(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2017 (26.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/182302 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)

(21) International Application Number:
PCT/EP2017/058480

(22) International Filing Date:
10 April 2017 (10.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16165909.9 19 April 2016 (19.04.2016) EP

(71) Applicant: **NAGRAVISION S.A.** [CH/CH]; Route de Genève 22-24, 1033 Cheseaux-sur-Lausanne (CH).

(72) Inventors: **BRIQUE, Olivier**; Chemin des Mélampyres 28, 1805 Jongny (CH). **SERVET, Patrick**; ch. de Sous-le-Mont 38, 1033 Cheseaux-sur-Lausanne (CH).

(74) Agent: **LEMAN CONSULTING S.A. 284**; Chemin de Précossy 31, 1260 Nyon (CH).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title:** METHOD AND SYSTEM TO DETECT ABNORMAL MESSAGE TRANSACTIONS ON A NETWORK

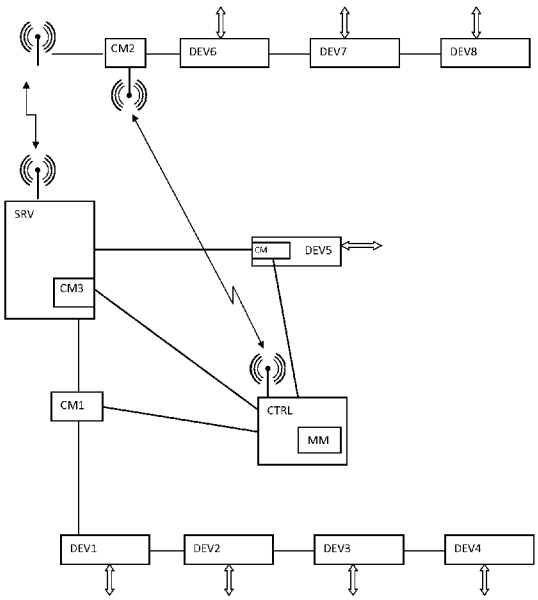


Fig. 1

(57) **Abstract:** The present disclosure is in the field of surveillance system of a network, in particular of an industrial network connecting various devices in charge of collecting data or giving commands. According to one embodiment, it is proposed a surveillance system connectable to a network, comprising a communication module and a management module, said system being configured to, during an initialization phase: a. intercept a first message, being sent to a first device, b. intercept a second message being a response from the first device to the first message, c. calculate a time interval between the interception of the first message and the interception of the second message, d. repeat the steps a to c in order to determine further time intervals, e. determine a distribution of said time intervals, f. storing in reference with the first device, the distribution of time intervals, and during a surveillance phase, said system being configured to: g. intercept a third message being sent to the first device, h. intercept a fourth message being a response from the first device to the third message, i. calculate a new time interval between the interception of the third and the fourth message, j. verify that the new time interval is within the distribution of time intervals.

WO 2017/182302 A1

METHOD AND SYSTEM TO DETECT ABNORMAL MESSAGE TRANSACTIONS ON A NETWORK

Introduction

The present disclosure is in the field of surveillance system of a network, in particular of an industrial network connecting various devices in charge of collecting data or giving commands.

Background Art

Protection against software attacks is a main concern in the industry and in particular in the case of a network of devices controlling or supervising a plant, a factory or a manufacture. In these cases, we have numerous devices collecting data and giving commands under the supervision of one or more servers.

The protocol used for the communication with these devices is usually basic without protection since it was not intended to by accessible outside the premises. The response for the security threat was made on the server, in particular to the connection of the server with the outside world.

New threat models have been demonstrated since, for example, the server/controller of a nuclear plant, communicating to the devices spread in the plant, is also connected to other networks having access to servers or computers outside the plant. Even if particular care has been taken to protect the inside network, a risk has been detected that a third party can access to the final devices and influence the tasks for which these devices have been designed. One can imagine if the device in charge of acquiring the temperature inside the kernel of a nuclear plant can be altered, the consequence could be huge.

One major problem to improve the security of these devices is the difficulty to upgrade the internal software (generally embedded software) and/or upgrade the communication protocol, designed sometimes more than 20 years ago.

Brief description of the figures

The present disclosure will be better understood thanks to the attached figures in which:

- figure 1 illustrates the network and the various elements of the system,

- figure 2 illustrates the incoming and outgoing messages to a device,

- figure 3 illustrates the format of a message,

- figure 4 illustrates the process for processing a message

- figure 5 illustrates one example of the communication module.

Detailed description

According to one embodiment of the disclosure, it is proposed a method to supervise a network connected to a first device, said method comprising, during an initialization phase:

a. intercepting a first message from the network, said message being sent to a first device,

b. intercepting a second message from the network, said second message being a response from the first device to the first message,

c. calculating a time interval between the interception of the first and the interception of the second message,

d. repeating the steps a to c in order to determine further time intervals,

e. determining a distribution of said time intervals,

e. storing, in reference with the first device, the distribution of time intervals,

and during a surveillance phase, said method comprising:

f. intercepting a third message from the network, said message being sent to the first device,

g. intercepting a fourth message from the network, said fourth message being a response from the first device to the third message,

h. calculating a time interval between the third and the fourth message,

i. verifying that the new time interval is within the distribution of time intervals.

