

SECURE OUT-OF-BAND SYMMETRIC ENCRYPTION KEY DELIVERY

FIELD

[0001] The present embodiments relate to the fields of cryptographic communication systems and cryptographic communication in networks.

BACKGROUND

[0002] Encryption and decryption are commonly used for cryptographic communication over various networks. Typical encrypted communication uses symmetric keys to encrypt and decrypt data between 2 points. These keys are typically derived from Diffie-Hellman negotiation at the beginning of the data exchange utilizing the same link. With enough computing power, eavesdropping on the data link would allow the attacker to deduct the symmetric keys from the exchange. So far this danger was strictly theoretical, but advent of quantum computers makes this brute-force attack vulnerability very real.

[0003] QKD (Quantum Key Distribution) systems are currently being developed to provide symmetric keys to both parties with strong physical guarantee from eavesdropping. Practical usage of QKD systems is currently inhibited by limitations regarding distance and the fact of only being able to work as a pair of devices (Alice/Bob) with no capabilities to expand the network to more than pairs of Alice/Bob.

SUMMARY

[0004] A method is disclosed for secure out-of-band symmetric encryption key delivery. A first trusted node in a network receives a request. The request is from a first one of a pair of user devices. The request is to deliver symmetric encryption keys to the pair of user devices. The first trusted node delivers a second one of the symmetric encryption keys to a second one of the pair of user devices. The symmetric encryption key is delivered via further trusted nodes in the network. The first trusted node receives confirmation from one of the further trusted nodes in the network. The confirmation is of delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices. The first trusted node delivers a first one of the symmetric encryption keys to the first one of the pair of user devices. This delivery is responsive to the confirmation of the delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices. In an aspect, there is provided a method for secure out-of-band symmetric encryption key delivery, comprising:

receiving, at a first trusted node in a network, a request from a first one of a pair of user devices to deliver symmetric encryption keys to the pair of user devices, the request to be

interpreted by the first trusted node as an instruction to generate the symmetric encryption keys in response to receiving the request, deliver one of the symmetric encryption keys to a second one of the pair of user devices in response to receiving the request, confirm delivery of the one of the symmetric encryption keys to the second one of the pair of user devices, and after confirming such delivery in response to receiving the request, deliver another one of the symmetric encryption keys to the first one of the pair of user devices;

generating, at the first trusted node, a first one and a second one of the symmetric encryption keys, in response to receiving the request, wherein neither the first one nor the second one of the pair of user devices has one of the symmetric encryption keys as a result of the generating prior to the deliveries;

delivering, from the first trusted node via the trusted nodes in the network, the second one of the symmetric encryption keys to the second one second one of the pair of user devices, in response to receiving the request;

receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of the delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices that was in response to the first trusted node receiving the request; and

delivering, from the first trusted node in the network, a first one of the symmetric encryption keys to the first one of the pair of user devices, responsive to the confirmation of the delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices that was in response to the first trusted node receiving the request. In an aspect, there is provided tangible, non-transitory, computer-readable media having instructions thereupon which, when executed by a processor, cause the processor to perform a method comprising:

receiving, at a first trusted node in a network, a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device, the request to be interpreted by the first trusted node as an instruction to generate the symmetric encryption keys in response to receiving the request, deliver one of the symmetric encryption keys to the second user device in response to receiving the request, confirm delivery of the one of the symmetric encryption keys to the second user device, and after confirming such delivery in response to receiving the request, deliver another one of the symmetric encryption keys to the first user device;

generating, at the first trusted node, a first and a second symmetric encryption key, in response to receiving the request, wherein neither the first nor the second device has one of

the symmetric encryption keys as a result of the generating prior to the deliveries of the symmetric encryption keys;

delivering, from the first trusted node via trusted nodes in the network, the second symmetric encryption key to the second user device, in response to receiving the request;

receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request; and

delivering, from the first trusted node in the network, the first symmetric encryption key, first and second symmetric encryption keys being symmetric to each other, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request. In an aspect, there is provided an apparatus for secure out-of-band symmetric encryption key delivery, comprising:

