Chapter 17
SCADA: Analysis of Attacks on Communication Protocols

T. C. Pramod and N. R. Sunitha

Abstract SCADA (supervisory control and data acquisition) systems are used to monitor and control the processes of industrial facilities remotely. The use of standard technologies and interconnections between the systems lead to variety of security attacks. SCADA systems are being the part of many critical applications of the society. Any minute deviation in the normal operation of the system results in serious consequences. Hence, securing the industrial control systems is a high priority issue. One can provide security and safety to the system by identifying possible sources of threats and objectives of attackers and continuous monitoring of the operations of the system. In this paper, attack incidents occurred on command and control systems are presented (from the year 1982 to 2017), the general attacker goals on SCADA systems are discussed, SCADA communication protocols and its normal/abnormal behaviors are analyzed using the Wireshark tool.

Keywords Critical infrastructures · DNP3 · Industrial control systems · ModbusTCP · SCADA attacks · SCADA security · Stuxnet · Ransomware · Wireshark

17.1 Introduction

Critical infrastructures are the primary needs of the society. As the need for such infrastructures is increasing along with technological improvements, the global usage, interconnections, and sophistication in the operations of these infrastructures are also increasing. In order to reduce the complexity, there is a need for simple and efficient process supporting remote control of various activities, which can be achieved through automation. Thus, these infrastructures heavily depend on industrial control system (ICS) such as SCADA systems, distributed control systems

T. C. Pramod (✉) · N. R. Sunitha
Department of Computer Science, Siddaganga Institute of Technology, Tumakuru, Karnataka, India

N. S. V. Rao et al. (eds.), *Proceedings of International Symposium on Sensor Networks, Systems and Security*, https://doi.org/10.1007/978-3-319-75683-7_17

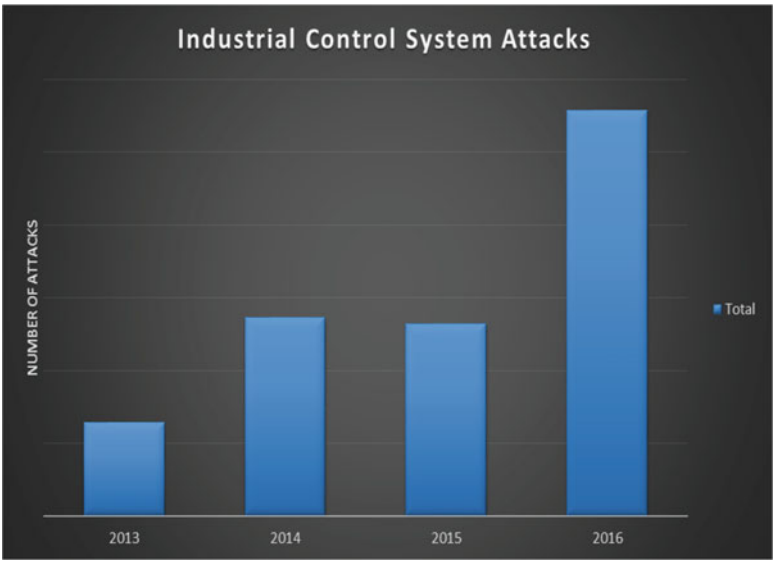

Fig. 17.1 Industrial control system attacks [2]

(DCS), and Remote Terminal Units (RTU). Presently, the critical infrastructures such as electric power grids, water distribution plants, paper and pulp industry, oil refineries, chemical production and processing, and manufacturing plants are the major examples in which the SCADA systems are playing a critical role [1].

In the past, considering security for the industrial automation domain had less attention. From the year 2010, due to massive security attacks, the implication of security features for command and control systems is proliferating. Figure 17.1 shows the total attacks on ICS on different years [2]. The following are the reasons for the proliferation of cyberattacks on the ICS:

- The use of standard technologies in the automation systems is increasing. The use of COTS (commercial off-the-shelf) hardware and software products, common internet protocols and solutions, and Windows- and Unix-like operating systems is quite common in the industrial automation systems.
- To achieve cost-effectiveness, fast decision-making and to optimize the production and manufacturing processes, the industrial networks are increasingly interconnected.
- Initially, the industrial communication protocols (Modbus, DNP3, etc.) were designed as serial communication protocols (to run over a serial connection). Over time, these protocols are used as application layer protocols on top of the TCP/IP stack. But, the lack of adoption of security measures and cryptographic mechanisms provides a way for the hackers to interrupt the normal communications.