According to the main embodiment, the target device is not modified, only the traffic on the network connecting the target device is analyzed. This analysis is based on the response time of the target device, the response time being the time interval between an incoming message to the target device and an outgoing message from the target device.

The method according to the main embodiment of the disclosure is divided into two phases, a learning phase or initialization phase, and an operational phase.

During the learning phase, a management module in charge of the supervision of the network, records the response time of the devices. For that purpose, the management

module have access to the network connected to the target and then can analyze the messages exchanged with this device.

During the learning phase, the management module records the response time or the time interval for a given target and compiles a distribution of time intervals. This distribution of time intervals is associated with a device or a device type. Preferably, the plurality of time intervals is measured in the same condition i.e. the information requested, i.e. the first message is of the same message type.

During the operational phase, the management module measures the time interval for a given target, i.e. the time interval between the incoming message and the outgoing message and compares the measured duration with the distribution of time intervals.

In case that the measured time interval is outside a range defined by the distribution of time intervals, an alarm is set.

In reference of the figure 1, a network comprises at least one server SRV and a plurality of devices DEV1 to DEV8. Connected to the network is a controller CTRL in charge of controlling the devices. The controller CTRL comprises a management module in charge of collecting time intervals and determining if a time interval is within a distribution of time intervals.

The figure 1 describes different embodiments which can be used alone or in combination.

The devices of the present disclosure could be sensors, captors, actuators, cameras or part of a machine to control the proper functioning of the machine. Each device has a device address used by the server to send a message to said device and to identify the response.

According to one embodiment, the devices are wired connected as illustrated by the devices DEV1 to DEV4. They could be also connected wirelessly as it is the case for the devices DEV6 to DEV8. In both cases the server can send messages to the devices and receive messages from the devices.

Communication module

This module is in charge of analyzing the traffic on the network. This module can have several communication interfaces able to acquire messages from a variety of communication networks. A message detected by the communication module is analyzed and the recipient and/or the initiator are/is identified. When a message is addressed to a device, the communication module stores in its memory the current time and the identification of the

recipient, i.e. the address of the recipient). When the communication module detects a response from this recipient by the analysis of the network's traffic, the communication module calculates the time interval between the time recorded at the sending and the current time while detecting the response. This time interval is sent to the management module MM of the controller CTRL with the identification of the device.

An example of a communication module is illustrated at the figure 5. In this example, the communication module CM comprises a first communication channel C1, connected to the network common to the target devices, and a second communication channel C2 with the management module MM.

It is to be noted that the same communication network can be used for collecting the messages to and from the devices and to communicate with the management module MM. The messages received through the first communication channel C1 are processed by a processor P of the communication module and the address of the recipient or the originator is extracted. The processor P has access to a memory MEM to store a record comprising at least the identification of the message, i.e. the target address and the current time. For that purpose, the communication module may comprise a clock module CK to provide the current time.

The format of a message is illustrated at the figure 3. It comprises at least a first section B0 which is the header comprising the recipient address and a second section B1 defining a message type. The instruction is interpreted by the device to carry out the requested task and a response is sent back to confirm the proper execution of the instruction. The message can further contain a data payload is section B2, for example if the server defines an action or set operating values. As an example, a device controlling a door could receive an instruction to modify the position of a selected door and the payload defines that the selected door should be opened at 20%.

According to a particular embodiment, the communication module comprises further information about the format of the messages. The messages sent and received from a device can have different types. When a message is analyzed, a message type is determined. The message type could be identified by the content of the message and describe the type of operation that the target device should perform, i.e. the instruction given to the device. This can be the request of a data, as a temperature for example, the initialization of the

device, e.g. by setting the operating mode of the device, or a software download. Depending on the message type, the device will react differently to the instruction and the response time to this message can vary. In this embodiment, in the memory of the communication module, the sending time, the device address and the message type are stored. When the analysis of the traffic detects a response from the same device, the time interval is calculated and a record is sent to the management module comprising at least the device address and the time interval. It can further comprise the message type.

Some communication protocols implement, on the device side, two types of response. OSI is essentially a data communications management structure, which breaks data communications down into a manageable hierarchy of seven layers. Each layer has a defined purpose and interfaces with the layers above it and below it. By laying down standards for each layer, some flexibility is allowed so that the system designers can develop protocols for each layer independent of each other. By conforming to the OSI standards, a system is able to communicate with any other compliant system, anywhere in the world. The protocol comprises several layers, e.g. OSI Model). The first type of response can be generated at the transport layer and could be just an acknowledgment of the reception of the message sent by the server. At that time, the application layer of the target device has still not processed the message. In the frame of the present disclosure, the first type of acknowledgment will be named "transport response message" and the second type of response "application response message". The communication module, in an embodiment, may calculate the time interval from the interception of the "application response message" only and discard, while analysing the responses sent by a device, the "transport response message". The "application response message" is the one produced by the application layer of the device such as the metering temperature, control a circuit-breaker, a door etc. The header of the message contains the specification of the message type and in this particular case, from which layer it has been produced.

