(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2011/051741

(22) International Filing Date:
7 February 2011 (07.02.2011)

(25) Filing Language:
English

(26) Publication Language:
English

(71) Applicant (for all designated States except US): ABB RESEARCH LTD [CH/CH]; Affolternstrasse 44, CH-8050 Zurich (CH).

(72) Inventors; and

(75) Inventors/Applicants (for US only): THRYBOM, Linus [SE/SE]; Kronhjortsgatan 31, S-72242 Västerås (SE).
ÅKERBERG, Johan [SE/SE]; Högalid Hedensberg, S-72595 Västerås (SE).


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

(54) Title: DEVICE AND METHOD FOR SECURING ETHERNET COMMUNICATION

![Diagram of a network device and its components]

(57) Abstract: The present invention relates to a device (1) for transmitting and receiving an Ethernet data frame including raw bits, comprising a physical layer (PHY, 42) for transmitting and receiving the data frame. The device further comprises a hardware component arranged adjacent to the physical layer (PHY, 42). The hardware component (2) is configured to generate a cryptographic checksum (SecTag) based on the raw bits of the data frame and add the cryptographic checksum to the end of the data frame so as to form a extended data frame to be transmitted to the PHY and verify the cryptographic checksum (SecTag) in the data frame received from the PHY.
DEVICE AND METHOD FOR SECURING ETHERNET COMMUNICATION

FIELD OF THE INVENTION

The present invention relates to the field of Ethernet communication security for low end electrical devices having limited resources in terms of processing capability and memory.

PRIOR ART

A Network Interface, denoted by NI, is a computer hardware implementation of a network interface controller for connecting a computer to a computer network. A NI normally comprises an electronic circuit for facilitating Ethernet communication using a physical layer, denoted as PHY and a data link layer of OSI standard. Typically the data link layer includes a Media Access Control sub-layer, denoted as MAC.

To send data to the network, the NI receives an outbound payload data from the computer or a data processing unit, and the MAC constructs an Ethernet frame including the payload data, MAC destination and MAC source, and a checksum, and outputs the frames via a Local Area Network (LAN) interface through the PHY. On the other hand, to receive data from the network, the NI receives an inbound frame through the PHY, checks the checksum of the frame at MAC and send the payload data encapsulated in the frame to the computer or the data processing unit in case that the checksum is correctly verified.

In an industrial system, wherein for instance a plurality of electrical devices are connected via a LAN and communicated via Ethernet, it is required that a communicated data frame is originated from an authorized source and the data content in the frame should not be modified during the communication, in order to assure the integrity of various information communicated within the LAN.
One of characteristics of such an electrical device is that it has a limited computing resources and a compact size, which limits its computing capability in terms of performance. Furthermore, since such an industrial system requires fast response, communication latency should be as low as possible.

The existing technologies such as IPSec and MACSec provide limited solutions. The former provides protection for IP packets only on a point to point channel, while the latter one creates a new Ethernet frame comprising a new header and payload, which increases the communication latency.

A US patent, with a patent No. US 7502925, describes a method for providing data integrity protection for a TCP data frame. The method calculates an integrity check value and placing the check value in the ESP authentication portion at the end of a TCP data frame. The value is calculated and inserted on the fly to reduce latency of a conventional TCP processing.

OBJECTS AND SUMMARY OF THE INVENTION

The object of the present invention is to provide a device for enabling Ethernet data frames to be transmitted in an authentication and integrity manner.

A further object of the invention is to enable Ethernet data frames to be transmitted with low latency.

The first object is achieved by a device as defined in the preamble of claim 1, characterized that the device further comprises a hardware component arranged adjacent to the physical layer and the hardware component is configured to generate a cryptographic checksum based on the raw bits of the data frame and add the cryptographic checksum to the end of the data frame so as to form an extended data frame to be
transmitted to the PHY and, verify the cryptographic checksum in the data frame received from the PHY.

For a host computer, the PHY is an entrance of data transmitted and received from Ethernet. By placing the hardware component adjacent to the PHY, the invention enables Ethernet data frames to be transmitted with authenticity and integrity for all the protocols based on Ethernet, which enhances security aspects for Fieldbus communication and related industrial Ethernet protocols as well. Therefore, transmission of falsified data to industrial devices in an industrial system is prevented.

A further advantage of the invention is that there is no need to change an existing hardware and/or software communication stack of a host device. Since the hardware component can be implemented and integrated into a network interface.

According to one embodiment of the invention, the device further comprises a media access control layer for providing addressing and channel access control and interfacing to the PHY. The hardware component arranged between the physical layer and the media access control layer.

