WHAT IS CLAIMED IS:

1. A network computing system, comprising:

a network adapter that transmits and receives data via a transport protocol;

a memory device that at least temporarily stores data received at the network adapter;

a processor that processes at least some of the received data, including:

applying one or more transport protocol heuristics to selective acknowledgement (SACK) messages received at the network adapter from a network node, the transport protocol heuristics identifying one or more threshold values for operational functions that are performed when processing the SACK messages;

determining, by applying the one or more transport protocol heuristics to the SACK messages received from the network node, that at least one of the one or more threshold values for one or more of the transport protocol heuristics have been reached, wherein the determining further includes determining that the network node is attempting to acknowledge a plurality of send attempts to increase the size of a sendmap; and

in response to determining that at least one of the one or more threshold values have been reached:

identifying the network node as a security threat; and

taking one or more remedial actions to mitigate the security threat associated with the identified network node.

2. The network computing system of claim 1, wherein applying the one or more transport protocol heuristics to the SACK messages includes incrementing one or more counters associated with the operational functions as the SACK messages are processed.

3. The network computing system of claim 2, wherein the counters indicate when at least one of the one or more threshold values for one or more of the transport protocol heuristics have been reached.

4. The network computing system of claim 2, wherein one or more of the counters are modified upon receiving an acknowledgement (ACK) message.

5. The network computing system of claim 1, wherein the security threat comprises an attacking node that is carrying out an attack against the network computing system.

6. The network computing system of claim 1, wherein at least one of the one or more remedial actions used to mitigate the security threat comprises ignoring at least some of the SACK messages received from the network node.

7. The network computing system of claim 1, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages comprises an indication of whether an ACK position is to be moved within the sendmap.

8. The network computing system of claim 7, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages comprises a measurement of how far the ACK position is to be moved within the sendmap.

9. The network computing system of claim 1, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages comprises an indication of how many SACK messages are received within a specified time period.

10. The network computing system of claim 1, further comprising filtering the SACK messages to remove previously received SACK messages.

11. The network computing system of claim 10, wherein filtering the SACK messages further comprises removing duplicate SACK messages.

12. The network computing system of claim 10, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages comprises an indication of how many SACK messages were filtered within a specified time period.

13. A computer-implemented method, comprising:

applying one or more transport protocol heuristics to selective acknowledgement (SACK) messages received at a network adapter from a network node, the transport protocol heuristics identifying one or more threshold values for operational functions that are performed when processing the SACK messages;

determining, by applying the one or more transport protocol heuristics to the SACK messages received from the network node, that at least one of the one or more threshold values for one or more of the transport protocol heuristics have been reached, wherein the determining further includes determining that the network node is attempting to acknowledge a plurality of send attempts to increase the size of a sendmap; and

in response to determining that at least one of the one or more threshold values have been reached:

identifying the network node as a security threat; and

taking one or more remedial actions to mitigate the security threat associated with the identified network node.

14. The computer-implemented method of claim 13, wherein applying the one or more transport protocol heuristics to the SACK messages includes incrementing one or more counters associated with the operational functions as the SACK messages are processed.

15. The computer-implemented method of claim 14, further comprising adding a decay factor to the sendmap to reduce one or more counters associated with ACK or SACK messages.

16. The computer-implemented method of claim 15, wherein the network node is identified as a security threat while the ACK or SACK messages are being removed.

17. The computer-implemented method of claim 16, wherein upon determining that at least one of the one or more threshold values are no longer met by the network node, the network node is subsequently removed from being classified as a security threat.

18. The computer-implemented method of claim 13, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages is dynamically changed based on one or more current operating conditions at the network computing system.

19. The computer-implemented method of claim 13, wherein at least one of the one or more threshold values for operational functions that are performed when processing the SACK messages is dynamically changed based on the occurrence of a specified trigger.

20. A non-transitory computer-readable medium comprising one or more computer-executable instructions that, when executed by at least one processor of a computing device, cause the computing device to perform the method of any one of claims 13-19.