Management module

This module MM is in charge of establishing a distribution of time intervals during an initialization phase. During this phase, the management module receives the records from the communication module, each record comprising at least the device address and the time interval. For a specific device, the management module stores all time intervals and

calculates a distribution of time intervals. This distribution can be in the form of a minimum value and a maximal value, or a central value with deviations. The management module can add tolerances to take into account the variation of operating parameter of a device, such as the temperature, e.g. +/- 10%.

The initialization phase can be defined manually by an operator defining when the initialization phase starts and when its ends. It can be also automatic and handled by the management module itself. Each time that a new device address is detected, the management module records a number of transactions, i.e. a record from the controller module, to determine the distribution of time intervals. This can be done by storing the first ten records or storing records during a first period, for example 24 hours.

It is to be noted that the management module can be in operational phase for some devices and in initialization phase for other devices, which could be the case for example for a new device in the environment.

In case that the communication module transmits also the message type, the distribution of time intervals is established per message type and per device. A plurality of distribution of time intervals can be associated with one device, each distribution of time intervals being associated with a message type.

According to a particular embodiment, the management module can retrieve a device type from the address of the device. For that purpose, the management module comprises a database in which the device addresses are listed with a device type. The network can connect several temperature sensors, each having a different address. However, they share the same device type.

As a particular embodiment, the distribution of time intervals is established per device type instead of per device. Each time a record is received from the communication module, the address is converted into a device type and the associated distribution of time intervals is used. In this case, several devices which have the same device type, can define the distribution of time intervals for said device type.

The operational phase of the management module is basically a comparison of the time interval received from the communication module with the distribution of time intervals. If the received time interval is outside the distribution of time intervals, an alarm is set. This

alarm can be a message to a console, this message comprising the address of the device or is sent to another system for analysis.

In this embodiment, when a record is received from the communication module, the address is used to identify the distribution of time intervals to be used for the verification.

In case that a message type is added into the record, the device's address and the message type is used to retrieve the distribution of time intervals.

In case that the distribution of time intervals is defined in relation to a device type, the address is converted into device type using the internal database of the management module and the corresponding distribution of time intervals is retrieved for the comparison.

In another embodiment, the device type and the message type are used to retrieve the distribution of time intervals.

We have therefore the following cases wherein (DOTI stands for Distribution Of Time Intervals:

Device Address ⟶ DOTI

Device Address ⟶ Device Type ⟶ DOTI

Device Address and Message Type ⟶ DOTI

Device Address ⟶ Device Type and Message Type ⟶ DOTI

According to one embodiment, a new device in the network having a known device type and therefore in which a distribution of time intervals is already stored according to this device type, can be immediately be under the surveillance of the management module without going through an initialization phase for said device.

According to one embodiment, the management module can generate a test message which will play the role of the first message. This test message is sent through the network during the learning phase or the surveillance phase. The management module can format a test message to a specific device, thus triggering the calculation of the time interval until the response is received. This test message can be a pre-recorded message, for example to test the presence of a device. This test message can be also one of the messages sent to the device by the server and recorded by the management module.

According to a particular embodiment, the management module may send a reboot message as test message to a device, said device responding to the reboot message once the reboot of the device is terminated.

Organization of the various modules

In the figure 1, several implementation modes are shown and can be used alone or in combination. According to a first implementation (not represented), the communication module and the management module are located in the server SRV. This server is the one controlling and exploiting the data from and to the devices. The server SRV is already a computer and a new software module comprising the two above mentioned modules is implemented. The communication module has then a natural connection with the traffic exchanged on the network and the management module receives internally the records from the communication module.

In a second embodiment, an independent controller CTRL comprises at least the management module receiving the time interval records from a remote communication module. The figure 1 illustrates several embodiments in which:

- the communication module CM3 is located in the server SRV and transmits the time interval record to the management module of the controller CTRL.

- the communication module CM is located directly into a device (e.g. device DEV5)

- the communication module CM1 is connected to the wired main network,

- the communication module CM2 is connected to a remote network and wirelessly connected to the controller CTRL.

According to the present disclosure, one or more communication modules, as described above, can intercept messages exchanged to the devices and send the time interval records to the controller.

The figure 2 illustrates the way the communication module works. A time T1 and a time T2 are the times between a first message or incoming message is sent to a first device on line M line M and a second message or outgoing message on -line M' corresponding to the response sent from the first device. The incoming message M is the message received by the first device and the outgoing message M' is a message sent by the first device in response to the incoming first message M. The times T1 and T2 are recorded during the

initialization phase and allow the management module to calculate the distribution of time intervals. During the operational phase, the time Tn is the time interval between the reception of the first message by the first device and the sending of the response to the first message from the first device for the same device or a device of the same type as explained above. The time Tn is within the distribution of time intervals and the management module will not set an alarm for the device involved in these two messages.

