ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 12(34), DOI: 10.17485/ijst/2019/v12i34/147550, September 2019* ISSN (Online) : 0974-5645

SCADA Communication Real Time Protocols

Sara Tamy[1]*, Hicham Belhadaoui[1], Mahmoud Almostafa Rabbah[1], Nabila Rabbah[2] and Mounir Rifi[1]

[1]RITM Laboratory, ESTC, Hassan II University, BP. 8012, Oasis, Casablanca, Morocco; saratamy@yahoo.fr, belhadaoui_hicham@yahoo.fr, mrabbah@gmail.com, rifi.mounir@gmail.com
[2] Laboratory of Structural Engineering, Intelligent Systems and Electrical Energy, ENSAM, Hassan II University, BP. 20000, Casablanca, Morocco; nabila_rabbah@yahoo.fr

Abstract

Objectives/Method: SCADA networks are crucial for industrial organizations, and play an important role in real time industrial communication. Today, with the fourth industrial revolution, infrastructures are increasingly connected to the corporate network and to Internet, which makes them more dependent on networks and communication protocols used. This connectivity can help optimize manufacturing and distribution processes while reducing costs, but it also exposes the industrial network to security issues. The purpose of this article is to describe the architecture of SCADA networks and present the most used SCADA communication protocols such as Modbus TCP, IEC 60870-5-104, DNP3, ETHERCAT, SERCOS III, OPC AU, MQTT and SNMP, to provide a comparative study that allows us to choose the most appropriate protocol for industrial communication, especially in the context of Industry 4.0. **Applications/Improvements:** We have presented a comparative study to describe the most used SCADA communication protocols. We therefore present the archetecture of each protocol, the quality of service, the context of use, the security, the frame and other information that allow us to choose the most appropriate protocol to apply in the Industry 4.0. **Findings:** OPC UA is often considered as the next reference for industrial communications, it is a multi-level protocol that includes a security layer to indicate whether future communications will be signed, encrypted or in plain text.

Keywords: Ethernet Protocols, Industry4.0, Session Hijacking, DDoS, Sniffing

1. Introduction

The real-time industrial network is an important element for the construction of automated manufacturing systems. Thus, in order to meet the real-time requirements of field devices like controllers, actuators and sensors, many standard providers have developed various field bus protocols that have a significant advantage over widely used Ethernet. (IEEE 802.3) in terms of deterministic characteristics. However, the field bus application was limited because of a high hardware cost and the complexity to interface with multi-provider products. With the objective of solving these problems, is adopted by industrial sector. But its non-deterministic behavior renders it unsuitable to real time applications, in which the frames containing real time information's, like control command and the alarm signal, have to be delivered at specified period of time.

Recently, switched Ethernet development has presented very promising opportunities to industrial applications by eliminating uncertainties in the functioning of the network, which leads as a result to spectacular improvement of the performances[1].

Generally, the data exchanged over the industrial network is divided into two categories: real-time data which have a strict time constraint and the value of the data is significantly reduced as the time of communication increases and non-real-time data that do not have strict deadlines for communication delays during the exchange of data. The non-real-time data have to be transmitted reliably over networks and delivers data without error, loss or duplication, while real-time data is mainly about the needed time to reach the destination[1]. Thus, we have to choose the protocol used to satisfy the requirements of industrial network 4.0.

**Author for correspondence*

This study focuses on many important protocols that are open, standard and have emerged as contenders to offer the best performance for real-time Ethernet field buses the standards being compared are Modbus/TCP, IEC 60870-5-104, DNP3, Ether cat, SERCOS III, OPC AU, MQTT and SNMP. There are other technologies that leverage Ethernet as well, but their components are not sufficiently published, or promulgated in the open source community to be considered standard and open.

This article is organized as follows: In section II, we present SCADA architecture, in section III, we present the most popular and used SCADA protocols to provide a comparative study of its. In section IV we discuss some security threats, related works is discussed in section V, and we close with a discussion and conclusion in Section VI.

2. SCADA Architecture

Traditionally, SCADA systems have been connected by a Local Area Network (LAN), thus, the network was safety, and the production was centralized.

Presently, with the increasing demand of SCADA over the word, the SCADA architecture has fundamentally changed[2]. The actuators and sensors are supervised and controlled on the SCADA network through using PLC (Programmable Logic Controller) or a PC, and to ensure a remote access we have to use a gateway which defines protocol conversion mechanisms to allow communication between too different networks[3]. An Example of SCADA network is shown in Figure 1. In SCADA network, typical communications allow the exchange of control messages.

