PRACE NAUKOWE POLITECHNIKI WARSZAWSKIEJ
z. 96 Transport 2013

Marcin Bednarek

Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki
Katedra Informatyki i Automatyki

Tadeusz Dąbrowski

Wojskowa Akademia Techniczna, Wydział Elektroniki
Instytut Systemów Elektronicznych

KONCEPCJA BEZPIECZNEJ TRANSMISJI DANYCH W MOBILNYM SYSTEMIE ROZPROSZONYM

Rękopis dostarczono, kwiecień 2013

Streszczenie: W artykule przedstawiono koncepcję bezpiecznej transmisji danych w mobilnym systemie rozproszonym złożonym ze stacji procesowych i operatorskiej. Stacje procesowe systemu są połączone drogą radiową za pomocą radiomodemów, co umożliwia instalację stacji w ruchomych obiektach transportowych. Podano przykłady zastosowania prezentowanych zagadnień w systemach transportowych, a także potencjalne miejsca występowania zagrożeń dla bezpieczeństwa transmisji. Opisano możliwe warianty zabezpieczenia komunikacji. Przybliżono założenia koncepcji bezpiecznej komunikacji w systemie.
Słowa kluczowe: radiomodem, bezpieczeństwo, system rozproszony

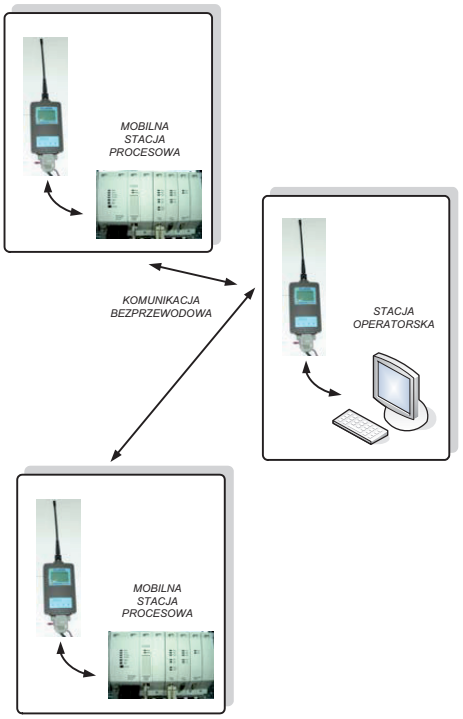
1. WPROWADZENIE

Pod pojęciem mobilnego systemu rozproszonego należy rozumieć, na potrzeby niniejszego opracowania, rozproszony system składający się ze stacji:

- master – nadrzędnej stacji operatorskiej, której zadaniem jest inicjowanie, utrzymywanie i kończenie połączeń ze stacjami procesowymi, prowadzenie diagnostyki komunikacji w całym systemie, realizacja oddziaływania operatorskiego oraz wizualizacji procesu sterowanego przez stacje procesowe;
- slave – podrzędnych stacji procesowych, których zadaniem jest realizacja programów sterowania procesem w odległych względem stacji operatorskiej miejscach oraz reakcja na zapytania kierowane do nich ze stacji operatorskiej.

Stacje procesowe rozpatrywanego systemu, a przynajmniej ich część jest połączona z pozostałymi drogą radiową (rys. 1) za pomocą radiomodemów, co umożliwia instalację stacji procesowych w ruchomych obiektach. Przykładowymi obszarami zastosowania tego typu systemu rozproszonego są instalacje:

- systemów kontroli pojazdów służb ratunkowych;
- systemów komunikacji urządzeń transportowych w halach fabrycznych;
- systemów koordynacji sygnalizacji świetlnej;
- systemów monitoringu pojazdów służb komunalnych;
- systemów monitoringu parametrów atmosferycznych;
- systemów sterowania bramami, rampami itp. [11].



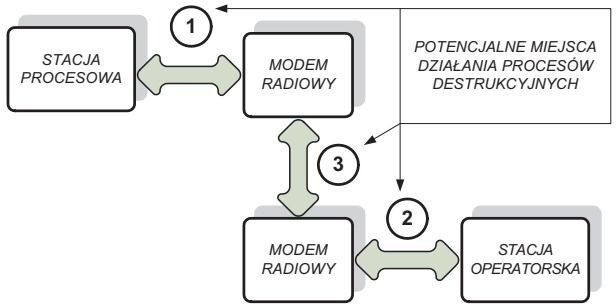
Rys. 1. Komunikacja radiomodemowa w systemie

2. ZAGROŻENIA TRANSMISJI

W przypadku realizacji połączeń stacji operatorskiej z mobilną stacją procesową, istotne znaczenie ma zabezpieczenie transmisji przed nieuprawnionym dostępem. Potencjalnymi,