- Incorporation of wireless technologies in the industrial automation systems. Many security attacks are possible in wireless solutions [3].
- Insecure communication links are also a security concern. The communication between the control center and remote locations may take place using the Internet/radio or microwave/leased lines. Compromising these communication links is easy for the hackers [4].
- Connection of industrial automation network with third-party vendors, contractors, alliance partners, and outsourcing also leads to cyberattack incidents.
- Significant information about automation and control systems is freely available to the public sector. Search engines like Google dorks [5], Shodan [6], and Pastebin [7] provide significant information about the industrial control systems online.

To secure the infrastructures, solutions like secure communications (encryption and decryption) and intrusion detection systems (IDS) can be used. Since the lifetime of ICS is high, i.e., in decades, many industries contain legacy hardware and software systems. Also, in some real-time industrial applications, the latency involved in performing cryptographic operations may not be tolerable. This introduces the difficulty to incorporate encryption/decryption operations. In such cases, IDS can be used for monitoring the malicious activities. Also, some of the proprietary or legacy protocols used in ICS may not be supported by current IT security tools such as firewalls or IDS. An alternate solution is the use of forensic techniques where details like where the attack originated, the processed involved, and the responsible identity for the attacks can be determined.

The rest of this paper is organized as follows: In Sect. 17.2, an overview of SCADA systems is presented. In Sect. 17.3, attack incidents (year 1982–2017) occurred on SCADA systems are discussed. In Sect. 17.4, attacker goals on SCADA systems are discussed in general. In Sect. 17.5, possible attacks on Modbus and DNP3 protocols are listed. In Sect. 17.6, using the Wireshark tool, Modbus packets are analyzed, and Sect. 17.7 gives the conclusion.

17.2 SCADA Systems

SCADA systems are designed to monitor and control the industrial processes remotely. Figure 17.2 shows the architecture of the SCADA systems. It consists of the following devices:

- HMI (human-machine interface): HMI provides an interface for the operator to interact with the system and to view and react to the process status and historical events [1].
- MTU (Master Terminal Unit): MTU is the higher-level device in the SCADA system, which collects the data from the distributed field-level equipments by issuing commands, stores and processes the data, and displays the information in the form of graphs, curves, and tables to HMI.
- SUBMTU: To alleviate the burden of the primary MTU, SUBMTUs are used.

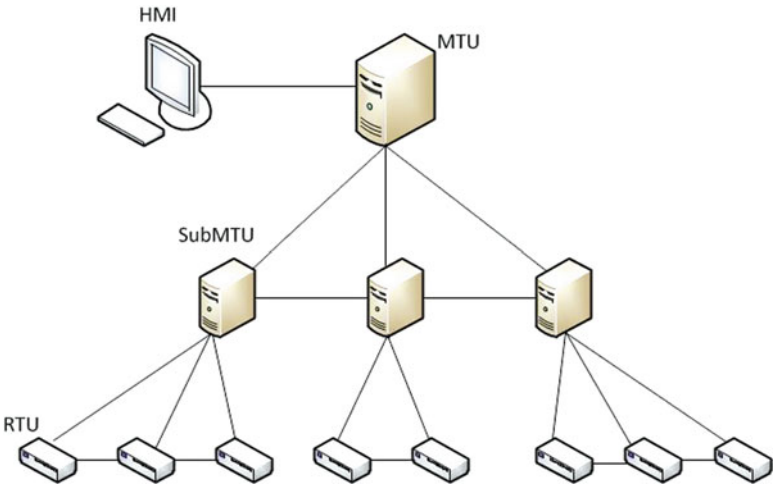

Fig. 17.2 SCADA architecture [8]

- RTU (remote terminal unit): RTUs are used for data acquisition from sensor devices and actuators. They send the collected data to master terminal unit (MTU) in digital format. They are located remotely from the control center.

17.2.1 Behavior of the SCADA Systems

- *Traffic periodicity:* In SCADA systems, the packet transmission rate is periodic in nature. The stability is due to the automated process. Communications occur based on polling mechanism (HMI polls PLC at a fixed frequency).
- *Fixed number of devices:* The network consists of fixed number of devices.
- *Continuous operation:* The systems are intended to operate ceaselessly for a long time.
- *Limited number of protocols:* The number of protocols used in SCADA network is less.
- *Limited number of packets:* The network has low throughput. The communications are regular in nature.
- *Limited human-initiated actions:* The HMI-to-PLC communication is extremely regimented device-to-device communication, with minimal human-initiated actions.

17.3 Attack Incidents on Command and Control Systems

A view on attack incidents occurred on command and control systems is portrayed in Table 17.1 (from the year 1982–2017).