In another example, a time Tp as shown in figure 2 is outside the distribution of time intervals. In this case, once the time interval Tp is received by the management module and the comparison determines that the time interval Tp is outside the distribution of time intervals, the alarm is set.

In figure 4, one example of the flowchart executed by the control module and the management module is illustrated. The control module receives the messages intercepted on a network and analyses them. The first test made by the communication module is to determine if the message is an incoming message M or an outgoing message M'. In order to discriminate the incoming and outgoing messages, the headers of the messages are analyzed. The communication module is able to extract from the messages at least the recipient address and/or the initiator address. According to one example, in a simple environment with one server communicating with several devices, the devices do not add the server address, while responding to the server. One device only inserts its address in the message in order to allow the server to identify the originator of the message. The header of the message comprises an indication that this message is a message intended to the server.

When the message is an incoming message M, the control module extracts the identification of the recipient IDn and stores said information IDn with the current time CT as a first time Ta, i.e. the time corresponding to the interception of the incoming message M. A record is stored in the memory of the control module with the identification of the recipient IDn and the first time Ta.

When an outgoing message is detected, the control module extracts from the message the identification of the sender IDn. The control module then retrieves in the memory the record corresponding to the identification of the sender IDn in order to retrieve the first time Ta.

With the current time CT (which corresponds to the time of the interception of the outgoing message M'), the control module calculates the time interval D between the current time

and the first time Ta, i.e. D = CT – Ta. This time interval D is transferred to the management module with the identification of the device IDn for further analysis.

The management module, using the identification of the device, can retrieve the distribution of time intervals corresponding to said device. The management module then compares the received time interval D with the distribution of time intervals and determines if an alarm is set or not. Setting an alarm does not necessary mean that the device should be deactivated. We could have the case in which the device is temporarily busy with another task and the management module can comprise a filter to count the alarms for a given device. When a predetermined threshold of alarms is reached, a signal is sent to the console for further processing by an operator, or a message is transferred to a hierarchically higher system.

When the device does not reply after a predetermined time, the server can repeat the step of sending the message to the device. The control module will preferably store in its memory the current time of the last message and do not take into account, in the calculation of the time interval, the current time of the first attempt. This could be for example the case when a device is switched off or the network is interrupted. According to one particular embodiment, the control module stores with the identification IDn and the time Ta, a flag R meaning that no response was received from this specific device following the first attempt. This information can be part of the record sent to the management module for further analysis.

Example with SCADA

A Supervisory Control And Data Acquisition system or SCADA system refers to the combination of telemetry and data acquisition. SCADA encompasses the collecting of the information via a remote terminal unit RTU , transferring it back to a central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. The required control actions are then conveyed back to the process.

A SCADA system consists of a number of remote terminal units RTUs collecting field data and sending that data back to a master station via a communication system. The master station displays the acquired data and also allows the operator to perform remote control tasks. The accurate and timely data allows for optimization of a plant operation and process. A further benefit is to have more efficient, reliable and most importantly, safer operations.

This all results in a lower cost of operation compared to earlier non-automated systems. On a more complex SCADA system there are essentially five levels or hierarchies:

- Field level instrumentation and control devices
- Marshalling terminals and RTUs
- Communications system
- The master station(s)
- The commercial information technology (IT) or data processing department computer system

The RTU provides an interface to the field analog and digital sensors situated at each remote site.

The communications system provides the pathway for communications between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The physical layer is the physical media over which the messages according to a protocol are transmitted. The physical layer specifies the electrical specifications, timing, pin-outs and so on. The data element at this level is essentially a bit, i.e. it is concerned with how to pass one bit of data at a time across the physical media. The definition of the physical layer also includes the functions for controlling the media, such as the details required to establish and maintain the physical link, and to control data flow.

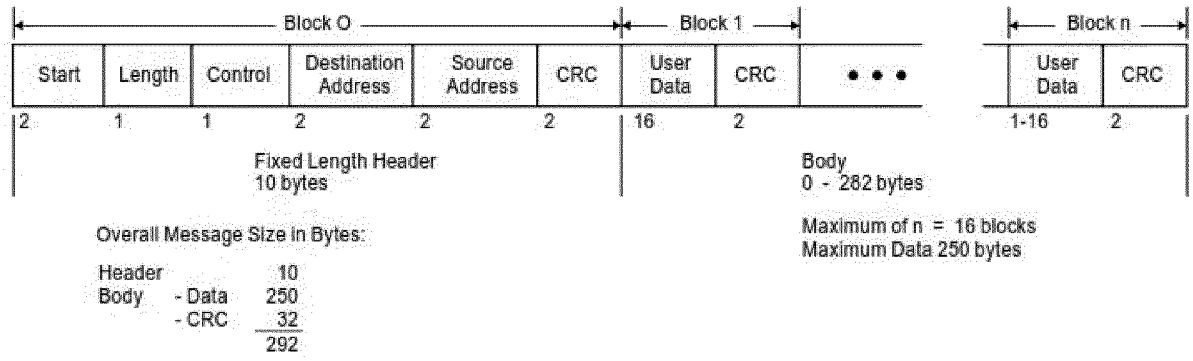
The data link layer on the frame of a SCADA system is specified in a protocol named “DNP3”. The purpose of the data link layer is to establish and maintain reliable communication of data over the physical link. Link establishment involves setting up the logical communications link between a sender and a receiver. The protocol DNP3 supports either connection oriented or connection-less operation. Thus, if a channel operates over a public switched telephone network line or PSTN line and requires connection by dialing before the communication can begin, the data link layer manages this without any direction from higher levels.