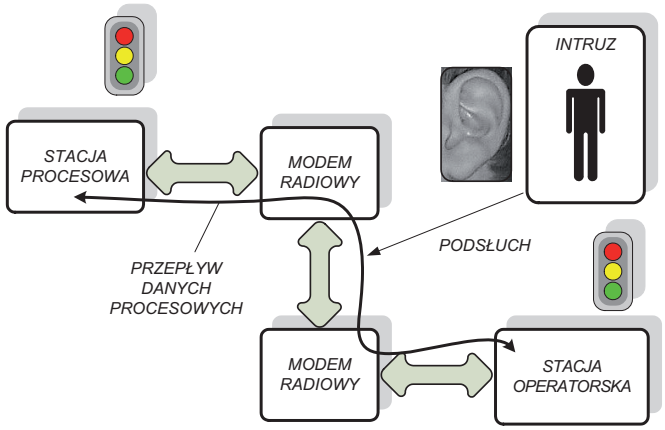
newralgicznymi miejscami, w których system transmisji [2] narażony jest na destrukcyjne oddziaływania intruzów przedstawiono na rys. 2.:

- połączenie stacja procesowa – radiomodem (rys. 2 – oznaczone „1”);
- połączenie radiomodem – radiomodem (oznaczone „3”);
- połączenie radiomodem – stacja operatorska (oznaczone „2”).



Rys. 2. Przesył danych w rozpatrywanym systemie

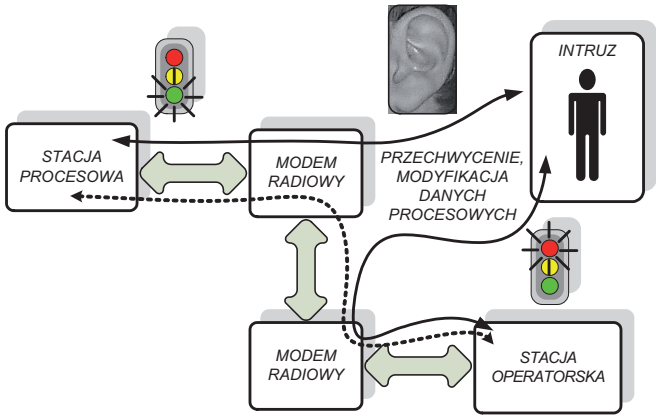
System zestawiony w sposób przedstawiony schematycznie na rys. 2 (niezabezpieczony), jest narażony na ataki ze strony intruzów. Może to być np. atak na poufność [3]. Rys. 3 przedstawia zasadę takiego ataku, w odniesieniu do rozpatrywanego systemu. Niezabezpieczona transmisja radiowa jest podsłuchiwana przez intruza. Pozyskane, skradzione, poufne dane mogą być w niewłaściwy sposób wykorzystane. Tutaj są to dane dotyczące np. sterowania sygnalizacją świetlną i systemem transportowym.



Rys. 3. Ilustracja ataku na poufność komunikatu

O ile przykład z rys. 3 przedstawia atak nie polegający na ingerencji w przesyłane dane, to kolejny, z rys. 4, ilustruje atak typu MIM (ang. *Man In The Middle* [10]). Niebezpieczeństwo przechwycenia komunikatu, jego modyfikacji oraz podrobienia jest istotne z punktu widzenia

systemów krytycznych ze względu na wypełniane funkcje. Przechwytując prawdziwy komunikat oraz wysyłając podrobiony, fałszywy, może on w taki sposób skonstruować polecenie dla stacji procesowej, aby zmienić sposób wykonywania np. programu sterowania sygnalizatorem świetlnym, włączając „zieloną falę" dla nieuprawnionego pojazdu. Z kolei przechwycenie i podrobienie odpowiedzi stacji procesowej może spowodować zablokowanie stacji operatorskiej (atak typu *DoS* [7]).