17.4 Attacker's Goals on SCADA Systems

By observing the key characteristics of the SCADA systems, we have identified some of the general attacker objectives:

- **Gaining access into the SCADA network:** In order to perform malicious activities and to disrupt the normal processes, the primary goal of the attacker is to enter the SCADA network. The attackers may enter the system via vendors/contractors (third party), disgruntled employees, unsecured remote field sites, IT network, SCADA transmission media, wireless interface, Internet, corporate network, remote access, infected USB or laptops, physical attack, or poorly configured firewalls.
- **Identifying SCADA devices and available ports in the network:** Once the attacker gets access into the network, their intention is to identify the devices, ports used/opened, and communication paths. Recognizing who is master, who are slaves, and protocols used for communication is their curiosity.
- **Switching on/switching off the devices:** The operations of SCADA systems are remote based. The attacker may send a command to switch off the device in place of controller's command to switch on the device and vice versa.
- **Reading data from the devices:** The communication protocols were designed without considering cryptographic features. Reading the conversation between master and slave devices or reading the data directly from the slave or master device is the attacker interests.
- **Writing data into the devices:** The lack of authentication helps the attackers to write the data into the devices. The attacker likes to overwrite the existing programs or modify the configurations of the devices.
- **Disrupting the communications:** Sending invalid commands, delaying the response or reply between the devices, performing packet loss, overflow in the communication path, modifying the transmitted readings, and sending misleading values to the system operator are the attacker interests.
- **Compromising the devices:** Virus, Worms, and Trojans are used to compromise the devices. Through the compromised devices, the attacker controls the operations of the industrial plant.
- **System-related threats:** Exploit software/configuration vulnerabilities of the SCADA system (buffer overflow due to illegal packet size, exploiting bug, stack overflow, misconfigured radio network).

Table 17.1 Command and Control Systems attack incidents

Year	Place	Attacks
1982	Russian-Siberian pipeline	Trojan was used to take control of the SCADA system [9]
1992	Chevron refinery in Richmond, California	Former employee crippled the functionality of the alert system by hacking the computers [10]
1994	Salt River Project in Arizona	Gained access into the network through dial-up modem. Controlling the water channels and collecting employee's log-in and password and customer information were the attacks observed [11]
1997	Worcester Airport, Massachusetts	Accessed and crippled the service of computer in the telephone company. The telephone service was disconnected for airport departments [12]
1999	Gazprom in Russia	Hacker was associated with the employee of the gas company to take control of gas flow [13]
1999	Bellingham, Washington	Leakage in the gas flow; disabling the monitoring and controlling functionality of control systems [14]
2000	Queensland, Australia	A former employee has taken control of Maroochy Shire water control system. The huge amount of sewage water was spilled into rivers, hotels, and parks [15]
2001	California	The attack was to gain access into the computer network of the command and control system [12]
2003	Ohio, USA	Worm (SQL Slammer) was used to mask the display and plant processes of Davis-Besse nuclear power plant [16]
2003	Florida, USA	Virus "Sobig" was used to turn off the train signaling systems of the CSX Corporation (transportation service provider) [12]
2004	Gulf of Mexico	Virus "Sasser" was used to perform a buffer overflow attack and propagate the vulnerability to other systems [17]
2007	Willows, USA	The dismissed employee installed an illicit software on Tehama-Colusa Canal Authority SCADA system [18]
2010	Natanz, Iran	Virus "Stuxnet" was used to exploit zero-day vulnerabilities. The target was Siemens PLCs. Changing the computer code and altering the speed of centrifuges were the attacker objectives [19]
2011	America, Europe, and Asia	"Night Dragon" Trojan social engineering was used to gather the operational blueprints and project financial information of control systems [20]

(continued)

Table 17.1 (continued)