According to one embodiment of the invention, the hardware component is further configured to process the raw bits of the data frame on a basis of a byte when generating or verifying the cryptographic checksum. By processing the data frame on the basis of a byte, or 8 bits, it enables low transmission latency, since the device may start transmission of the data frame without completing the generation of the signature for an outbound data frame or verification of the data frame for an inbound data frame.

Furthermore, the memory needed to store the data frame can be reduced to a small area of fixed size, mainly depending on the length of the signature.

The principal of the invention is also applicable to a data block with fixed size, wherein the generation and verification of a cryptographic checksum
are performed on the data block based a data block cryptographic algorithm.

According to one embodiment of the invention, the hardware component is further configured to calculate a new checksum based on the extended data frame and add the new checksum to the new data when the extended data frame is transmitted to the PHY.

According to one embodiment of the invention, the hardware component further comprises a memory for storing a cryptographic key set and the cryptographic key set is arranged to generate the cryptographic checksum on the data frame to be transmitted to the PHY and to verify the cryptographic checksum in the data frame received from the PHY.

The cryptographic key set is either a secret key or a plurality of keys including at least one public key and a private key. In case that a symmetric-key algorithm is used, a cryptographic checksum is generated or verified by the secret that is shared between two such devices. The cryptographic checksum is used for authenticating and verifying the data frame. While in case that an asymmetric-key algorithm is used, the cryptographic checksum is a digital signature and is generated by the private key stored in the memory of one device and is verified by the corresponding public key stored in the memory of another device. This means that the private key is owned only by a specific device, while the public key is shared among the other device.

According to one embodiment of the invention, the hardware component is one of the following programmable logic devices, denoted by PLD, for example FPGA, CPLD, or ASIC.

According to one embodiment of the invention, the hardware component is adapted to be integrated to the PHY or the MAC.

According to one embodiment of the invention, the hardware component is further configured to send an error signal to the MAC so as to discard the
data frame when the verified signature is not consistent with the original data frame. Optionally, the hardware component may be further configured to send an error signal to the MAC in case that the data frame is corrupted.

Furthermore, such a device may be used in an industrial electronic device configured to communicate with other industrial electrical devices based on Ethernet protocols and Ethernet based fieldbus communication network such as IEC61850, PROFINET IO etc. In an industrial system including a plurality of industrial electrical devices, data are communicated between the industrial electrical devices for various purposes, for example for controlling and protecting electrical devices in the system. In some of the cases, it is sensitive with respect to jitter and latency and therefore data have to be transmitted among the devices in a range of milliseconds, for example 1ms-50ms. Therefore, it is particularly important that data are transmitted with low latency to ensure that the control and protection functions are conducted within the boundaries of real time or jitter requirements.

Such a device may be enclosed in an electronic device which can be plugged into a second electronic device when it is mechanically and electrically connected to the second electronic device. This means that in case that there is no such Ethernet communication security provided on the second electronic device, by plugging the first electronic device, the second device is able to communicate with other devices, wherein the data frame is being authenticated and verified on the fly.

The first electronic device may further comprise a communication interface for receiving or sending data frames to the second electronic device. The communication interface can be any of PCI, ISA, PCI-E, FireWire, USB or Ethernet.

BRIEF DESCRIPTION OF THE DRAWINGS
The invention will now be explained more closely by the description of different embodiments of the invention and with reference to the appended figures.

Fig. 1 illustrates a schematic block diagram of the device, according to one embodiment of the invention.

Fig. 2a illustrates a flow diagram of the device, according to one embodiment of the invention, wherein a cryptographic checksum is generated and appended to the end of an outbound data frame to be transmitted to Ethernet.

Fig. 2b illustrates a flow diagram of the device, according to one embodiment of the invention, wherein a cryptographic checksum is verified for an inbound data frame to be transmitted to a host computer.

Fig. 3 illustrates a schematic diagram of a constructed data frame to be transmitted, the constructed data frame including a cryptographic checksum and a new calculated checksum, according to one embodiment of the invention.

Fig. 4 illustrates a schematic block diagram of an electrical device including the invented device, according to one example of the invention.

Fig. 4a illustrates a schematic block diagram of an electrical device including the invented device, wherein, the interface is an Ethernet interface.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Fig. 1 illustrates a schematic block diagram of the device, according to one embodiment of the invention. The device comprises an Input/Output interface 40 including a physical layer PHY 42 for interfacing to a Network 150 and a hardware component 2 including a Memory 20 and a computing
engine 10. PHY can be one of 802.3 PHY, HPNA 1.0/2.0 PHY, or the like. In an alternate embodiment, the PHY may be included within the device as a separate component. The Input/Output Interface 40 is an ETHERNET interface such as Gigabit ETHERNET, Fast Ethernet etc. The HW component 2 is arranged adjacent, or just next to the PHY and comprises a SecMAC unit 12 and a FSC unit 14. The SecMAC unit 12 is adapted to calculate a security tag for an outbound data received from a host computer 100 and for verifying a security tag for an inbound data frame received from the network 150 via PHY 42.