Rys. 4. Ilustracja ataku na integralność komunikatu

3. TRANSMISJA DANYCH W SYSTEMIE ROZPROSZONYM

Zakładając użycie otwartych systemów przemysłowych zapewniających połączenie urządzeń różnych producentów, można zastosować kilka sposobów zabezpieczenia transmisji:

- Rozwiązania firmowe zapewniane przez urządzenia radiowe, zabezpieczające transmisję z wykorzystaniem dedykowanych protokołów, stosujących kryptograficzne metody ochrony przesyłanych danych. Rozwiązanie to zapewnia ochronę przed intruzami tylko połączenia „modem radiowy – modem radiowy" (bezpieczeństwo danych transmitowanych na odcinku 3 – rys. 2).
- Zastosowanie komunikacji szyfrowanej z użyciem VPN (wirtualnej sieci prywatnej) polegające na utworzeniu wirtualnego szyfrowanego połączenia pomiędzy komputerem-stacją operatorską a tzw. bramą. Rozwiązanie problematyczne ze względu na dodatkowe ogniowo transmisji - bramę, pomiędzy radiomodemem a stacją procesową (bezpieczeństwo danych transmitowanych na odcinkach 2 i 3 oraz na części odcinka 1 – rys. 2).
- Wykonanie szyfrowania danych na poziomie stacji procesowej i deszyfrowania tych danych w stacji operatorskiej oraz analogicznej „ścieżki" powrotnej

komunikatu. Zapewnia to bezpieczny przesył komunikatów na wszystkich odcinkach 1-3, zaznaczonych na rys. 2.

Koncepcja rozwiązania ostatniego z wymienionych sposobów jest tematem rozważań w kolejnych punktach niniejszego opracowania.

4. KONCEPCJA TRANSMISJI BEZPIECZNEJ

Zastosowanie zabezpieczenia komunikacji w postaci szyfrowania wysyłanych komunikatów zapewnia bezpieczeństwo transmisji niezależnie od zastosowanego sposobu transmisji radiowej. Przykładem takiego rozwiązania jest połączenie stacji procesowej AC800F [5] ze stacją operatorską wyposażoną w system SCADA [6]. Może to być pakiet wizualizacji InTouch [4].

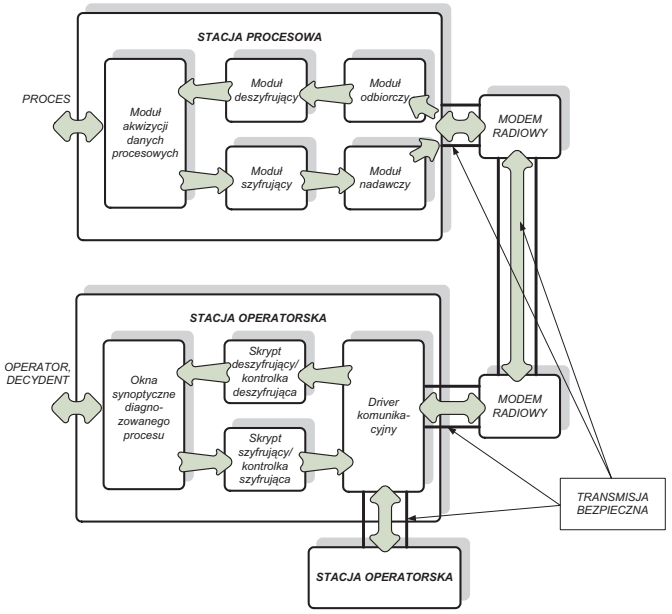
Założenia (w tym wstępne ograniczenia) koncepcji komunikacji są następujące:

1. Po stronie stacji operatorskiej odbywa się dozorowanie procesu sterowanego przez stację procesową. Stacja operatorska udostępnia obrazy synoptyczne wizualizujące stan procesu sterowanego przez stację procesową, wyświetla wskazówki doradcze dla operatora/decydenta systemu.
2. Komunikacja pomiędzy urządzeniami prowadzona jest według przemysłowego protokołu Modbus [8].
3. Komunikacja radiowa stanowi „przeźroczystą", dla obydwu stron, linię transmisyjną. Widoczna jest ona jako zwykłe łącze szeregowe.
4. Stacje uczestniczące w komunikacji nie ingerują w sposób transmisji radiowej.
5. Urządzenia komunikują się według zasady master (stacja operatorska) – slave (stacja procesowa) [8]. Stacja operatorska inicjuje połączenie, a stacja procesowa odpowiada (w bardziej ogólnym przypadku omawianego zabezpieczenia model wymiany informacji w procesie komunikacji nie ma większego znaczenia).

