What is claimed is:

1. An apparatus comprising:

a first logic to receive from a first node a synchronization portion of a message including the synchronization portion and a data portion, and to generate a set of state information using the synchronization portion, to synchronize the apparatus with the first node; and

a second logic to decrypt the data portion using the set of state information to obtain a decrypted message and to provide the decrypted message to a consuming logic of the apparatus, wherein the message is to be communicated from the first node via an open channel.

2. The apparatus of claim 1, further comprising:

third logic to encrypt a second unencrypted message, generated by the consuming logic, with the set of state information to generate a second encrypted message; and

a transmission logic to send a second message to a second node with a synchronization portion formed of at least a portion of the set of state information and a data portion formed of the second encrypted message.

3. The apparatus of claim 2, wherein the transmission logic is to send the second message to the second node via an open channel.

4. The apparatus of claim 2, wherein the third logic is to encrypt the second unencrypted message via an invertible non-linear function having a first input corresponding to the second unencrypted message and a second input corresponding to the set of state information.

5. The apparatus of claim 1, wherein the synchronization portion comprises a phase of a chaotic system and the set of state information comprises a complete state of the chaotic system.

6. The apparatus of claim 5, wherein the phase of the chaotic system comprises a linear combination of the complete chaotic system state.

7. The apparatus of claim 1, further comprising a plurality of nodes of a network having a substantially common chaotic system state.

8. The apparatus of claim 7, wherein the first logic is to perform a chaos-based synchronization of the network to generate the set of state information from the synchronization portion.

9. The apparatus of claim 8, wherein the chaos-based synchronization is to be performed according to a generalized Lorenz system.

10. The apparatus of claim 1, wherein the generated set of state information is at least substantially the same in the apparatus as a second set of state information used in the first node to encrypt the data portion of the message.

11. The apparatus of claim 10, wherein the generated set of state information and the second set of state information are derived without a secret key.

12. A method comprising:

receiving a message from a sender node in a receiver node;

parsing the message and sending a synchronization portion of the message to a chaotic system logic and sending an encrypted portion of the message to a decryption logic;

updating, in the chaotic system logic, synchronization of the receiver node using the synchronization portion, including calculating a state of a chaotic system based at least in part on the synchronization portion; and

decrypting, in the decryption logic, the encrypted portion using the state of the chaotic system.

13. The method of claim 12, further comprising decrypting the encrypted portion according to an inverted non-linear function using the chaotic system state.

14. The method of claim 12, further comprising:

encrypting, in an encryption logic, data using the chaotic system state to generate a second encrypted portion;

generating, in the chaotic system logic, a second synchronization portion using the chaotic system state; and

transmitting a second message from the receiver node, the second message including the second synchronization portion and the second encrypted portion.

15. The method of claim 14, further comprising encrypting the second encrypted portion according to a non-linear function using the chaotic system state.

16. The method of claim 14, further comprising generating the second synchronization portion according to a linear combination of at least a portion of the chaotic system state.

17. The method of claim 14, further comprising sending the second message via an open wireless channel to another node of the system, the system including the sender node and the receiver node.

18. An apparatus comprising means to perform a method as claimed in any one of claims 12 to 17.

19. A machine-readable storage medium including machine-readable instructions, when executed, to implement a method as claimed in any one of claims 12 to 17.

20. A system comprising:

a first node including a first means for receiving from a second node a synchronization portion of a first message including the synchronization portion and a data portion, and for generating a first set of state information of a chaotic system using the synchronization portion, and a second means for decrypting the data

portion using the first set of state information, wherein the first message is to be communicated from the second node via an open channel; and

the second node coupled to the first node, the second node including a function means for encrypting the data portion of the first message according to a function and using a second set of state information of the chaotic system, the second set of state information at least substantially equivalent to the first set of state information, and a transmission means for sending the first message to the first node with the synchronization portion formed of at least a portion of the second set of state information.

21. The system of claim 20, wherein the system comprises a wireless network of nodes including the first and second nodes.

22. The system of claim 21, wherein the wireless network comprises a body area network, the first and second nodes comprising sensors.

23. The system of claim 22, wherein the system comprises a sensor network having a plurality of sensors including the first and second nodes and a collection system to receive messages from the plurality of sensors, to generate a report therefrom, to encrypt the report, and to communicate the report to a central system, the central system external to the sensor network.

24. An apparatus comprising:

means for receiving a message from a sender node in a receiver node;

means for parsing the message into a synchronization portion and an encrypted portion;

means for updating synchronization of the receiver node using the synchronization portion, including means for calculating a state of a chaotic system based at least in part on the synchronization portion; and

decryption means for decrypting the encrypted portion using the state of the chaotic system.