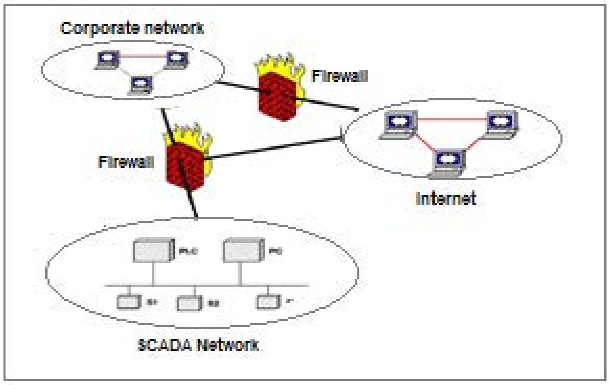


Figure 1. SCADA architecture.

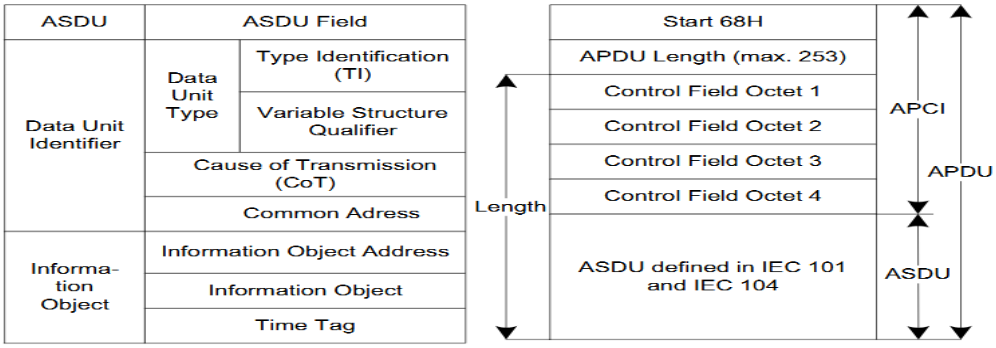
Between the master and the slave devices. A master controls the operations of slaves.

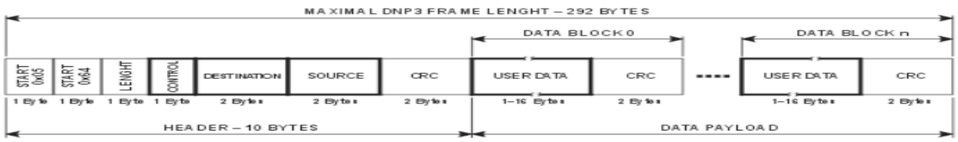
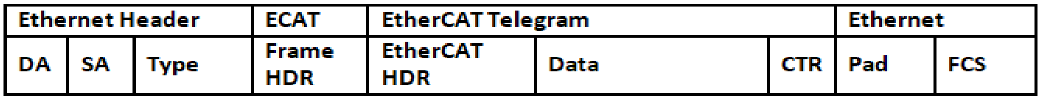
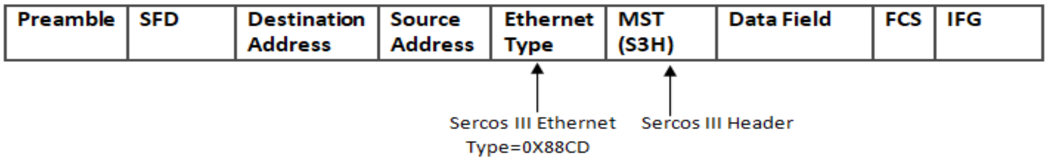
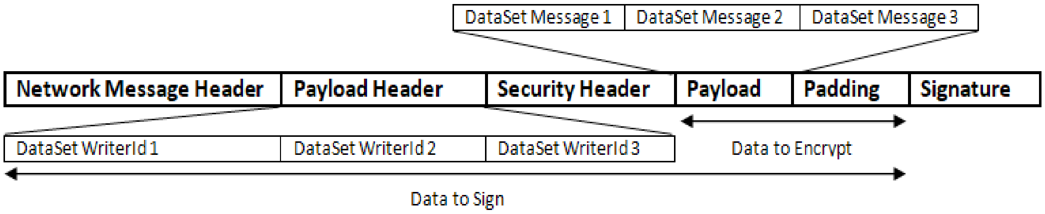
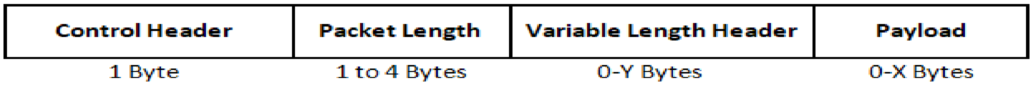
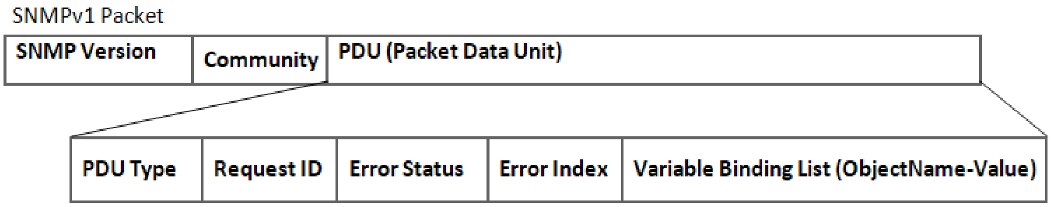
Slave devices are generally a simple actuators or sensors that can transmit messages to a control device and execute actions on command from a master device. Some devices can communicate only via alarms or status messages. As many devices have a common bus, the protocol has to distinguish the critical and non-critical messages. For example, an alert message has to take priority over message for an update of the data. Thus, the network protocol used should have characteristics which ensure delivery of critical messages and respect a real time constraints[4]. We will present some of these protocols in the next section.