The data unit at the link layer level may be called the frame. The frame has a maximum size of 292 bytes including CRC codes, and carries a total of 250 bytes of information from the higher levels. The frame includes 16-bit source and destination addresses in its header. These provide for 65 536 different addresses. The address range FFF0–FFFF is reserved for broadcast messages, which are intended to be processed by all receivers. The addresses are logical in the sense that it is possible for one physical device to have more than one logical address. In such a case the different addresses would appear as separate devices to the master station.

The frame header also contains a function code. The functions supported by this are those required to initialize and test the operation of each logical link between a sender and a receiver. As an additional security feature every frame transmitted can request a confirmation of receipt. This is termed link layer confirmation.

One example of the frame format is based on a FT3 format frame as specified in IEC 870-5-1 standard. The format specifies a 10 byte header, followed optionally by up to 16 data blocks. The overall message size is limited to 292 bytes, which provides for a maximum data capacity of 250 bytes. Thus a fully packed frame will comprise the header plus 16 data blocks, with the last block containing 10 data bytes.

Table 1



• START: 2 bytes: 0564 (hex)

• LENGTH: Count of user data in bytes, plus 5, not counting CRC bytes. This represents all data, excluding CRC codes following the LENGTH count byte. Its range is 0–255. This is convenient as it is the largest length count that may be represented by 1 byte (=FF hex).

• CONTROL: Frame control byte. See below.

• DESTINATION ADDRESS: 2 byte destination address (LSB, MSB)

• SOURCE ADDRESS: 2 byte source address (LSB, MSB)

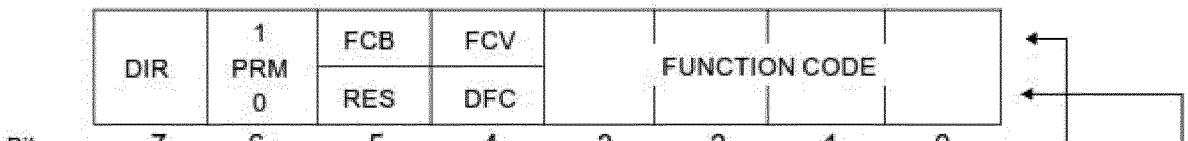
• CRC: 2 byte cyclic redundancy check code

• USER DATA: Each block has 16 bytes of user data. Last block has 1–16 as required. In case of a full frame the last block will have 10 bytes of user data.

Control byte

The control byte follows the start and length bytes in the frame format. It provides for control of data flow over the physical link, identifies the type, and indicates the direction. The interpretation of most of the control byte is dependent on whether the communication is a primary or a secondary message.

Table 2



Primary to Secondary Function Codes

CODE	DESCRIPTION
0	Reset Link
1	Reset User Process
2	Test Link
3	User Data - Confirm Expected
4	User Data - No Confirm
9	Request Link Status

Secondary to Primary Function Codes

CODE	DESCRIPTION
0	Confirm - ACK
1	Confirm - NACK
11	Respond - Link Status
14	Link Not Functioning
15	Link Not Used

In the frame of the present disclosure, the Destination Address and the Source Address are extracted from a message by the communication module in order to determine the time interval between the interception of two messages for a given device. Additionally, the Control Byte can be used to detect the type of messages and to apply a different distribution of time interval in function of the message type.

The management module could be part of a wider surveillance system, such as a Security information and event management or SIEM software products and services. Security information and event management SIEM software products and services combine security

information management SIM and security event management SEM, and provide real-time analysis of security alerts generated by network hardware and applications. A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements. A SIEM product is available as software, appliances or managed services; these products are also used to log security data and generate reports for compliance purposes.

The functionalities of a SIEM may be as following:

- Data aggregation: Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

- Correlation: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution

- Alerting: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.

- Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.

- Compliance: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.

- Retention: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

- Forensic analysis: The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

Although embodiments of the present disclosure have been described with reference to specific example embodiments, different modifications and changes may be made to these embodiments without departing from the broader scope of these embodiments. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense. The accompanying drawings that form a part hereof, show by way of illustration, and not of limitation, specific embodiments in which the subject matter may be practiced. The illustrated embodiments are described in sufficient detail to enable those skilled in the art to practice the teachings disclosed herein. Other embodiments may be utilized and derived there from, such that structural and logical substitutions and changes may be made without departing from the scope of this disclosure. This Detailed Description, therefore, is not to be taken in a limiting sense, and the scope of various embodiments is defined only by the appended claims, along with the full range of equivalents to which such claims are entitled.

