherein a client gateway node hosted on the caller edge device initiates a call or session using the following sequence of steps:

the client gateway node contacts an undifferentiated metamorphic node with a request for an address of the callee edge device;

the undifferentiated metamorphic node contacted by the client gateway node transforms into a name server node;

the name server node obtains the requested address of the callee edge device from a diffuse data cloud and delivers the requested address to the client gateway node; and

the name server node transforms back into an undifferentiated metamorphic node.

14. The method of Claim 13 wherein, after the name server node transforms back into an undifferentiated metamorphic node, no record of the addresses obtained by the name server node from the diffuse data cloud is retained in the undifferentiated metamorphic node into which the name server node transforms.

15. The method of Claim 7 wherein:

the caller edge device encrypts data in the packet in accordance with a cryptographic key;

the caller edge device transmits the cryptographic key used to encrypt the data in the packet to the callee edge device; and

the callee edge device uses the cryptographic key transmitted by the caller edge device to decrypt the data in the packet.

16. The method of Claim 1 further comprising:

causing said first task node to scramble an incoming packet by changing an order of the data segments in the packet in accordance with a first scrambling algorithm so as to produce a scrambled packet;

causing said first task node to split said scrambled packet into multiple scrambled packets;

causing said first task node to encrypt each of the multiple scrambled packets so as to produce multiple encrypted scrambled packets and to transmit the multiple encrypted scrambled packets to other task nodes; and

causing a final task node to receive encrypted scrambled packets, decrypt each the received encrypted scrambled packets so as to produce multiple received scrambled packets, and assemble the received scrambled packets thereby to recreate the scrambled packet produced in the first task node; and

causing the final task node to unscramble the scrambled packet produced in the first task node thereby to recover the incoming packet received by the first task node.

17. A method of routing data packets over a communication network, said communication network comprising a plurality of nodes, the method comprising:

subdividing data into one of the following categories:

data used to perform a name server function, said name server function comprising identifying device names and their corresponding dynamic addresses;

data used to perform an authority node function, said authority node function comprising developing routes of the data packets over a network of task nodes; and

data used to perform a task node function, said task node function comprising concealing the content of data packets using concealment algorithms;

providing the nodes with data needed to perform one of said name server function, said authority node function, or said task node function;

fragmenting each of the categories of data into files in accordance with an algorithm, said algorithm being based on a state such as time, wherein a key is required in order to defragment some or all of the files; and

causing a node to perform at least one of the following concealment methods:

scrambling an incoming packet by changing an order of the data segments in the incoming packet in accordance with a scrambling algorithm, said scrambling algorithm being created in accordance with a first state;

encrypting the incoming packet in accordance with an encryption algorithm and an encryption key, said encryption algorithm and said encryption key being created in accordance with said first state.

18. The method of claim 17 further comprising storing the fragmented data in multiple devices, no single device containing sufficient content to reconstruct the data prior to the fragmentation.

19. The method of Claim 17 wherein a gateway node in the network requests a destination address from the data used to perform a name server function.

20. The method of claim 17 wherein a gateway node delivers data used to perform a name server function to an authority node in order to enable the authority node to access data in a diffuse data cloud, including a table of node-to-node hop times.