3. Protocols Frame

In this section we present the frames of the SCADA protocols (Table1).

Table 1. The frames of the SCADA protocols

Protocol	Trame
Modbus/TCP	Transaction Identifier | Protocol Identifier | Length Field | Unit Identifier | PDU (data) | Checksum
IEC104	 ASDU ASDU Field Data Unit Identifier Data Unit Type Type Identification (TI) Variable Structure Qualifier Cause of Transmission (CoT) Common Adress Information Object Information Object Address Information Object Time Tag Length Start 68H APDU Length (max. 253) Control Field Octet 1 Control Field Octet 2 Control Field Octet 3 Control Field Octet 4 ASDU defined in IEC 101 and IEC 104 APCI APDU ASDU

DNP3	 MAXIMAL DNP3 FRAME LENGHT – 292 BYTES DATA BLOCK 0 DATA BLOCK n START 0x05 START 0x64 LENGHT CONTROL DESTINATION SOURCE CRC USER DATA CRC USER DATA CRC 1 Byte 1 Byte 1 Byte 1 Byte 2 Bytes 2 Bytes 2 Bytes 1–16 Bytes 2 Bytes 1–16 Bytes 2 Bytes HEADER – 10 BYTES DATA PAYLOAD
Ethercat	 Ethernet Header ECAT EtherCAT Telegram Ethernet DA SA Type Frame HDR EtherCAT HDR Data CTR Pad FCS
SERCOS	 Preamble SFD Destination Address Source Address Ethernet Type MST (S3H) Data Field FCS IFG Sercos III Ethernet Type=0X88CD Sercos III Header
OPC AU	 DataSet Message 1 DataSet Message 2 DataSet Message 3 Network Message Header Payload Header Security Header Payload Padding Signature DataSet WriterId 1 DataSet WriterId 2 DataSet WriterId 3 Data to Encrypt Data to Sign
MQTT	 Control Header Packet Length Variable Length Header Payload 1 Byte 1 to 4 Bytes 0-Y Bytes 0-X Bytes
SNMP	 SNMPv1 Packet SNMP Version Community PDU (Packet Data Unit) PDU Type Request ID Error Status Error Index Variable Binding List (ObjectName-Value)

4. Security Threats

In this section we will present some security threats such as DoS/DDoS attack, sniffing and session hijacking.

4.1 DoS / DDOS Attack

DoS (Denial of Service) are attack that consists of sending many messages from computers, in order to overwhelm a company's servers and paralyze its website for several hours, to block access to Internet users. DoS attacks are very easy to put up and very difficult to prevent.

There is different denial of service attacks: Flooding, Smurf, TCP-SYN flooding, Buffer overflow [5].

With DDoS attacks, an attacker may generate traffic similar to the legitimate one, making the defense mechanisms difficult with the use of multiple sources, the attack strength increases[6].

