

TITLE:
**METHOD AND APPARATUS FOR DETECTING ANOMALIES OF AN
INFRASTRUCTURE IN A NETWORK**

ABSTRACT

The present invention relates to a method and an apparatus for detecting anomalies of an infrastructure in a network comprising analysing a data packet exchanged in a network and identifying the network protocol and all the fields, defining an identified protocol and identified fields of said data packet, and, extracting identification fields, to identify a device of the infrastructure, matching the identified device with a plurality of predefined standard devices in a predefined devices knowledge database, to recognise a matching device, retrieving one or more allowed fields and one or more allowed protocols of the matching device from the database, comparing the allowed fields and the allowed protocols respectively with the identified fields and the identified protocol, defining at least one critical state of the infrastructure and signalling an anomaly of the infrastructure when at least one of the critical states is identified.

[FIG. 1]