ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2005
Seria: TRANSPORT z. 57 Nr kol. 1675

Przemysław GORCZYCA, Jakub MŁYŃCZAK

PROTOKOŁY TRANSMISYJNE W STEROWANIU RUCHEM KOLEJOWYM

Streszczenie. Zaawansowane technologicznie skomputeryzowane systemy sterowania ruchem kolejowym potrzebują określonych, standardowych protokołów komunikacyjnych. Obecnie każde z urządzeń używa własnego standardu komunikacyjnego, co powoduje zwielokrotnienie niezależnych kanałów komunikacyjnych. Ta sytuacja ze względów technicznych i ekonomicznych wymaga pilnej zmiany.

TRANSMISSION PROTOCOL FOR RAILWAY TRAFFIC CONTROL

Summary. Advanced computerised systems of railway traffic control needs specified standarised communication protocols. At present each of traffic control device uses its own communication standard, requires the multiplication of independent communication channels. This situation needs to have been changed urgently because of the technical and economical reasons.

1. WSTĘP

Intensywna komputeryzacja techniki sterowania ruchem kolejowym (srk) powoduje pilną potrzebę opanowania chaosu technologicznego, jaki powstaje w wyniku instalowania w ramach jednego obszaru sterowania urządzeń srk bazujących na różnych standardach w sensie interfejsu komunikacyjnego, wykorzystywanego medium, przyjętego standardu komunikacyjnego i protokołu komunikacyjnego. Powoduje to zwielokrotnianie kanałów komunikacyjnych, co w znacznym stopniu zwiększa koszty instalacji urządzeń na obiektach oraz podraża i komplikuje proces eksploatacji urządzeń srk.

2. STANDARDY KOMUNIKACYJNE W URZĄDZENIACH SRK NA KOLEJACH POLSKICH

W ostatnim czasie można zauważyć pozytywną tendencję w wykorzystywaniu standardowych sieci przemysłowych do komunikacji pomiędzy urządzeniami sterowania ruchem oraz pomiędzy nimi a centrami zarządzania. Bardzo często jednak brak wytycznych do stosowania określonych protokołów prowadzi do wdrażania rozwiązań opartych na zmodyfikowanych standardach, często powstających na potrzeby konkretnych aplikacji. Efektem tego jest hipotetyczna sytuacja, w której dwa urządzenia, które mogłyby korzystać z tego samego medium transmisyjnego, ze względu na użyty nietypowy protokół lub jego modyfikację, muszą korzystać z wydzielonego łącza w celu zachowania bezpiecznej transmisji.

Obecnie w Polsce istnieje kilka komputerowych i hybrydowych systemów sterowania ruchem kolejowym. Do nich należą m.in.: Ebilock 850, Ebilock 950, Simis-W, OSA-H, SUP-3M, itp. Wykorzystanie różnych standardów wymiany danych: Profibus, RS485, RS232, CAN, Arcnet, szczególnie w wersjach zmodyfikowanych utrudnia połączenie tych urządzeń w jeden spójny system. Dodatkową przeszkodą jest komercyjny charakter niektórych wykorzystywanych standardów.

3. PODSTAWOWE ZAŁOŻENIA

Przyjęty standard powinien być powszechny zarówno w sensie wykorzystania jak i dostępności, przy zachowaniu wysokiego bezpieczeństwa, niezawodności transmisji, dużej elastyczności rozbudowy oraz niskiej ceny instalacji i utrzymania. W zależności od tego, na jakim poziomie urządzenia mają się ze sobą komunikować, należy rozpatrywać różne protokoły transmisji i różne poziomy komunikacji.

Dla celów wymiany danych pomiędzy nastawnicami (np. w przypadku Lokalnego Centrum Sterowania) należy rozważać komunikację z wykorzystaniem otwartych systemów komunikacji bazujących na sieciach rozległych - pozwoli to na stworzenie sieci o bardzo dużej elastyczności z możliwością zastosowania standardowych rozwiązań zarówno w warstwie architektury, jak i w warstwie protokołów komunikacyjnych.