A DDoS attack usually consists of two steps. In[7] the first step, an attacker uses the systems vulnerabilities then takes control and making them "zombies" In the second step, the attacker issues commands to attack the victim the attacker spoofs IP address of the traffic source, thereby disabling identification of the attack source

4.2 Sniffing

A packet sniffer is a software or hardware, which intercepts and record traffic passing through a digital network or part of a network. In[8] this type of threat, the attack is not active, because the malicious entity only listens to the conversations exchanged in the network and copy

Table 2. Comparative table of SCADA protocol

	Modbus/TCP	IEC 60870-5-104	DNP3	Ethercat	SERCOS III	OPC AU	MQTT	SNMP
Architecture	Master/Slave	Master/Slave	Master/Slave	Master/Slave	Master/Slave	Client/Server	Publish/ Subscribe	Client/Server
TCP/UDP port number	-502/TCP	-2404/TCP	-20000/TCP	-34980/TCP -34980/UDP	TCP or UDP	-4840/TCP or UDP OPC UA over TLS/SSL: -4843/TCP or UDP	-1883/TCP or UDP Secure MQTT : -8883/TCP or UDP	-161/TCP or UDP On the agent side. -162/TCP or UDP On master side
QoS	--	--	Two types of data: -static data (class 0) -Event data (class 1,2 and 3)	--	--	-transparent, secure and correct communication. -Communication for any type of data with any type of system.	3 types of Qos: -At most once -At least once -Exactly once	--
Context of use	Real-time Industrial applications						IoT	- network manager
Security	No form of authentication or data encryption	-Plaintext Mode Message Transmission -Lack of Authentication Mechanism:	No form of authentication or data encryption	Black channel (Transmit safe and non safe information).	SIL3 (safety integrity level3)	-authentication and authorization, - auditing -encryption and data integrity via signatures	SSL (Secure Socket Layer)	SNMPV3: -User based Security Model -View based Access Control Model
More detail	-Simple and easy to implement. -Connection oriented - Payloads are limited to at most 253 bytes to maintain compatibility with Modbus over serial lines.	-flexible -performance -Applied to SCADA systems -Defines application protocol control information to detect the start and the end of the ASDUs of IEC101.	-Open -Optimized -Developed for SCADA systems	-Eliminate the bottlenecks of conventional field bus systems. -Use a Principe of processing on the fly	-Simple -Deterministic -Fast -Guaranteed hard real time synchronous data exchange between controllers and devices -Peer-to-peer communications -Flexible network topologies.	- Open - Real-time applications. - Service-oriented architecture - Robust security -Integral information model.	-Open - MQTT v3.1.1 is an OASIS standard -Robust -Each MQTT Implementation is free to provide its own version of security features.	-Simple -minimal -without memory -Use a management Information Base

all transmitted messages, to extract the data that interest him.

4.3 Session Hijacking

The session hijacking may be performed at two different levels: Application or Network level. Network layer hijacking requires TCP or UDP sessions, while session hijacking on the application layer is done using HTTP sessions. Generally, the attack on the network level is more interesting for the attackers because they have not to be customized from web applications basis; they have to attack just the data flow of protocol, which remains common for all web applications[9].

In TCP Session Hijack, TCP hijacks are meant to intercept the already established TCP sessions between two communicating parties and then pretend to be one of them, finally redirect the TCP traffic to it by injecting spoofed IP packets[10].

5. Literature Survey

In this section we will discuss in detail some of the existing works that are relevant to this article.

In[11] describe a secure version of the Modbus protocol that includes integrity, non repudiation, and authentication. The experimental results obtained using a power plant test bench show that the enhanced protocol ensures safety functionality with minimal overload. The new protocol helps to protect against multiple attacks, but it does not address scenarios if an attacker takes control of a master and sends malicious Modbus messages to slave devices, or where an attacker captures the master unit's private key and falsifies malicious Modbus messages that are signed with the stolen key.

In study[12], propose a prototype of an intrusion detection system that detects complex attacks for SCADA systems using Modbus and DNP3 communication protocols, through an internal representation of the controlled SCADA system. They also present the rule language powerful enough to express the critical states of the system.

In[13] present an approach to secure mqttprotocole they propose the "CA" Certification Authority solution in order to generate two types of certificates, the first for clients and the second for topics . If there is a group of clients certified by the same CA and want to exchange messages via a topic, the CA generates a private key and a certificate for this topic. These will be published for certified clients, to allow the safe exchange of messages. When a new client wishes to participate in the flow of a topic safety, it has to send a certificate request to be able to decrypt the published messages. This approach achieves an acceptable level of security, but it presents the problem of network saturation in the event of a large number of users.