Such embodiments of the inventive subject matter may be referred to herein, individually and/or collectively, by the term “invention” merely for convenience and without intending to voluntarily limit the scope of this application to any single inventive concept if more than one is in fact disclosed. Thus, although specific embodiments have been illustrated and described herein, it should be appreciated that any arrangement calculated to achieve the same purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the above description.

Claims

1. Surveillance system connectable to a network, comprising a communication module (CM) and a management module (MM), said system being configured to, during an initialization phase:

a. intercept a first message from the network, said first message being sent to a first device (DEV1…DEV8),

b. intercept a second message from the network, said second message being a response from the first device (DEV1…DEV8) to the first message,

c. calculate a time interval (T1) between the interception of the first message and the interception of the second message,

d. repeat the steps a. to c. in order to determine further time intervals,

e. determine a distribution of said time intervals,

f. storing in reference with the first device (DEV1…DEV8), the distribution of time intervals,

and during a surveillance phase, said system being configured to:

g. intercept a third message from the network, said message being sent to the first device (DEV1…DEV8),

h. intercept a fourth message from the network, said fourth message being a response from the first device (DEV1…DEV8) to the third message,

i. calculate a new time interval (Tn) between the interception of the third message and the interception of the fourth message,

j. verify that the new time interval (Tn) is within the distribution of time intervals.

2. Surveillance system of claim 1, wherein it is further configured to analyze the messages on the network and to extract an addressing portion of the message to determine to which device this message is addressed to, or from which device this message is originating from.

3. Surveillance system of claim 2, wherein it is further configured to analyze the messages to further extract a message type, said distribution of time intervals being determined by message type.

4. Surveillance system of any of the claims 1 to 3, wherein it is configured to calculate the time interval between the interception of first and the interception of the second message, the management module (MM) is configured to determine the distribution of time intervals, and is configured to verify that the new time interval is within the distribution of time intervals.

5. Surveillance system of claim 4, wherein the communication module (CM) is located into the first device (DEV5), the management module (MM) is located into a controller (CTRL) connected with the first device (DEV1…DEV8) to receive the time intervals calculated by the communication module (CM).

6. Surveillance system of claim 4, wherein the communication module (CM) further comprises communication means with a surveillance server, said server comprising the management module (MM).

7. Method to supervise a network connected to a first device (DEV1…DEV8), said method comprising, during an initialization phase:

a. intercepting a first message from the network, said message being sent to a first device (DEV1…DEV8),

b. intercepting a second message from the network, said second message being a response from the first device (DEV1…DEV8) to the first message,

c. calculating a time interval (T1) between the interception of the first message and the interception of the second message,

d. repeating the steps a to c in order to determine further time intervals,

e. determining a distribution of said time intervals,

e. storing, in reference with the first device (DEV1…DEV8), the distribution of time intervals,

and during a surveillance phase, said method comprising:

f. intercepting a third message from the network, said message being sent to the first device (DEV1…DEV8),

g. intercepting a fourth message from the network, said fourth message being a response from the first device (DEV1…DEV8) to the third message,

h. calculating a new time interval between the interception of the third message and the interception of the fourth message,

i. verifying that the new time interval is within the distribution of time intervals.

8. Method of claim 7, wherein it comprises:

- analyzing the messages on the network and extracting an addressing portion of the message to determine to which device this message is addressed to or from which device this message is originating from.

9. Method of claim 7 or 8, wherein it comprises:

- analyzing the messages to further extract a message type, said distribution of time intervals being determined by message type.

10. Method of any of the claims 7 to 9, wherein the distribution of time intervals is organized by type of devices, said method comprises:

- intercepting a fifth message from the network, said message being sent to a second device, said device being of the same type of the first device,

- intercepting a sixth message from the network, said sixth message being a response from the second device to the fifth message,

- calculating a new time interval between the interception of the fifth message and the interception of sixth message,

the verification is carried out with the device type distribution of time intervals.

11. Method of any of the claims 7 to 9, wherein the first device generates transport layer message and application layer message, the method comprising the steps of :

after intercepting the second or the fourth message, discarding the intercepted message if the second of fourth message is a transport layer message.

