

CLAIMS

WHAT IS CLAIMED IS:

1. A method of securely providing a trusted time comprising:
receiving at a network interface controller (NIC) a neighbor list comprising a plurality of entries for a corresponding plurality of neighbor devices wherein each of the plurality of entries comprises:
a unique device identity of a time server which the plurality of neighbor devices has reached; and
an inception time of a time server certificate corresponding to the unique device identity;
sorting the plurality of entries within the neighbor list to obtain a sorted neighbor list; and
sending a time request to a first neighbor device of the plurality of neighbor devices based at least in part on the sorted neighbor list.
2. The method of claim 1, further comprising determining a minimum time to at least temporarily validate time for the NIC, the minimum time being determined by:
obtaining the minimum time from a local storage of the first device based at least in part on the first device having no time;
identifying, for each of a plurality of certificates, a largest inception time; and
setting the minimum time based at least in part on a first certificate being available.

3. The method of claim 2, further comprising:

- receiving, at the first device, a time response from the first neighbor device;
- performing a preliminary check on the time response;
- determining whether the certificate exists in a local storage of the first device;
- requesting the certificate from the first neighbor device based at least in part on the certificate not existing in the local storage of the first device;
- determining whether the certificate is received from the first neighbor device;
- blacklisting the first neighbor device based at least in part on the certificate not being received from the first neighbor device;
- validating the time based at least in part on the certificate being received from the first neighbor device; and
- validating the time based at least in part on the certificate existing in the local storage of the first device.

4. The method of claim 1, wherein the sorting of the plurality of entries within the neighbor list to obtain the sorted neighbor list comprises:

- identifying a new link to be added to the sorted neighbor list, the new link comprising:
 - a route to the time server; and
 - a first cost value of the route;
- setting a current position of the new link at a start of the sorted neighbor list;
- determining if an end of the sorted neighbor list has been reached;

inserting the new link into the current position in the sorted neighbor list based at least in part on the end of the neighbor list having been reached; and

based at least in part on the end of the sorted neighbor list having not been reached:

determining whether the first cost value for the new link is greater than or less than a second cost value for a second link associated with the current position;

setting the current position of the second link to be a next item in the sorted neighbor list based at least in part on the first cost value for the new link being greater than the second cost value for the second link associated with the current position; and

inserting the new link into the current position in the sorted neighbor list based at least in part on the first cost value for the new link being less than the second cost value for the second link associated with the current position.

5. The method of claim 4, further comprising:

determining that both the new link and the second link are unsecure links; and

based at least in part on both the new link and the second link are the unsecure links:

determining whether a first trust value associated with the new link is greater than or less than a second trust value associated with the second link;

setting the current position of the second link to be the next item in the sorted neighbor list based at least in part on the first trust value associated with the new link being less than the second trust value associated with the second link; and

inserting the new link into the current position in the sorted neighbor list based at least in part on the first trust value associated with the new link being greater than the second trust value associated with the second link.

6. The method of claim 5, further comprising:

determining that the first trust value associated with the new link is equal to the second trust value associated with the second link;

determining whether the first cost value associated with the new link is greater than or less than the second cost value associated with the second link;

setting the current position of the second link to be the next item in the sorted neighbor list based at least in part on the first cost value associated with the new link being less than the second cost value associated with the second link; and

inserting the new link into the current position in the sorted neighbor list based at least in part on the first cost value associated with the new link being greater than the second cost value associated with the second link.

7. The method of claim 6, wherein the first trust value and the second trust value include a value of:

a first value if no customer certificates are associated with the new link or the second link, respectively;

a second value if an expired customer certificate that is based on a minimum time is associated with the new link or the second link, respectively; and

a third value if the customer certificates associated with the new link or the second link, respectively, passed a minimum time validation check.

8. The method of claim 1, wherein sending the time request to the first neighbor device of the plurality of neighbor devices based at least in part on the sorted neighbor list comprises:

- selecting the first neighbor device at a top of the sorted neighbor list;
- moving the first neighbor device to a blacklist; and
- sending a first challenge with the time request.

9. A non-transitory computer-readable medium storing instructions that, when executed, cause a processor to perform operations, comprising:

- receiving at a network interface controller (NIC) of a first device a neighbor list comprising a plurality of entries for a corresponding plurality of neighbor devices wherein each of the plurality of entries comprises:

- a unique device identity of a time server which the plurality of neighbor devices has reached; and

- an inception time of a time server certificate corresponding to the unique device identity;

- sorting the plurality of entries within the neighbor list to obtain a sorted neighbor list; and

- sending a time request to a first neighbor device of the plurality of neighbor devices based at least in part on the sorted neighbor list.

10. The non-transitory computer-readable medium of claim 9, the operations further comprising determining a minimum time, the minimum time being determined by:

- determining whether the first device has a time;
- obtaining the minimum time from a local storage of the first device based at least in part on the first device having no time;
- identifying, for each of a plurality of certificates, a largest inception time;
- determining if a first certificate is available;
- retrieving the first certificate based at least in part on the first certificate being unavailable;
- determining if the retrieving is successful;
- removing the first certificate from the neighbor list based at least in part on the retrieving being unsuccessful;
- setting the minimum time based at least in part on the retrieving being successful;

and

- setting the minimum time based at least in part on the first certificate being available.

11. The non-transitory computer-readable medium of claim 10, the operations further comprising:

- receiving, at the first device, a time response from the first neighbor device;
- performing a preliminary check on the time response;
- determining whether the certificate exists in a local storage of the first device;

requesting the certificate from the first neighbor device based at least in part on the certificate not existing in the local storage of the first device;

determining whether the certificate is received from the first neighbor device;

blacklisting the first neighbor device based at least in part on the certificate not being received from the first neighbor device;

validating the time based at least in part on the certificate being received from the first neighbor device; and

validating the time based at least in part on the certificate existing in the local storage of the first device.

12. The non-transitory computer-readable medium of claim 9, wherein sorting the plurality of entries within the neighbor list to obtain the sorted neighbor list comprises performing a bubble sort or a quick sort of the plurality of entries, and wherein the sorting is based at least in part on one or more factors including a cost of a secure route to the time server, a trust value associated with a new link, a second trust value associated with a second link, a cost of a pending route, or combinations thereof.

13. The non-transitory computer-readable medium of claim 9, wherein the time server certificate is unique to one of a plurality of time servers.

14. The non-transitory computer-readable medium of claim 9, wherein the time server certificate is derived from a customer certificate authority.

15. The non-transitory computer-readable medium of claim 9, the operations further comprising storing the sorted neighbor list on the NIC.

16. The non-transitory computer-readable medium of claim 9, wherein sending the time request to the first neighbor device of the plurality of neighbor devices based at least in part on the sorted neighbor list comprises:

- selecting the first neighbor device at a top of the sorted neighbor list;
- moving the first neighbor device to a blacklist; and
- sending a first challenge with the time request.