a plurality of nodes of a network to form trusted nodes in a peer-to-peer or mesh network; and

a first trusted node, of the trusted nodes, to:

receive a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device, the request to be interpreted by the first trusted node as an instruction to generate the symmetric encryption keys in response to receiving the request, deliver one of the symmetric encryption keys to the second user device in response to receiving the request, confirm delivery of the one of the symmetric encryption keys to the second user device, and after confirming such delivery in response to receiving the request, deliver another one of the symmetric encryption keys to the first user device;

generating, at the first trusted node, first and second symmetric encryption keys, in response to receiving the request, wherein neither the first user device nor the second user device devices has one of the symmetric encryption keys as a result of the generating prior to the deliveries;

deliver, from the first trusted node via the trusted nodes, the second symmetric encryption key to the second user device, in response to receiving the request;

receive, from one of the trusted nodes, confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request; and

deliver, from the first trusted node, a first symmetric encryption key that is symmetric to the second symmetric encryption key, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request.

[0005] A tangible, non-transitory, computer-readable media is disclosed. The media has instructions thereupon which, when executed by a processor, cause the processor to perform a method. A first trusted node in a network receives a request from a first user device. The

CLAIMS

~~What is claimed is:~~

- ~~1. A method for secure out-of-band symmetric encryption key delivery, comprising:
———receiving, at a first trusted node in a network, a request from a first one of a pair of user devices to deliver symmetric encryption keys to the pair of user devices;
———delivering, from the first trusted node via the trusted nodes in the network, a second one of the symmetric encryption keys to a second one of the pair of user devices;
———receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices; and
———delivering, from the first trusted node in the network, a first one of the symmetric encryption keys to the first one of the pair of user devices, responsive to the confirmation of the delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices.~~
- ~~2. The method of claim 1, wherein the first and second ones of the symmetric encryption keys are guaranteed by the trusted nodes to be delivered to only the first and second ones of the pair of user devices.~~
- ~~3. The method of claim 1, wherein the delivering the second one of the symmetric encryption keys comprises delivering the second one of the symmetric encryption keys through the network between nodes that are pre-configured to trust each other as trusted nodes.~~
- ~~4. The method of claim 1, wherein the trusted nodes in the network comprise nodes in a peer-to-peer or mesh network each in a one-to-one, one-to-many, or many-to-many configuration.~~
- ~~5. The method of claim 1, further comprising:
———performing just in time optimal pathfinding during delivery of the first and second ones of the symmetric encryption keys.~~
- ~~6. The method of claim 1, further comprising:
———performing just in time load balancing during delivery of the second one of the symmetric encryption keys.~~

~~7. The method of claim 1, further comprising:~~

~~———generating and delivering quantum keys to each of two or more trusted nodes in the network.~~

~~8. The method of claim 1, further comprising:~~

~~———encrypting each of one or more node to node transmissions with a quantum key, during delivery of the first and second ones of the symmetric encryption keys.~~

~~9. The method of claim 1, further comprising:~~

~~———performing just in time optimal pathfinding based on availability of quantum keys during delivery of the first and second ones of the symmetric encryption keys.~~

~~10. A tangible, non-transitory, computer-readable media having instructions thereupon which, when executed by a processor, cause the processor to perform a method comprising:~~

~~———receiving, at a first trusted node in a network, a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device;~~

~~———delivering, from the first trusted node via trusted nodes in the network, a second symmetric encryption key to the second user device;~~

~~———receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of delivery of the second symmetric encryption key to the second user device; and~~

~~———delivering, from the first trusted node in the network, a first symmetric encryption key, first and second symmetric encryption keys being symmetric to each other, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device.~~

~~11. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:~~

~~———preconfiguring nodes in the network to trust each other as trusted nodes in a mesh network or peer-to-peer network.~~