25. The apparatus of claim 24, further comprising:

means for encrypting data using the chaotic system state to generate a second encrypted portion;

means for generating a second synchronization portion using the chaotic system state; and

means for transmitting a second message from the receiver node, the second message including the second synchronization portion and the second encrypted portion.

What is claimed is:

1. An apparatus comprising:

a first logic to receive from a first node a synchronization portion of a message including the synchronization portion and a data portion, and to generate a set of state information using the synchronization portion, to synchronize the apparatus with the first node; and

a second logic to decrypt the data portion using the set of state information to obtain a decrypted message and to provide the decrypted message to a consuming logic of the apparatus, wherein the message is to be communicated from the first node via an open channel.

2. The apparatus of claim 1, further comprising:

third logic to encrypt a second unencrypted message, generated by the consuming logic, with the set of state information to generate a second encrypted message; and

a transmission logic to send a second message to a second node with a synchronization portion formed of at least a portion of the set of state information and a data portion formed of the second encrypted message.

3. The apparatus of claim 2, wherein the transmission logic is to send the second message to the second node via an open channel.

4. The apparatus of claim 2, wherein the third logic is to encrypt the second unencrypted message via an invertible non-linear function having a first input corresponding to the second unencrypted message and a second input corresponding to the set of state information.

5. The apparatus of claim 1, wherein the synchronization portion comprises a phase of a chaotic system and the set of state information comprises a complete state of the chaotic system.

6. The apparatus of claim 5, wherein the phase of the chaotic system comprises a linear combination of the complete chaotic system state.

7. The apparatus of claim 1, further comprising a plurality of nodes of a network having a substantially common chaotic system state.

8. The apparatus of claim 7, wherein the first logic is to perform a chaos-based synchronization of the network to generate the set of state information from the synchronization portion.

9. The apparatus of claim 8, wherein the chaos-based synchronization is to be performed according to a generalized Lorenz system.

10. The apparatus of claim 1, wherein the generated set of state information is at least substantially the same in the apparatus as a second set of state information used in the first node to encrypt the data portion of the message.

11. The apparatus of claim 10, wherein the generated set of state information and the second set of state information are derived without a secret key.

12. At least one computer readable medium including instructions that when executed enable a system to:

receive a message from a sender node in a receiver node;

parse the message and send a synchronization portion of the message to a chaotic system logic and send an encrypted portion of the message to a decryption logic;

update, in the chaotic system logic, synchronization of the receiver node using the synchronization portion, including calculation of a state of a chaotic system based at least in part on the synchronization portion; and

decrypt, in the decryption logic, the encrypted portion using the state of the chaotic system.

13. The at least one computer readable medium of claim 12, further comprising instructions that when executed enable the system to decrypt the encrypted portion according to an inverted non-linear function using the chaotic system state.

14. The at least one computer readable medium of claim 12, further comprising instructions that when executed enable the system to:

encrypt, in an encryption logic, data using the chaotic system state to generate a second encrypted portion;

generate, in the chaotic system logic, a second synchronization portion using the chaotic system state; and

transmit a second message from the receiver node, the second message including the second synchronization portion and the second encrypted portion.

15. The at least one computer readable medium of claim 14, further comprising instructions that when executed enable the system to encrypt the second encrypted portion according to a non-linear function using the chaotic system state.

16. The at least one computer readable medium of claim 14, further comprising instructions that when executed enable the system to generate the second synchronization portion according to a linear combination of at least a portion of the chaotic system state.

17. The at least one computer readable medium of claim 14, further comprising instructions that when executed enable the system to send the second message via an open wireless channel to another node of the system, the system including the sender node and the receiver node.

18. A system comprising:

a first node including a first logic to receive from a second node a synchronization portion of a first message including the synchronization portion and a data portion, and to generate a first set of state information of a chaotic system using the synchronization portion, and a second logic to decrypt the data portion using the first set of state information, wherein the first message is to be communicated from the second node via an open channel; and

the second node coupled to the first node, the second node including a function engine to encrypt the data portion of the first message according to a function and using a second set of state information of the chaotic system, the second set of state information at least substantially equivalent to the first set of state information, and a transmission logic to send the first message to the first node with the synchronization portion formed of at least a portion of the second set of state information.

19. The system of claim 18, wherein the system comprises a wireless network of nodes including the first and second nodes.

20. The system of claim 19, wherein the wireless network comprises a body area network, the first and second nodes comprising sensors.

21. The system of claim 18, wherein the system comprises a sensor network having a plurality of sensors including the first and second nodes and a collection system to receive messages from the plurality of sensors, to generate a report therefrom, to encrypt the report, and to communicate the report to a central system, the central system external to the sensor network.