Moduły na rys.5, ilustrującym proponowany proces komunikacji, oznaczają wydzieloną, spójną część programu sterującego, odpowiadającą za wykonanie funkcji wymienionej w ich nazwie. Są to fragmenty schematów np. w języku FBD [9, 1] lub innym języku programowania sterowników. Proces bezpiecznej transmisji przebiega według następującego schematu (rys. 5):

1. Przed wysłaniem komunikatu-pytania następuje dokonanie szyfrowania wartości pola danych. Wykonywane jest to za pomocą odpowiedniego skryptu lub specjalnej kontrolki. Możliwe jest też przeniesienie pewnych obliczeń za pomocą odwołania do arkusza kalkulacyjnego.
2. Komunikat z zaszyfrowanym polem danych przesyłany jest do stacji procesowej z wykorzystaniem zasady podanej wyżej (wg punktów 1-5).
3. Odpowiednio skonfigurowana stacja procesowa otrzymuje komunikat z zaszyfrowanym poleceniem. Zapytania o wartości zmiennych procesowych powinny być formułowane w postaci poleceń ustawiających pewną wartość.
4. Następuje deszyfrowanie polecenia (moduł deszyfrujący) oraz automatyczna odpowiedź (moduł nadawczy) zgodnie z wymaganiami protokołu.

5. Stacja procesowa dokonuje szyfrowania żądanych danych wykorzystując do tego celu przygotowany moduł szyfrujący. Jest to zespół bloków funkcyjnych szyfrujący dane wejściowe z ustalonym wcześniej kluczem, analogicznym do tego, którego używa skrypt stacji operatorskiej (szyfrowanie symetryczne).
6. Następnie stacja procesowa oczekuje na kolejną wymianę poleceń, w ramach której przesyła zaszyfrowane dane do stacji operatorskiej, wykorzystując do tej operacji ww. moduły.
7. Następuje proces odbioru danych (realizowany przez driver komunikacyjny stacji operatorskiej), deszyfrowania danych oraz ich prezentacji np. w formie graficznej.



Rys. 5. Procedury zabezpieczające

5. PODSUMOWANIE

Przedstawiona w opracowaniu koncepcja bezpiecznej transmisji danych w mobilnym systemie rozproszonym może być rozbudowana o kolejne rozwiązania uzupełniające, pozwalające m.in. na:

1. Bezpieczną dystrybucję kluczy symetrycznych poprzez zastosowanie w początkowej fazie procesu komunikacji szyfrowania asymetrycznego i, następującego po nim, przejścia do szyfrowania symetrycznego.

2. Rozbudowę systemu o kolejne stacje operatorskie (por. rys. 5) z zastosowaniem szyfrowania danych na poziomie komunikacji wykorzystującej protokoły przemysłowe bazujące na standardach Ethernet i TCP/IP (niezależnego od mechanizmów oferowanych przez standardowe protokoły).
3. Zgrupowanie fragmentów programu, odpowiedzialnych za realizację funkcji wybranych modułów z rys. 5 i utworzenie bloków użytkownika (ang. *User Function Block*), w celu ich łatwiejszego, wielokrotnego wykorzystania.
4. Rozbudowę modułu szyfrującego o funkcję wyboru algorytmu kryptograficznego.

Opisana koncepcja pozwala na implementację mechanizmów zabezpieczających w rozwiązaniach pozbawionych funkcji ochrony transmitowanych danych oraz na zastosowanie standardowych protokołów komunikacyjnych sieci przemysłowych.

Bibliografia

1. Bednarek M.: Wizualizacja procesów – laboratorium, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2004 (wydanie II, bez zmian).
2. Bednarek M., Będkowski L., Dąbrowski T.: Wieloprocesowe ujęcie eksploatacji układu komunikacji. Diagnostyka, nr 34/2005, s. 37.
3. Dennig D.: Wojna informacyjna i bezpieczeństwo informacji. WNT, Warszawa 2002.
4. Dokumentacja elektroniczna pakietu Wonderware Archestra.
5. Dokumentacja elektroniczna systemu AC800F.
6. Legierski T. i inni: Programowanie sterowników PLC. Wydawnictwo pracowni J. Skalmierskiego, Gliwice 1998.
7. Maiwald E.: Bezpieczeństwo w sieci. Kurs podstawowy. Edition 2000, Kraków 2001.
8. Modicon Modbus Protocol Reference Guide. PI-MBUS-300 Rev. J, Modicon Inc., June 1996.
9. Norma PN-EN 61131-3. Sterowniki programowalne – Języki programowania.
10. Stamp M.: Information security. Principles and practice. John Willey and Sons, Hoboken, New Jersey 2006.
11. http://www.astor.com.pl/rozwiazania/realizacje.html

CONCEPT OF THE SECURE TRANSMISSION IN MOBILE DISTRIBUTED SYSTEM

Summary: The concept of secure data transmission in a mobile distributed system composed of the process stations and the operator stations is presented. Process stations are connected to the system via radio modems. It allows the installation in mobile transport facilities. The examples of the application of the presented issues in transport systems, as well as the potentially locations of the security risks of transmission are given. The possible options for secure communications are described. The assumptions of the concept of a secure communication system are explained.
Keywords: radio-modem, security, distributed system