Year	Place	Attacks
2012	America, Europe, and Asia	Virus "Duqu" was used to gather the control system data [21]
2012	Iran, Lebanon, Syria, and Sudan	Virus "Flame" was used to steal sensitive information, sniff the traffic, and capture the screenshots [22]
2012	Canada	Chinese hackers stole the project files of the product (OASyS SCADA) belonging to the SCADA maker "Telvent" [23]
2014	USA and Europe	Virus "Havex" was used to steal the information from the infected computers by installing remote access tool. The virus was distributed using vendor websites and email attachments [24]
2014	USA	Malware "BlackEnergy" was used to compromise the HMI of control systems [25]
2014	Germany	Social engineering and spear phishing were used to damage the German steel plant (blocked the shutdown functionality of blast furnace) [26]
2015	Finland, the UK, and the USA	The report entitled "SCADA attacks are on the rise" by Dell security team mentioned that attacks on SCADA systems are doubled compared to the previous year [27]
2015	Ukraine	Trojan BlackEnergy is used to cut off the power in several regions of Ukraine [28]. The BlackEnergy backdoor was used to plant a KillDisk component onto the targeted computers
2016	–	Irongate malware, similar to Stuxnet, was used to hack the Siemens industrial control systems [29]
2016	European energy company	Furtim malware is used to create a backdoor on targeted ICS. The intention was to extract data or potentially shut down the energy grid [30]
2016	USA	Using a cellular modem, the attackers compromised the dam's command and control system [2]
2016	San Francisco	Public transport system was infected with ransomware, allowing passengers to ride free during the busy Thanksgiving holiday weekend [31]
2017	Austria	Hacking attack that took over the hotel's entire electronic key management system. Hotel's computer system and payment systems were also compromised [32]
2017	–	Researchers simulated a piece of ransomware taking control of a water treatment plant and poisoning a city's water supply [33]

- **Insider attacks:** Gaining access rights, getting the credentials of engineer/operator, stealing the passwords, altering the employee data, and manipulating the access list are the attacker interests.
- **Attack on acquisition data:** The attacker may try to control the collection of valid entries in the logs or may alter/delete the recorded entries.
- **Crashing the devices for a period of time:** Access the devices, keeping the device in busy mode, and disrupting the normal traffic flow are attacker interests.
- **Attacks on SCADA systems:** The primary targets include the master, field devices, and communication paths. The following are the possible attacks:
  Master level: Violating authorization, data modification, DOS attack, bypass control, information leakage, illegitimate use, physical attack, resource exhaustion, theft, tunneling, introducing virus, worms and Trojan horse, and unauthorized access.
  Communication link: Data modification, eavesdropping, replay attack, man in the middle attack, rerouting the messages, sniffing, and traffic analysis.
  Field level: Violating authorization, DOS attack, data modification, sniffing, spoofing, and physical attack.

17.5 Possible Attacks on Modbus TCP and DNP3 Protocols

Modbus [34] and DNP3 [35] are the commonly used communication protocols to connect industrial devices. Modbus is a master-slave protocol. Communications are polling based. The master device sends a request message to the slave device. Upon receiving the request, the slave device sends either a normal response or an exception. It is predominantly used in the gas and oil sectors [36]. Recently, Modbus has been extended to support the TCP/IP stack (Modbus TCP) [34]. The protocol is simple and reliable, but it does not provide any security feature (authentication and confidentiality). Messages are exchanged in plain text. This leads to the possibility of security attacks in the industrial networks [36].

DNP3 consists of four layers (application, pseudo-transport, data link, and physical). DNP3 is commonly used in North America for power grids and oil refiners [35].

- **Possible Attacks on Modbus TCP protocol:** Table 17.2 shows the Modbus TCP attacks with respect to TCP, and Table 17.3 shows the Modbus TCP attacks with respect to Modbus TCP.
- **Possible Attacks on DNP3 Protocol:**
  Table 17.4 shows the DNP3 attacks with respect to data link layer. Table 17.5 shows the DNP3 attacks with respect to pseudo-transport layer. Table 17.6 shows the DNP3 attacks with respect to application layer.

Table 17.2 Modbus TCP attacks with respect to TCP [37]

Modbus TCP attacks	With respect to TCP
Irregular TCP framing	The intention is to jeopardize by creating improperly framed messages
TCP FIN flood	Intentionally terminate the TCP connection by setting a FIN flag
TCP RST flood	Intentionally reset the TCP connection by setting a RST flag
TCP pool exhaustion	Prevent the Modbus device to accept new connections. The intention is to exhaust the connections to achieve DOS attack

Table 17.3 Modbus TCP attacks with respect to Modbus TCP

Modbus TCP attacks	With respect to Modbus TCP
Broadcasted message spoofing	Broadcasting false messages to slave devices
Replaying	Attacker fools the devices by resending the stored data
Controlling the devices	Behave as master and directly control the slave devices
Perform malicious activities with function code (FC) and subfunction code (SFC)	FC: 08 and SFC:0A—clears all counters and diagnostic registers of the addressed field device. FC: 08 SFC: 01—enables remote restart FC: 17—return the status information of the addressed field device
Network scanning	Acquiring information about the field devices by sending favorable message to all addresses
Delay in response	Introducing delay in response, in slave to master communication. FC:08-04—enforce listen mode
Retrofitting the device	Man-in-the-middle attack by introducing the device in the unprotected communication path
DOS attack	Flood with large number of Modbus packets with invalid CRC A large number of packets with invalid CRC may crash or make the system go to idle state