Dla celów wymiany danych pomiędzy urządzeniami wykonawczymi należy rozważyć standardowe protokoły typu punkt-punkt. Podejście takie pozwoli na uniezależnienie infrastruktury od ewoluujących komercyjnych standardów.

Z racji obszaru, w ramach którego jest dokonywana wymiana danych pomiędzy nastawnicami lub nastawnicami i centrami dyspozytorskimi, protokół powinien zapewniać, oprócz pewności i autentyczności danych, również zabezpieczenie przed ingerencją z zewnątrz. Wymiana danych procesowych pomiędzy nastawnicą a urządzeniami wykonawczymi ze względu na lokalny zakres przesyłu informacji nie wymaga zabezpieczenia przed zewnętrzną ingerencją, natomiast zabezpieczenie przed błędami, przekłamaniami i zaginięciem pakietów ma priorytet.

4. WYMAGANIA STAWIANE PROTOKOŁOM TRANSMISYJNYM DO WYMIANY DANYCH PROCESOWYCH POMIĘDZY URZĄDZENIAMI SRK

Specjalizowane rozwiązania, poza niezaprzeczalną zaletą wysokiego stopnia integracji z kontrolowanymi urządzeniami, niosą ze sobą wiele wad, takich jak wysokie koszty urządzenia na etapie projektowania (opłaty licencyjne), a co ważniejsze dla zarządcy sieci, również zwiększenie kosztów wdrożenia urządzeń (adaptacja istniejących lub wdrożenie nowych urządzeń warstwy 1 i 2 modelu ISO/OSI). Dodatkowo brak określonego standardu komunikacyjnego może spowodować współistnienie na danym obszarze kilku standardów, co znacznie podwyższa koszty inwestycji i eksploatacji całego systemu. Równie ważna jest też tendencja w tworzeniu dużych obszarów sterowania i diagnostyki – ujednolicenie stosowanych protokołów na poziomie lokalnego systemu srk ułatwi poszerzanie okręgów sterowania i okręgów diagnostycznych w oparciu o istniejące urządzenia warstw od 1 do 4 modelu ISO/OSI.

Ze względu na różnorodność zadań stawianych komunikacji w systemie sterowania ruchem należy rozróżnić protokoły sieciowe do wymiany danych procesowych pomiędzy nastawnicami, centrami sterowania, centrami dyspozytorskimi, centrami utrzymania urządzeń oraz protokoły transmisji szeregowej typu punkt-punkt do wymiany danych procesowych pomiędzy dwoma urządzeniami sterowania ruchem na poziomie zależnościowym.

Dokumenty normatywne formułujące wymagania stawiane transmisji danych pomiędzy urządzeniami zabezpieczenia ruchu to uznaniowe normy PN-EN 50159-1 oraz PN-EN 50159-2 opracowane przez CENELEC. Należy również uwzględnić warunki bezpiecznej transmisji sformułowane w dokumencie „Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym" opracowanym przez Centrum Naukowo-Techniczne Kolejnictwa, będącym obowiązującym wymaganiem na PKP (CNTK, luty 1998r.).

5. PROTOKOŁY SIECIOWE DO WYMIANY DANYCH PROCESOWYCH – TENDENCJE ŚWIATOWE

Obecnie światowe tendencje budowy sieci przemysłowych koncentrują się na wykorzystaniu w lokalnych połączeniach rozproszonych systemów sterowania sieci Ethernet i protokołu TCP/IP jako podstawowego łącza wymiany danych procesowych. Podstawowe zalety Ethernetu to otwartość standardu – mimo że Ethernet opracowywany jest przez firmy komercyjne, to zatwierdzany jest przez IEEE (Institute of Electrical and Electronics Engineers), popularność standardu – jest najpowszechniejszym standardem dla sieci rozległych, uniwersalność - pozwala na komunikację zarówno dużych systemów jak i pojedynczych urządzeń, niska cena, elastyczność topologii Ethernetu – możliwa jest zarówno praca z topologią gwiazdy jak i magistrali. Wszystkie te cechy wpływają na rosnącą popularność Ethernetu jako podstawowej sieci na potrzeby wymiany danych procesowych w zastosowaniach przemysłowych.