~~12. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:~~

~~———performing just in time optimal pathfinding in the network.~~

~~13. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:~~

~~———performing just in time load balancing in the network.~~

~~14. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:~~

~~———generating quantum keys in two or more neighboring trusted nodes; and~~

~~———encrypting and decrypting the first or the second symmetric encryption key, using the quantum keys.~~

~~15. An apparatus for secure out of band symmetric encryption key delivery, comprising:~~

~~a plurality of nodes of a network to form trusted nodes in a peer-to-peer or mesh network;
and~~

~~a first trusted node, of the trusted nodes, to:~~

~~———receive a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device;~~

~~———deliver, from the first trusted node via the trusted nodes, a second symmetric encryption key to the second user device;~~

~~———receive, from one of the trusted nodes, confirmation of delivery of the second symmetric encryption key to the second user device; and~~

~~———deliver, from the first trusted node, a first symmetric encryption key that is symmetric to the second symmetric encryption key, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device.~~

~~16. The apparatus of claim 15, wherein the trusted nodes are further to:~~

~~———perform just in time optimal pathfinding in the peer-to-peer or mesh network.~~

~~17. The apparatus of claim 15, wherein the trusted nodes are further to:~~

~~———perform just in time load balancing in the network.~~

~~18. The apparatus of claim 15, wherein the trusted nodes are further to:~~

~~———generate quantum keys in two or more neighboring trusted nodes; and~~

~~———encrypt and decrypt the first or the second symmetric encryption key during delivery, using the quantum keys.~~

~~19. The apparatus of claim 15, wherein the trusted nodes are further to:~~
~~———use encryption and decryption with quantum keys, for each node to node transmission during delivery of the first and second symmetric encryption keys.~~

~~20. The apparatus of claim 15, wherein the trusted nodes are further to:~~
~~———perform just in time optimal pathfinding based on availability of quantum keys during delivery of the first and second symmetric encryption keys.~~

CLAIMS

1. A method for secure out-of-band symmetric encryption key delivery, comprising:
receiving, at a first trusted node in a network, a request from a first one of a pair of user
devices to deliver symmetric encryption keys to the pair of user devices, the request to be
interpreted by the first trusted node as an instruction to generate the symmetric encryption
keys in response to receiving the request, deliver one of the symmetric encryption keys to a
second one of the pair of user devices in response to receiving the request, confirm delivery of
the one of the symmetric encryption keys to the second one of the pair of user devices, and
after confirming such delivery in response to receiving the request, deliver another one of the
symmetric encryption keys to the first one of the pair of user devices;
generating, at the first trusted node, a first one and a second one of the symmetric
encryption keys, in response to receiving the request, wherein neither the first one nor the
second one of the pair of user devices has one of the symmetric encryption keys as a result of
the generating prior to the deliveries;
delivering, from the first trusted node via the trusted nodes in the network, the second
one of the symmetric encryption keys to the second one second one of the pair of user devices,
in response to receiving the request;
receiving, at the first trusted node, from one of the trusted nodes in the network,
confirmation of the delivery of the second one of the symmetric encryption keys to the second
one of the pair of user devices that was in response to the first trusted node receiving the
request; and
delivering, from the first trusted node in the network, a first one of the symmetric encryption
keys to the first one of the pair of user devices, responsive to the confirmation of the delivery
of the second one of the symmetric encryption keys to the second one of the pair of user
devices that was in response to the first trusted node receiving the request.
2. The method of claim 1, wherein the first and second ones of the symmetric encryption
keys are guaranteed by the trusted nodes to be delivered to only the first and second ones of
the pair of user devices.