17.6 Modbus Packet Analysis Using Wireshark Tool

The following section gives the analysis made on the captured packets (Fig. 17.3).
Number of packets: 21,159
Protocol: Modbus

- To check the request and reply packets of the master and slave devices, the following filters can be used:
  Filter the specific source IP: ip.src==10.0.0.57
  Filter the specific destination IP: ip.dst==10.0.0.3
- What is the time taken (delay) for the request and response packets (response time)?
  In Fig. 17.4, the time difference between 7th (query) and 8th (response) packets is 0.000792 s.

Table 17.4 DNP3 attacks with respect to data link layer [38]

DNP3 attacks	With respect to data link layer
Modifying the destination address	Send the request message to other devices (reroute the request)
False data broadcasting	Send erroneous data to all devices
Masking the available function	Function code: 14/15 is used to send a message to the master. It indicates functionality is not implemented or not functioning in the outstation device
Length overflow attack	Specifying invalid length in the length field of the message
Reset the device	The attack uses the function code: 1 to make the targeted device restart
Masking the device	The attack sets the DFC flag to 1 to intimate the master that the slave is busy and cannot handle the request

Table 17.5 DNP3 attacks with respect to pseudo-transport layer

DNP3 attacks	With respect to pseudo-transport layer
Fragmented message interruption	Interrupt the reassembly process of fragmented messages by setting the FIR and FIN flag with invalid time
Alter the transport sequence	Inserting the series of frames to cause processing errors

Table 17.6 DNP3 attacks with respect to application layer

DNP3 attacks	With respect to application layer
Perform malicious activities with function codes	DNP3 message with function code (FC) to outstations FC:02 $\Longrightarrow$ writes data objects to an outstation FC:09/10(No ack) $\Longrightarrow$ freeze and clear the data objects FC: 17 $\Longrightarrow$ reinitialize data objects FC: 18 $\Longrightarrow$ terminate the running applications FC: 21 $\Longrightarrow$ damage the unsolicited messages from slave to master
Send invalid internal indications (IIN) (16 bit)	Attacker sets the bit, which is reserved to intimate the master that the configuration file of the outstation is corrupted

- In SCADA system, packet transmission rate is periodic in nature (Sect. 17.2.1). By observing the response time, we can classify the communication patterns as normal (N)/retransmission (R)/miss (M)/abnormal (A) as follows (Fig. 17.5):
  - **Normal (N):** This state indicates that the communication pattern between the devices is normal. If the timing difference between the request and response