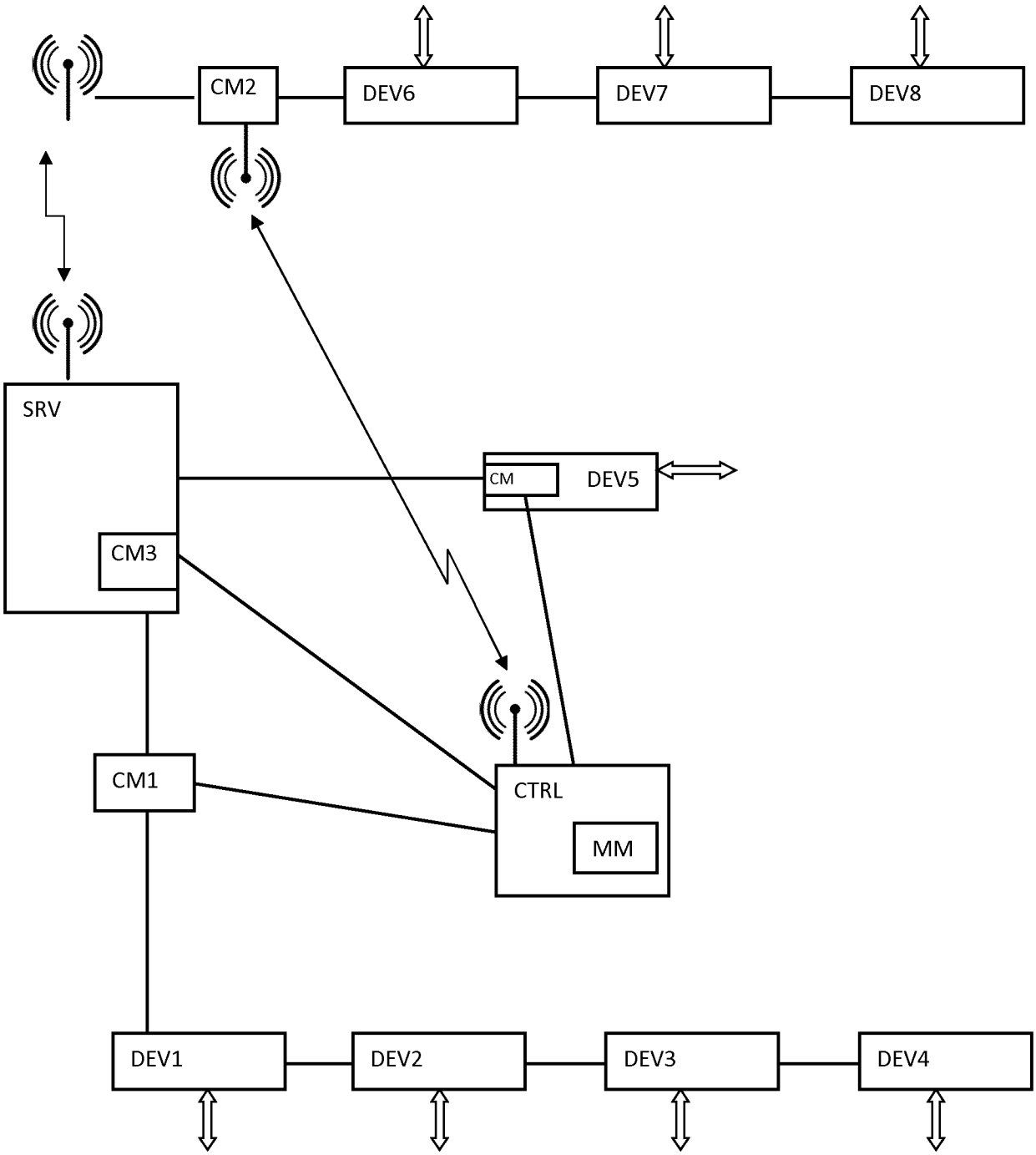

CM2
DEV6
DEV7
DEV8
SRV
CM
DEV5
CM3
CM1
CTRL
MM
DEV1
DEV2
DEV3
DEV4

Fig. 1

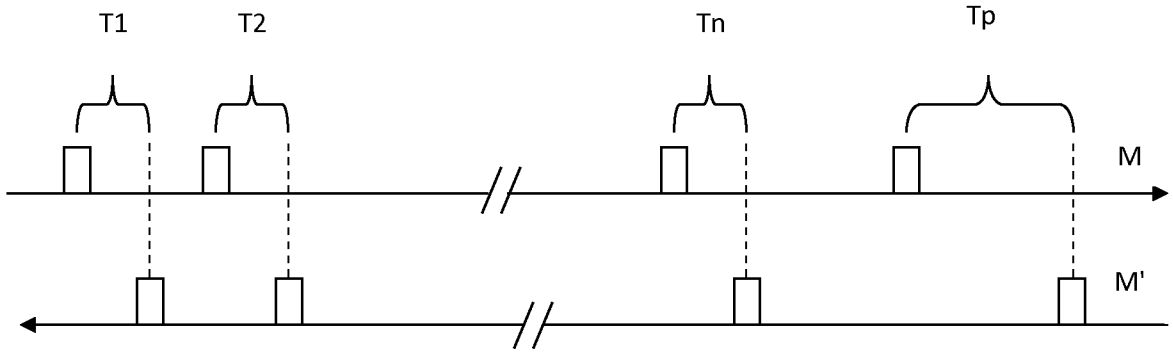


Fig. 2

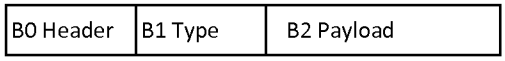


Fig. 3

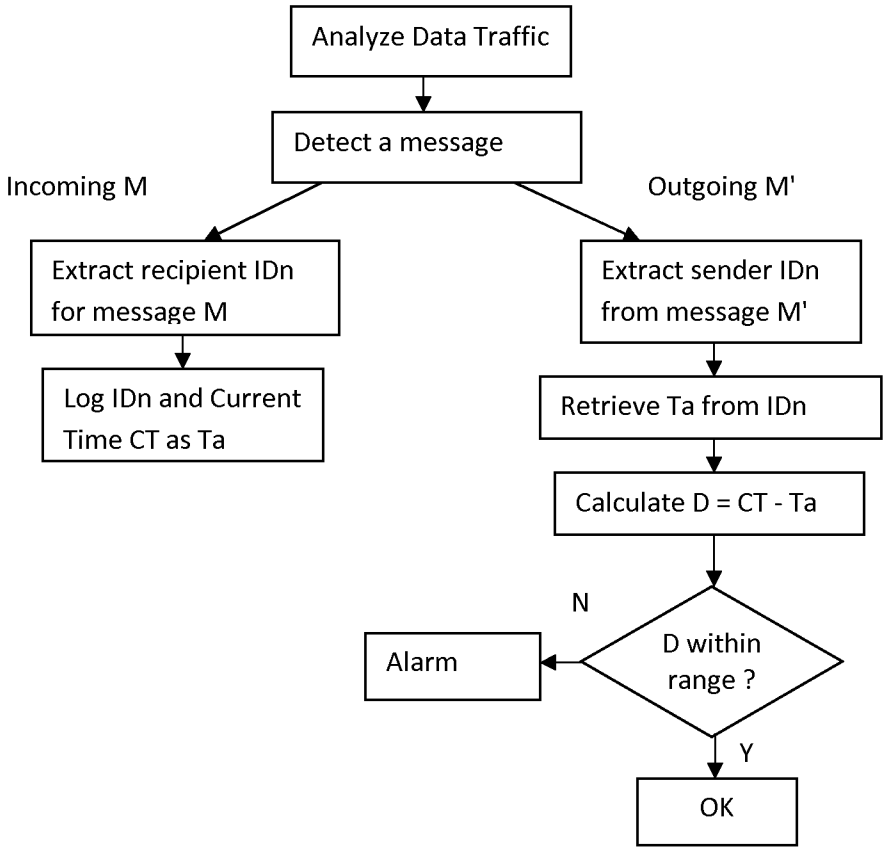


Fig. 4

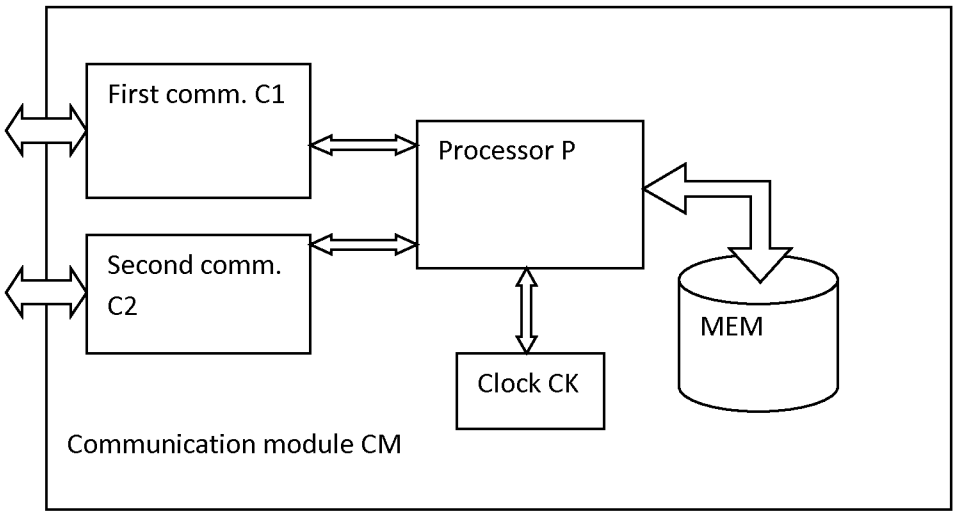

First comm. C1
Processor P
Second comm. C2
MEM
Clock CK
Communication module CM

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/058480

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/26
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/126019 A1 (MEMON NASIR [US] ET AL) 14 May 2009 (2009-05-14) paragraph [0052] - paragraph [0062] paragraph [0039] paragraph [0047] - paragraph [0051] paragraph [0029] paragraph [0059] - paragraph [0062] paragraph [0042] -----	1-11
X	US 6 041 352 A (BURDICK MATT [US] ET AL) 21 March 2000 (2000-03-21) column 1, line 14 - line 26 column 1, line 53 - line 60 column 2, line 18 - line 20 column 6, line 11 - line 26 column 8, line 16 - line 30 ----- -/--	1-11

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2017	18/05/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Medvesan, Oana

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/058480

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/159267 A1 (GYORFFY JOHN [CA]) 21 June 2012 (2012-06-21) the whole document -----	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/058480

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009126019 A1	14-05-2009	NONE	
US 6041352 A	21-03-2000	JP H11346238 A	14-12-1999
		US 6041352 A	21-03-2000
US 2012159267 A1	21-06-2012	US 2012159267 A1	21-06-2012
		US 2013346808 A1	26-12-2013
		US 2014379908 A1	25-12-2014
		US 2017026495 A1	26-01-2017