5.1. Protokół TCP/IP dla zastosowań wymiany danych procesowych pomiędzy urządzeniami SRK

Protokół TCP/IP - jest ogólną nazwą całej rodziny protokołów i oprogramowania udostępniającego szereg usług sieciowych. Podstawę ich stanowią dwa typy usług wykorzystywanych przez wszystkie programy użytkowe:
- bezpołączeniowe przenoszenie,
- transport niezawodnymi strumieniami.

Podstawowe cechy odróżniające protokół TCP/IP od innych protokołów, również spełniających powyższe założenia, to:
- wymiana pakietów odbywa się niezależnie od warstwy sprzętowej,
- identyfikowanie urządzeń przez unikalny adres, jednoznacznie rozpoznawany w całej sieci. Informacja adresowa służy także do podejmowania decyzji o wyborze trasy pakietu od nadawcy do odbiorcy,
- potwierdzanie odbioru pakietów między nadawcą a odbiorcą docelowym, nawet gdy komputery nie są podłączone do tej samej sieci fizycznej.

Rodzina protokołów TCP/IP, z uwagi na to że obejmuje kilka warstw modelu ISO/OSI, może być przedstawiana w formie zredukowanego modelu ISO/OSI (rys.1).

Model ISO/OSI	Model TCP/IP
Warstwa aplikacji	Poziom aplikacji
Warstwa prezentacji	
Warstwa sesji	
Warstwa transportowa	Poziom transportowy
Warstwa sieciowa	Poziom sieciowy
Warstwa łącza danych	Poziom dostępu do sieci
Warstwa fizyczna	

Rys. 1. Modele ISO/OSI i TCP/IP
Fig. 1. The model of ISO/OSI and TCP/IP

Protokół IP nie ma ochrony przed możliwością podsłuchiwania i modyfikowania sieciowych transmisji. Problem ten zwykle jest rozwiązywany na wyższych poziomach (od poziomu 5 modelu ISO/OSI wzwyż) poprzez na przykład zastosowanie oprogramowania szyfrującego dane w warstwie aplikacyjnej (PGP, protokoły SSH i SSL), modyfikacje w warstwach systemu operacyjnego (nieprzewidywalne numery sekwencyjne TCP jako obrona przed blind spoofingiem – techniką podszywania się pod zaufanego użytkownika, poprzez losowe wybieranie numeru seryjnego urządzenia) itp. Niestety, takie rozwiązania znacznie zwiększają wymagania co do warstwy sprzętowej urządzeń wymieniających dane. Innym rozwiązaniem tego problemu są modyfikacje protokołu TCP/IP poprawiające znacznie jego bezpieczeństwo. Protokoły opracowane w oparciu o TCP/IP to m.in. SRTP (Alstom/GE Fanuc), MELSEC (Mitsubishi), EtherNet/IP (Allen-Bradley), Industrial Ethernet (Siemens), SuiteLink (Wonderware), FINS (Omron), Modbus over TCP (Schneider), Uni-TE (Schneider).

Niestety, mimo bezsprzecznych zalet tych podstandardów, takich jak:
- przezroczystość dla wyższych warstw modelu ISO/OSI,
- ochrona przed atakiem aktywnym (bezpośrednia ingerencja),
- ochrona przed atakami pasywnymi (bierny podsłuch),

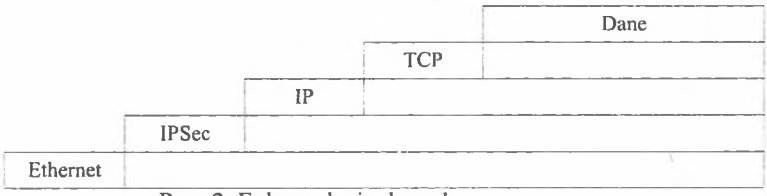
protokoły te nie chronią przed atakami polegającymi na analizie relacji przesyłanych danych (traffic analysis) oraz co najważniejsze, są to rozwiązania komercyjne, a więc rozpatrywanie ich jako stadardów ogólnych nie jest wskazane.