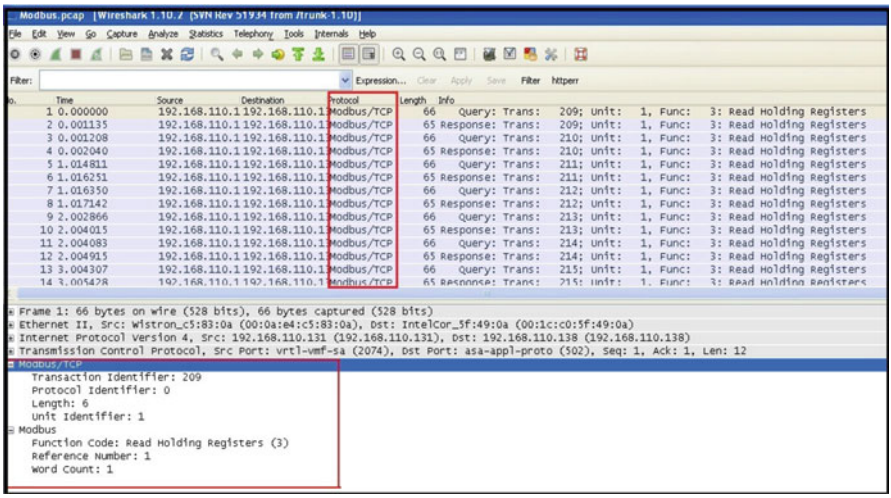

Fig. 17.3 Modbus packets

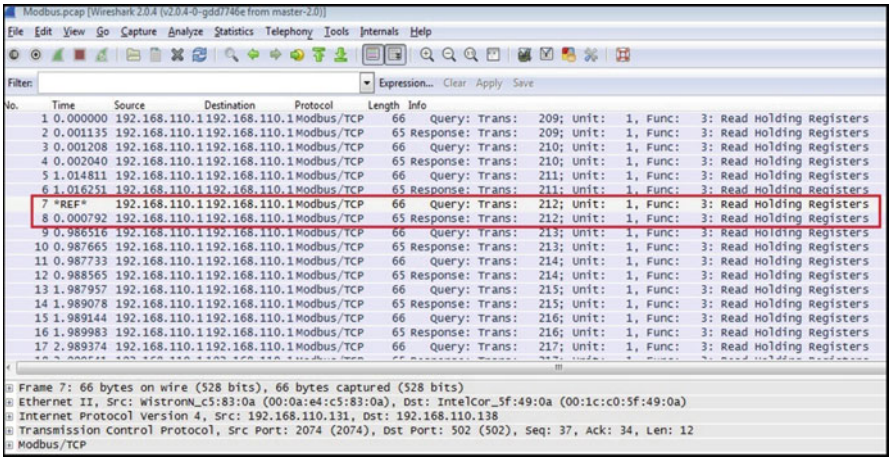

Fig. 17.4 Response time between the request-reply packets

packets is within the normal threshold time (NT), then it is classified as normal packet (Case 1), i.e., WaitingTime (WT) = (T2-T1) <=NT.

SCADA systems are static in nature (Sect. 17.2.1). The IP addresses assigned to the systems are not changed frequently. These features help to consider some more parameters to classify the packet as normal or not. Additional parameters that can be considered along with the timing parameter are IP address, packet size, protocol used, and transaction ID.

Cases	Communication between the two devices [Source IP – Destination IP]	Request/Query Message (Rq)	Reply Message (Rp)	Time Difference	State Estimation			
					N	R	M	A
1	D1-D2	Rq @ time T1	Rp @ time T2	T2-T1<=NT				
2	D1-D2	Rq @ time T1 Rq @ time T2	- Rp @ time T3	NT<T3-T1<=RT				
3	D1-D2	Rq @ time T1 Rq @ time T2	- -	WT>RT				
4	D1-D2	Rq @ time T1	Rp @ time T2 Rp @ time T3 Rp @ time T4	T2-T1<=NT				

Fig. 17.5 State estimation

The packet can be classified as normal packet, if the packet contains valid IP addresses, valid protocol, valid packet size, and same transaction ID between the request and reply packets.

- **Retransmission (R):** If the timing difference between the request and response packets is greater than the normal threshold time but less than the retransmission threshold time (RT), it is classified as retransmission packet, i.e., NT<(WT=(T3-T1))<=RT. Reaching this state does not mean that there is malicious activity, but normal communication patterns are missing.
  The reasons for retransmission states are as follows: device was not ready to handle the request due to congestion or poor communication link or due to security attack (Case 2).
- **Miss (M):** The sender sends the request, but does not receive any reply from the receiver, leading to missing state. In this case, because of no reply, it is not possible to calculate the timing difference. Instead, if the waiting time is greater than retransmission threshold time, i.e., WT > RT, the packet is classified as missing state.
  The reasons for missing state are congestion or poor communication link or packet drop (Case 3).
- **Abnormal (A):**The sender sends the request, but receiver tries to send number of duplicate response messages in short span of time. In this case, the timing difference between the request and the first response is within the normal threshold time, but without request messages the receiver has sent multiple replies, this leads to the abnormal state. Flooding number of packets in a short span of time leads to DoS attack (Case 4).

