WE CLAIM

1. A method for determining trustworthiness of individual nodes in distributed computing systems, the said method is characterized by considering the malicious behavior of the individual nodes as a trustworthiness parameter, wherein the said trustworthiness of individual nodes is determined by the computer implemented steps of:

   a. forwarding at least one data packet by first node to its neighboring second node;
   b. monitoring the next-hop delivery of forwarded data packet by second node to third node by the first node;
   c. computing the forwarding index of the second node using the monitored next-hop delivery by the first node;
   d. finding the individual confidence level of second node using forwarding index of the second node over the average time period by the first node;
   e. observing the forwarding trend of the second node and updating the individual confidence level of second node by the first node for determining long-term trustworthiness of individual nodes in distributed computing systems.

2. A method as claimed in claim 1, wherein the first node forwards the subsequent data packet to other than the second node if it is determined that data packet are not next-hop delivered to the third node by the second node.

3. A method as claimed in claim 1, wherein the first node broadcasts the confidence level of the second node to all neighboring nodes.

4. A method as claimed in claim 1, wherein the first node receives broadcast of the confidence level of the second node from all neighboring nodes.

5. A method as claimed in claim 4, wherein the first node dynamically updates the confidence level of second node after receiving broadcast of the confidence level of the second node from all the other neighboring nodes.

6. A method as claimed in claim 5, wherein the first node stores the dynamically updated confidence level of its neighboring second node in a scalar matrix.

7. A method as claimed in claim 6, wherein the scalar matrix of the first node comprises the confidence level value of the second node which is grater than zero and less than one.

8. A method as claimed in claim 1, further classifies the trustworthiness of individual nodes in distributed computing systems for distinguishing between malicious node, defective node and accuser node.

9. A method as claimed in claim 1, wherein long-term evaluation of trustworthiness of individual nodes in distributed computing systems eliminates the transient characteristics of short-term trustworthiness computation.

10. A method as claimed in claim 1, wherein distributed computing systems are wireless sensor networks (WSN).

11. A method as claimed in claim 1, wherein the trustworthiness determination is applicable to each node in distributed computing system.

12. A system for determining trustworthiness of individual nodes in distributed computing systems, the said system characterized by considering the malicious behaviors of the individual nodes as a trustworthiness parameter, wherein the said trustworthiness of individual nodes is determined by:

   a. means for forwarding at least one data packet by first node to its neighboring second node;

b. means for monitoring the next-hop delivery of forwarded data packet by second node to third node by the first node;
c. means for computing the forwarding index of the second node using the monitored next-hop delivery by the first node;
d. means for finding the individual confidence level of second node using forwarding index of the second node over the average time period by the first node;
e. means for observing the forwarding trend of the second node and updating the individual confidence level of second node by the first node for determining long-term trustworthiness of individual nodes in distributed computing systems.

13. A system as claimed in claim 12, wherein the first node forward the subsequent data packet to other than the second node if it is determined that data packet are not next-hop delivered to the third node by the second node.

14. A system as claimed in claim 12, wherein the first node broadcasts the confidence level of the second node to all neighboring nodes.

15. A system as claimed in claim 12, wherein the first node receives broadcast of the confidence level of the second node from all neighboring nodes.

16. A system as claimed in claim 15, wherein the first node dynamically updates the confidence level of second node after receiving broadcast of the confidence level of the second node from all the other neighboring nodes.

17. A system as claimed in claim 16, wherein the first node stores the dynamically updated confidence level of its neighboring second node in a scalar matrix.

18. A system as claimed in claim 17, wherein the scalar matrix of the first node comprises the confidence level value of the second node which is grater than zero and less than one.

19. A system as claimed in claim 12, further classifies the trustworthiness of individual nodes in distributed computing systems for distinguishing between malicious node, defective node and accuser node.

20. A system as claimed in claim 12, wherein long-term evaluation of trustworthiness of individual nodes in distributed computing systems eliminates the transient characteristics of short-term trustworthiness computation.

21. A system as claimed in claim 12, wherein distributed computing systems are wireless sensor networks (WSN).

22. A system as claimed in claim 12, wherein the trustworthiness determination is applicable to each node in distributed computing system.