In this example, the host computer comprises a communication stack 110, a plurality of network drivers 120 and network interface 130 including the device 1, a Media Access Control layer MAC 30 and a host interface 50. The communication stack 110 and network drivers 120 are arranged for interfacing the host interface in order to handle different Ethernet protocols used for transmitting Ethernet data frames. The MAC is arranged next to the device 1 and interfaces, on another side, to the host interface.

Practically, as shown in Figure, the hardware component can be integrated into a NI of a host computer. Furthermore, the hardware component 2 can be implemented on one of programmable logic devices such as FPGA, CPLD, or ASIC and therefore it is easily and flexible to be integrated to the NI either in between PHY and MAC or, to PHY or MAC of the NI.

Specifically, Figure 2a and 2b illustrate two schematic processes of how an outbound data frame and an inbound data frame are handled respectively. In both theses two examples, the device 1 also includes a MAC.

As shown in Figure 2a, for an outbound data frame, the SecMAC unit 12 is configured to calculate the security tag in form of cryptographic checksum or cryptographic checksum, denoted as SecTag on a basis of byte, or 8 bits while the device may afterwards transmit the byte(s) just being calculated. Upon the completion of the calculation, it appends the calculated SecTag at the end of data frame or alternatively in a specific
reserved field of the Ethernet frame. A new checksum on the original data frame and the SecTag is then further calculated by the FCS unit 14. The security tag SecTag is typically a Message Authentication Code and calculated using any possible symmetrical cryptographic scheme based on a secret key stored in the Memory 20, for example HMAC-SHA1 algorithm. Alternatively, the security tag SecTag can be calculated using an asymmetrical cryptographic scheme wherein the memory is used for storing at least one private key and a number of public keys. Since the security tag SecTag is calculated on a basis of bytes, the maximum transmission latency is kept low, regardless of the frame length. It should be understood that it would be possible to combine symmetrical cryptographic scheme and asymmetrical cryptographic scheme to achieve a MAC as well.

In another direction, as shown in Figure 2b, for an inbound data frame received from the Network 150, the FCS unit 14 is configured to check the checksum FCS. In case that the checksum is inconsistent with the data frame including the SecTag an error signal RX_ERR is sent to MAC. Optionally, the data frame may be forwarded to the MAC so that the data frame will be discarded at the MAC. Another possibility could be disabling DATA signal which results in a bas data frame so that the MAC will throw the data frame away. The SecMAC unit 12 is configured to verify the security tag SecTag in the frame. In case that the data frame is inconsistent with the security tag SecTag, the computing engine 10 will send an error signal, RX_ERR to the MAC. Thereafter, the data frame will be discarded so as to prevent a falsified data packet. In this manner, a data frame transmitted based on an Ethernet protocol is provided with authenticity while its integrity can be verified accordingly. Moreover, such a data frame can be transmitted in any one of the following manners, unicast, multicast or broadcast.

Because the hardware component is arranged between the PHY and MAC, it makes it possible to provide the security functions for data frames to be transmitted on the fly. Furthermore, since the calculation is based on byte or a block rather than a complete data frame, it enables low transmission
latency when a data frame is transmitted, which fulfills the requirement of low transmission latency for an industrial system. Moreover, by appending the calculated SecTag at the end of an original data frame to be transmitted, it makes it possible to transmit the data frame on the fly due to the fact that the transmission of the data frame can be made in parallel with the calculation of the SecTag.

Figure 3 illustrates a schematic diagram of a constructed data frame being transmitted in a communication line. The transmitted data frame including a cryptographic checksum SecTag and a new calculated checksum FCS. The cryptographic checksum SecTag is calculated based on the original content of the data frame and the new checksum FCS is calculated based on the content of the original data frame and the SecTag.

Figure 4 illustrates a schematic diagram of an embodiment of the invention, wherein the device is enclosed in a casing of an electronic device 200. The electronic device 200 is adapted to be mechanically and electrically removable-connected to another, a second, electronic device, in this example, the host computer 100, through a host interface 50 such as PCI, ISA, PCI-E, FireWire, USB or Ethernet.