3. The method of claim 1, wherein the delivering the second one of the symmetric encryption keys comprises delivering the second one of the symmetric encryption keys through the network between nodes that are pre-configured to trust each other as trusted nodes.
4. The method of claim 1, wherein the trusted nodes in the network comprise nodes in a peer-to-peer or mesh network each in a one-to-one, one-to-many, or many-to-many configuration.
5. The method of claim 1, further comprising:
performing just-in-time optimal pathfinding during delivery of the first and second ones of the symmetric encryption keys.
6. The method of claim 1, further comprising:
performing just-in-time load-balancing during delivery of the second one of the symmetric encryption keys.
7. The method of claim 1, further comprising:
generating and delivering quantum keys to each of two or more trusted nodes in the network.
8. The method of claim 1, further comprising:
encrypting each of one or more node to node transmissions with a quantum key, during delivery of the first and second ones of the symmetric encryption keys.
9. The method of claim 1, further comprising:
performing just-in-time optimal pathfinding based on availability of quantum keys during delivery of the first and second ones of the symmetric encryption keys.
10. A tangible, non-transitory, computer-readable media having instructions thereupon which, when executed by a processor, cause the processor to perform a method comprising:
receiving, at a first trusted node in a network, a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device, the request to be interpreted by the first trusted node as an instruction to generate the symmetric

encryption keys in response to receiving the request, deliver one of the symmetric encryption keys to the second user device in response to receiving the request, confirm delivery of the one of the symmetric encryption keys to the second user device, and after confirming such delivery in response to receiving the request, deliver another one of the symmetric encryption keys to the first user device;

generating, at the first trusted node, a first and a second symmetric encryption key, in response to receiving the request, wherein neither the first nor the second device has one of the symmetric encryption keys as a result of the generating prior to the deliveries of the symmetric encryption keys;

delivering, from the first trusted node via trusted nodes in the network, the second symmetric encryption key to the second user device, in response to receiving the request;

receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request; and

delivering, from the first trusted node in the network, the first symmetric encryption key, first and second symmetric encryption keys being symmetric to each other, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request.

11. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:

preconfiguring nodes in the network to trust each other as trusted nodes in a mesh network or peer-to-peer network.

12. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:

performing just-in-time optimal pathfinding in the network.

13. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:

performing just-in-time load-balancing in the network.

14. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:
- generating quantum keys in two or more neighboring trusted nodes; and
- encrypting and decrypting the first or the second symmetric encryption key, using the quantum keys.
15. An apparatus for secure out-of-band symmetric encryption key delivery, comprising:
- a plurality of nodes of a network to form trusted nodes in a peer-to-peer or mesh network; and
- a first trusted node, of the trusted nodes, to:
- receive a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device, the request to be interpreted by the first trusted node as an instruction to generate the symmetric encryption keys in response to receiving the request, deliver one of the symmetric encryption keys to the second user device in response to receiving the request, confirm delivery of the one of the symmetric encryption keys to the second user device, and after confirming such delivery in response to receiving the request, deliver another one of the symmetric encryption keys to the first user device;
- generating, at the first trusted node, first and second symmetric encryption keys, in response to receiving the request, wherein neither the first user device nor the second user device devices has one of the symmetric encryption keys as a result of the generating prior to the deliveries;
- deliver, from the first trusted node via the trusted nodes, the second symmetric encryption key to the second user device, in response to receiving the request;
- receive, from one of the trusted nodes, confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request; and
- deliver, from the first trusted node, a first symmetric encryption key that is symmetric to the second symmetric encryption key, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device that was in response to the first trusted node receiving the request.
16. The apparatus of claim 15, wherein the trusted nodes are further to:

perform just-in-time optimal pathfinding in the peer-to-peer or mesh network.

17. The apparatus of claim 15, wherein the trusted nodes are further to:

perform just-in-time load-balancing in the network.

18. The apparatus of claim 15, wherein the trusted nodes are further to:

generate quantum keys in two or more neighboring trusted nodes; and

encrypt and decrypt the first or the second symmetric encryption key during delivery,
using the quantum keys.

19. The apparatus of claim 15, wherein the trusted nodes are further to:

use encryption and decryption with quantum keys, for each node to node transmission
during delivery of the first and second symmetric encryption keys.

20. The apparatus of claim 15, wherein the trusted nodes are further to:

perform just-in-time optimal pathfinding based on availability of quantum keys during
delivery of the first and second symmetric encryption keys.

