Protokoły komunikacyjne w przemyśle

Bazan Michał

Agenda

- Znaczenie komunikacji w przemyśle
- Wprowadzenie teoretyczne
- Przykład zastosowania Modbus TCP/IP oraz Ethernet IP
- Bezpieczeństwo komunikacji

Komunikacja w przemyśle

- Zastosowania w przemyśle
- Rodzaje systemów komunikacyjnych w przemyśle
- Znaczenie bezpieczeństwa i niezawodności dla przemysłu

Modbus TCP/IP

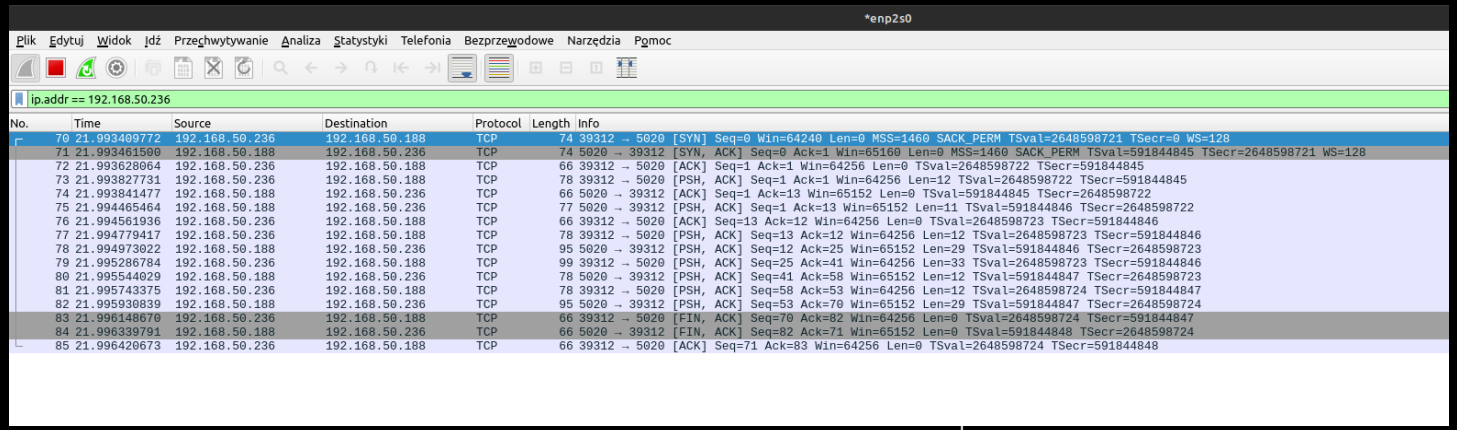
- Standardowa infrastruktura Ethernet
- Klient-serwer
- Z góry zdefiniowane instrukcje

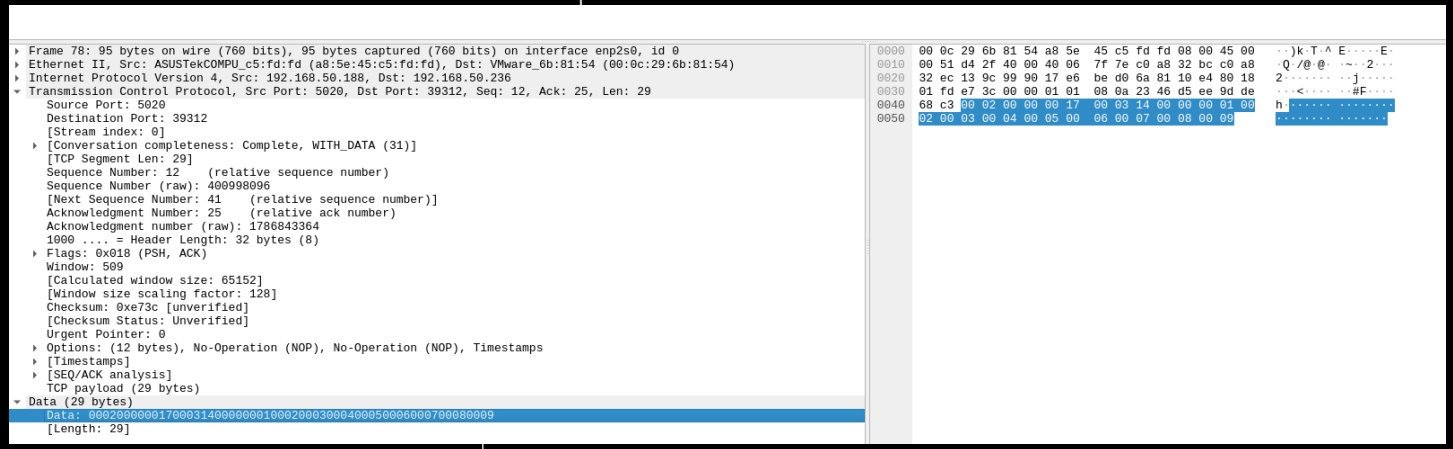
Wady i zalety Modbus TCP/IP

- Prosta implementacja
- Kompatybilność z urządzeniami
- Standardowa infrastruktura Ethernet

- Ograniczone funkcje
- Brak mechanizmów zabezpieczeń
- Ograniczona ilość urządzeń