5.2. Protokół IPSEC

Protokół IPSec został opracowany w latach 1992-1998 przez IETF (Internet Engineering Task Force) jako uzupełnienie funkcjonalne protokołu IP o ochronę danych. Ważnym aspektem przemawiającym za IPSec jest to, iż stanowi on integralną część protokołu IPv6 – następcy protokołu IPv4. Tym samym urządzenia i systemy operacyjne obsługujące protokół IPv6 obsługują również protokół IPSec.

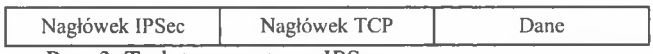
Protokół IPSec zapewnia:
- integralność oraz poufność danych przesyłanych za pomocą IP, niezależnie od protokołów stosowanych w wyższych warstwach modelu ISO/OSI, realizowane przez zastosowanie metod kryptograficznych, w przeciwieństwie do prostych sum kontrolnych protokołu IP i TCP, które co prawda, pozwalają wykryć uszkodzenie pakietu powstałe wskutek niedoskonałości transmisji, ale nie zabezpieczają przed celowymi zmianami wprowadzonymi w złych intencjach,
- gwarancję autentyczności łączących się stron,

- przezroczystość IPSec dla protokołów wyższych warstw modelu ISO/OSI. Jest ona zapewniana dzięki enkapsulacji pakietów poszczególnych warstw (rys. 2). Dzięki takiemu podejściu IPSec jest niewidoczny dla aplikacji warstw od 4 do 7 i pozwala na tworzenie aplikacji w środowisku o niższym poziomie zabezpieczeń.



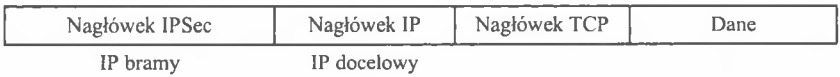
Rys. 2. Enkapsulacja danych
Fig. 2. Data encapsulation

Standardowym trybem pracy protokołu IPSec jest tryb transportowy (rys. 3), stosowany gdy host końcowy jest węzłem realizującym IPSec.



Rys. 3. Tryb transportowy IPSec
Fig. 3. Transportation mode of IPSec protocol

Ze względu na to, że spora część urządzeń pracujących np. w obszarze sieci lokalnej centrum sterowania obszarowego może pracować poza protokołem IPSec, wymagane jest tunelowanie (rys.4) zapewniające ochronę danych w obszarze łączącym dwie sieci (np. sieć lokalnego centrum sterowania i nastawnicy komputerowej).



Rys. 4. Tryb tunelowy IPSec
Fig. 4. Tunel mode of IPSec protocol

Integralność oraz poufność danych jest zapewniona poprzez dwa mechanizmy: nagłówek AH (Authentification Header) oraz nagłówek ESP (Encapsulation Security Payload). Gwarancja autentyczności łączących się stron jest zapewniona poprzez szyfrowane tunele SA (Security Association). Szyfrowane tunele leżą u podstaw architektury IPSec. Idea tuneli polega na łączeniu dwóch hostów kanałem komunikacyjnym identyfikowalnym poprzez unikalny 32-bitowy numer SPI (Security Parameters Index).

Model ISO/OSI	Model TCP/IP	Protokoły i realizowane funkcje bezpieczeństwa
Warstwa aplikacji	Poziom aplikacji	Protokoły wyższego poziomu (zapewnienie kontroli ważności czasowej, kontrola kolejności wiadomości)
Warstwa prezentacji		
Warstwa sesji		
Warstwa transportowa	Poziom transportowy	TCP
Warstwa sieciowa	Poziom sieciowy	IP
		IPSec (zapewnienie integralności, poufności, uwierzytelnienia)
Warstwa łącza	Poziom dostępu do sieci	Ethernet (zapewnienie zgodności elektromagnetycznej)
Warstwa fizyczna		

Rys. 5. Realizowane funkcje bezpieczeństwa na tle modeli ISO/OSI i TCP/IP
Fig. 5. The realised security functions against the background ISO/OSI and TCP/IP models

Jak widać na rysunku 5 protokół IPSec zapewnia trzy ważne mechanizmy bezpieczeństwa, których obecność w dolnej warstwie modeli sieciowych jest szczególnie pożądana.