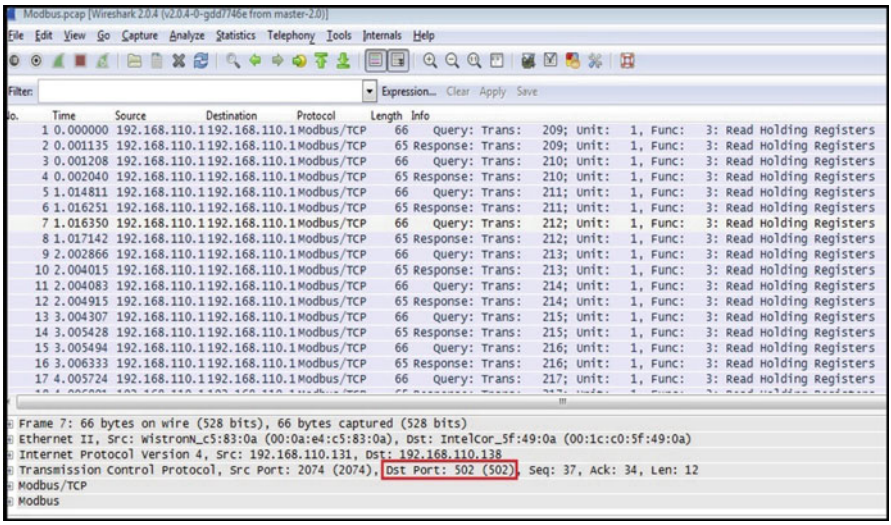

Fig. 17.6 Modbus port number and payload size

- The port used for communication (Modbus uses port 502) and the payload that is limited to at most 253 bytes in Modbus communications can be observed using Wireshark (Fig. 17.6).
- The function codes between the request and response message can be observed by using the Filter: modbus.functioncode==“function code number.” The function code number could be 3, 5, 18, etc. If any packet contains invalid function code, it shall be considered as invalid/malicious packets.
- IO graph: Wireshark IO graphs show the overall traffic seen in a capture file which is usually measured in bytes per second (Fig. 17.7).

17.7 Conclusion

SCADA systems are being the part of critical infrastructures. The proliferation of security attacks and cybercrime incidents on SCADA systems enforcing the industries to consider security is a critical issue. In this paper, attack incidents occurred on SCADA systems (from the year 1982 to 2017) is listed. The attacker goals on SCADA systems are discussed in general. The possible attacks on Modbus TCP protocol are analyzed using the Wireshark tool.

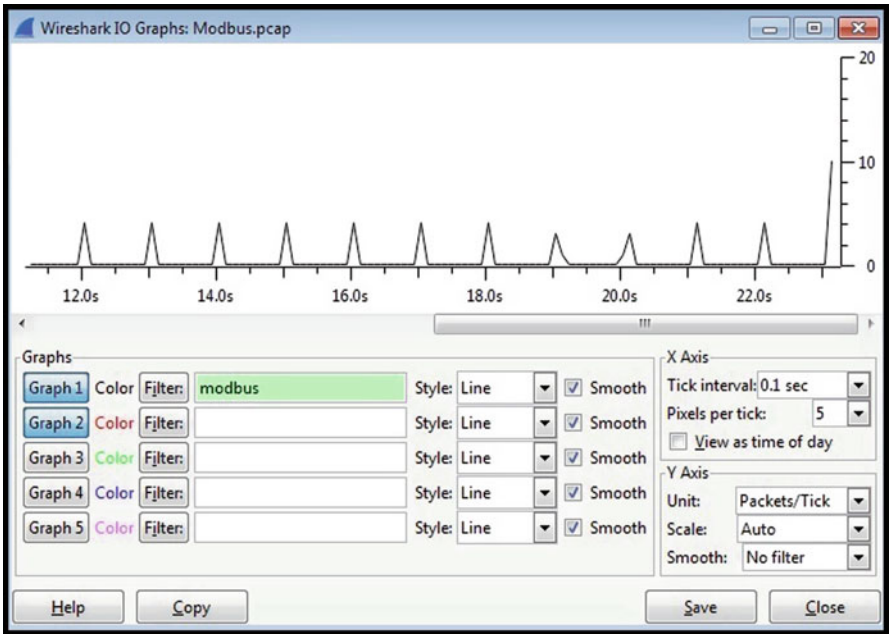

Fig. 17.7 IO graph

References

1. Spellman, F.R.: Energy Infrastructure Protection and Homeland Security. Bernan Press, Lanham (2016)
2. McMillen, D.: Attacks targeting industrial control systems (ics) up 110 percent. https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/. Accessed July 2017
3. Sastry, S., Cardenas, A.A., Roosta, T.: Rethinking security properties, threat models, and the design space in sensor networks: a case study in scada systems. Ad Hoc Netw. **7**, 1434–1447 (2009)
4. Dacey, R.F.: Critical infrastructure protection: challenges and efforts to secure control systems: gao-04-628t. GAO Reports **1**, 29–30 (2004)
5. Google dorks. http://www.exploit-db.com/google-dorks/. Accessed 1 Feb 2017
6. Shodan. https://www.shodan.io/. Accessed 1 Feb 2017
7. Wilhoit, K.: Who is really attacking your ics equipment. Trend Micro Incorporated (2013)
8. Sunitha, N.R. et al.: Kmi for scada and wirelesshart in iacs. In: 2015 IEEE 20th Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–4. IEEE, New York (2015)
9. Daniela, T.: Communication security in scada pipeline monitoring systems. In: Roedunet International Conference (RoEduNet), 2011 10th, pp.1–5. IEEE, New York (2011)
10. Denning, D.E.: Cyberterrorism: the logic bomb versus the truck bomb. Glob. Dialogue **2**(4), 29 (2000)
11. Turk, R.J., et al.: Cyber Incidents Involving Control Systems. Idaho National Engineering and Environmental Laboratory, Idaho Falls (2005)
12. Miller, B., Rowe, D.: A survey scada of and critical infrastructure incidents. In: Proceedings of the 1st Annual Conference on Research in Information Technology, pp. 51–56. ACM, New York (2012)