Zagrożenia


*enp2s0
Plik Edytuj Widok Idź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
ip.addr == 192.168.50.236
No. Time Source Destination Protocol Length Info
70 21.993409772 192.168.50.236 192.168.50.188 TCP 74 39312 → 5020 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2648598721 TSecr=0 WS=128
71 21.993461500 192.168.50.188 192.168.50.236 TCP 74 5020 → 39312 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=591844845 TSecr=2648598721 WS=128
72 21.993628064 192.168.50.236 192.168.50.188 TCP 66 39312 → 5020 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2648598722 TSecr=591844845
73 21.993827731 192.168.50.236 192.168.50.188 TCP 78 39312 → 5020 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=12 TSval=2648598722 TSecr=591844845
74 21.993841477 192.168.50.188 192.168.50.236 TCP 66 5020 → 39312 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=591844845 TSecr=2648598722
75 21.994465464 192.168.50.188 192.168.50.236 TCP 77 5020 → 39312 [PSH, ACK] Seq=1 Ack=13 Win=65152 Len=11 TSval=591844846 TSecr=2648598722
76 21.994561936 192.168.50.236 192.168.50.188 TCP 66 39312 → 5020 [ACK] Seq=13 Ack=12 Win=64256 Len=0 TSval=2648598723 TSecr=591844846
77 21.994779417 192.168.50.236 192.168.50.188 TCP 78 39312 → 5020 [PSH, ACK] Seq=13 Ack=12 Win=64256 Len=12 TSval=2648598723 TSecr=591844846
78 21.994973022 192.168.50.188 192.168.50.236 TCP 95 5020 → 39312 [PSH, ACK] Seq=12 Ack=25 Win=65152 Len=29 TSval=591844846 TSecr=2648598723
79 21.995286784 192.168.50.236 192.168.50.188 TCP 99 39312 → 5020 [PSH, ACK] Seq=25 Ack=41 Win=64256 Len=33 TSval=2648598723 TSecr=591844846
80 21.995544029 192.168.50.188 192.168.50.236 TCP 78 5020 → 39312 [PSH, ACK] Seq=41 Ack=58 Win=65152 Len=12 TSval=591844847 TSecr=2648598723
81 21.995743375 192.168.50.236 192.168.50.188 TCP 78 39312 → 5020 [PSH, ACK] Seq=58 Ack=53 Win=64256 Len=12 TSval=2648598724 TSecr=591844847
82 21.995930839 192.168.50.188 192.168.50.236 TCP 95 5020 → 39312 [PSH, ACK] Seq=53 Ack=70 Win=65152 Len=29 TSval=591844847 TSecr=2648598724
83 21.996148670 192.168.50.236 192.168.50.188 TCP 66 39312 → 5020 [FIN, ACK] Seq=70 Ack=82 Win=64256 Len=0 TSval=2648598724 TSecr=591844847
84 21.996339791 192.168.50.188 192.168.50.236 TCP 66 5020 → 39312 [FIN, ACK] Seq=82 Ack=71 Win=65152 Len=0 TSval=591844848 TSecr=2648598724
85 21.996420673 192.168.50.236 192.168.50.188 TCP 66 39312 → 5020 [ACK] Seq=71 Ack=83 Win=64256 Len=0 TSval=2648598724 TSecr=591844848


Frame 78: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface enp2s0, id 0
Ethernet II, Src: ASUSTekCOMPU_c5:fd:fd (a8:5e:45:c5:fd:fd), Dst: VMware_6b:81:54 (00:0c:29:6b:81:54)
Internet Protocol Version 4, Src: 192.168.50.188, Dst: 192.168.50.236
Transmission Control Protocol, Src Port: 5020, Dst Port: 39312, Seq: 12, Ack: 25, Len: 29
Source Port: 5020
Destination Port: 39312
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 29]
Sequence Number: 12 (relative sequence number)
Sequence Number (raw): 400998096
[Next Sequence Number: 41 (relative sequence number)]
Acknowledgment Number: 25 (relative ack number)
Acknowledgment number (raw): 1786843364
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 509
[Calculated window size: 65152]
[Window size scaling factor: 128]
Checksum: 0xe73c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (29 bytes)
Data (29 bytes)
Data: 000200000017000314000000010002000300040005000600070080009
[Length: 29]
0000 00 0c 29 6b 81 54 a8 5e 45 c5 fd fd 08 00 45 00
0010 00 51 d4 2f 40 00 40 06 7f 7e c0 a8 32 bc c0 a8
0020 32 ec 13 9c 99 90 17 e6 be d0 6a 81 10 e4 80 18
0030 01 fd e7 3c 00 00 01 01 08 0a 23 46 d5 ee 9d de
0040 68 c3 00 02 00 00 00 17 00 03 14 00 00 00 01 00
0050 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09

Ethernet/IP

- Standardowa infrastruktura Ethernet
- TCP/IP oraz UDP
- Common industrial protocol oraz standardowe ramki Ethernet

Wady i zalety Ethernet/IP

- Wysoka przepustowość
- Obsługa dużej liczby urządzeń
- Zintegrowane funkcje bezpieczeństwa

- Złożoność implementacji
- Wyższe wymagania sprzętowe

Mitygowanie zagrożeń

- Wykorzystanie nowoczesnych protokołów
- VPN
- Szyfrowanie danych
- Autoryzacja i autentykacja