6. PROTOKOŁY TRANSMISJI SZEREGOWEJ TYPU PUNKT-PUNKT

Wymiana danych procesowych pomiędzy dwoma urządzeniami sterowania ruchem na poziomie zależnościowym wymaga wysokiego poziomu zabezpieczenia przed przekłamaniami, natomiast takie cechy protokołu, jak poufność czy też gwarancja autentyczności, są mniej istotne. Oczywiście, należy uwzględnić, że przy braku weryfikacji autentyczności system może być podatny na działania dywersyjne, jednak tworzenie transmisji z wykorzystaniem transmisji szeregowej zazwyczaj wiąże się z wydzieleniem dla tego typu łączności specjalizowanego łącza transmisyjnego, co utrudnia dostęp osób niepowołanych do kanału komunikacyjnego. Wprowadzenie do tego typu urządzeń autentykacji może owocować zbytnim przeformatowaniem systemu.

6.1. Protokoły punkt-punkt mogące znaleźć zastosowanie w wymianie danych procesowych urządzeń SRK

Protokół HDLC (High Level Data Link Control) jest protokołem warstwy łącza, służącym do transmisji danych w sieci synchronicznej. Jego specyfikacja jest poddana standaryzacji przez międzynarodową organizację standaryzacyjną ISO. Protokół ten jest protokołem zorientowanym bitowo - dane są monitorowane bit po bicie. Transmisja w postaci ciągu bitów odbywa się bez żadnych dodatkowych danych kontrolnych. Informacje w ramce zawierają jednak komendy sterujące i zwrotne. Protokół HDLC obsługuje transmisję dupleksową - dane przesyłane są jednocześnie w obydwu kierunkach, co zwiększa przepustowość.

Protokół PPP (Point to Point Protocol) zapewnia komunikację szeregową z wykorzystaniem linii dedykowanych i komutowanych, łączących urządzenia i systemy komputerowe działające w różnych protokołach. Istnieją trzy metody transmisji datagramów w łączach dwupunktowych za pomocą protokołu PPP, przez:

- kapsułkowanie datagramów z udziałem protokołu HDLC,

- rozszerzenie funkcji protokołu LCP (Link Control Protocol) warstwy łącza logicznego do ustawienia, konfigurowania i testowania łączy danych. Protokół LCP specyfikuje metody kapsułkowania i wymiarowania pakietów, a także spełnia funkcje kontrolne (zakładanie i utrzymanie połączenia),
- współpracę ze zbiorem protokołów NCP (Network Control Protocols) warstwy sieciowej wyposażonych we własne procedury i pakiety do zakładania, utrzymania i zakończenia połączenia.

6.2. Protokoły HDLC i PPP – OCENA ZABEZPIECZEŃ

Łącza synchroniczne pozwalają na przesyłanie strumieni bitów, jednak szczególnie ważne jest zachowanie podziału strumienia na bajty, a także zachowanie podziału ciągu bajtów na pakiety. Prosty mechanizm protokołu HDLC umożliwia zachowanie takiego podziału. Do zaznaczenia początku i końca pakietu danych służy ciąg bitów 01111110. Dzięki niemu odbiornik ma pewność, że następujące po nim bity są kolejno pierwszym, drugim, itd. bajtem przesyłanych danych. Jeżeli jakikolwiek fragment danych składa się z więcej niż pięciu jedynek pod rząd, wstawiane jest dodatkowe zero, aby zapobiec pomyleniu flagi z danymi. Dodatkowo, żeby zapewnić integralność przesyłanych danych, na końcu pakietu jest dodawana 16-bitowa suma kontrolna CRC16. Dzięki zastosowaniu sum kontrolnych i jednoznacznych sygnałów błędów, protokół HDLC cechuje dobry poziom zabezpieczeń, chociaż kosztem pewnej nadmiarowości, co jednak nie powinno opóźniać przekazywania sygnałów.

