

CLAIMS

What is claimed is:

- 5 1. A method of characterising a programmable logic controller (PLC) in a networked control system using at least one processor, the networked control system comprising a plurality of programmable logic controllers (PLCs), including the PLC, and a communication network layer based on which the plurality of PLCs communicate with each other, the method comprising:
- 10 obtaining network traffic data from the communication network layer;
determining scan cycle related timing profile information associated with the PLC based on the network traffic data obtained; and
generating characterising information associated with the PLC based on the determined scan cycle related timing profile information for characterising the PLC.
- 15 2. The method according to claim 1, wherein the scan cycle related timing profile information associated with the PLC comprises timing information associated with a series of request messages indicated as sent by the PLC to the communication network layer in the network traffic data obtained.
- 20 3. The method according to claim 2, wherein the timing information associated with the series of request messages indicated as sent by the PLC is inter message timing information associated with the series of request messages indicated as sent by the PLC.
- 25 4. The method according to claim 2 or 3, further comprising introducing a time delay to each of a plurality of request messages sent by the PLC.
5. The method according to claim 4, wherein the time delay is a predetermined time delay.
- 30 6. The method according to claim 5, wherein the time delay is a random time delay.
7. The method according to claim 6, wherein the random time delay is determined based on a clock of the PLC.

8. The method according to any one of claims 2 to 7, wherein said generating characterising information associated with the PLC comprises extracting one or more time and/or frequency domain features from the timing information associated with the series of
5 request messages indicated as sent by the PLC, wherein the characterising information comprises the extracted one or more time and/or frequency domain features.
9. The method according to claim 8, wherein the extracted one or more time and/or frequency domain features is one or more time and frequency domain features.
10
10. The method according to claim 8 or 9, wherein the set of request messages has a sample size in a range of 30 to 500.
11. The method according to any one of claims 8 to 10, wherein
15 the PLC is configured to recursively perform a scan cycle comprising an input reading stage, a control logic execution stage, and an output writing stage, and request messages sent by the PLC are sent at the control logic execution stage.
12. The method according to claim 11, wherein the plurality of PLCs are configured to
20 communicate with each other based on a request-response model.
13. The method according to any one of claims 8 to 12, further comprising:
labeling the extracted one or more time and/or frequency domain features of the characterising information with an identity information of the PLC to produce labeled features
25 associated with the PLC; and
training a machine learning model based on the labeled features associated with the PLC to produce a PLC classifier configured for PLC identification.
14. A programmable logic controller (PLC) characterising system for characterising a PLC
30 in a networked control system, the networked control system comprising a plurality of programmable logic controllers (PLCs), including the PLC, and a communication network layer based on which the plurality of PLCs communicate with each other, the PLC characterising system comprising:

a memory; and

at least one processor communicatively coupled to the memory and configured to perform the method of characterising the PLC in the networked control system according to any one of claims 1 to 12.

5

15. A method of attack detection in a networked control system using at least one processor, the networked control system comprising a plurality of programmable logic controllers (PLCs) and a communication network layer based on which the plurality of PLCs to communicate with each other, the method comprising:

10

obtaining second network traffic data from the communication network layer;

determining second scan cycle related timing profile information associated with a programmable logic controller (PLC) of the plurality of PLCs based on the second network traffic data obtained;

15

generating second characterising information associated with the PLC based on the determined second scan cycle related timing profile information; and

detecting whether the networked control system is subject to an attack in relation to the PLC based on the second characterising information associated with the PLC and reference characterising information associated with the PLC.

20

16. The method according to claim 15, wherein the reference characterising information associated with the PLC is characterising information generated according to the method of any one of claims 1 to 12.

25

17. The method according to claim 15 or 16, wherein the second scan cycle related timing profile information associated with the PLC comprises second timing information associated with a second series of request messages indicated as sent by the PLC to the communication network layer in the second network traffic data obtained.

30

18. The method according to claim 17, wherein the second timing information associated with the second series of request messages sent by the PLC is inter message timing information associated with the second series of request messages indicated as sent by the PLC.

19. The method according to claim 17 or 18, further comprising introducing a time delay to each of a second plurality of request messages sent by the PLC.
20. The method according to claim 19, wherein the time delay is a predetermined time
5 delay.
21. The method according to claim 20, wherein the time delay is a random time delay.
22. The method according to claim 21, wherein the random time delay is determined based
10 on a clock of the PLC.
23. The method according to any one of claims 17 to 22, wherein said generating second characterising information associated with the PLC comprises extracting one or more second time and/or frequency domain features from the second timing information associated with the
15 second series of request messages indicated as sent by the PLC, wherein the second characterising information comprises the extracted one or more second time and/or frequency domain features.
24. The method according to claim 23, wherein the extracted one or more second time
20 and/or frequency domain features is one or more time and frequency domain features.
25. The method according to claim 23 or 24, wherein the second series of request messages has a sample size in a range of 30 to 500.
- 25 26. The method according to any one of claims 23 to 25, wherein
the PLC is configured to recursively perform a scan cycle comprising an input reading stage, a control logic execution stage, and an output writing stage, and
request messages sent by the PLC are sent at the control logic execution stage.
- 30 27. The method according to claim 26, wherein the plurality of PLCs are configured to communicate with each other based on a request-response model.
28. The method according to any one of claims 23 to 27, wherein

said detecting whether the networked control system is subject to an attack in relation to the PLC is based on the second characterising information associated with the PLC and the PLC classifier produced according to the method of claim 13.

5 29. The method according to claim 28, said detecting whether the networked control system is subject to an attack in relation to the PLC comprises:

producing, by the PLC classifier, a classification result based on the second characterising information associated with the PLC; and

10 determining whether the networked control system is subject to an attack in relation to the PLC based on the classification result from the PLC classifier.

30. An attack detection system for attack detection in a networked control system using at least one processor, the networked control system comprising a plurality of programmable logic controllers (PLCs) and a communication network layer based on which the plurality of PLCs
15 to communicate with each other, the attack detection system comprising:

a memory; and

at least one processor communicatively coupled to the memory and configured to perform the method of attack detection in the networked control system according to any one of claims 15 to 29.

20

31. A computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform the method of characterising a programmable logic controller (PLC) in a networked control system according to any one of claims 1 to 13.

25

32. A computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform the method of attack detection in a networked control system according to any one of claims 15 to 29.

30