Claims

1. A method for determining reliability of a node in a distributed computing system, the method characterized by:

forwarding data packets from a first node to a second node;

monitoring a next-hop delivery of the data packets from the second node to a third node, wherein the monitoring is performed by the first node;

computing a forwarding index of the second node based on the monitoring, wherein the forwarding index is computed by the first node based upon a number of the data packets requested to be forwarded from the second node to the third node and a number of the data packets actually forwarded by the second node to the third node;

finding an individual confidence level of the second node, wherein the individual confidence level is computed by the first node by dividing a summation of number of the data packets requested to be forwarded over an average time period and a summation of the number of the data packets actually forwarded over the average time period by the second node;

checking a forwarding trend of the second node to the third node based on the forwarding index;

updating dynamically the individual confidence level of the second node by the first node based on the forwarding trend; and

determining a trust value of the node based on a threshold confidence level and the individual confidence level by the first node, wherein the trust value is indicative of the reliability of the node in the distributed computing system.

2. The method as claimed in claim 1, further comprising forwarding at least one data packet to another node other than the second node.

3. The method as claimed in claim 1, further comprising broadcasting the individual confidence level of the second node to one or more neighboring nodes by the first node other than the second node.

4. The method as claimed in claim 1, further comprising receiving a broadcast of another confidence level of the second node from one or more neighboring nodes by the first node.

5. The method as claimed in claim 4, further comprising updating dynamically the individual confidence level of the second node after receiving the broadcast of the another confidence level of the second node from the one or more neighboring nodes of the first node.

6. The method as claimed in claim 5, wherein the first node computes and stores the dynamically updated confidence level of the second node in a scalar matrix.

7. The method as claimed in claim 6, wherein the scalar matrix of the first node comprises the individual confidence level value of the second node as a number greater than zero and less than one.

8. The method as claimed in claim 1, further comprising classifying the reliability of the nodes in the distributed computing system, wherein the nodes are classifies as: a malicious node, a defective node and an accuser node.

9. The method as claimed in claim 1, wherein distributed computing system isa wireless sensor networks (WSN).

10. A system for determining reliability of anode in a distributed computing system, the system characterized by:

a processor; and

a memory disposed in communication with the processor and storing processor-executable instructions, the instructions comprising instructions for:

forwarding data packetsfrom afirst node to asecond node;

monitoring anext-hop delivery of thedata packet from thesecond node to a third node, wherein the monitoring is performed by the first node;

computing a forwarding index of the second node based on the monitoring, wherein the forwarding index is computed by the first node based on a number of the data packets requested to be forwarded from the second node to the third node and a number of the data packets actually forwarded by the second node to the third node;

finding an individual confidence level of the second node, wherein the individual confidence level is computed by the first node by dividing a summation of number of the data packets requested to be forwarded over an average time period and a summation of the number of the data packets actually forwarded over the average time period by the second node;

checking a forwarding trend of the second node to the third node based on the forwarding index;

updating dynamically the individual confidence level of the second node by the first node based on the forwarding trend; and

determining a trust value of the node based on a threshold confidence level and the individual confidence level by the first node, wherein the trust value is indicative of the reliability of the node in the distributed computing system.

11. Thesystem as claimed in claim 10, wherein the instructions further comprises instructions for: forwarding at least one data packet to another node other than the second node.

12. The system as claimed in claim 10, wherein the instructions further comprises instructions for broadcasting the individual confidence level of the second node to one or more neighboring nodes by the first node other than the second node.

13. The system as claimed in claim 10, wherein the instructions further comprises instructions for receiving a broadcast of another confidence level of the second node from one or more neighboring nodes by the first node.

14. The system as claimed in claim 13, wherein the first node dynamically updates the individual confidence level of the second node after receiving the broadcast of the another confidence level of the second node from the one or more neighboring nodes.

15. The system as claimed in claim 14, wherein the first node computes and stores the dynamically updated confidence level of the second node in a scalar matrix.

16. The system as claimed in claim 15, wherein the scalar matrix of the first node comprises the individual confidence level value of the second node as a number greater than zero and less than one.

17. The system as claimed in claim 10, wherein the instructions further comprises instructions forclassifying the reliabilityof thenodes in the distributed computing system, wherein the nodes are classified as: a malicious node, a defective node and an accuser node.

18. The system as claimed in claim 10, wherein the distributed computing system is a wireless sensor network (WSN).