Protokół PPP obejmuje swym działaniem trzy najniższe warstwy modelu ISO-OSI:

- warstwa fizyczna definiuje transmisję poprzez łącza synchroniczne i asynchroniczne z użyciem protokołów EIA-232E, EIA-422, EIA-433, V.24, oraz V.35. Tym samym mechanizmy zabezpieczeń tychże protokołów „sprzętowych" są dziedziczone na protokół PPP,
- warstwa sterowania składa się z dwóch części: protokołu DLLP (Data Link Layer Protocol), który jest nieznacznie zmodyfikowaną wersją protokołu HDLC, a więc DLLP dziedziczy zabezpieczenia protokołu HDLC i protokołu LCP (Link Control Protocol), który zakłada i utrzymuje łącze między dwoma połączonymi stacjami. Dostarcza on informacji sterującej połączeniem szeregowym i stosuje się go do ustanawiania połączenia logicznego, negocjacji parametrów konfiguracyjnych połączenia, utrzymywania połączenia, sprawdzania jakości połączenia i rozłączania połączenia. Jest więc to również czynnik zwiększający bezpieczeństwo przesyłanych danych,
- warstwa sieciowa zawiera zbiór protokołów NCP (Network Control Protocol). Ponieważ każdy protokół sieciowy posiada swój własny protokół NCP wyposażony w procedury kontrolne, pozwala to PPP na przesyłanie danych pochodzących z różnych protokołów sieciowych, wraz z zabezpieczeniami, jakie oferują te protokoły.

7. PODSUMOWANIE

Sieć Ethernet wraz z protokołem TCP/IP opartym na protokole IPSec zapewnia wysoki stopień bezpieczeństwa danych procesowych zarówno w zamkniętych sieciach wewnętrznych, jak również z wykorzystaniem sieci publicznych. Protokół IPSec zapewnia ochronę na poziomie warstwy sieciowej modelu ISO/OSI, przy zagwarantowaniu przezroczystości tej warstwy dla protokołu TCP/IP. Protokół IPSec jest opisanym, zatwierdzonym i wolnym w sensie licencjonowania standardem. IPSec spełnia stawiane wymagania w newralgicznym obszarze integralności, poufności i uwierzytelnienia. Pozostałe warunki bezpiecznej transmisji dla urządzeń sterowania ruchem kolejowym, nakładane przez wymagania i normy, należy spełnić na poziomie aplikacji. Jest to rozwiązanie naturalne, ze

względu na zakres funkcji bezpieczeństwa wymagających uzupełnienia, a które są zdeterminowane funkcjonowaniem komunikujących się aplikacji.

Uwzględniając mechanizmy bezpieczeństwa protokołów HDLC i PPP oraz biorąc pod uwagę wydzielone kanały, w jakich wybrane protokoły będą pracować, należy podkreślić, że zwiększanie bezpieczeństwa przesyłanych danych procesowych powinno odbywać się wyłącznie na wyższych poziomach modelu ISO/OSI, z uwzględnieniem lokalnych uwarunkowań, nie wchodzących w skład ogólnej polityki bezpieczeństwa.

Otwarte protokoły transmisyjne pozwalają poza obniżeniem kosztów wdrożenia i eksploatacji urządzenia srk, na podniesienie konkurencyjności i innowacyjności na rynku producentów urządzeń na potrzeby prowadzenia ruchu. Wybór otwartych standardów dobrze wpisuje się w coraz powszechniejsze europejskie tendencje wykorzystywania otwartych, niekomercyjnych rozwiązań teleinformatycznych.

Literatura

1. Krawczyk P.: Struktura i historia protokołu IPSec, http://echelon.pl/pubs/cbi_ipsec.html
2. MS Studio Grupa - Rodzina protokołów TCP/IP, http: //forum.msstudio.com.pl
3. WIKIPEDIA, http ://pl.wikipedia.org/wiki/TCP-IP
4. Groele J., Groele R.: - Podstawy protokołu TCP/IP, http://www.staff.amu.edu.pl/~psi/informatyka/tcpip/
5. Gaj P.: Zastosowanie protokołu TCP/IP do transmisji informacji dla potrzeb przemysłowych systemów kontrolno-nadzorczych, autoreferat pracy doktorskiej, Gliwice 2003.
6. Encyklopedia Wydawnictwa Robomatic, http://www.robomatic.pl/?id=enchaslo&idh=282
7. Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym, Centrum Naukowo-Techniczne Kolejnictwa, Warszawa 1998.

Recenzent: Doc. dr inż. Zbigniew Ginalski