CLAIMS

1. A network apparatus comprising:

a packet payload compressor (PPC) operable to:

receive a packet copied from a network, the packet comprising a source, destination, and a payload;

extract a value of a field comprised in the payload;

provide a computed value of the field based on the source and destination of the packet;

compare the extracted value and the computed value; and

compress the field if the extracted value is the same as the computed value, and

a traffic shaper operable to transmit a compressed packet comprising the compressed field.

2. The network apparatus in accordance with claim 1, wherein the computed value is determined responsive to data in a dataset that comprises a plurality of link identifiers (link IDs), each link ID associated with:

a packet source and a packet destination;

at least one field identifier; and

a compression category associated a field identifier of the at least one identifier.

3. The network apparatus in accordance with claim 2, wherein the compression category is associated with a rule for determining the computed value.

4. The network apparatus in accordance with claim 2, wherein the compression category is associated with a rule for how to compress the field.

5. The network apparatus in accordance with claim 2, wherein the PPC is operable to provide the computed value by:

extracting the copied packet's source and destination and the identifier of the field;

identifying the copied packet with a link ID that is associated in the dataset with the copied packet's source and destination;

assigning the field with a compression category associated in the dataset with the link ID and field identifier; and

generating the computed field value with a function associated with the compression category.

6. The network apparatus in accordance with claim 5, wherein the function generates a same value each time a new packet identified with the link ID is received by the PPC.

7. The network apparatus in accordance with claim 5, wherein the function is a linearly increasing function that increases each time a new packet identified with the link ID is received by the PPC.

8. The network apparatus in accordance with claim 5, wherein the function is a linearly decreasing function that decreases each time a new packet identified with the link ID is received by the PPC.

9. The network apparatus in accordance with claim 5, wherein the function increases or decreases within predefined limits each time a new packet having the Link ID is received by the PPC.

10. The network apparatus in accordance with claim 5, wherein the function is a discrete function assuming values from a limited set of discrete values.

11. The network apparatus in accordance with claim 5, wherein the function is a function of the value of more than one field in the packet.

12. The network apparatus in accordance with claim 2, wherein the PPC is operable to generate a new dataset by:

receiving a plurality of packets copied from the network over a period of time;

binning packets having a same source and destination in a same bin;

assigning a link ID to bin;

extracting values of a field comprised in payloads of the received packets;

tabulating the extracted values; and

assigning a compression category to the field responsive to the tabulated values and the link ID assigned to the bin.

13. The network apparatus in accordance with claim 12, wherein the PPC is configured to generate a new dataset when the PPC detects at least one mismatch between the extracted field value and the computed value.

14. The network apparatus in accordance with claim 13, wherein the PPC is configured to generate a new dataset when the PPC detects a predetermined plurality of mismatches.

15. The network apparatus in accordance with claim 1 further comprising a log that receives and saves compressed packets generated by the PPC.

16. The network apparatus in accordance with claim 15, wherein the log is operable to release at least a portion of the saved compressed packets to the traffic shaper for transmission to the IDS hub, when triggered by a signal.

17. The network apparatus in accordance with claim 16 further comprising a computational unit that is operable to received copied packets and analyze the packets to detect a possible anomalous event, wherein the detection generates the signal for the log to release the at least a portion of the saved compressed packages.

18. The network apparatus in accordance with claim 1, wherein the packet is an industrial protocol packet, the network is an industrial control system (ICS) network, and the compressed packet is transmitted to an intrusion detection system (IDS) hub.

19. A method for evaluating and compressing a packet, the method comprising:

receiving a copy of a packet being propagated through a network, the packet comprising a source, destination, and a payload;

extracting a value of a field in the payload;

providing a computed value of the field based on the source and destination of the packet;

comparing the extracted value with the computed value;

compressing the field if the extracted value is the same as the computed value; and

transmiting a compressed packet comprising the compressed field.

20. The method in accordance with claim 19, wherein providing the computed value comprises:

extracting the copied packet's source and destination and an identifier of the field;

querying a dataset to have assigned a compression category associated with the source, destination, and field identifier; and

generating the computed field value with a function associated with the compression category.