13. Tsang, R.: Cyberthreats, vulnerabilities and attacks on scada networks. University of California, Berkeley, Working Paper (2010). http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf (as of 28 Dec 2011)
14. Mustard, S.: Security of distributed control systems: the concern increases. Comput. Control Eng. J. **16**(6), 19–25 (2005)
15. Stamp, J., Dillinger, J., Young, W., DePoy, J.: Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories (2003)
16. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H.: Scada security in the light of cyber-warfare. Comput. Secur. **31**(4), 418–436 (2012)
17. Canavan J.: The evolution of malicious irc bots. In: Virus Bulletin Conference, pp. 104–114 (2005)
18. Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., Sastry S.: Challenges for securing cyber physical systems. In: Workshop on Future Directions in Cyber-Physical Systems Security, p. 5 (2009)
19. Hernández Jiménez, J., Chen, Q., Nichols, J., Calhoun, C., Sykes, S.: Towards a cyber defense framework for scada systems based on power consumption monitoring. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
20. Night dragon. http://www.pcworld.com/article/219251/article.html. Accessed 17 Jan 2017
21. Misra, S., Maheswaran, M., Hashmi, S.: Case studies of selected iot deployments. In: Security Challenges and Approaches in Internet of Things, pp. 77–94. Springer, Berlin (2017)
22. Cyberwars. https://www.rt.com/news/flame-stuxnet-kaspersky-iran-607/. Accessed 17 December 2017
23. Maker of smart-grid control software hacked. https://www.wired.com/2012/09/scada-vendor-telvent-hacked/. Accessed 17 January 2017
24. Meshram, A., Haas, C.: Anomaly detection in industrial networks using machine learning: a roadmap. In: Machine Learning for Cyber Physical Systems, pp. 65–72. Springer, Berlin (2017)
25. Meara, K.O., Shick, D., Spring, J., Stoner, E.: Malware capability development patterns respond to defenses: two case studies (2016)
26. Green, B., Prince, D., Busby, J., Hutchison, D.: The impact of social engineering on industrial control system security. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 23–29. ACM, New York (2015)
27. Flowers, A.S., Smith, S.C., Oltramari, A.: Security taxonomies of industrial control systems. In: Cyber-security of SCADA and Other Industrial Control Systems, pp. 111–132. Springer, Berlin (2016)
28. Khan, R., Maynard, P., McLaughlin, K., Laverty, D., Sezer, S.: Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In: 4th Int'l Symposium ICS & SCADA Cyber Security Research. BCS, pp. 53–63 (2016)
29. https://thehackernews.com/2016/06/irongate-stuxnet-malware.html/. Accessed 17 January 2017
30. Leyden, J.: Scada malware caught infecting european energy company. https://www.theregister.co.uk/2016/07/12/scada-malware/. Accessed July 2017
31. Ransomware attack on san francisco public transit gives everyone a free ride. https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware. Accessed July 2017
32. Hackers take over a hotels computer system, lock guests in rooms and hold hotel to ransom. goo.gl/9JRsOA. Accessed July 2017
33. Rsa 2017: Researchers create ransomware for industrial control systems. goo.gl/eYPxxY. Accessed July 2017
34. Goldenberg, N., Wool, A.: Accurate modeling of modbus/tcp for intrusion detection in scada systems. Int. J. Crit. Infrastruct. Prot. **6**(2), 63–75 (2013)
35. Amoah, R., Camtepe, S., Foo, E. Formal modelling and analysis of dnp3 secure authentication. J. Netw. Comput. Appl. **59**, 345–360 (2016)

36. Ramos, R., Barbosa, R.: Anomaly detection in SCADA systems-a network based approach. PhD thesis, Centre for Telematics and Information Technology, University of Twente (2014)
37. Huitsing, P., Chandia, R., Papa, M., Shenoi, S.: Attack taxonomies for the modbus protocols. Int. J. Crit. Infrastruct. Prot. **1**, 37–44 (2008)
38. East, S., Butts, J., Papa, M., Shenoi, S.: A taxonomy of attacks on the dnp3 protocol. In: International Conference on Critical Infrastructure Protection, pp. 67–81. Springer, Berlin (2009)