In[14] constructed a model discriminating between normal and abnormal packets using a support vector machine based on an ICS communication profile, representing only the intervals and length of the packets, and applied and IDS to their model. The proposed IDS were also evaluated using intrusion tests on cyber security test bench. Despite the fact that the IDS was built according to the limited attributes (intervals and length) of the packets, the IDS has successfully detected cyber attacks by monitoring the expected attack rate.

6. Discussion

Throughout this study, we tried to present the most widely used industrial protocols based on Ethernet. The MQTT and SNMPv3 protocols are open, light and robust. The most recent version of the MQTT features include basic user security that allows authentication using a connect packet, and data can be encrypted using SSL (Secure Sockets Layer). SNMPv3 presents the security mechanisms to be used in conjunction with SNMPv1 or SNMPv2.

Modbus/TCP, IEC 104, DNP3, Ether cat and Serco's are industrial protocols that maximize flexibility, performance and efficiency, designed for the control and supervision of real-time industrial applications. These protocols are deterministic but they are not secure. OPC UA is often considered as the next reference for industrial communications, it is a multi-level protocol that includes a security layer to indicate whether future communications will be signed, encrypted or in plain text. Generally the choice of protocol depends on the work context. Table 2 presents a summary of the protocols discussed.

7. Conclusion

Today the technology industry continues to grow, thus, the barriers between information, communication and automation technologies are progressively disappearing. Factories tend to be closer to customers. The key factors in this regard are safety of communication and guarantee of quality of service. In this study we have presented the comparative studies of the most used industrial protocols, and presented some security threats. Our next work is to secure industrial network by using Intrusion Detection System (IDS), and to ameliorate it we will use machine learning algorithms.

8. References

1. Lee KC, Lee S. Performance evaluation of switched Ethernet for real-time industrial communications. Computer Standards & Interfaces. 2002; 24(5): 411–423. https://doi.org/10.1016/S0920-5489(02)00070-3.
2. Tamy S, Nabila R, Mahmoud Almostafa R. Study of Strategies for Real-Time Supervision of Industrial Network Security. Smart Application and Data Analysis for Smart Cities. 2018; 1–5. https://doi.org/10.2139/ssrn.3185336.
3. Shahzad A, Musa S, Aborujilah A. The SCADA review: system components, architecture, protocols and future security trends. Am. J. Appl. Sci. 2014, 11(8): 1418. https://doi.org/10.3844/ajassp.2014.1418.1425.
4. Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Computers & Security. 2006; 25(7): 498–506. https://doi.org/10.1016/j.cose.2006.03.001.
5. GNU Free Documentation License [internet]. https://www.gnu.org/licenses/fdl-1.3.fr.html. Date accessed: 03/11/2008.
6. Markovic-Petrovic JD, Stojanovic MD. Analysis of SCADA system vulnerabilities to DDoS attacks. In: 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services. 2013; 591–594. https://doi.org/10.1109/TELSKS.2013.6704448.
7. Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys. 2007; 39(1): 3. https://doi.org/10.1145/1216370.1216373.
8. Jung S, Song J, et Kim S. Design on SCADA test-bed and security device. Int. J. Multimed. Ubiquitous Eng. 2008, 3 (4), pp. 75-86.
9. Zhang Y, Wang L, Xiang Y. Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. IEEE Transactions on Power Systems. 2016; 31(6): 4379–4394. https://doi.org/10.1109/TPWRS.2015.2510626.
10. Kapoor S. Session hijacking exploiting TCP, UDP and HTTP sessions [internet]. https://linuxsecurity.com/news/host-security/session-hijacking-exploiting-tcp-udp-and-http-sessions. Date accessed: 25/07/2006.
11. Fovino IN, Carcano A, Masera M. Design and implementation of a secure Modbus protocol. In: International conference on critical infrastructure protection. Springer, Berlin, Heidelberg. 2009; 83–96. https://doi.org/10.1007/978-3-642-04798-5_6.
12. Fovino IN, Carcano A, Murel, Lacheze TD. Modbus/DNP3 state-based intrusion detection system. In: 2010 24th IEEE International Conference on Advanced Information Networking and Applications. 2010; 729–736. https://doi.org/10.1109/AINA.2010.86.
13. Mektoubi A, Hassani HL, Zakari A. Nouvelle approche de communication sécurisée des objets connectés basée sur le Protocole MQTT. Revue Méditerranéenne des Télécommunications. 2016; 6(2) 1–5.
14. Terai A, Abe S, Kojima S. Cyber-attack detection for industrial control system monitoring with support vector machine based on communication profile. In: 2017 IEEE European Symposium on Security and Privacy Workshops. 2017; 132–138. https://doi.org/10.1109/EuroSPW.2017.62.