Figure 4a illustrates a particular schematic block diagram of an electrical device of Figure 4, wherein the host interface is an Ethernet interface PHY 44. The host computer can be a handheld, a laptop or a device as such. A particular case is that when an field engineer wants to inspect an industrial system comprising electrical devices capable of communicating data with each other in such a security manner, by plugging in the electronic device 200, he can join the network work and communicate with the other devices in the system. The MAC could be optional in this case as indicated by dot lines.
CLAIMS

1. A device (1) for transmitting and receiving an Ethernet data frame including raw bits, comprising a physical layer (PHY, 42) for transmitting and receiving the data frame, characterized in that the device further comprises a hardware component arranged adjacent to the physical layer (PHY, 42) and the hardware component (2) is configured to
   - generate a cryptographic checksum (SecTag) based on the raw bits of the data frame and add the cryptographic checksum to the end of data frame so as to form an extended data frame to be transmitted to the PHY and,
   - verify the cryptographic checksum (SecTag) in the data frame received from the PHY (PHY, 42).

2. Device according to claim 1, wherein the device further comprises a media access control layer (MAC, 30) for providing addressing and channel access control and interfacing to the physical layer (PHY, 30) and the hardware component arranged between the physical layer (PHY) and the media access control layer (MAC).

3. Device according to claim 1, wherein the hardware component (2) is further configured to process the raw bits of the data frame on a basis of byte when generating or verifying the cryptographic checksum.

4. Device according to claim 1, wherein the hardware component (2) is further configured to calculate a new checksum (FCS) based on the extended data frame and add the new checksum to the end of the extended data frame when the extended data frame is transmitted to the PHY.

5. Device according to claim 1, wherein the hardware component (10) further comprises a memory (20) for storing a cryptographic key set and the cryptographic key set is arranged to generate the cryptographic checksum on the data frame to be transmitted to the PHY and to verify the cryptographic checksum in the data frame received from the PHY.
6. Device according to claim 4, wherein the cryptographic key set is either a secret key or a plurality of keys including at least one public key and a private key.

7. Device according to claim 1, wherein the hardware component is one of the following programmable logic devices (PLD): Field-Programmable Gate Array (FPGA), Complex Programmable Logic Device (CPLD), or Application Specific Integrated Circuits (ASIC).

8. Device according to any of previous claims, wherein the hardware component is adapted to be integrated to the PHY or the MAC.

9. Device according to any of previous claims, wherein device further comprises a media access control layer (MAC, 30) for providing addressing and channel access control and interfacing to the physical layer (PHY, 30) and the hardware component (2) is further configured to, when the verified cryptographic checksum is not consistent with the original data frame, send an error signal (RX_ERR) to the MAC so as to discard the data frame.

10. An electronic device (200) comprising a device (1) according to claim 1 or 2, wherein the electronic device (200) further comprises a casing enclosing the device and is adapted to be mechanically and electrically removable-connected to another, a second, electrical device.

11. Electronic device according to claim 10, wherein the electrical device further comprises a communication interface (50) for receiving or sending data frames to the second electrical device.

12. Electronic device according to claim 11, wherein the communication interface is any of PCI, ISA, PCI-E, FireWire, USB or Ethernet.
Fig. 1
Fig. 3

MAC Destination
MAC Source
802.1Q tag (optional)
Ethertype or length

Payload data
FCS'
SecTag
FCS
### INTERNATIONAL SEARCH REPORT

**INTERNATIONAL APPLICATION**

**PCT/EP2011/051741**

**A. CLASSIFICATION OF SUBJECT MATTER**

**INV.** H04L9/32  
**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 practical, search terms used)**

EP0-Internal

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>paragraphs [0016], [0019], [0026] - [0028]; figure 1A</td>
<td>4-6</td>
</tr>
<tr>
<td>Y</td>
<td>paragraphs [0034] - [0040]; figures 1C, 1D</td>
<td>4</td>
</tr>
<tr>
<td>Y</td>
<td>HONG JIANG ET AL: &quot;Simulation and Analysis of MAC Security Based on NS2&quot;,</td>
<td>5, 6</td>
</tr>
<tr>
<td></td>
<td>MULTIMEDIA INFORMATION NETWORKING AND SECURITY, 2009. MINES '09. INTERNATIONAL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 18 November 2009 (2009-11-18), pages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>502-505, XP031592193, ISBN: 978-0-7695-3843-3 page 1 - page 2, left-hand column</td>
<td></td>
</tr>
</tbody>
</table>

**Further documents are listed in the continuation of Box C.**

**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 document 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

---

**Date of the actual completion of the international search:** 2 November 2011

**Date of mailing of the international search report:** 09/11/2011

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

**Authorized officer:** Horbach, Christian
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2010229013 A1</td>
<td>09-09-2010</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TW 200840279 A</td>
<td>01-10-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2008123652 A1</td>
<td>29-05-2008</td>
</tr>
</tbody>
</table>